# هيكلية الشبكة 802.11

## الأهداف التعليمية:

- التعرف على المسح السلبي والمسح النشط وكيفية وصل الطرفيات في كل منهما.
- الإلمام بكيفية إجراء عمليتي المصادقة والانضمام ضمن الشبكات اللاسلكية المحلية.
- اكتساب المعرفة النظرية اللازمة لإعداد الشبكات اللاسلكية المحلية ضمن واحدة من مجموعات الخدمات المتاحة تبعاً للخدمة المطلوبة منها.
- فهم الهدف من التوثق وكيفية تحقيقه.

## قائمة المصطلحات

| | |
|---|---|
| scanning | المسح |
| Passive scanning | المسح السلبي |
| Active scanning | المسح النشط |
| Service Set ID | معرّف مجموعة الخدمات |
| Beacon | الإطار المرشد |
| probe requests | طلبات السبر |
| Probe responses | إجابات السبر |
| time-stamp | طابع زمني |
| Traffic Indication Map (TIM) | خريطة بيان حركة مرور المعطيات |
| sleep mode | نمط النوم |
| broadcast | النشر |
| Authentication | التوثق أو المصادقة |
| Association | الانضمام أو الارتباط |
| Wired Equivalent Privacy (WEP) | الخصوصية السلكية المكافئة |
| Extensible Authentication Protocol (EAP) | بروتوكول المصادقة القابل للتوسيع |
| Authorization | التخويل |
| Accounting | التدوين |
| Basic Service Set (BSS) | مجموعة الخدمات الأساسية |
| Extended Service Set (ESS) | مجموعة الخدمات الموسعة |
| Independent Basic Service Set (IBSS) | مجموعة الخدمات الأساسية المستقلة |

| | |
|---|---|
| ad-hoc network | شبكة الأقران |
| peer-to-peer network | شبكة نظير إلى نظير |
| Roaming | التجوال |
| handover | التسليم |
| Reassociation | إعادة الانضمام |
| load balancing | موازنة الحمل |
| channel reuse | إعادة استخدام القناة |
| Tunnels | الأنفاق |
| active mode | الوضع النشط |
| Continuous Aware Mode “CAM” | وضع الإدراك المستمر |
| power save | توفير الطاقة |
| Power Save Polling “PSP” | وضع استقصاء توفير الطاقة |

يغطي هذا الفصل بعض المفاهيم الأساسية الموجودة في بنية شبكة ٨٠٢.١١، تم الاستناد في معظم الموضوعات الواردة في هذا الفصل إلى المعيار ٨٠٢.١١، وهي مطلوبة لربط الأجهزة المتوافقة مع ٨٠٢.١١، في هذا الفصل سنقوم بشرح العملية التي يتصل بها المستخدمين بنقطة وصول والمصطلحات المستخدمة في تنظيم شبكات LAN اللاسلكية وكيفية إدارة الاستطاعة في أجهزة مشتركي الشبكة المحلية اللاسلكية.

دون الفهم العميق للمبادئ التي تم سيتم تناولها ضمن هذا الفصل سيكون من الصعب جدًا تصميم شبكة LAN لاسلكية أو إدارتها أو استكشاف أعطالها وإصلاحها، يحتوي هذا الفصل على بعض الخطوات الأساسية لكل من تصميم وإدارة الشبكة المحلية اللاسلكية، أثناء إدارتك لشبكات LAN اللاسلكية سيسمح لك فهم هذه المفاهيم بإدارة عملياتك اليومية بشكل أكثر ذكاءً.

## ١- توضع الشبكة اللاسلكية:

عند تثبيت جهاز مشترك LAN لاسلكي وضبطه وبدء تشغيله (مثل طرفية USB أو بطاقة PCMCIA) ستقوم الطرفية تلقائيًا بمحاولة التقاط إشارة لاسلكية ضمن مجالها الترددي (وهو ما يطلق عليه مصطلح الاستماع listening) لمعرفة ما إذا كانت هناك شبكة LAN لاسلكية داخل النطاق، تكتشف الطرفية أيضًا ما إذا كان بإمكانها الاقتران بالشبكة LAN اللاسلكية التي وجدتها، تسمى عملية الاستماع هذه بالمسح scanning، ويحدث المسح قبل أي عملية أخرى لأن المسح هو الطريقة التي تعثر بها الطرفية على الشبكة.

هناك نوعان من المسح للعثور على نقطة وصول: المسح السلبي Passive scanning والمسح النشط Active scanning، تتبع الطرفيات قيمة محددة تقوم بإرسالها نقطة الوصول، تسمى هذه القيمة بمعرّف مجموعة الخدمات (Service Set ID) والتي ترسل ضمن إطار إدارة يطلق عليه مصطلح الإطار المرشد Beacon، تعتبر هذه الطريقة الأساسية التي تستخدمها الطرفيات للعثور على أي نقطة وصول.

### ١-١- معرف مجموعة الخدمات:

معرف مجموعة الخدمات (SSID) هو قيمة أبجدية رقمية وحيدة حساسة لحالة الأحرف تتكون من ٢-٣٢ محرفًا تستخدم في الشبكات المحلية اللاسلكية كاسم للشبكة، يتم استخدامه لتجزئة الشبكات كإجراء أمني بدائي، كما يستخدم في عملية الانضمام إلى الشبكة، يتم إرسال قيمة SSID في الإطارات المرشدة وطلبات السبر (probe requests) واجابات السبر (probe responses) وأنواع أخرى من الإطارات، يجب إعداد الطرفيات بمعرف SSID الصحيح من أجل الانضمام إلى الشبكة، حيث يقوم الفني المسؤول بإعداد SSID (والذ يسمى أحيانًا ESSID) في كل نقطة وصول ضمن الشبكة. تتمتع بعض الطرفيات بالقدرة على استخدام أي قيمة SSID بدلاً من SSID واحدة فقط يحددها مدير الشبكة يدويًا، ففي حال الرغبة في أن تتجول الطرفيات بمرونة بين مجموعة من نقاط الوصول فيجب

إعداد كل من الطرفيات وجميع نقاط الوصول بمعرفات SSID متطابقة، أهم نقطة حول SSID هي أنه يجب أن يتطابق تمامًا بين نقاط الوصول والطرفيات.

### ١-٢- الإطار المرشد:

الإطارات المرشدة هي إطارات قصيرة يتم إرسالها من نقطة الوصول إلى الطرفيات (عندما تكون الشبكة في نمط البنية التحتية) أو من محطة إلى محطة (عندما تكون الشبكة في نمط Ad-hoc) من أجل تنظيم ومزامنة الاتصالات اللاسلكية على شبكة LAN اللاسلكية، تخدم الإطارات المرشدة عدة وظائف أهمها:

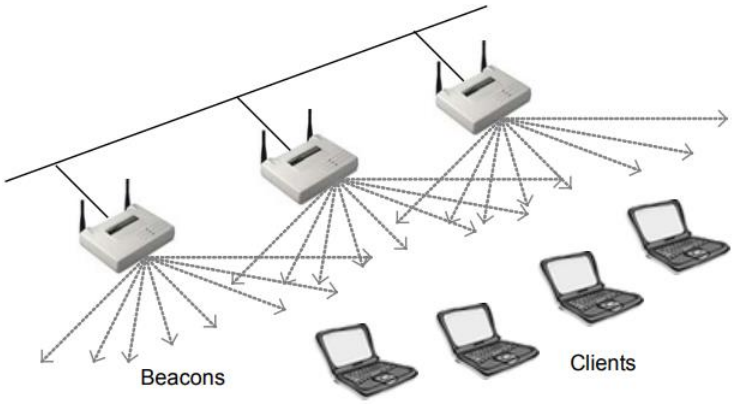
- **المزامنة**: تقوم الإطارات المرشدة بمزامنة الطرفيات من خلال طابع زمني time-stamp في لحظة الإرسال بالضبط، عندما تستقبل الطرفية الإطار المرشد تقوم بتغيير ساعتها الخاصة بحيث تعكس ساعة نقطة الوصول، بمجرد إجراء هذا التغيير تتم مزامنة الساعتين. تضمن مزامنة ساعات وحدات الاتصال تنفيذ جميع الوظائف الحساسة للوقت كالطيف المنثور بالقفز الترددي FHSS دون أخطاء، يحتوي الإطار المرشد أيضًا على الفاصل الزمني بين الإطارات المرشدة الذي يُعلم المحطات بعدد المرات التي يجب أن تستقبل فيها هذا الإطار.
- **مجموعة معاملات القفز الترددي أو السلسلة المباشرة**: تحتوي الإطارات المرشدة على معلومات موجهة خصيصًا لتكنولوجيا الطيف المنثور التي يستخدمها النظام، على سبيل المثال ضمن نظام FHSS يتم تضمين معاملات زمن القفز وزمن السكون وتسلسل القفزات ضمن الإطار المرشد، وضمن نظام DSSS يحتوي الإطار المرشد على معلومات القناة.
- **معلومات SSID**: تبحث المحطات ضمن الإطارات المرشدة عن SSID للشبكة التي ترغب في الانضمام إليها، وعند العثور على هذه المعلومات تنظر المحطة في عنوان MAC الخاص بالمكان الذي نشأ فيه الإطار المرشد وترسل طلب مصادقة على أمل الاقتران بنقطة الوصول صاحبة هذا الإطار. في حال تم إعداد الطرفية على خيار قبول أي SSID ستحاول الطرفية الانضمام إلى الشبكة من خلال نقطة الوصول الأولى التي ترسل إطار مرشد أو تلك التي تتمتع بأقوى قوة إشارة إذا كانت هناك نقاط وصول متعددة.
- **خريطة بيان حركة مرور المعطيات Traffic Indication Map (TIM)**: يتم استخدام TIM كمؤشر على الطرفيات التي تعمل ضمن نمط النوم sleep mode والتي لها حزم بيانات ضمن قائمة الانتظار في نقطة الوصول، يتم تمرير هذه المعلومات في كل إطار مرشد إلى جميع الطرفيات المرتبطة. في نمط النوم تعمل الطرفيات المتزامنة على تشغيل أجهزة الاستقبال الخاصة بها والاستماع إلى الإطار المرشد والتحقق من TIM لمعرفة ما إذا كانت مدرجة، وفي حال لم تكن مدرجة تقوم بإيقاف تشغيل أجهزة الاستقبال الخاصة بها وتستمر في النوم.

- **السرعات المدعومة**: هناك العديد من السرعات المدعومة في الشبكات اللاسلكية تبعاً لمستوى الأجهزة المستخدمة، على سبيل المثال يدعم الجهاز المتوافق مع IEEE802.11b السرعات ١١ و٥.٥ و٢ و١ ميجابت في الثانية، يتم تمرير هذه المعلومة ضمن الإطارات المرشدة لإعلام الطرفيات بالسرعات المدعومة ضمن نقطة الوصول.

هناك المزيد من المعلومات التي يتم تمريرها داخل الإطارات المرشدة إضافة إلى المعلومات السابقة التي تغطي كل ما يمكن اعتباره مهمًا من وجهة نظر مدير الشبكة.

### ١-٣- المسح السلبي:

المسح السلبي هو عملية مراقبة الإطارات المرشدة على كل قناة لفترة زمنية محددة بعد إعداد الطرفية، يتم إرسال هذه الإطارات عن طريق نقاط الوصول (في نمط البنية التحتية) أو الطرفيات (في النمط Ad-hoc). تستمع الطرفية التي تبحث عن شبكة إلى الإطارات المرشدة إلى أن تجد الإطار الذي يحتوي على SSID الشبكة التي ترغب في الانضمام إليها، ومن ثم تحاول الطرفية الانضمام إلى الشبكة من خلال نقطة الوصول التي ترسل المرشد. يبين الشكل (٣-١) عملية المسح السلبي.




الشكل (٣-١): المسح السلبي.

يمكن في الشبكات التي تحتوي على نقاط وصول متعددة أن يتم إرسال SSID الشبكة التي ترغب الطرفية في الانضمام إليها عن طريق أكثر من نقطة وصول واحدة، في هذه الحالة ستحاول الطرفية الانضمام إلى الشبكة عبر نقطة الوصول بأقوى قوة إشارة وأقل معدل خطأ في البت.

تستمر الطرفيات في المسح السلبي حتى بعد الارتباط بنقطة وصول، يوفر المسح السلبي الزمن اللازم لإعادة الاتصال بالشبكة إذا تم فصل (قطع الارتباط) الطرفية عن نقطة الوصول التي تتصل بها حاليًا، من خلال الاحتفاظ

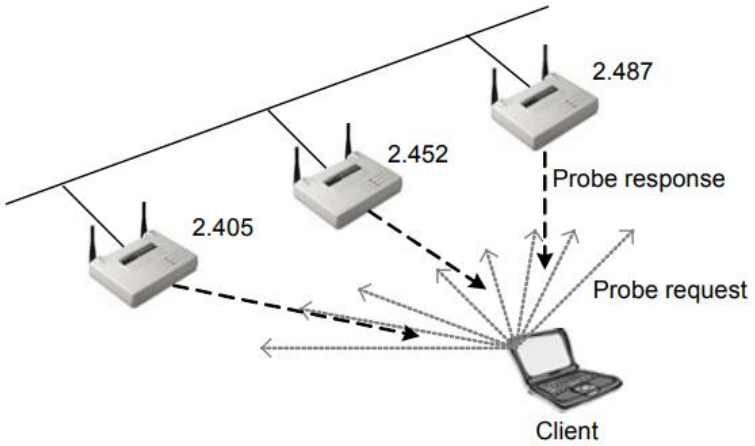
بقائمة نقاط الوصول المتاحة وخصائصها (القناة وقوة الإشارة وSSID وغيرها) يمكن للطرفية تحديد موقع أفضل نقطة وصول بسرعة في حالة انقطاع اتصالها الحالي لأي سبب.

تتجول الطرفيات من نقطة وصول إلى أخرى بعد وصول إشارة الراديو من نقطة الوصول حيث تتصل المحطة إلى مستوى منخفض معين من قوة الإشارة، يتم تنفيذ التجوال حتى تبقى الطرفية متصلة بالشبكة، تستخدم الطرفيات المعلومات التي تم الحصول عليها من خلال المسح السلبي لتحديد موقع أفضل نقطة وصول تالية (أو شبكة مخصصة) لاستخدامها في الاتصال مرة أخرى بالشبكة، لهذا السبب عادةً ما يتم تحديد التداخل بين خلايا نقطة الوصول بنسبة ٢٠-٣٠٪ تقريبًا، يسمح هذا التداخل للطرفيات بالتجول بمرونة بين نقاط الوصول أثناء قطع الاتصال وإعادة الاتصال دون علم المستخدم.

نظرًا لأن عتبة الحساسية في بعض أجهزة الراديو لا تعمل بشكل صحيح سيرى مدير الشبكة أحيانًا بقاء راديو متصل بنقطة وصول حتى تنقطع الإشارة بسبب قوة الإشارة المنخفضة للغاية بدلاً من التجوال إلى نقطة وصول أخرى لديها إشارة أفضل، هذا الموقف هو مشكلة معروفة في بعض الأجهزة ويجب إبلاغ الشركة المصنعة إذا كنت تواجه هذه المشكلة.

### ١-٤- المسح النشط:

يتضمن المسح النشط إرسال إطار طلب سبر من محطة لاسلكية، ترسل الطرفيات إطار السبر عندما تبحث بنشاط عن شبكة للانضمام، يحتوي إطار السبر إما على SSID للشبكة التي ترغب في الانضمام إليها أو SSID النشر broadcast، إذا تم إرسال طلب سبر يحدد SSID فلن تستجيب سوى نقاط الوصول التي تخدم SSID بإطار استجابة سبر، وفي حال تم إرسال إطار طلب سبر باستخدام SSID النشر فستستجيب جميع نقاط الوصول المتاحة بإطار استجابة سبر كما يوضح الشكل (٣-٢).




الشكل (٣-٢): المسح النشط.

تتمثل نقطة السبر بهذه الطريقة في تحديد نقاط الوصول التي يمكن للطرفية من خلالها الاتصال بالشبكة، بمجرد العثور على نقطة وصول مع SSID المناسب تبدأ الطرفية خطوات المصادقة والارتباط للانضمام إلى الشبكة من خلال نقطة الوصول.

المعلومات التي يتم تمريرها من نقطة الوصول إلى الطرفية في إطارات استجابة السبر متطابقة تقريبًا مع المعلومات الخاصة بالإطارات المرشدة، تختلف إطارات استجابة السبر عن الإطارات المرشدة فقط من حيث أنها لا تحتوي على الطابع الزمني ولا تتضمن خريطة بيان حركة مرور المعطيات (TIM).

تساعد قوة إشارة إطارات استجابة السبر التي تتلقاها بطاقة الكمبيوتر الشخصي في تحديد نقطة الوصول التي ستحاول بطاقة الكمبيوتر الارتباط بها، تختار الطرفية بشكل عام نقطة الوصول ذات أقوى إشارة وأقل معدل خطأ في البت (BER)، معدل الخطأ في البت (BER) هو نسبة الحزم التالفة إلى الحزم الجيدة التي يتم تحديدها عادةً بواسطة نسبة الإشارة إلى الضجيج للإشارة، إذا كانت قمة الإشارة الراديوية في مكان ما بالقرب من أرضية الضجيج فقد يخلط جهاز الاستقبال بين إشارة البيانات والضجيج.

## ٢- التوثق والانضمام

تتكون عملية الاتصال بشبكة LAN لاسلكية من عمليتين فرعيتين منفصلتين، تحدث هذه العمليات الفرعية دائمًا بنفس الترتيب وتسمى التوثق والانضمام، على سبيل المثال عندما نتحدث عن بطاقة كمبيوتر لاسلكي متصلة بشبكة LAN لاسلكية فإننا نقول إن بطاقة الكمبيوتر الشخصي قد تمت مصادقتها بواسطة نقطة وصول معينة وربطتها بها. يجب الانتباه إلى أنه عندما نتحدث عن الارتباط فإننا نتحدث عن اتصال ضمن الطبقة الثانية، وتتعلق المصادقة مباشرةً ببطاقة الكمبيوتر الراديوية وليس بالمستخدم، يعد فهم الخطوات المتضمنة في توصيل الطرفية بنقطة وصول أمرًا بالغ الأهمية للأمان واستكشاف الأخطاء وإصلاحها وإدارة الشبكة المحلية اللاسلكية.

### ٢-١- التوثق أو المصادقة Authentication:

الخطوة الأولى في الاتصال بشبكة LAN لاسلكية هي المصادقة، المصادقة هي العملية التي يتم من خلالها التحقق من هوية العقدة اللاسلكية (بطاقة الكمبيوتر الشخصي أو طرفية USB وغيرها) بواسطة الشبكة (عادةً نقطة الوصول) التي تحاول العقدة الاتصال بها، يحدث هذا التحقق عندما تتحقق نقطة الوصول التي تتصل بها الطرفية من أن هذه الطرفية هي من تقوله، بعبارة أخرى تستجيب نقطة الوصول للطرفية التي تطلب الاتصال عن طريق التحقق من هوية الطرفية قبل حدوث أي اتصال. في بعض الأحيان تكون عملية المصادقة فارغة، مما يعني أنه على الرغم من أنه يتعين على كل من الطرفية ونقطة الوصول المضي قدمًا خلال هذه الخطوة من أجل الارتباط، إلا

أنه لا توجد هوية خاصة مطلوبة بالفعل للارتباط، هذا هو الحال عندما يتم تثبيت معظم نقاط الوصول الجديدة وبطاقات الكمبيوتر بإعداداتها الافتراضية، سيتم التطرق إلى نوعين من عمليات المصادقة لاحقًا في هذا الفصل.

تبدأ الطرفية عملية المصادقة بإرسال إطار طلب مصادقة إلى نقطة الوصول (في نمط البنية التحتية)، ستقبل نقطة الوصول هذا الطلب أو ترفضه، وبعد ذلك تخطر الطرفية بقرارها بإطار استجابة المصادقة، يمكن إنجاز عملية المصادقة عند نقطة الوصول أو قد تمرر نقطة الوصول هذه المسؤولية إلى خادم مصادقة مثل خوادم RADIUS، يقوم خادم RADIUS بإجراء المصادقة استنادًا إلى قائمة معايير ثم يعيد نتائجه إلى نقطة الوصول حتى تتمكن نقطة الوصول من إعادة النتائج إلى الطرفية.

### ٢-٢- الانضمام أو الارتباط Association:

بمجرد مصادقة الطرفية اللاسلكية تقوم الطرفية بعد ذلك بالارتباط بنقطة الوصول، حالة الارتباط هي الحالة التي يُسمح فيها للطرفية بتمرير البيانات عبر نقطة وصول، إذا كانت بطاقة الكمبيوتر لديك مرتبطة بنقطة وصول فأنت متصل بنقطة الوصول هذه وبالتالي مرتبط بالشبكة.

تتم عملية الارتباط على النحو التالي: عندما ترغب الطرفية بالاتصال ترسل طلب مصادقة إلى نقطة الوصول وتتلقى استجابة المصادقة، بعد اكتمال المصادقة ترسل الطرفية إطار طلب انضمام إلى نقطة الوصول التي ترد على الطرفية بإطار استجابة للانضمام إما بالسماح بهذا الانضمام أو عدم السماح به.

### ٢-٣- حالات التوثق والانضمام:

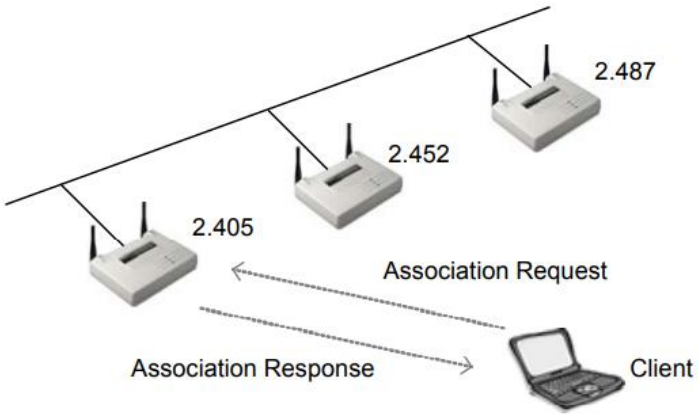
تتكون عملية المصادقة والارتباط الكاملة من ثلاث حالات متميزة:

- غير موثق وغير مرتبط
- موثق وغير مرتبط
- موثق ومرتبط

**غير موثق وغير مرتبط**: في هذه الحالة الأولية يتم فصل العقدة اللاسلكية تمامًا عن الشبكة ولا يمكنها تمرير الإطارات عبر نقطة الوصول، تحتفظ نقاط الوصول بجدول لحالات اتصال الطرفية يعرف باسم جدول الانضمام، من المهم ملاحظة اختلاف المصنعين بكيفية الإشارة إلى الحالة غير المصادق عليها وغير المرتبطة في جدول ارتباط نقاط الوصول الخاصة بهم، يعرض هذا الجدول عادةً "**غير مصادق**" لأي طرفية لم تكمل عملية المصادقة أو حاولت المصادقة وفشلت.

**موثق وغير مرتبط**: في هذه الحالة الثانية اجتازت الطرفية اللاسلكية عملية المصادقة، إلا أنه لم يتم ربطها بعد بنقطة الوصول، لا يُسمح للطرفية حتى الآن بإرسال أو استقبال البيانات من خلال نقطة الوصول، سيظهر جدول انضمام نقطة الوصول عملياً "**مصدق عليه**"، نظرًا لأن الطرفيات تجتاز مرحلة المصادقة وتتقدم فورًا إلى مرحلة الانضمام بسرعة كبيرة (ميلي ثانية)، نادرًا ما تشاهد خطوة "المصادقة" على نقطة الوصول، من المرجح جدًا أنك سترى "**غير مصادق عليه**" أو "**مرتبطًا**" وهو ما يقودنا إلى المرحلة الأخيرة.

**موثق ومرتبط**: في هذه الحالة النهائية تكون العقدة اللاسلكية متصلة تمامًا بالشبكة وقادرة على إرسال واستقبال البيانات من خلال نقطة الوصول التي تتصل بها العقدة **(مرتبطة)**، يوضح الشكل (٣-٣) طرفية ترتبط بنقطة وصول، من المحتمل أن ترى كلمة "**مرتبطة**" في جدول انضمام نقطة الوصول للإشارة إلى أن هذه الطرفية متصلة بالكامل ومصرح لها بتمرير حركة المرور عبر نقطة الوصول، كما يمكنك الاستنتاج من وصف كل حالة من هذه الحالات الثلاث. يتم تنفيذ إجراءات أمان الشبكة اللاسلكية المتقدمة عند النقطة التي يحاول العميل عندها المصادقة.




الشكل (٣-٣): الانضمام.

### ٢-٤- أنماط التوثق:

يحدد المعيار IEEE 802.11 طريقتين للمصادقة: مصادقة النظام المفتوح ومصادقة المفتاح المشترك، الأبسط والأكثر أمانًا من الطريقتين هو مصادقة النظام المفتوح، كي تتم مصادقة الطرفية يجب أن تمر بسلسلة من الخطوات باستخدام نقطة الوصول، تختلف هذه السلسلة من الخطوات اعتمادًا على عملية المصادقة المستخدمة، سنناقش كل عملية مصادقة محددة بواسطة المعيار ٨٠٢.١١ وكيف تعمل ولماذا يتم استخدامها.

**مصادقة النظام المفتوح:**

مصادقة النظام المفتوح هي طريقة للمصادقة المعدومة ويتم تحديدها بواسطة IEEE 802.11 كإعداد افتراضي في إعدادات الشبكة المحلية اللاسلكية، باستخدام هذه الطريقة للمصادقة يمكن للطرفية الارتباط بأي نقطة وصول تستخدم

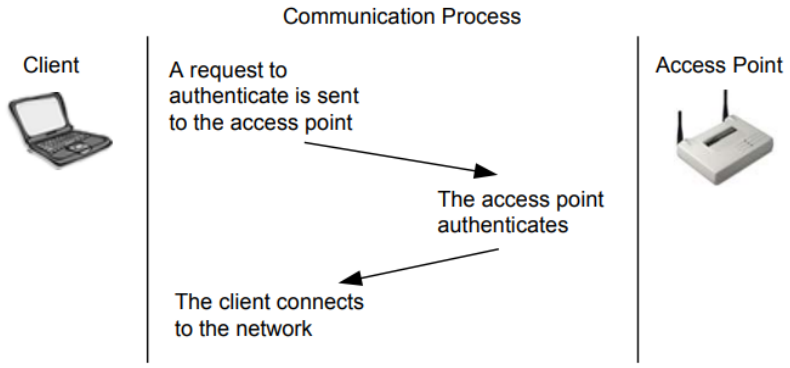
مصادقة النظام المفتوح التي تعتمد فقط على وجود معرف مجموعة الخدمة الصحيح (SSID)، يجب أن تتطابق معرفات SSID ضمن كل من نقطة الوصول والطرفية قبل السماح للطرفية بإكمال عملية المصادقة، ستتم مناقشة استخدامات SSID المتعلقة بالأمان في الفصول القادمة، تُستخدم عملية مصادقة النظام المفتوح بشكل فعال في كل من البيئات الآمنة وغير الآمنة.

تتم عملية مصادقة النظام المفتوح على النحو التالي:

١- تقدم الطرفية اللاسلكية طلبًا للانضمام بنقطة الوصول.

٢- تصادق نقطة الوصول على الطرفية وترسل استجابة إيجابية وتصبح الطرفية مرتبطةً (متصلةً)

يبين الشكل (٣-٤) المراحل السابقة.




الشكل (٣-٤): خطوات مصادقة النظام المفتوح.

تعتبر مصادقة النظام المفتوح هي عملية بسيطة للغاية، يمتلك مدير الشبكة المحلية اللاسلكية خيار استخدام تشفير الخصوصية السلكية المكافئة Wired Equivalent Privacy (WEP) مع مصادقة النظام المفتوح، إذا تم استخدام WEP مع عملية مصادقة النظام المفتوح فلا يزال هناك عدم تحقق من مفتاح WEP على كل جانب من الاتصال أثناء المصادقة، بدلاً من ذلك يتم استخدام مفتاح WEP فقط لتشفير البيانات بمجرد مصادقة الطرفية وربطها.

تُستخدم مصادقة النظام المفتوح في عدة سيناريوهات، إلا أن هناك سببان رئيسيان لاستخدامها، أولاً: تعتبر مصادقة النظام المفتوح هي الأكثر أمانًا من بين طريقتين للمصادقة للأسباب سنوضحها لاحقاً، ثانيًا: من السهل إعداد مصادقة النظام المفتوح لأنها لا تتطلب أي إعداد على الإطلاق، تم إعداد جميع أجهزة شبكة LAN اللاسلكية المتوافقة مع ٨٠٢.١١ لاستخدام مصادقة النظام المفتوح افتراضيًا، مما يجعل من السهل البدء في إنشاء شبكة LAN اللاسلكية وتوصيلها فور إخراج التجهيزات الخاصة بها من عبواتها.

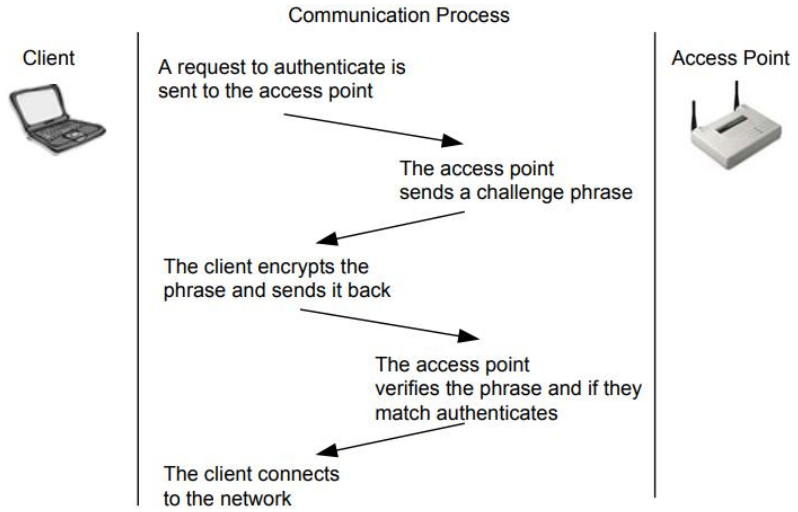
**مصادقة المفتاح المشترك:**

مصادقة المفتاح المشترك هي طريقة مصادقة تتطلب استخدام WEP، يستخدم تشفير WEP المفاتيح التي يتم إدخالها (عادةً بواسطة مدير الشبكة) في كل من الطرفية ونقطة الوصول، يجب أن تتطابق هذه المفاتيح على كلا الجانبين حتى يعمل WEP بشكل صحيح، تستخدم مصادقة المفتاح المشترك مفاتيح WEP في نسختين كما سيتم توضيحه في هذه الفقرة.

تتم مصادقة المفتاح المشترك على النحو التالي:

١- تطلب الطرفية الارتباط بنقطة وصول، هذه الخطوة هي نفس خطوة مصادقة النظام المفتوح.
٢- تشكل نقطة الوصول كلمى تحدي للطرفية، هذا التحدي يتم إنشاؤه عشوائيًا وهو نص عادي، يتم إرساله من نقطة الوصول إلى الطرفية بشكل واضح.
٣- تستجيب الطرفية للتحدي، تستجيب الطرفية عن طريق تشفير نص التحدي باستخدام مفتاح WEP الخاص بالطرفية وإرساله مرة أخرى إلى نقطة الوصول.
٤- تستجيب نقطة الوصول لاستجابة الطرفية، تقوم نقطة الوصول بفك تشفير استجابة الطرفية المشفرة للتحقق من تشفير نص التحدي باستخدام مفتاح WEP مطابق، من خلال هذه العملية تحدد نقطة الوصول ما إذا كانت الطرفية تمتلك مفتاح WEP الصحيح أم لا، إذا كان مفتاح WEP الخاص بالطرفية صحيحًا ستستجيب نقطة الوصول بشكل إيجابي وتقوم بمصادقة الطرفية، إذا كان مفتاح WEP الخاص بالطرفية غير صحيح ستستجيب نقطة الوصول سلبًا ولن تصادق على الطرفية مما يترك الطرفية غير مصادقة وغير مرتبطة.

يبين الشكل (٣-٥) مراحل المصادقة بالمفتاح المشترك:




الشكل (٣-٥): المصادقة بالمفتاح المشترك.

من الممكن أن تبدو لك عملية مصادقة المفتاح المشترك أكثر أمانًا من مصادقة النظام المفتوح، ولكن كما سنرى لاحقاً فهي ليست كذلك، حيث تفتح مصادقة المفتاح المشترك الباب أمام المتسللين المحتملين، من المهم فهم كلا الطريقتين التي يتم استخدام WEP فيها. يمكن استخدام مفتاح WEP أثناء عملية مصادقة المفتاح المشترك للتحقق من هوية الطرفية، ولكن يمكن استخدامه أيضًا لتشفير البيانات التي ترسلها الطرفية من خلال نقطة الوصول، سنقوم بمناقشة هذا النوع من استخدام WEP بمزيد من التفصيل لاحقاً.

### ٢-٥- أمن التوثق:

لا تعتبر مصادقة المفتاح المشترك آمنة لأن نقطة الوصول تنقل نص التحدي بشكل واضح وتتلقى نفس نص التحدي المشفر باستخدام مفتاح WEP، يسمح هذا السيناريو للمتسلل الذي يستخدم برامج خاصة بهذا النمط من الاختراق برؤية كل من التحدي الواضح والتحدي المشفر، بوجود هاتين القيمتين يمكن للمتسلل استخدام برنامج تحليل بسيط لاشتقاق المفتاح WEP، بمجرد الحصول على المفتاح WEP يمكن للمتسلل فك تشفير حركة المرور المشفرة، ولهذا السبب تعتبر مصادقة النظام المفتوح أكثر أمانًا من مصادقة المفتاح المشترك.

من المهم لمدير الشبكة اللاسلكية أن يفهم أن كلاً من مصادقة النظام المفتوح ومصادقة المفتاح المشترك ليس آمنًا، ولهذا السبب فإن إيجاد حلول أمنية للشبكات المحلية اللاسلكية بالإضافة إلى ما يحدده المعيار ٨٠٢.١١ مهم وضروري.

### ٢-٦- المفاتيح السرية المشتركة والشهادات:

المفاتيح السرية المشتركة هي عبارة عن سلاسل من الأرقام أو النصوص التي يشار إليها عادةً بمفتاح WEP، الشهادات هي طريقة أخرى لتعريف المستخدم تُستخدم ضمن الشبكات اللاسلكية، تمامًا كما هو الحال مع مفاتيح WEP يتم وضع الشهادات (وهي مستندات مصادقة) على جهاز الطرفية مسبقًا، يتم إجراء هذا الوضع بحيث تكون آلية المصادقة موجودة بالفعل في الطرفية عندما يرغب المستخدم في المصادقة على الشبكة اللاسلكية، تم تنفيذ كلتا الطريقتين تاريخياً بطريقة يدوية إلا أن هناك تطبيقات متاحة اليوم تسمح بأتمتة هذه العملية.

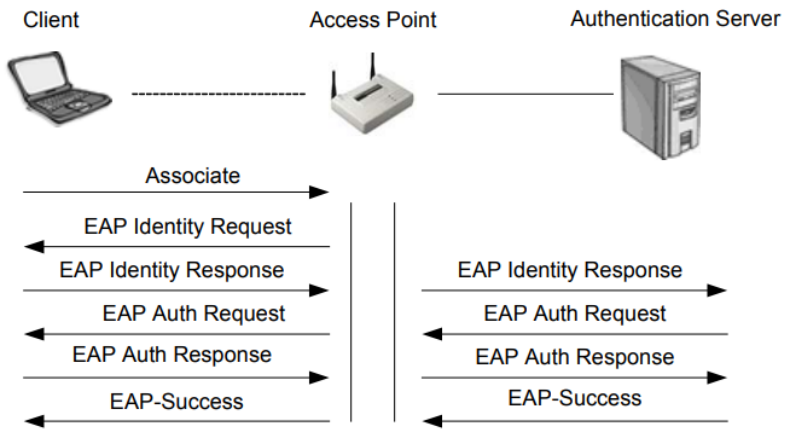
### ٢-٧- بروتوكولات المصادقة الحديثة:

هناك العديد من حلول وبروتوكولات أمان المصادقة الجديدة اليوم، بما في ذلك VPN و802.1x باستخدام بروتوكول المصادقة القابل للتوسيع Extensible Authentication Protocol (EAP)، تتضمن العديد من حلول الأمان تمرير المصادقة إلى خوادم المصادقة بدءًا من نقطة الوصول مع إبقاء الطرفية في انتظار أثناء مرحلة المصادقة، يحتوي نظام التشغيل Windows XP على دعم لكل من ٨٠٢.١١ و802.1x وEAP، تدعم الشركات المصنعة للشبكات المحلية اللاسلكية هذه المعايير، لهذا السبب من السهل رؤية أن حل مصادقة 802.1x وEAP يمكن أن يكون حلاً شائعًا في الحلول الأمنية الخاصة بالشبكات المحلية اللاسلكية.

**802.1x و EAP:**

يعد المعيار 802.1x (التحكم في الوصول إلى الشبكة استناداً إلى المنفذ) جديدًا نسبيًا، ولا تتمتع الأجهزة التي تدعمه بالقدرة على السماح بالاتصال بالشبكة في الطبقة الثانية إلا إذا نجحت مصادقة المستخدم، يعمل هذا البروتوكول بشكل جيد مع نقاط الوصول التي تحتاج إلى القدرة على إبقاء المستخدمين مفصولين إذا لم يكن من المفترض أن يكونوا على الشبكة. EAP هو بروتوكول من الطبقة الثانية وهو بديل مرن لـ PAP أو CHAP ضمن PPP يعمل عبر الشبكات المحلية، يسمح EAP باستخدام برامج مساعدة في أي من طرفي الارتباط والتي يمكن من خلالها استخدام العديد من طرق المصادقة. في الماضي تم استخدام PAP و/أو CHAP لمصادقة المستخدم وكلاهما يدعم استخدام كلمات المرور. تبينت الحاجة إلى بديل أقوى وأكثر مرونة مع الشبكات اللاسلكية نظرًا لأن التطبيقات الأكثر تنوعًا تكثر مع الشبكات اللاسلكية مقارنة بالشبكات السلكية.

عادةً ما يتم تحقيق مصادقة المستخدم باستخدام خادم RADIUS ونوع من قاعدة بيانات المستخدم ( Native RADIUS وNDS وActive Directory وLDAP وغيرها)، يبين الشكل (٣-٦) عملية المصادقة باستخدام EAP، يتضمن المعيار 802.11i الجديد دعم كل من 802.1x وEAP وAAA والمصادقة المتبادلة وتوليد المفاتيح، والتي لم يتم تضمين أي منها في المعيار ٨٠٢.١١ الأساسي، "AAA" هي اختصار للمصادقة Authentication (تحديد هويتك) والتخويل Authorization (سمات تسمح لك بأداء مهام معينة على الشبكة) والتدوين Accounting (توضح ما قمت به وأين كنت على الشبكة).




الشكل (٣-٦): 802.1x وEAP.

في النموذج المعياري 802.1x تتكون مصادقة الشبكة من ثلاث أجزاء: طالب المصادقة والمصدق وخادم المصادقة.

نظرًا لضرورة تحقيق أمان شبكة LAN اللاسلكية ومع توفر أنواع مصادقة EAP التي توفر وسيلة لتأمين اتصال LAN اللاسلكي، يقوم المصنعون بتطوير وإضافة أنواع مصادقة EAP إلى نقاط وصول الشبكة المحلية اللاسلكية الخاصة بهم، تعد معرفة نوع EAP المستخدم أمرًا مهمًا في فهم خصائص طريقة المصادقة مثل كلمات المرور وإنشاء المفاتيح والمصادقة المتبادلة والبروتوكول، تتضمن بعض أنواع مصادقة EAP الشائعة:

- **EAP-MD-5 challenge**: أقدم نوع مصادقة EAP، وهو يكرر بشكل أساسي حماية كلمة مرور CHAP على شبكة LAN لاسلكية، يمثل EAP-MD5 نوعًا من دعم EAP الأساسي بين أجهزة 802.1x.
- **EAP-Cisco Wireless**: يُطلق عليه أيضًا Lightweight Extensible Authentication Protocol (LEAP)، أي بروتوكول المصادقة الموسعة خفيف الوزن. يتم استخدام هذا النوع من مصادقة EAP بشكل أساسي في نقاط وصول شبكة LAN اللاسلكية من Cisco، يوفر LEAP الأمان أثناء تبادل بيانات الاعتماد، ويشفر نقل البيانات باستخدام مفاتيح WEP التي يتم إنشاؤها ديناميكيًا، ويدعم المصادقة المتبادلة.
- **EAP-TLS**: TLS هي اختصار Transport Layer Security وتعني أمان طبقة النقل. يوفر EAP-TLS مصادقة متبادلة قائمة على الشهادة للطرفية والشبكة، حيث يعتمد EAP-TLS على الشهادات من جانب الطرفية والخادم لإجراء المصادقة وباستخدام مفاتيح WEP المستندة إلى المستخدم والجلسة والتي يتم إنشاؤها ديناميكيًا لتأمين الاتصال، يتضمن نظام التشغيل Windows XP مستخدم EAP-TLS كما يدعم نظام التشغيل Windows 2000 المصادقة باستخدام EAP-TLS.
- **EAP-TTLS**: TTLS هي اختصار Tunneled TLS. EAP-TTLS هو امتداد لـ EAP-TLS، وهو يوفر مصادقة متبادلة قائمة على الشهادة للطرفية والشبكة، على عكس EAP-TLS لا يتطلب EAP-TTLS سوى شهادات من جانب الخادم مما يلغي الحاجة إلى إعداد الشهادات لكل طرفية شبكة LAN لاسلكية. بالإضافة إلى ذلك يدعم EAP-TTLS بروتوكولات كلمات المرور القديمة بحيث يمكنك نشرها مقابل نظام المصادقة الحالي لديك (مثل Active Directory أو NDS). يقوم EAP-TTLS بتأمين نقل مصادقة الطرفية بشكل آمن داخل سجلات TLS مما يضمن بقاء المستخدم مجهولاً أمام المتنصتين على الوصلة اللاسلكية، يتم توزيع مفاتيح WEP المستندة إلى المستخدم والجلسة والتي يتم إنشاؤها ديناميكيًا لتأمين الاتصال.
- **EAP-SRP**: SRP هي اختصار Secure Remote Password وتعني استخدام كلمات المرور عن بعد بشكل آمن. SRP هو بروتوكول مصادقة آمن يعتمد على كلمات المرور وتبادل المفاتيح، وهو بوفر

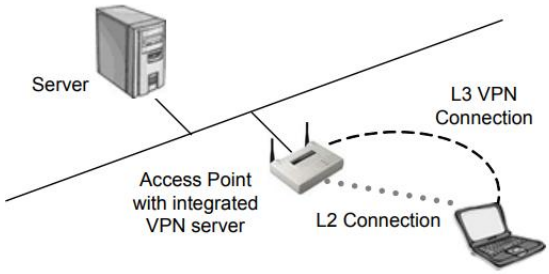
حلاً لمشكلة مصادقة الطرفيات على الخوادم بشكل آمن في الحالات التي يجب فيها على مستخدم برنامج الطرفية حفظ سر صغير (مثل كلمة المرور) ولا يحمل أي معلومات سرية أخرى. يحمل الخادم أداة تحقق لكل مستخدم مما يسمح للخادم بمصادقة الطرفية، ومع ذلك إذا تم اختراق أداة التحقق فلن يُسمح للمهاجم بانتحال شخصية الطرفية، بالإضافة إلى ذلك يتبادل SRP سرًا مشفرًا قويًا كمنتج ثانوي للمصادقة الناجحة والتي تمكن الطرفين من التواصل بشكل آمن.

- **EAP-SIM (GSM)**: EAP-SIM هي آلية لمصادقة الوصول إلى شبكة IP المتنقلة وإنشاء مفتاح التسجيل باستخدام وحدة تعريف مشترك GSM (SIM). الأساس المنطقي لاستخدام GSM SIM مع Mobile IP هو الاستفادة من البنية التحتية الحالية لشبكات GSM المرخصة مع قاعدة المستخدمين الحالية وقنوات توزيع بطاقة SIM الحالية، باستخدام تبادل مفاتيح SIM لا يلزم ارتباط أمان آخر مُكوّن مسبقًا إلى جانب بطاقة SIM على العقدة المتنقلة. لا تكمن الفكرة في استخدام تقنية الوصول إلى الوصلة الراديوية للشبكة GSM ولكن استخدام ترخيص GSM SIM مع Mobile IP عبر أي طبقة ارتباط (على سبيل المثال على شبكات الوصول إلى الشبكة المحلية اللاسلكية).

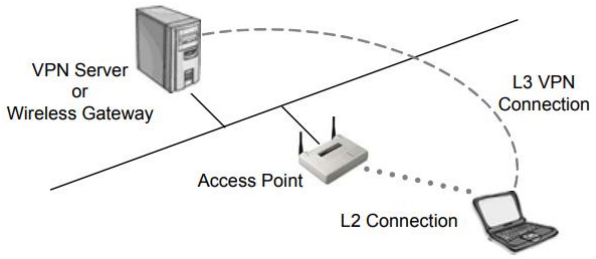
من المحتمل أن تتزايد قائمة أنواع مصادقة EAP السابقة مع دخول المزيد والمزيد من المصنعين إلى سوق التدابير الأمنية الخاص بالشبكات المحلية اللاسلكية. إن فهم ماهية EAP وكيفية استخدامه بشكل عام هو عنصر أساسي في أن تكون فعالًا كمدير شبكة لاسلكية.

**حلول VPN:**

توفر تقنية VPN وسيلة لنقل البيانات بأمان بين جهازي شبكة عبر وسيط نقل بيانات غير آمن، وهو يستخدم بشكل شائع لربط أجهزة الكمبيوتر أو الشبكات البعيدة بخادم الشركة عبر الإنترنت، أيضاً يتم استخدام VPN كحل لحماية البيانات على شبكة لاسلكية. تعمل VPN عن طريق إنشاء نفق فوق بروتوكول مثل IP، وتكون حركة المرور داخل النفق مشفرة ومعزولة تمامًا كما يتضح من الشكلين (٣-٧) و(٣-٨). توفر تقنية VPN ثلاثة مستويات من الأمان: مصادقة المستخدم والتشفير ومصادقة البيانات.




الشكل (٣-٧): نقطة وصول مع خادم VPN متكامل مع الشبكة.




الشكل (٣-٨): نقطة وصول مع خادم VPN خارجي.

- تضمن مصادقة المستخدم أن المستخدمين المصرح لهم فقط (عبر جهاز معين) قادرون على الاتصال وإرسال واستقبال البيانات عبر الشبكة اللاسلكية.
- يوفر التشفير حماية إضافية لأنه يضمن أنه حتى إذا تم اعتراض عمليات الإرسال فلا يمكن فك تشفيرها بدون وقت وجهد كبيرين.
- تضمن مصادقة البيانات سلامة البيانات الموجودة على الشبكة اللاسلكية مما يضمن أن كل حركة المرور تأتي من الأجهزة المصادق عليها فقط.

يتطلب تطبيق تقنية VPN لتأمين شبكة لاسلكية أسلوبًا مختلفًا عما هو عليه عند استخدامها على الشبكات السلكية للأسباب التالية:

- تقوم وظيفة المكرر المتضمنة في نقاط الوصول اللاسلكية بإعادة توجيه حركة المرور تلقائيًا بين محطات LAN اللاسلكية التي تتصل معًا والتي تظهر على نفس الشبكة اللاسلكية.
- من المحتمل أن يمتد نطاق الشبكة اللاسلكية إلى ما وراء الحدود المادية للمكتب أو المنزل مما يمنح المتسللين وسيلة لتهديد الشبكة.

تجعل السهولة وقابلية التوسع (التي يمكن من خلالها نشر حلول الشبكة المحلية اللاسلكية) من الشبكات اللاسلكية حلاً مثالياً للعديد من البيئات المختلفة، نتيجة لذلك يختلف تنفيذ الحل الأمني باستخدام تكنولوجيا VPN بناءً على احتياجات كل نوع من هذه البيئات، على سبيل المثال يمكن للمتسلل الذي لديه جهاز تنصت لاسلكي (إذا حصل على مفتاح WEP) أن يقوم بفك تشفير الحزم في الزمن الحقيقي، باستخدام الحل VPN لن تكون الحزم مشفرة فحسب بل ستكون نفقًا أيضًا. توفر طبقة الأمان الإضافية التي توفرها حلول VPN العديد من الفوائد على مستوى الوصول.

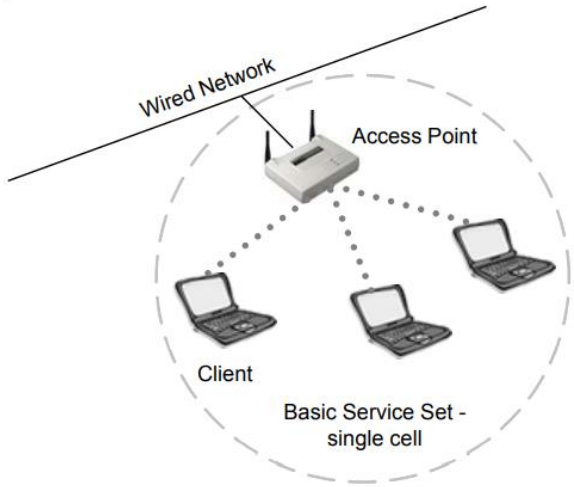
## ٣- مجموعات الخدمات

مجموعة الخدمات هي مصطلح يستخدم لوصف المكونات الأساسية لشبكة LAN لاسلكية تعمل بكامل طاقتها، بمعنى آخر هناك ثلاث طرق لتكوين شبكة LAN لاسلكية وتتطلب كل طريقة مجموعة مختلفة من الأجهزة، الطرق الثلاث لتكوين شبكة LAN لاسلكية هي:

- مجموعة الخدمات الأساسية Basic Service Set (BSS).
- مجموعة الخدمات الموسعة Extended Service Set (ESS).
- مجموعة الخدمات الأساسية المستقلة Independent Basic Service Set (IBSS).

### ٣-١- مجموعة الخدمات الأساسية:

عند توصيل نقطة وصول واحدة بشبكة سلكية ومجموعة من المحطات اللاسلكية يُشار إلى تكوين الشبكة على أنه مجموعة خدمات أساسية (BSS)، تتكون مجموعة الخدمات الأساسية من نقطة وصول واحدة وطرفية لاسلكية واحدة أو أكثر كما هو موضح في الشكل (٣-٩)، تستخدم مجموعة الخدمات الأساسية وضع البنية التحتية، وهو وضع يتطلب استخدام نقطة وصول حيث تعبر جميع حركات المرور اللاسلكية من خلال نقطة الوصول، ولا يسمح بالإرسال المباشر ما بين طرفيتين.



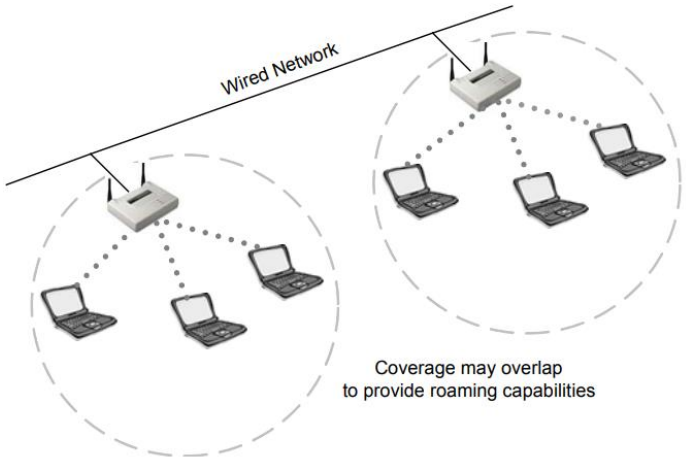

الشكل (٣-٩): مجموعة الخدمات الأساسية.

يجب على كل طرفية لاسلكية استخدام نقطة الوصول للاتصال بأي طرفية لاسلكية أخرى أو أي جهاز مضيف سلكي على الشبكة، تغطي BSS خلية واحدة أو منطقة راديوية حول نقطة الوصول مع مناطق معدل بيانات متفاوتة (دوائر متحدة المركز) بسرعات بيانات مختلفة مقاسة بالواحدة Mbps، وتعتمد سرعات البيانات في هذه الدوائر متحدة المركز على التكنولوجيا المستخدمة، في حال كانت BSS مكونة من تجهيزات 802.11b فستكون للدوائر

متحدة المركز سرعات بيانات تبلغ ١١ و٥.٥ و٢ و١ ميجابت في الثانية، وتصبح معدلات البيانات أصغر كلما ابتعدت الدوائر عن نقطة الوصول. يحتوي BSS على SSID واحد وهو خاص به لا يمكن أن يتماثل مع BSS أخرى.

### ٣-٢- مجموعة الخدمات الموسعة:

تعرّف مجموعة الخدمات الموسعة على أنها مجموعتان أو أكثر من مجموعات الخدمات الأساسية المتصلة بنظام توزيع مشترك كما هو موضح في الشكل (٣-١٠)، يمكن أن يكون نظام التوزيع سلكيًا أو لاسلكيًا أو LAN أو WAN أو أي طريقة أخرى للاتصال بالشبكة، ويجب أن تحتوي ESS على نقطتي وصول على الأقل تعملان في نمط البنية التحتية. كم في BSS يجب أن تمر جميع الحزم ضمن ESS عبر إحدى نقاط الوصول.



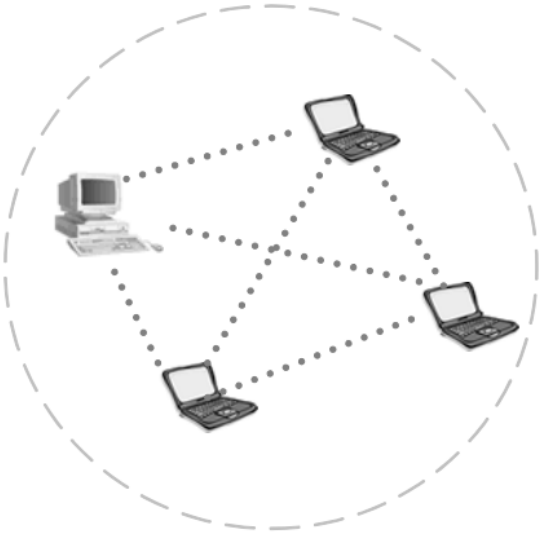

الشكل (٣-١٠): مجموعة الخدمات الموسعة.

وفقًا للمعيار ٨٠٢.١١ من الخصائص الأخرى لمجموعات الخدمات الموسعة: تغطي خلايا متعددة وتسمح (إلا أنها لا تتطلب) بإمكانية التجوال ولا تتطلب نفس SSID في كلتا مجموعتي الخدمة الأساسية.

### ٣-٣- مجموعة الخدمات الأساسية المستقلة:

تُعرف مجموعة الخدمات الأساسية المستقلة أيضًا باسم شبكة الأقران ad-hoc network، لا تحتوي IBSS على نقطة وصول أو أي وصول آخر إلى نظام توزيع، وهي تغطي خلية واحدة ولديها SSID واحد كما هو موضح في الشكل (٣-١١)، تتناوب الطرفيات في IBSS مسؤولية إرسال الإطارات المرشدة نظرًا لعدم وجود نقطة وصول لأداء هذه المهمة.

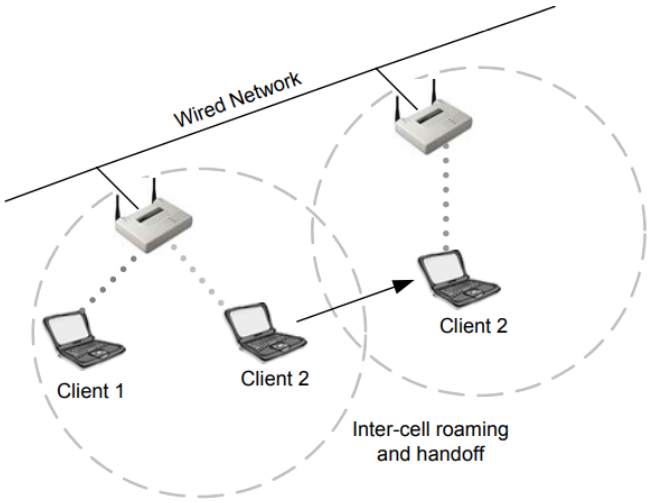
لنقل البيانات خارج IBSS يجب أن تعمل أحد الطرفيات ضمن الشبكة IBSS كبوابة أو جهاز توجيه باستخدام حل برمجي لهذا الغرض، ضمن IBSS تقوم الطرفيات بإجراء اتصالات مباشرة مع بعضهم البعض عند نقل البيانات، ولهذا السبب غالبًا ما يشار إلى IBSS على أنها شبكة نظير إلى نظير peer-to-peer network.



الشكل (٣-١١): مجموعة الخدمات الأساسية المستقلة.

### ٣-٤- التجوال Roaming:

التجوال هو عملية أو قدرة الطرفية اللاسلكية على الانتقال بمرونة من خلية (أو BSS) إلى أخرى دون فقدان الاتصال بالشبكة، تقوم نقاط الوصول بتسليم الطرفية من واحدة إلى أخرى بطريقة غير مرئية للطرفية، وهو ما يضمن اتصالاً غير منقطع، يوضح الشكل (٣-١٢) تجوال طرفية من BSS إلى BSS أخرى.




الشكل (٣-١٢): التجوال ضمن ESS.

عندما تكون أي منطقة في المبنى الذي يحتوي على الشبكة ضمن نطاق استقبال أكثر من نقطة وصول واحدة تتداخل تغطية الخلايا، تعد مناطق التغطية المتداخلة سمة مهمة لإعداد شبكة LAN اللاسلكية كونها تتيح التجوال المرن بين الخلايا المتداخلة، ويسمح التجوال لمستخدمي الهواتف المحمولة الذين لديهم طرفيات لاسلكية بالتنقل بحرية بين الخلايا المتداخلة والحفاظ باستمرار على اتصال الشبكة الخاص بهم.

عندما يكون التجوال مرناً يمكن الاحتفاظ بجلسة عمل أثناء الانتقال من خلية إلى أخرى، ويمكن أن توفر نقاط الوصول المتعددة تغطية التجوال اللاسلكي لمبنى أو حرم جامعي بأكمله.

عندما تتداخل منطقة تغطية نقطتي وصول أو أكثر يمكن للطرفيات الموجودة في المنطقة المتداخلة إنشاء أفضل اتصال ممكن بإحدى نقاط الوصول أثناء البحث المستمر عن أفضل نقطة وصول، من أجل تقليل فقد الحزم أثناء التبديل تتواصل نقاط الوصول "القديمة" و"الجديدة" لتنسيق عملية التجوال، تشبه هذه الوظيفة عملية التسليم handover في الشبكات الخلوية مع اختلافين رئيسيين:

- في نظام LAN القائم على حزم البيانات يمكن إجراء الانتقال من خلية إلى أخرى بين عمليات إرسال الحزم على عكس الاتصالات الهاتفية حيث قد يحدث الانتقال أثناء محادثة هاتفية.
- في نظام صوتي قد لا يؤثر قطع الاتصال المؤقت على المحادثة، بينما في بيئة قائمة على الحزم فإنه يقلل بشكل كبير من الأداء لأن بروتوكولات الطبقة العليا تعيد إرسال البيانات.

**المعايير:**

لا يحدد المعيار 802.11 كيفية إجراء التجوال، ولكنه يحدد الأسس الخاصة بذلك، تتضمن هذه الأسس كل من المسح النشط والسلبي وعملية إعادة الانضمام، تحدث عملية إعادة الانضمام عندما تتجول محطة لاسلكية من نقطة وصول إلى أخرى وتصبح مرتبطة بنقطة الوصول الجديدة.

يسمح المعيار 802.11 للطرفية بالتجول بين نقاط وصول متعددة تعمل على نفس القنوات أو قنوات منفصلة، على سبيل المثال كل ١٠٠ مللي ثانية قد ترسل نقطة وصول إطار مرشد يتضمن طابعًا زمنيًا لمزامنة الطرفية وخريطة مؤشر حركة المرور وإشارة إلى معدلات البيانات المدعومة ومعاملات أخرى. تستخدم الطرفيات المتجولة الإطار المرشد لقياس قوة اتصالها الحالي بنقطة الوصول، في حال كان الاتصال ضعيفًا يمكن للطرفية التي تقوم بالتجوال محاولة ربط نفسها بنقطة وصول جديدة.

لتلبية احتياجات الاتصالات اللاسلكية المتنقلة يجب أن يكون المعيار 802.11b متسامحًا مع انقطاع الاتصالات وإعادة إنشائها، يحاول المعيار ضمان الحد الأدنى من التعطيل لتسليم البيانات ويوفر بعض الميزات للتخزين المؤقت وإعادة توجيه الرسائل بين المجموعات BSS.

قد تكون عمليات التنفيذ الخاصة لبعض بروتوكولات الطبقة العليا مثل TCP/IP أقل تسامحًا، على سبيل المثال في شبكة تستخدم DHCP لتعيين عناوين IP قد تفقد عقدة تقوم بالتجوال اتصالها عندما تتحرك عبر حدود الخلية، ويتعين على العقدة بعد ذلك إعادة إنشاء الاتصال عندما تدخل BSS. تتوفر حلول برمجية لمعالجة هذه المشكلة بالذات.

يترك المعيار 802.11b الكثير من الوظائف التفصيلية لما يسميه نظام التوزيع للمصنعين، كان هذا القرار قرارًا متعمدًا من جانب المصممين المعياريين، إذ أنهم كانوا أكثر اهتمامًا بجعل المعيار مستقلاً تمامًا عن أي معايير شبكة أخرى موجودة، من الناحية العملية فإن الغالبية العظمى من شبكات LAN اللاسلكية 802.11b التي تستخدم طبولوجيا ESS متصلة بشبكات Ethernet LAN وتستفيد بشدة من TCP/IP، لقد تقدم بائعو شبكات LAN اللاسلكية من ناحية تقديم طرق خاصة لتسهيل التجوال بين العقد في ESS.

عندما تتجول محطة من نقطة وصول قديمة إلى نقطة وصول جديدة تكون نقطة الوصول الجديدة مسؤولة عن ضمان إخطار أي جسور بين نقطتي الوصول بشكل صحيح بالموقع الجديد للمحطة، لم يتم تحديد الطريقة التي يتم بها تحقيق ذلك، الشرط الوحيد هو أن يتم تنفيذ بعض الطرق التي تضمن أن الحزم ستتدفق بشكل صحيح إلى نقطة الوصول الجديدة للمحطة، يتناول المعيار IEEE 802.11f مسألة توحيد التجوال مع إدخال بروتوكول Inter Access Point (IAPP).

**الوصل:**

تعتبر طبقة MAC في المعيار ٨٠٢.١١ مسؤولة عن كيفية ارتباط الطرفية بنقطة الوصول، عندما تدخل طرفية ٨٠٢.١١ في نطاق نقطة وصول واحدة أو أكثر تختار الطرفية نقطة وصول ليتم الوصل معها (وتسمى أيضًا الانضمام إلى BSS) بناءً على قوة الإشارة ومعدلات خطأ الحزمة الملحوظة.

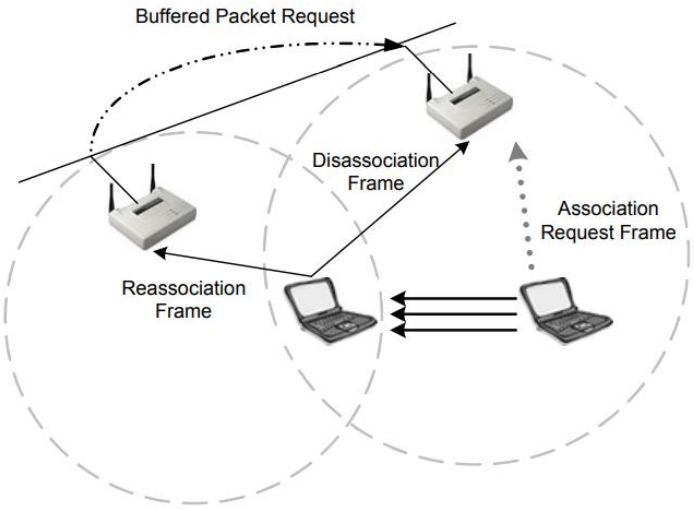
بمجرد الارتباط بنقطة الوصول تقوم المحطة بشكل دوري بمسح جميع قنوات ٨٠٢.١١ من أجل تقييم ما إذا كانت نقطة وصول مختلفة ستوفر خصائص أداء أفضل، في حال قررت الطرفية أن هناك إشارة أقوى من نقطة وصول مختلفة تعيد الطرفية الارتباط بنقطة الوصول الجديدة، وتضبط القناة الراديوية التي تم تعيين نقطة الوصول عليها. لن

تحاول المحطة التجوال حتى ينخفض مستوى الإشارة لديها إلى ما دون عتبة قوة الإشارة المحددة من قبل الشركة المصنعة.

### إعادة الانضمام Reassociation:

تحدث إعادة الانضمام عادةً لأن المحطة اللاسلكية قد ابتعدت فعليًا عن نقطة الوصول الأصلية مما يتسبب في ضعف الإشارة، في حالات أخرى تحدث إعادة الانضمام بسبب تغيير في الخصائص الراديوية في المبنى أو ببساطة بسبب حركة الشبكة العالية على نقطة الوصول الأصلية، في الحالة الأخيرة تُعرف هذه الوظيفة باسم موازنة الحمل load balancing نظرًا لأن وظيفتها الأساسية هي توزيع إجمالي حمل شبكة LAN اللاسلكية بكفاءة أكبر عبر البنية التحتية اللاسلكية المتاحة.

يختلف الانضمام وإعادة الانضمام بشكل طفيف فقط في استخدامهما، حيث يتم استخدام إطارات طلب الانضمام عند الانضمام إلى شبكة لأول مرة، وتُستخدم إطارات طلب إعادة الانضمام عند التجوال بين نقاط الوصول بحيث تعرف نقطة الوصول الجديدة كيفية التفاوض على نقل الإطارات المخزنة من نقطة الوصول القديمة وإعلام نظام التوزيع بأن الطرفية قد انتقلت، يوضح الشكل (٣-١٣) عملية إعادة الانضمام.




الشكل (٣-١٣): التجوال وإعادة الانضمام.

تسمح عملية الانضمام وإعادة الانضمام بنقاط الوصول ديناميكيًا لمديري الشبكات بإعداد شبكات LAN لاسلكية بتغطية واسعة جدًا عن طريق إنشاء سلسلة من خلايا ٨٠٢.١١ المتداخلة في جميع أنحاء المبنى أو عبر الحرم الجامعي، لتحقيق النجاح يستخدم مدير تكنولوجيا المعلومات بشكل مثالي إعادة استخدام القناة channel reuse مع الحرص على إعداد كل نقطة وصول على قناة ٨٠٢.١١ DSSS لا تتداخل مع قناة تستخدمها نقطة وصول

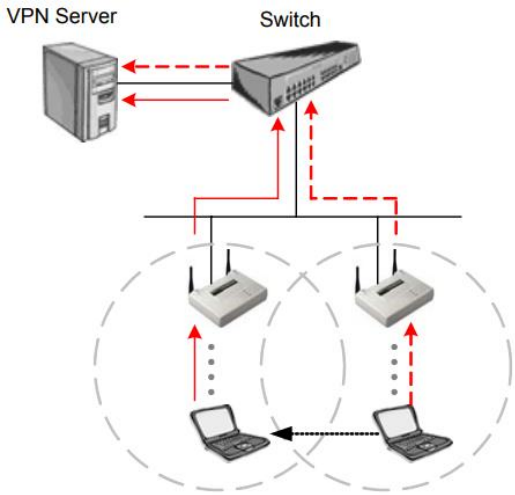
مجاورة. في حين أن هناك ١٤ قناة متداخلة جزئيًا محددة في ٨٠٢.١١ DSSS لا يوجد سوى ٣ قنوات لا تتداخل على الإطلاق، وهذه هي الأفضل للاستخدام للتغطية متعددة الخلايا، في حال كانت نقطتا وصول في نطاق بعضهما البعض وتم إعدادهما على نفس القنوات أو على قنوات متداخلة جزئيًا، فقد يتسببان في حدوث بعض التداخل لبعضهما البعض، وبالتالي خفض إجمالي عرض المجال الترددي المتاح في منطقة التداخل.

**استخدام VPN:**

عادةً ما يتم تنفيذ حلول VPN اللاسلكية بطريقتين: أولاً يتم استخدام خادم VPN مركزي من نقاط الوصول، يمكن أن يكون هذا الخادم ضمن جهاز مستقل أو خادمًا به تطبيق VPN يعمل عليه، كلاهما يخدم نفس الغرض ويوفر نفس النوع من الأمان والاتصال، يوفر وجود الخادم VPN (الذي يعمل أيضًا كبوابة وجدار حماية) بين المستخدم اللاسلكي والشبكة الأساسية مستوى من الأمان مشابهًا لشبكات VPN السلكية.

الطريقة الثانية هي مجموعة موزعة من خوادم VPN، تقوم بعض الشركات المصنعة بتطبيق خادم VPN في نقاط الوصول الخاصة بهم، يوفر هذا النوع من الحلول الأمان للمكاتب الصغيرة والمؤسسات المتوسطة الحجم دون استخدام آلية مصادقة خارجية مثل RADIUS، لقابلية التوسع تدعم نقطة الوصول التي تحتوي على خادم VPN الوصل مع خادم RADIUS.

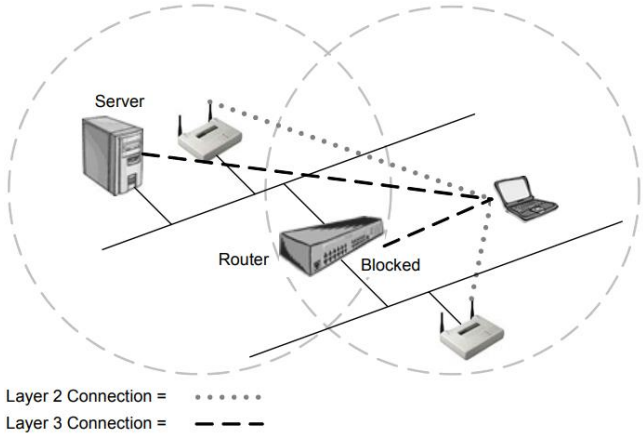
يتم إنشاء الأنفاق Tunnels من محطة الطرفية إلى خادم VPN كما هو موضح في الشكل (٣-١٤)، عندما يتجول المستخدم تتجول الطرفية بين نقاط الوصول عبر حدود الطبقة الثانية، هذه العملية مرنة لاتصال الطبقة الثالثة، ومع ذلك إذا تم إنشاء نفق لنقطة الوصول أو خادم VPN مركزي وتم تجاوز حدود الطبقة الثالثة فيجب توفير آلية من نوع ما للحفاظ على النفق عند عبور الحدود.




الشكل (٣-١٤): التجوال مع أنفاق VPN.

**حدود الطبقتين الثانية والثالثة:**

من قيود التكنولوجيا الحالية أن الشبكات السلكية غالبًا ما تكون مجزأة لسهولة الإدارة، غالبًا ما تقوم الشركات ذات المباني المتعددة مثل المستشفيات أو الشركات الكبيرة بتنفيذ شبكة LAN في كل مبنى ثم توصيل هذه الشبكات بأجهزة التوجيه، هذا التقسيم هو تقسيم على مستوى الطبقة الثالثة وله ميزتان رئيسيتان: أولاً يحتوي على عمليات البث بشكل فعال، وثانيًا يسمح بالتحكم في الوصول بين الأجزاء على الشبكة، يمكن أيضًا إجراء هذا النوع من التجزئة في الطبقة الثانية باستخدام شبكات VLAN ضمن المبدلات، غالبًا ما تُرى شبكات VLAN مرتبة طابقًا تلو الآخر في مباني المكاتب متعددة الطوابق أو لكل مبنى بعيد في الحرم الجامعي للأسباب نفسها، التقسيم في الطبقة الثانية بهذه الطريقة يقطع الشبكات تمامًا كما لو كان يتم تنفيذ شبكات متعددة، عند استخدام أجهزة التوجيه كما هو موضح في الشكل (٣-١٥) يجب أن يكون لدى المستخدمين طريقة للتجوال عبر حدود جهاز التوجيه دون فقد اتصال الطبقة الثالثة الخاصة بهم. لا تزال نقاط الوصول تحتفظ باتصال الطبقة الثانية، إلا أنه نظرًا لتغير شبكة IP الفرعية أثناء التجوال فسيتم قطع الاتصال بالخوادم على سبيل المثال، بدون إمكانية تجوال على مستوى الشبكات الفرعية (مثل استخدام حلول Mobile IP أو استخدام DHCP) يجب توصيل جميع نقاط الوصول لشبكة LAN اللاسلكية بشبكة فرعية واحدة.




الشكل (٣-١٥): التجوال عبر حدود الطبقة الثالثة.

## ٤- إدارة الاستطاعة

تعمل الطرفيات اللاسلكية في أحد وضعي إدارة الطاقة المحددين بواسطة معيار IEEE 802.11: **الوضع النشط** active mode والذي يُطلق عليه عادةً وضع الإدراك المستمر (Continuous Aware Mode "CAM")، ووضع **توفير الطاقة** power save والذي يُسمى عادةً وضع استقصاء توفير الطاقة (Power Save Polling "PSP").

يعتبر الحفاظ على الطاقة باستخدام وضع توفير الطاقة أمرًا مهمًا بشكل خاص لمستخدمي الأجهزة المحمولة الذين

يستخدمون أجهزة كمبيوتر محمولة أو أجهزة المساعد الرقمي الشخصي كونها تعمل على البطاريات، إذ يتيح إطالة عمر هذه البطاريات للمستخدم البقاء في وضع التشغيل والعمل لفترة أطول دون إعادة الشحن، يمكن لبطاقات LAN اللاسلكية استهلاك قدر كبير من الطاقة من البطارية أثناء وجودها في النمط CAM، وهو السبب الرئيسي في تضمين ميزات توفير الطاقة في المعيار ٨٠٢.١١.

## ٥- أساسيات التوزع الشبكي:

بمجرد انضمام طرفية لاسلكية إلى الشبكة ستتواصل هذه الطرفية مع بقية عناصر الشبكة عن طريق تمرير الإطارات عبر الشبكة بنفس الطريقة تقريبًا كأي شبكة IEEE 802 أخرى، لتوضيح مفهوم خاطئ شائع لا تستخدم الشبكات المحلية اللاسلكية إطارات ٨٠٢.٣ Ethernet، عملياً مصطلح Ethernet اللاسلكية هو عبارة عن تسمية خاطئة إلى حد ما، إذ تحتوي إطارات شبكة LAN اللاسلكية على معلومات أكثر مما تحتويه إطارات Ethernet الشائعة. سيتم التطرق إلى هذا الأمر خلال الفصل القادم بشيء من التفصيل.

يتضمن تخطيط شبكة LAN لاسلكية عملية جمع للمعلومات ومن ثم اتخاذ مجموعة من القرارات، فيما يلي قائمة بأهم المسائل الأساسية التي يجب تحديدها قبل بدء العمل الفعلي لتوزيع العناصر الشبكية:

- تحليل المرافق
- الشبكات الموجودة
- استخدام المنطقة والأبراج
- الغرض ومتطلبات العمل
- متطلبات النطاق الترددي والتجوال
- الموارد المتاحة
- متطلبات الأمن

جزء كبير من هذه المواضيع تم التطرق لها سابقاً وسيتم العمل على توضيح بقية هذه المواضيع خلال الفصول القادمة.

## مذاكرة

السؤال (١): يقصد بعملية الاستماع

- محاولة الطرفية التقاط إشارة لاسلكية ضمن مجالها الترددي
- التقاط الطرفية لكافة الإطارات أثناء العمل بالنمط النشط
- اكتشاف الطرفية للطرفيات المجاورة لها في الشبكة
- التقاط طرفية حركة مرور بشكل غير مخول.

السؤال (٢): الطريقة التي تعثر بها الطرفية على الشبكة

- Beacon
- Scanning
- Polling
- Association

السؤال (٣): هناك نوعان من المسح

- المسح السلبي والمسح الإيجابي
- المسح الخامل والمسح النشط
- المسح السلبي والمسح النشط
- المسح الخامل والمسح الإيجابي

السؤال (٤): يرسل معرّف مجموعة الخدمات (Service Set ID) ضمن إطار

- تحكم يطلق عليه مصطلح Polling
- تحكم يطلق عليه مصطلح Beacon
- إدارة يطلق عليه مصطلح Polling
- إدارة يطلق عليه مصطلح Beacon

السؤال (٥): معرف مجموعة الخدمات (SSID) هو

- قيمة أبجدية رقمية وحيدة حساسة لحالة الأحرف تتكون من ٢-٦٤ محرفًا
- قيمة رقمية وحيدة تتكون من ٢-٣٢ محرفًا
- قيمة أبجدية وحيدة حساسة لحالة الأحرف تتكون من ٢-٦٤ محرفًا
- قيمة أبجدية رقمية وحيدة حساسة لحالة الأحرف تتكون من ٢-٣٢ محرفًا

السؤال (٦): هي إطارات قصيرة يتم إرسالها من نقطة الوصول إلى الطرفيات (عندما تكون الشبكة في نمط البنية التحتية) أو من محطة إلى محطة (عندما تكون الشبكة في نمط Ad–hoc) من أجل تنظيم ومزامنة الاتصالات اللاسلكية على شبكة LAN اللاسلكية

- ACK
- Polling
- Beacon
- Association

السؤال (٧): تقوم الإطارات المرشدة بمزامنة الطرفيات من خلال

- SSID
- time–stamp
- FHSS
- DSSS

السؤال (٨): يتم استخدامه كمؤشر على الطرفيات التي تعمل ضمن نمط النوم sleep mode والتي لها حزم بيانات ضمن قائمة الانتظار في نقطة الوصول

- TIM
- BSS
- SSID
- Time-stamp

السؤال (٩): يدعم الجهاز المتوافق مع IEEE802.11b السرعات

- ١١ و٥.٥ و٢ و١ ميجابت في الثانية
- ١١ و٥.٥ و3 و١ ميجابت في الثانية
- ١١ و٥.٥ و4 و١ ميجابت في الثانية
- ١١ و٥.٥ و5 و١ ميجابت في الثانية

السؤال (١٠): عملية مراقبة الإطارات المرشدة على كل قناة لفترة زمنية محددة بعد إعداد الطرفية

- المسح الإيجابي
- المسح السلبي
- المسح الفعال
- المسح النشط

السؤال (١١): عادةً ما يتم تحديد التداخل بين خلايا نقطة الوصول بنسبة

- ١٠-٢٠٪ تقريبًا
- ٢٠-٣٠٪ تقريبًا
- ٣٠-٤٠٪ تقريبًا
- ٤٠-٥٠٪ تقريبًا

السؤال (١٢): يتضمن إرسال إطار طلب سبر من محطة لاسلكية

- المسح الإيجابي
- المسح السلبي
- المسح الفعال
- المسح النشط

السؤال (١٣): تختار الطرفية بشكل عام نقطة الوصول ذات

- أقوى إشارة
- أقل معدل خطأ في البت (BER)
- أقوى إشارة وأقل معدل خطأ في البت (BER)
- كل ما سبق غير صحيح

السؤال (١٤): تتكون عملية الاتصال بشبكة LAN لاسلكية من

- التوثق
- الانضمام
- التوثق ثم الانضمام
- الانضمام ثم التوثق

السؤال (١٥): تتعلق المصادقة مباشرةً ببطاقة الكمبيوتر الراديوية وليس بالمستخدم

- ببطاقة الكمبيوتر الراديوية
- بالمستخدم
- ببطاقة الكمبيوتر الراديوية والمستخدم
- غير ذلك

السؤال (١٦): هي العملية التي يتم من خلالها التحقق من هوية العقدة اللاسلكية (بطاقة الكمبيوتر الشخصي أو طرفية USB وغيرها) بواسطة الشبكة (عادةً نقطة الوصول) التي تحاول العقدة الاتصال بها

- Association

- Authentication
- Authorization
- Encryption

السؤال (١٧): في هذه الحالة يتم فصل العقدة اللاسلكية تمامًا عن الشبكة ولا يمكنها تمرير الإطارات عبر نقطة الوصول

- غير موثق وغير مرتبط
- موثق وغير مرتبط
- موثق ومرتبط
- مرتبط وغير موثق

السؤال (١٨): في هذه الحالة اجتازت الطرفية اللاسلكية عملية المصادقة، إلا أنه لم يتم ربطها بعد بنقطة الوصول

- غير موثق وغير مرتبط
- موثق وغير مرتبط
- موثق ومرتبط
- مرتبط وغير موثق

السؤال (١٩): في هذه الحالة تكون العقدة اللاسلكية متصلة تمامًا بالشبكة وقادرة على إرسال واستقبال البيانات من خلال نقطة الوصول التي تتصل بها العقدة

- غير موثق وغير مرتبط
- موثق وغير مرتبط
- موثق ومرتبط
- مرتبط وغير موثق

السؤال (٢٠): يحدد المعيار IEEE 802.11 للمصادقة:

- مصادقة النظام المفتوح
- مصادقة المفتاح المشترك
- مصادقة النظام المفتوح ومصادقة المفتاح المشترك
- غير ذلك

## الحل:

السؤال ١: A
السؤال ٢: B
السؤال ٣: C
السؤال ٤: D
السؤال ٥: D
السؤال ٦: C
السؤال ٧: B
السؤال ٨: A
السؤال ٩: B
السؤال ١٠: B
السؤال ١١: B
السؤال ١٢: D
السؤال ١٣: C
السؤال ١٤: C
السؤال ١٥: A
السؤال ١٦: B
السؤال ١٧: A
السؤال ١٨: B
السؤال ١٩: C
السؤال ٢٠: C

## المراجع:

[1] M Arunkumar, WIRELESS COMMUNICATIONS AND NETWORKS. 2020

[2] Certified Wireless Network Administrator study guide. 2021