



كتاب الشبكات اللاسلكية (CCNA Wireless) الإصدار الأول

المقدمة

بسم الله والصلاة والسلام على رسول الله وعلي أهله وصحبه ومن والاه إني يوم الدين

نبدأ باسم الله في تحضير كتاب بعنوان الشبكات اللاسلكية بحيث يكون هذا الكتاب شامل قدر

المستطاع بكل ما يتعلق بهذا النوع من الشبكات حتى يجد القارئ كل ما يريده ويحتاجه في عالم الشبكات

اللاسلكية مدعوماً في آخر هذا الكتاب بجانب من التطبيقات العملية بالإضافة إلى شرح كيفية عمل

Access point حتى تكون الصورة كاملاً بالنسبة للقارئ نسأل الله إن ينفع بهذا العمل

المسلمون جميعا ويجعل هذا العمل خالصا لوجهه وصدقا جاريا لوالدي الذي نسال الله ان يكون مثواه
الجنة.

وللعلم وبدون شك فاني لم أقوم بتأليف هذا الكتاب ولكن كل ما سوف أقوم به هو التجميع والتوليف
من مجموعة مصادر مختلفة منها كتاب سيسكو CCNA Wireless, QS_Wireless_Networking وبعض
الكتب المترجمة بلغة العربية حتى يكون هذا الكتاب وبشكل كبير مبسط وسهل الفهم والاستيعاب حتى
يتسنى للقارئ الفهم الصحيح لهذا النوع من الشبكات ويستفاد كل من له علاقة بهذه المجال.
وأخيرا أسف مسبقا علي أي خطأ إملائي أو أي خطأ غير مقصود .

معلومات عن الكاتب

- عبد السلام صالح الراشدي ليبيا بنغازي .
- ماجستير في علوم الحاسب الآلي من أكاديمية الدراسات العليا بنغازي سنة 2012 بمعدل 3.23 من 4 .
- دبلوم عالي في برمجة الحاسب الآلي من معهد العالي للتقنيات الحاسوب بنغازي في سنة 2004 بمعدل 72.
- دبلوم عالي في اللغة الانجليزية من المعهد العالي لإعداد المدرسين سنة 2005 بمعدل جيد جدا.

• شهادات , **MCSA , MCITP , MCTS , CCNA , TOFEL** ,

ICDL

- دورات في اللغة الانجليزية حتى مستوى upper intermediate في مركز اللغات
- بأكاديمية الدراسات العليا بنغازي .

عبد السلام صالح الراشدي

- دورة إدارة و تخطيط في مركز التدريب بضمان الاجتماعي .
- رئيس وحدة الشبكات في جامعة بنغازي (الكليات الطبية) .
- متعاون في قسم الشبكات في المعهد العالي للتقنيات الحاسوب بنغازي .
- عضو مؤسس لشركة تدمير للتقنية المعلومات .
- متعاون في جامعة بنغازي الأهلية وبعض المعاهد الأخرى .

أي تعليقات أو ملاحظات أو انتقادات علي عنواني الالكتروني

Abdo_it83@yahoo.com

المحتويات

الفصل الأول:- مقدمة عن الشبكات اللاسلكية

الفصل الثاني:- بعض المفاهيم في الشبكات

الفصل الثالث:- تقنيات الترميز modulation

الفصل الرابع:- معايير الشبكات اللاسلكية IEE 802.11

الفصل الخامس:- MODES OF WIRELESS LAN

الفصل السادس:- أنواع الشبكات اللاسلكية

الفصل السابع:- أمن الشبكات

الفصل الثامن:- أهم الشهادات في الشبكات اللاسلكية

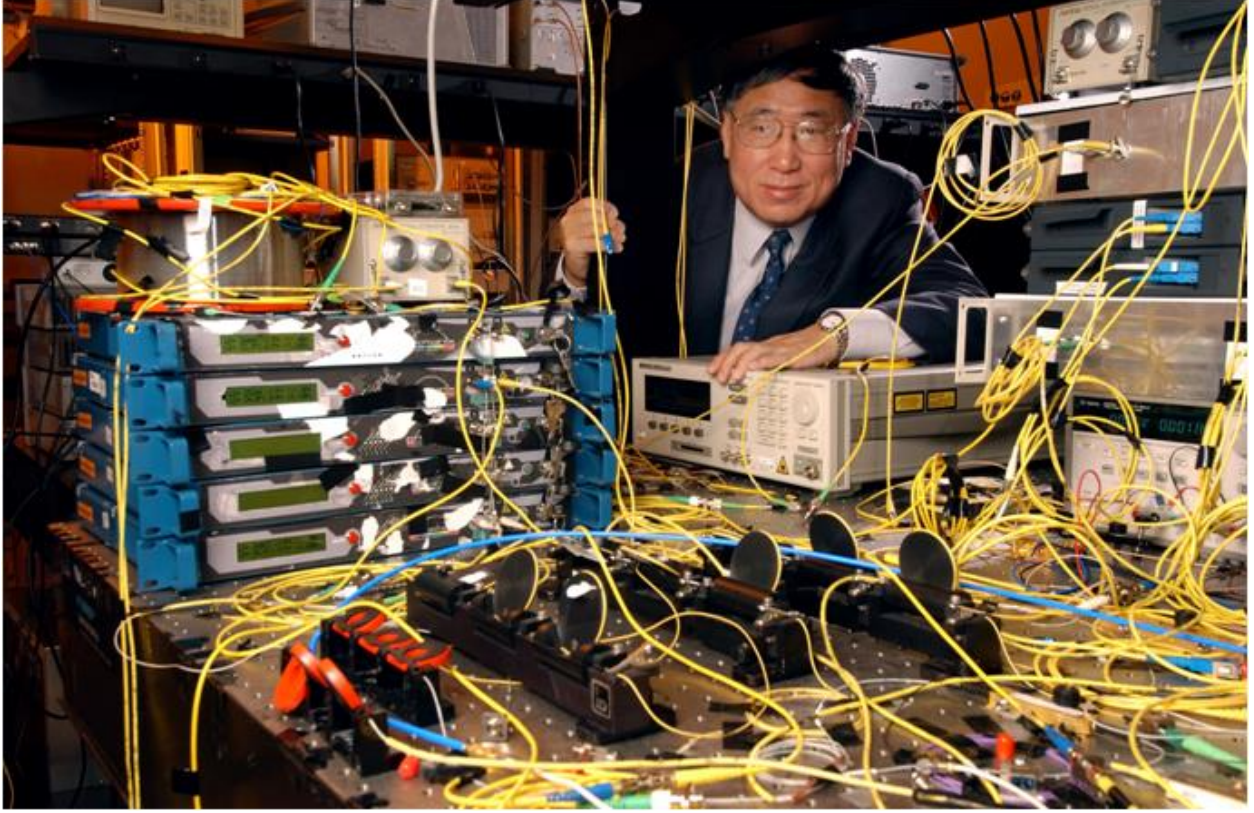
الفصل التاسع :- التطبيقات العملية

الفصل الأول

مقدمة عن الشبكات اللاسلكية :-

تعتبر الشبكات اللاسلكية الشبكة كبديل للشبكة السلكية بحيث توفر طريقة مرنا وبسيطة لنقل البيانات, حيث تقوم هذه الشبكة بث المعلومات عن طريق الموجات الكهرومغناطيسية, وهي بذلك تزيل الحاجة إلى الاتصالات السلكية وهكذا جمعت شبكة الاتصالات اللاسلكية بين توصيل البيانات وسهولة الوصول إلى المستخدم في أي مكان.

حيث هذه التقنية أخذت في الانتشار بسبب السهولة والمرونة في استخدامها, فهي تعطي الحرية المطلقة للشخص, ولا داعي لأن تبقى مقيدا ومرتبطا بنقطة اتصال معينة, أي أنه بإمكان الشخص استخدام جهازه المحمول موصلا بالشبكة بدون وسيط وبجربة كاملة في أي مكان داخل نطاق الشبكة.



بعض مزايا الشبكات اللاسلكية Wireless network :-

بناء شبكات في الأماكن المعزولة التي يصعب توصيلها بالأسلاك .

توفر درجة من الحرية في التنقل لبعض المستخدمين في شبكة سلكية.

عبد السلام صالح الراشدي



توفير اتصالات في الأماكن المزدحمة.

توفير اتصالات مؤقتة لشبكات سلكية في حال فشل هذه الأسلاك بتوفير الاتصال المطلوب لأي سبب كان.

المساعدة في عمل نسخة احتياطية من البيانات على شبكة سلكية إلى جهاز متصل لاسلكيا.

توفير اتصالات للمستخدمين كثيري التنقل.

بعض الأسباب التي ساعدت علي انتشار هذه التقنية:-

التطورات المتلاحقة في التقنيات والمنتجات اللاسلكية.

الانخفاض المتواصل في الأسعار، نظرا للتنافس المتزايد بين المصنعين.

الطلب المتزايد على هذه الشبكات بسبب الحرية الكبيرة التي توفرها للمستخدمين في التنقل دون أن يؤثر ذلك علي عملهم.

عيوب الشبكات اللاسلكية:-

معرضه للاختراق بشكل كبير.

مشاكل مع التداخل في البيانات عندما يكون هناك أكثر من شبكة لاسلكية في مبنى واحد.

سرعات نقل البيانات اقل بكثير من الشبكات السلكية.

لها تأثيرات جانبية على صحة الإنسان.

نظرة تاريخية علي الشبكات الالسلكية :-



علي الرغم من أن الشبكات الالسلكية لم ترى النور إلي في سنة 1990 و لكن الشبكات الالسلكية عرفت قبل هذه التاريخ بكثير, فقد بدأ بزوغ هذه التقنية من قبل فلكي بريطاني يدعى ابظو ويليا رتشل William Herschel في عام 1822 عندما اكتشف طيف أو أشعة غير مرئية للعين المجردة أسفل الطيف المرئي وقد سمي هذا الطيف بالأشعة تحت الحمراء- لأنها ظهرت تحت طيف الأشعة الحمراء, وقد أدا هذا الاكتشاف الي ظهور نظرية الأمواج الكهرومغناطيسية, Wave theory, والذي أثبت أيضا أن الموجات الكهرومغناطيسية تستطيع السير بسرعة تساوي سرعة الضوء .

قبل الخوض في أنواع الشبكات اللاسلكية والتقنيات المستخدمة وطريقة الربط أريد من القارئ أن يفكر معي لحظات فعندما أريد أن أرسل ملف صوتي من جهازي إلي جهاز زميلي فإن زميلي يستقبل هذا الملف في لحظات أو دقائق معدودة بالرغم إنا جهازي وجهاز زميلي ليس هناك أي اتصال سلكي بينهم فكيف تم هذا الاتصال أيضا عندما أريد أن اتصل بتليفون بشخص موجود في مكان بعيد فإنه يسمع صوتي وأنا أسمع صوته في لحظات وأيضا وأيضا وكثيرا من الأسئلة التي ربما تسال عنها ولا تجد لها أجابه لهذا أحببت إن يكون للقارئ الحق بان يعرف كل صغيره وكبيره علي كيفية الاتصال و نقل البيانات في الهواء بشكل أكثر تفصيلا حتى تكون الصورة أكثر وضوح فعندما يسمع كلمة تردد أو موجه أو bandwidth أو قناة فيعرف ما هي هذه الكلمات وعلي ماذا تدل كيف ما نقولوا نحنا باليبي يعرف الفول ومن زرعه سوف أقوم بسرد الفول أسف قصدي المصطلحات ذات العلاقة أولا بأول

تنتقل البيانات عبر الشبكات اللاسلكية عن طريق الموجات الكهرومغناطيسية بحيث تنتشر هذه الأمواج في الطيف المغناطيسية عن طريق ترددات وقنوات مختلفة حيث كل تردد وقناة لها صفات محددة ولوصول هذه الإشارات بشكل سريع فيجب علينا ترميز هذا الإشارات .

هناك أربع تقنيات أساسية تستخدم في إرسال البيانات في الشبكات اللاسلكية المحلية:-

1 . موجات الراديو أحادية التردد وتسمى أحياناً Radio Single-Frequency

2 . موجات الراديو عالية التردد ضيقة النطاق Narrow-Band High-Frequency Radio

3 . موجات راديو الطيف الانتشاري Spread-Spectrum Radio

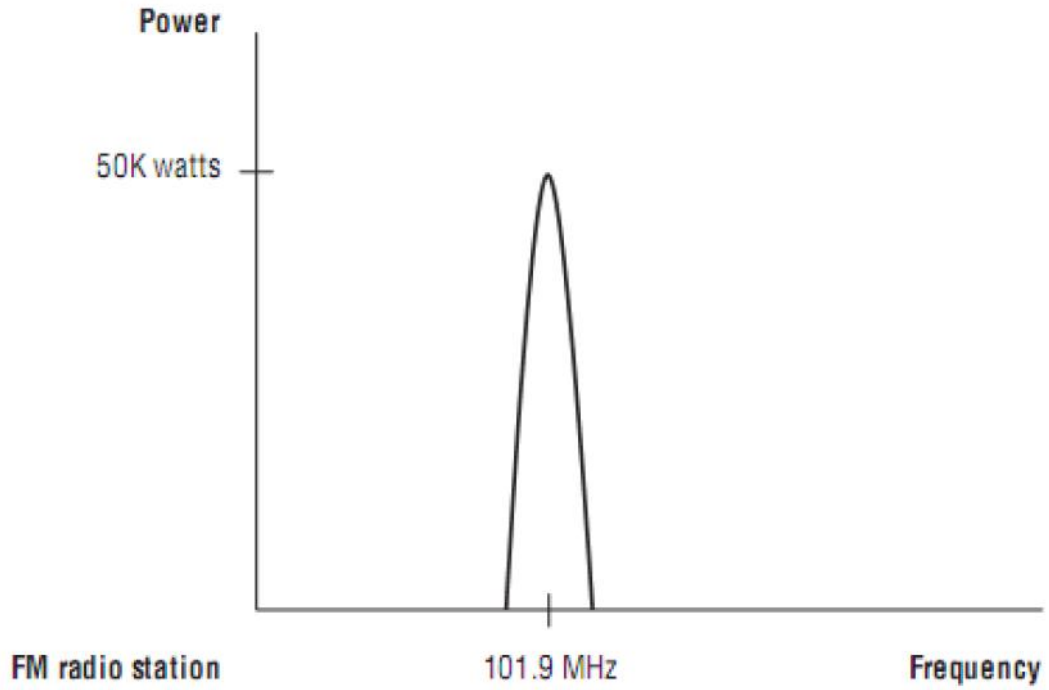
4 . موجات الأشعة تحت الحمراء Infrared

هنا سوف نتكلم علي أهم اثنين من هذه التقنيات والأكثر استخداماً الأولى:-

Narrow Band تستخدم هذه التقنية طاقة إرسال عالية تصل لعشرات آلاف من وحدات القدرة

"الوات" لإرسال ضيق من الطيف الكهرومغناطيسي يستطيع أن يصل بالإشارة إلى مئات الكيلومترات وذلك

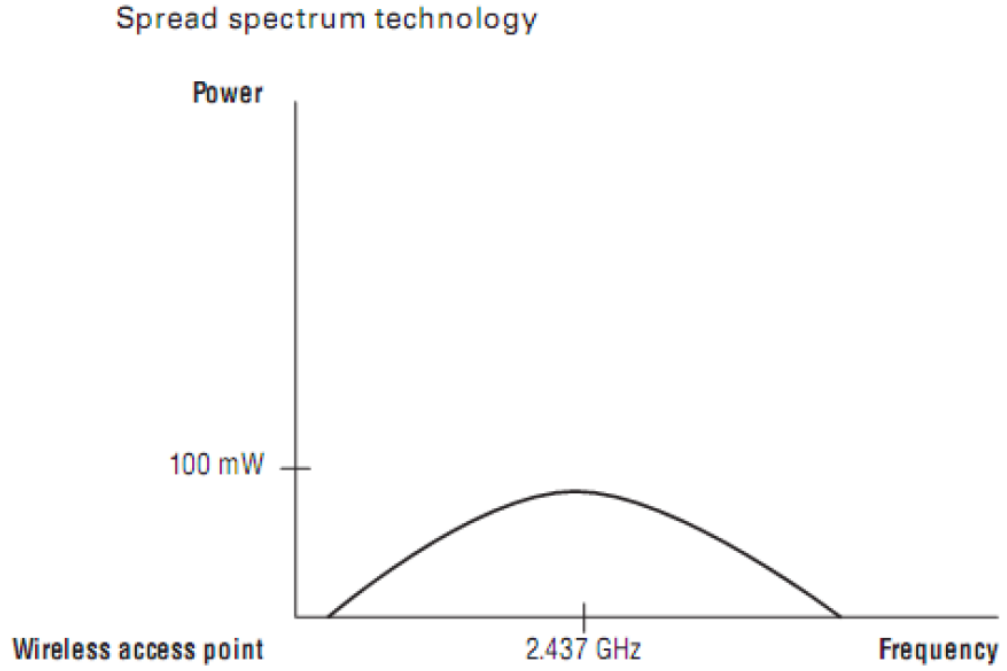
يستخدم محطات الإذاعة والتلفاز وغيري وتستخدم ترددات مرخصة مجوز مسبقاً



إما Spread Spectrum فإنه يعمل علي تردد 2.4 جيجا هرتز من الترددات غير المرخص ISM ويختص بالإشارات الرقمية ولقد تم اختراعها في سنة 1942 بواسطة الممثلة هدي Lamarr والموسيقار جورج Antheil وحصل علي براءة اختراع لاكتشافهم هذا وتم استخدامها علي نطاق واسع في التطبيقات العسكرية حتى جاء عام 1980 وقامت مؤسسة FCC المسؤولة عن الاتصالات في الولايات المتحدة ودعم هذه التقنية ثم بدأ الانتشار الحقيقي بهذه التقنية مع بزوغ عصر تكنولوجيا المعلومات والاتصالات وانتشار

شبكات WLAN و WPAN GPS

ويعمل spread spectrum بواسطة تقسيم الإشارة و ترميز أو تعليم كل منها ثم إرسالها علي كامل تردد القناة المستخدمة وبهذا تستطيع إن تنقل أكثر من إشارة في وقت واحد وهذا التقنية سوف تكلم عليها بتوسع في الفصل الثالث.



أي إنا بشكل عام يعمل الاتصال بموجات الراديو في شبكات الحاسب بشكل مشابه لما هو عليه في شبكات الإذاعة، فالجهاز المرسل يقوم بإرسال إشاراته باستخدام تردد معين ويقوم الجهاز المستقبل بضبط تردده ليتوافق مع تردد الجهاز المرسل لكي يتمكن من استقبال الإشارات. الاختلاف

الوحيد بين شبكات حاسب الراديو وشبكات الإذاعة هو أن الشبكات بموجات الراديو تقوم بإرسال

البيانات وليس الرسائل الصوتية.

الفصل الثاني

بعض المفاهيم المهمة في الشبكات اللاسلكية

تستخدم الاتصالات اللاسلكية الأمواج الكهرومغناطيسية لإرسال الإشارات إلى مسافات بعيدة ولكن كيف ستمكن من تحديد وجهة الأمواج المرسله من بطاقة الشبكة اللاسلكية الخاصة بك؟ ما الذي سيحدث عند انعكاس هذه الأمواج على الأشياء الموزعة ضمن الغرفة أو على المباني المحيطة بمسار الوصلة الخارجية؟ هل يمكنك استخدام عدة بطاقات للشبكة اللاسلكية دون أن تشوش على بعضها البعض؟

ولكي تفهم هذه الأسئلة فيجب عليك أن تعرف الأتي:-

الموجه الكهرومغناطيسية

لتوضيح ما هي الموجه قوم على سبيل المثال بإطلاق تذبذبات من الحبال الصوتية في حنجرتة والتي تسبب بدورها في تغيير ضغط الهواء في فمه. هذه التغيرات الدورية في ضغط الهواء تغادر فم المغني وتنتشر في

الفضاء الطلق بسرعة الصوت. أما يتسبب الحجر المرمي في بحيرة بإحداث اضطراب ينتشر عبر هذه البحيرة على شكل موجة.

أي بمعنى آخر يوجد تشابه كبير بين الموجات الكهرومغناطيسية و موجات البحار والمحيطات ولكن الفرق بين هذه الموجات هو أن موجات البحر تحمل في داخلها مياه والموجات الكهرومغناطيسية تحمل في داخل بيانات.

تمتلك الموجة سرعة معينة بالإضافة إلى تردد وطول موجة محددين .

سترتبط هذه الخواص ببعضها البعض وفق المعادلة التالية:-

$$\text{السرعة} = \text{التردد} \times \text{طول الموجة}$$

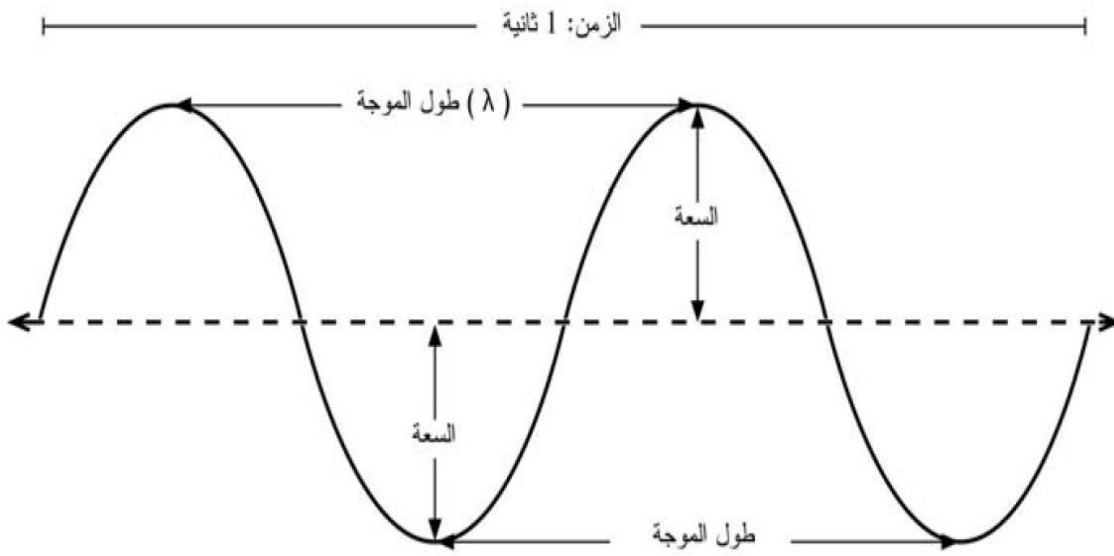
يمثل طول الموج المسافة بين نقطة معينة والجزء المكافئ لهذه النقطة في الموجة التي تليها، مثل المسافة بين أعلى

قمتي موجتين متاليتين. أما التردد فهو عدد الأمواج الكاملة التي تمرر خلال نقطة معينة في واحدة المسمى

Hertz الزمن .

تقاس السرعة بوحدة (متر/الثانية) والتردد بال(دورة/الثانية) أو الهرتز في حين يقاس طول الموجة بالأمتار) .

تمتلك الأمواج أيضاً خاصية أخرى تدعى السعة Amplitude وهي المسافة بين مركز الموجة وأبعد نقطة من إحدى قمتيها، والتي يمكن النظر إليها على أنها ارتفاع الموجة المائية على سبيل المثال التالي يوضح العلاقة بين التردد، طول الموجة والارتفاع.

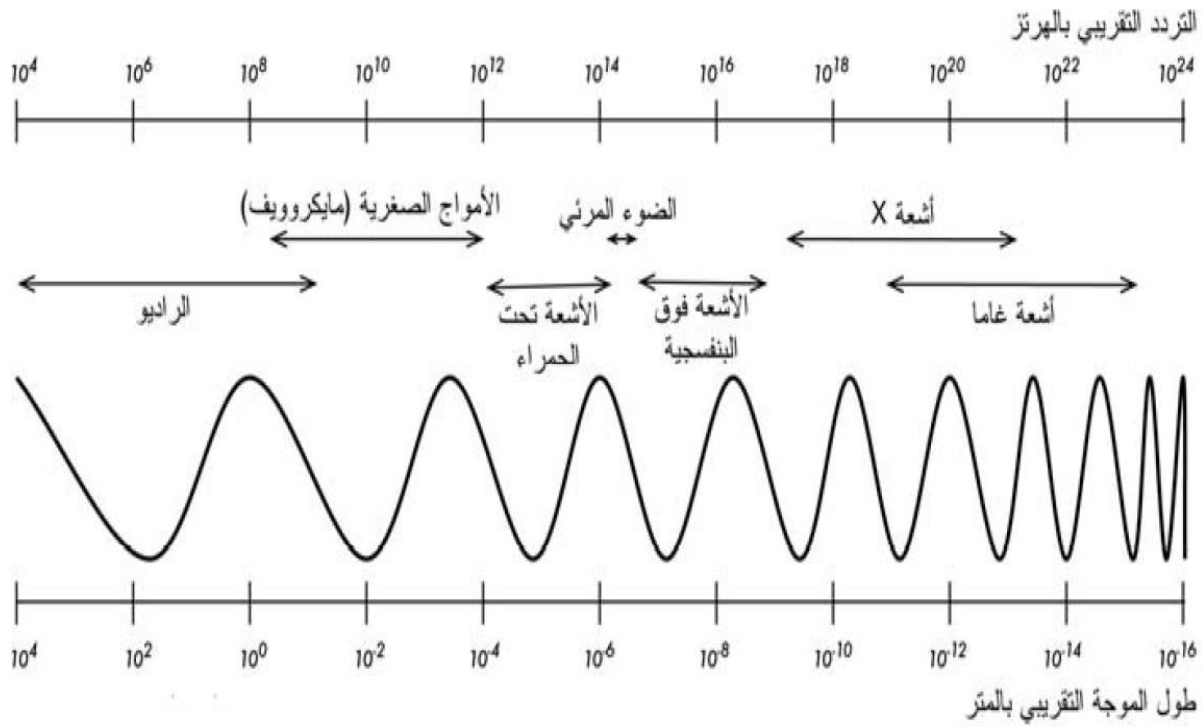


التردادات

يخطر الإرسال الإذاعي (FM) إلى البال والذي يستخدم تردداً يعادل 100 ميغاهرتز تقريباً على الفور عند الحديث عن الراديو. تسمى المنطقة الواقعة بين الراديو والأشعة تحت الحمراء والتي تتراوح تردداتها بين 1 وحتى 300 غيغاهرتز، بالأمواج الصغيرة (Microwave) وتتراوح أطوال الموجة المكافئة لها بين 30 سنتيمتراً حتى 1 ميليمتر.

يعتبر فرن الأمواج الصغيرة Microwave Oven أكثر استخدامات الأمواج الصغيرة شيوعاً، وهو يعمل ضمن نفس مجال ترددات معايير الشبكة اللاسلكية التي سنتعامل معها. يقع هذا المجال ضمن الحزم التي تركت مفتوحة للإستخدامات العامة دون الحاجة إلى الحصول علي ترخيص وهذا المدى الترددات هي التي سوف نركز علي في هذه الكتاب إن شاء الله.

تقوم ISM band على ترخيص، وهي تدعى حزمة التطبيقات الصناعية، العلمية والطبية بحث تقوم الحكومات عادة بتطبيق قوانين صارمة على غالبية الأجزاء المتبقية من الطيف الكهرومغناطيسية والتي قد يكلف الحصول على ترخيص للعمل ضمنها مبالغ طائلة، لا سيما تلك المستخدمة لأغراض البث الإذاعي والتلفزيوني إضافة إلى الاتصالات الصوتية واتصالات نقل البيانات. على الرغم من ذلك فإن غالبية الدول تتيح استخدام حزم التطبيقات الصناعية، العلمية دون الحاجة إلى ترخيص.



جدول تقسيم الترددات اللاسلكية، طبقاً لتقنيات استخدامها

التطبيقات	المدى الترددي	اسم الحيز
الاتصالات الإستراتيجية بالغواصات، في أعماق المياه الدولية، وفي سرعة التحرك الطبيعية	3-300 هرتز	ELF التردد المتناهي الانخفاض
تردد الصوت المسموع الطبيعي	300-3000 هرتز	VF الترددات الصوتية
اتصالات البحرية الإستراتيجية	3-30 كيلوهرتز	VLF الترددات المنخفضة جداً
اتصالات البحرية الإستراتيجية، الملاحة	30-300 كيلوهرتز	LF الترددات المنخفضة
الملاحة- الإذاعة بتعديل التردد	300-3000 كيلوهرتز	MF الترددات المتوسطة
إذاعة الموجات القصيرة، لاسلكي الهواء، رادار خلف الأفق	3-30 ميجاهرتز	HF الترددات العالية
الإذاعة بتعديل التردد، الإرسال التلفزيوني، اتصالات الشرطة، أجهزة اللاسلكي المحمولة في العربات أو الطائرات، الرادارات، شبكات اللاسلكي	30-300 ميجاهرتز	VHF الترددات العالية جداً
اتصالات الأقمار الصناعية، نظام تحديد المواقع العالمي، الهاتف الخليوي، الإرسال التلفزيوني، الرادار، الملاحة	300-3000 ميجاهرتز	UHF التردد فوق العالية
اتصالات الأقمار الصناعية، الإذاعة من خلال الأقمار الصناعية، الرادار، وصلات نقل المعلومات	3-30 جيجاهرتز	SHF الترددات فائقة الارتفاع
اتصالات الأقمار الصناعية، الرادارات المليمترية	30-300 جيجاهرتز	EHF الترددات المتناهية الارتفاع

الطيف الكهرومغناطيسية

تنتشر الأمواج الكهرومغناطيسية ضمن مجال واسع من الترددات حيث تنتشر هذا التردد في الهواء الجوي

ضمن عدة ترددات مختلفة هذا بالطيف الكهرومغناطيسي يعتبر الضوء أكثر الأجزاء المألوفة من هذا

الطيف بالنسبة للإنسان، وهو يشكل الجزء المرئي سينصب اهتمامنا في هذا الكتاب على الترددات الواقعة

ضمن المجال 2.412-2.484 غيغاهرتز والمستخدم في معايير الشبكات اللاسلكية المكافئة 802.11b ،

802.11g وطول موجة يعادل 12.5 سنتيمتراً تقريباً. (تعمل بعض التجهيزات المتوفرة في الأسواق أيضاً ضمن

مجال (5.805-5.1706 غيغاهرتز) والمكافئ لطول موجة يعادل تقريباً 5 سنتيمتراً ومن امثلة 802.11a .

بعض العوائق التي تؤثر في المسار الموجات



عبد السلام صالح الراشدي

الإمتصاص absorption

تضعف الأمواج الكهرومغناطيسية أو تتخامد بشكل عام عند اختراقها لشيء ما (مادة ما). يعتمد مقدار القدرة المفقودة على تردد هذه الأمواج وطبيعة المادة المخترقة. ففي حين يعتبر الزجاج النوافذ شفافاً بالنسبة للضوء فإن الزجاج المستخدم في النظارات الشمسية يجب قسطاً؛ كبيرة من كثافة الضوء بالإضافة إلى الإشعاع فوق البنفسجي.

تعتبر المادتين التاليتين أكثر المواد امتصاصاً للأمواج الصغيرة (المايكروبي):-

المعادن:- يمكن للإلكترونات أن تتحرك بحرية ضمن المعادن، وبالتالي تستطيع الاهتزاز وامتصاص قدرة الأمواج العابرة.

الماء:- تتسبب الأمواج الصغيرة في تزاخم جزيئات الماء حولها مما يتسبب في امتصاص طاقة هذه الأمواج

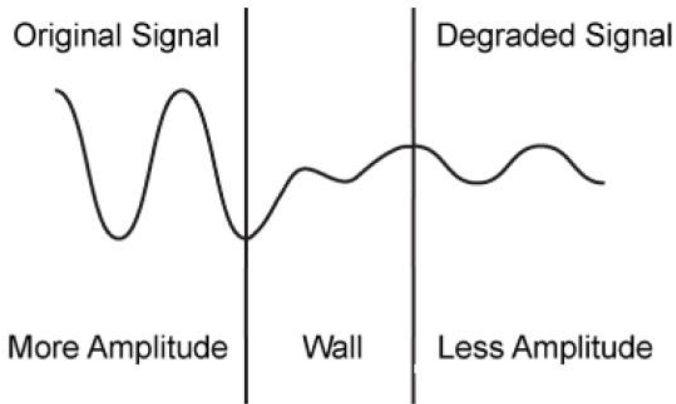
يمكننا في مجال الشبكات اللاسلكية اعتبار المعادن والماء مواد ماصة مثالية، أي أننا لن نتمكن من اختراق

هذه المواد مع أن الطبقات الرقيقة من الماء قد تسمح بمرور بعض القدرة منها. يتوجب علينا الانتباه أثناء

الحديث عن الماء إلى وجود عدة أشكال محتملة: مطر، ضباب ورطوبة، غيوم منخفضة وما إلى ذلك.

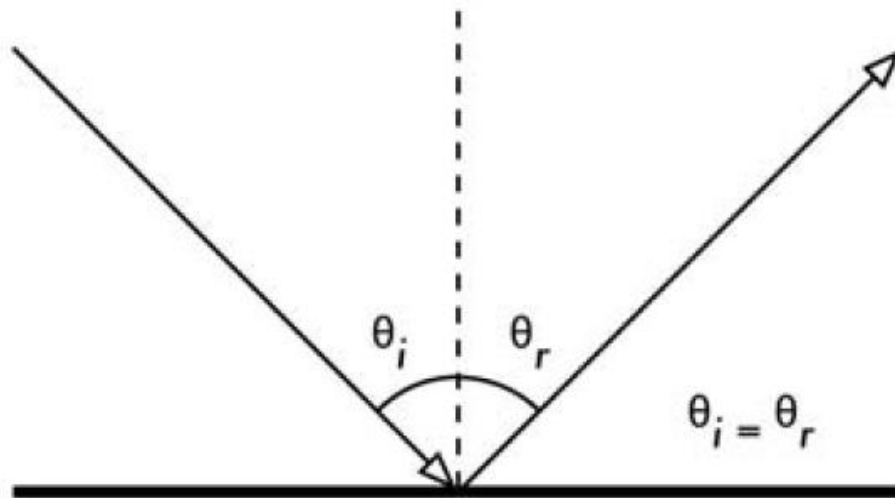
لتحدث أخيراً عن أنفسنا, تتشكل الماء غالبية جسم الإنسان بالإضافة إلى الكائنات الحية الأخرى (من أي أننا قد نعتبر بالنسبة الشبكات اللاسلكية كتلة كبيرة من الماء تسبب في الكثير من الامتصاص . من الأخطاء الشائعة لدينا عندما تركيب نقاط الولوج في المكاتب، مقاهي الإنترنت، المكتبات والمناطق المأهولة تثبيتها بشكل تجبر معه الإشارة اللاسلكية على اختراق الكثير من الناس.

Absorption

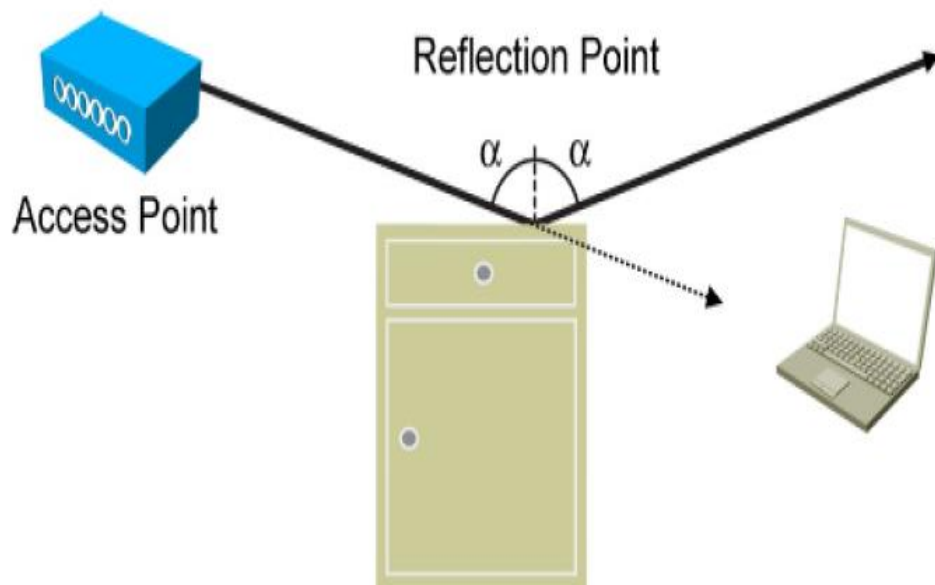


الانعكاس reflection

تنعكس الأمواج اللاسلكية تماماً كالضوء المرئي عند التقائها بمواد ذات خواص معينة: تعتبر الأسطح المائية والمعدنية من أكثر المواد العاكسة للأمواج اللاسلكية . يتم الانعكاس وفق قاعدة بسيطة للغاية، حيث تتساوى زاوية ورود الموجة إلى السطح العاكس مع زاوية انعكاسها عنه.



Reflection



التشويش

عند التعامل مع الأمواج فإن واحد + واحد قد لا تساوي اثنين، بل قد تساوي صفراً أيضاً! في مجال الشبكات

اللاسلكية بمعناه الأشمل للتعبير Interference يستخدم مصطلح التشويش عن الاضطرابات الناتجة عن

المصادر الخارجية للإشارات اللاسلكية القنوات المجاورة مثلاً. (أي أن الحديث عن التشويش في الشبكات

اللاسلكية يعني جميع الاضطرابات الناتجة عن الشبكات الأخرى وغيرها من مصادر الأمواج الصغيرة. ويعتبر

التشويش من أهم العقبات التي تواجه بناء الوصلات اللاسلكية، لا سيما في المناطق الحضرية المكثفة أو

المساحات المغلقة.

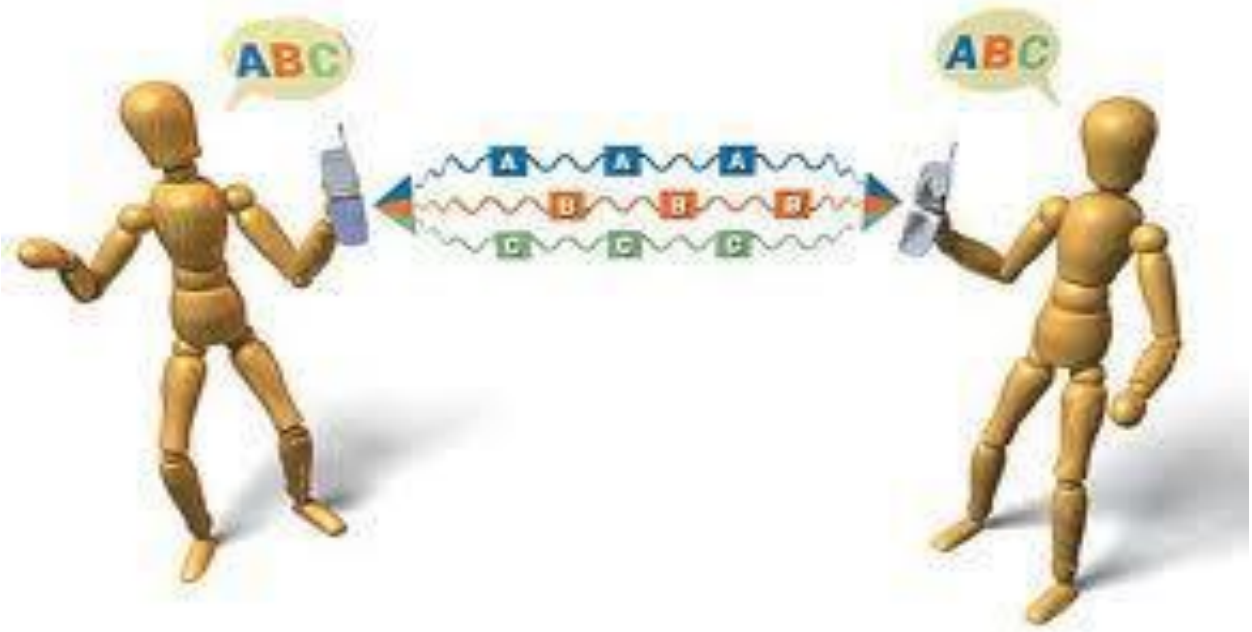


الفصل الثالث

الترميز modulation

تقنيات الترميز

يعتبر اختيار تقنية الترميز من العوامل الهامة التي تؤثر بشكل كبير على نقل البيانات ضمن معيار محدد . كلما كانت البيانات مزمنة بفاعلية أكثر كلما ازدادت سرعة نقل البيانات التي يمكن تحقيقها . من جهة أخرى فإن استخدام تقنية ترميز فعالة يتطلب تجهيزات متطورة قادرة على ترميز وفك ترميز البيانات . تعتمد تقنيات الترميز المختلفة المستخدمة في معايير IEEE 802.11 على فكرة بسيطة للغاية تهدف إلى استخدام أكبر عرض للحزمة يلزم نظرياً لإرسال "بت" واحد من البيانات للتغلب على التشويش . تقود الأساليب المختلفة لنشر البيانات ضمن الحزمة الراديوية إلى تقنيات الترميز المختلفة . سنين فيما يلي أكثر هذه التقنيات شيوعاً:-



الطيف الموزع عبر تغيير التردد FHSS

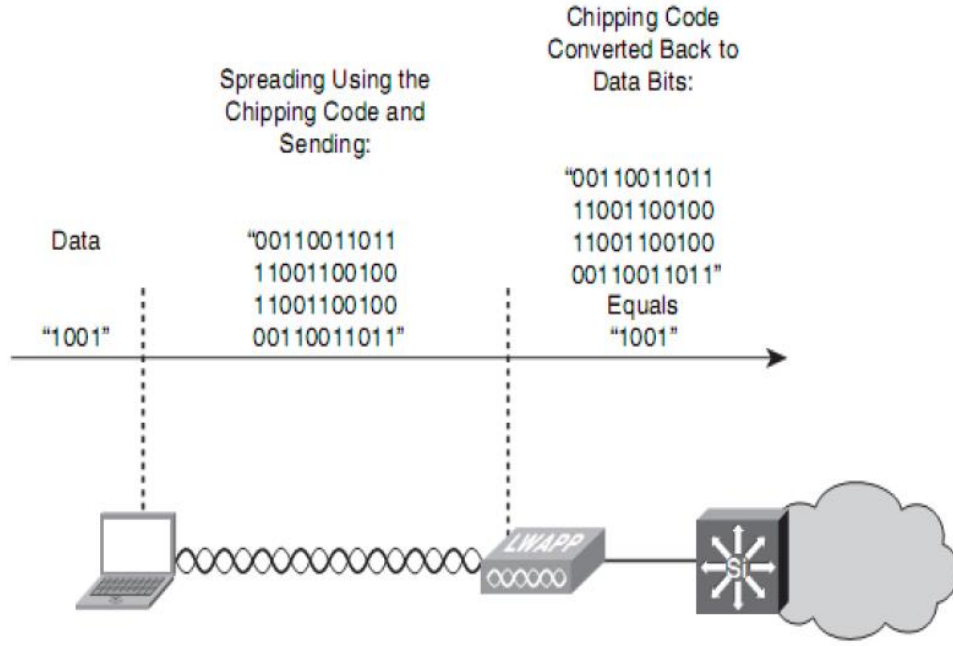
تعتمد تقنية FHSS على مبدأ الإرسال ضمن تردد واحد لمدة معينة، ومن ثم الانتقال بشكل عشوائي إلى تردد آخر، أي أن التردد الحامل للإشارة (الحامل) سيتغير مع الزمن أو أن المرسل سيقوم بتغيير التردد دورياً تبعاً لتسلسل محدد بشكل مسبق. يحقق المرسل التزامن مع المستقبل بفضل مرشحات تحتوي تسلسل الانتقالات وزمنها. تقسم حزمة الترددات المحددة في معايير IEEE 802.11 (ISM) والتي تمتد من 2.400 وحتى 2.4835 ميغاهرتز إلى 79 قناة عرض كل منها 1 ميغاهرتز ويتم التنقل بين الترددات كل

300 إلى 400 ميللي ثانية. يتم التنقل بقفزاتٍ حول ترددٍ مركزيٍّ لإحدى القنوات الـ 14 المحددة مسبقاً. لم يعد هذا الترميز مستخدماً في المنتجات الحالية.

الطيف الموزع عبر التتابع المباشر DSS Direct Sequence Systems

تتطلب تقنية DSS إرسال سلسلةٍ من البتات bits (والتي تدعى أحياناً بالضجيج ذي العشوائية الزائفة pseudo-random noise ويرمز لها اختصاراً بـ PN) في مقابل كل بت من البيانات. يتم استبدال كل بتٍ يحمل القيمة 1 بسلسلةٍ محددةٍ من البتات في حين يستبدل كل بتٍ يحمل القيمة 0 بسلسلةٍ متممةٍ. تحدد مواصفات الطبقة الفيزيائية لمعايير 802.11 سلسلةً من 11 بتاً (10110111000) لتمثيل الرقم 1 والسلسلة المتممة (01001000111) لتمثيل الرقم 0. يقوم ترميز DSS عوضاً عن تقسيم إشارة البيانات إلى أجزاء. يتم إرسالها عبر تردداتٍ مختلفةٍ بترميز كل بتٍ من البيانات ضمن رتلٍ أطول من البتات يدعى "رقاقة".

إتشر استخدام هذه التقنية على نطاقٍ واسعٍ بين الأعوام 1999 إلى 2005.



ترميز تقسيم التردد المتعامد OFDM Orthogonal frequency-division multiplexing

ويدعى أحياناً ترميز الطبقات المتعددة غير المترابط (Discrete Multi-Tone Modulation (DMT). وهي

تقنية ترميز تعتمد على فكرة الترميز المبني على تقسيم التردد Frequency Division Multiplexing

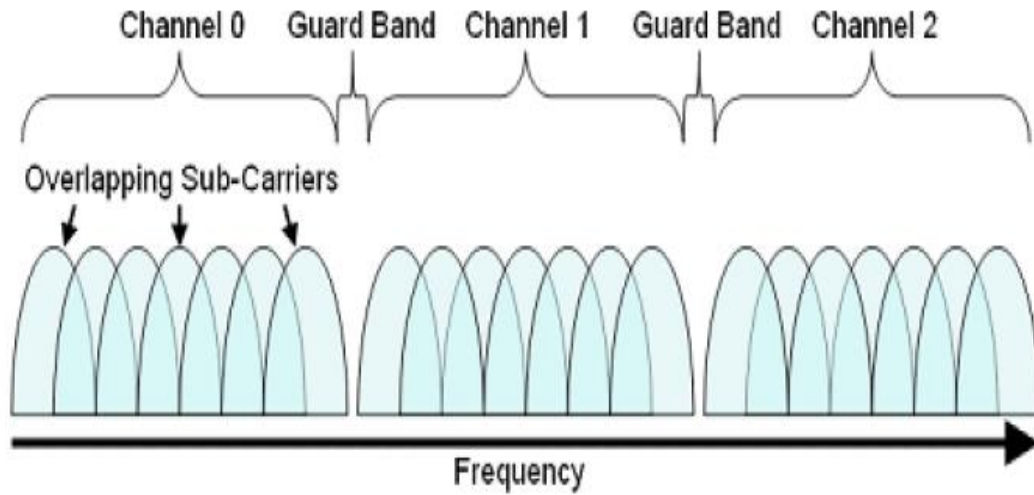
(FDM).

يعتمد ترميز FDM (والمستخدم في الراديو والتلفزيون) على مبدأ إرسال إشاراتٍ متعددةٍ في نفس الوقت

لكن عبر تردداتٍ مختلفةٍ. في ترميز OFDM يقوم مرسل واحد بالإرسال عبر عدة (عشراتٍ وحتى

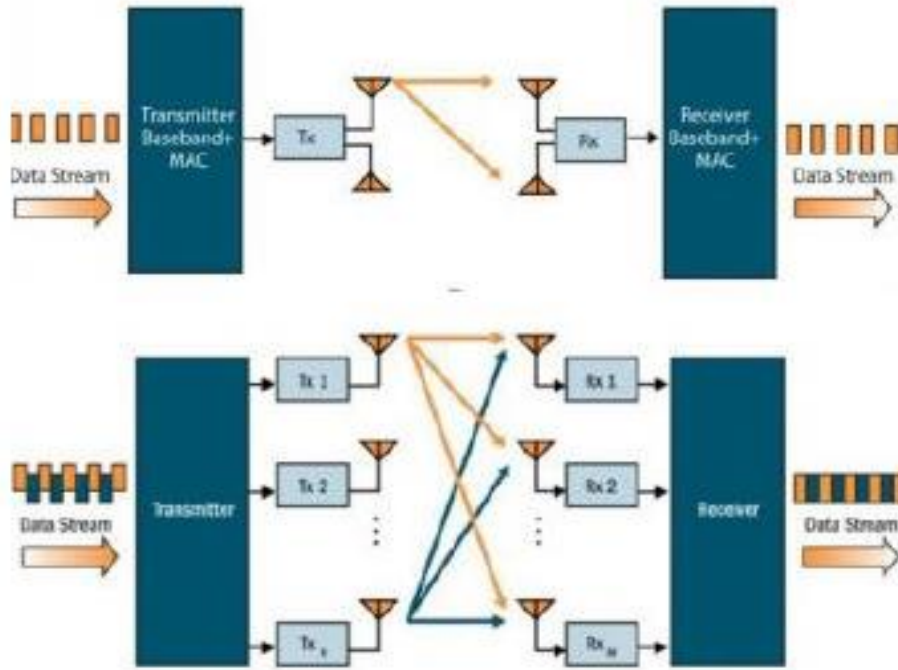
آلاف) الترددات المتعامدة المختلفة. الترددات المتعامدة هي ترددات مستقلة من جهة روابط الطور

النسبي بين هذه الترددات . يستخدم ترميز OFDM تقنيات ترميز متطورة في جميع مكوناته لإنتاج إشارات تتمتع بمناعة عالية ضد التشويش .



MIMO Multiple Input/Multiple Output

أحدي التقنيات التي يتم فيها استخدام أكثر من مستقبل ومرسل في نفس الجهاز وقد مكنت هذه التكنولوجيا الجديدة علوم الاتصالات خاصة الأجيال الحديثة لشبكات الجوال وشبكات الوايرلس WIFI IEEE 802.11n من زيادة تدفق البيانات عبر تمكين أكثر من مستخدم للإرسال والاستقبال في نفس الوقت عبر محطة عمل واحدة التي قد تكون Access Point في الشبكات اللاسلكية أو Base station في شبكات الموبايل ليس هذا فقط بل ساعدت هذه التقنية شبكات الواي ماكس علي الانتشار حيث أنها ركيزة أساسية لهذا النظام الشبكي والذي يجمع بين خصائص شبكات الواي فاي كجهة تقدم خدمات انترنت وشبكات الموبايل الخلية التي تقدم الخدمة عبر محطات وأبراج لاسلكية تغطي المدن .



الفصل الرابع

IEEE ومجموعات العمل التابعة له:-

يعتبر المعهد الدولي لمهندسي الكهرباء والإلكترون IEEE وهو منظمة دولية لا تهدف للربح - المطور الأساسي للمعايير الدولية، وعلى وجه الخصوص تلك المتعلقة بالاتصالات، تقنية المعلومات وتوليد الطاقة الكهربائية. يملك المعهد مجموعة من 900 معياراً قيد الاستخدام و 400 أخرى قيد التطوير.

من أكثر معايير IEEE شيوعاً مجموعة معايير IEEE 802 LAN/WAN والتي تتضمن معيار شبكات الإنترنت (IEEE 802.3) ومعيار الشبكات اللاسلكية (IEEE 802.11).

معايير IEEE 802 لشبكات المناطق المحلية والحضرية

تشير عائلة معايير IEEE 802 إلى شبكات المناطق المحلية (LAN) وشبكات المناطق الحضرية (MAN). ينحصر تعريف معايير IEEE 802 بالشبكات التي تنقل حزم البيانات متفاوتة الأحجام (مقارنةً بالشبكات التي تنقل البيانات ضمن وحداتٍ قصيرة ذات حجمٍ موحدٍ تدعى بالخلايا cells).

من هذه الأجزاء معيار IEEE 802.11 للشبكات اللاسلكية ومعيار IEEE 802.16 للشبكات اللاسلكية السريعة.

تاريخ المعيار الشبكات اللاسلكية IEEE 802.11

يمكن توصيف معيار IEEE 802.11 ببساطة بأنه معيار شبكات الإيثرنت اللاسلكية.

لقد حدد المعيار الأصلي IEEE 802.11 الذي أطلق في العام 1997 بروتوكول الوصول إلى الحامل بتحسس الناقل مع تجنب التصادم CSMA/CA كآلية الوصول إلى الحامل، تماماً كما هو الحال في شبكات الإيثرنت. تعتمد جميع تعديلات المعيار IEEE 802.11 على نفس آلية الوصول. إلا أن فاعلية بروتوكول CSMA/CA ضعيفة جداً نتيجة تضحيته بقسط كبير من عرض الحزمة في سبيل ضمان وثوقية إرسال البيانات. تتواجد هذه المحدودية في جميع التقنيات المعتمدة على بروتوكول CSMA/CA.

يحدد معيار IEEE 802.11 أيضاً سرعتين أساسيتين لنقل البيانات: 1 و 2 ميغابت في الثانية للإرسال عبر الأشعة تحت الحمراء (IR) أو الأمواج الراديوية العاملة بتردد 2.4 غيغاهرتز. على الرغم من

عدم وجود أي تطبيق عملي حتى الآن للإرسال عبر الأشعة تحت الحمراء، إلا أنها مازالت جزءاً من المعيار الأصلي.

ظهرت في الأسواق عدة منتجات صممت وفقاً للمواصفات الأصلية لمعيار IEEE 802.11 لكنها سرعان ما استبدلت بمنتجات متوافقة مع معيار IEEE 802.11b بعد إقرار التعديل b على المعيار الأساسي في العام 1999.

الجوانب التقنية لمعايير IEEE 802.11

ينبغي معيار IEEE 802.11 كما هو الحال في جميع معايير IEEE 802 – الطبقتين الأولى والثانية من نموذج OSI المعياري (Open Systems Interconnection) وهي الطبقة الفيزيائية (L1) وطبقة وصلة البيانات (L2). تبين الفقرة التالية مقتضيات هاتين الطبقتين في سياق الشبكات اللاسلكية.

الطبقة الأولى (802.11 PHY)

تضطلع الطبقة الفيزيائية بمهمة نقل الإشارات المتعلقة بالأصفر 0 والواحدات 1 للبيانات التي يرغب

المرسل بإرسالها إلى المستقبل بشكل صحيح.

عبد السلام صالح الراشدي

تتعامل الطبقة الفيزيائية بشكل رئيس مع: ترميز البيانات

تعديلات معايير IEEE 802.11

تعتبر التعديلات a، b، و g (والتي قد حققت إنتشاراً واسعاً في السوق بفضل منتجات متوافقة ذات أسعار معقولة) أكثر التعديلات شيوعاً ضمن عائلة معايير 802.11. من التعديلات الأخرى ضمن نفس العائلة و n وهي عبارة عن تحسينات وتطويرات أو تصحيحات لمواصفات سابقة ضمن هذه العائلة. سنلقي فيما يلي نظرة على التعديلات a, b, g, n.

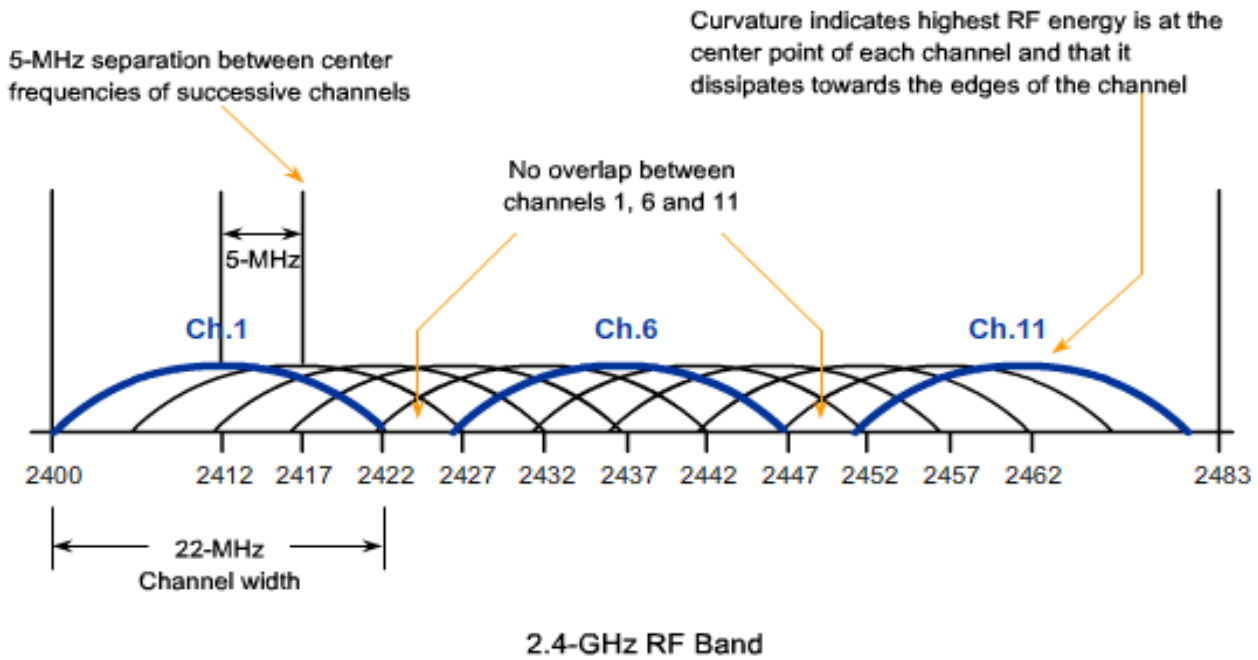
IEEE 802.11b

يتضمن معيار IEEE 802.11b تحسيناتٍ عن المعيار الأصلي 802.11 لدعم نقل البيانات بسرعاتٍ أكبر (5.5 و 11 ميغابت في الثانية). يستخدم هذا المعيار نفس أسلوب الوصول إلى الناقل المحدد في المعيار الأصلي 802.11.

يستخدم معيار IEEE 802.11b تقنية الطيف الموزع عبر التتابع المباشر DSSS والمحددة أيضاً في المعيار الأصلي.

عبد السلام صالح الراشدي

يمكن لأي بطاقة للشبكة اللاسلكية متوافقة مع معيار 802.11b نظرياً أن تنقل البيانات بسرعة 11 ميغابت في الثانية، إلا أنها ستقوم بتخفيض هذه السرعة (وفق مقياس الإختيار المتكيف لسرعة نقل البيانات) إلى 5.5 ثم 2 ومن ثم إلى 1 ميغابت في الثانية في حال حدوث أي ضياع في حزم البيانات. تعتبر السرعات الدنيا لنقل البيانات أقل حساسية للتشويش والتلاشي لأنها تستخدم أسلوباً أكثر وثوقية لترميز البيانات (أي أن العلاقة بين الإشارة والضجيج تصبح أفضل في السرعات الدنيا).



802.11b / g			
التردد المركزي (غيغاهرتز GHz)	رقم القناة	التردد المركزي (غيغاهرتز GHz)	رقم القناة
2.447	8	2.412	1
2.452	9	2.417	2
2.457	10	2.422	3
2.462	11	2.427	4
2.467	12	2.432	5
2.472	13	2.437	6
2.484	14	2.442	7

IEEE 802.11a

يستخدم هذا المعيار (تماماً كما هي الحال في معيار IEEE 802.11b) نفس البروتوكول الأساسي المحدد في المعيار الأصلي. يعمل معيار IEEE 802.11a ضمن حزمة التردد 5 غيغاهرتز ويستخدم تقنية ترميز تقسيم التردد المتعامد OFDM مما يعطيه القدرة على بلوغ سرعة قصوى لنقل البيانات تعادل 54 ميغابت في الثانية. يمكن تخفيض هذه السرعة باستخدام الإختيار المتكيف لسرعة نقل البيانات إلى 48، 36، 24، 18، 12، 9 و 6 ميغابت في الثانية إذا ما اقتضت الحاجة.

لم يبلغ معيار IEEE 802.11a حتى يومنا هذا الإنتشار الواسع الذي حققه نظيره IEEE 802.11b . من معوقات استخدام هذا المعيار: تواجد المعيار السابق IEEE 802.11b على نطاقٍ واسعٍ، ضعف المنتجات الأولية التي صممت وفقاً لهذا المعيار والقوانين الأكثر صرامةً في حزمة الترددات 5 غيغاهرتز.

IEEE 802.11g

لقد تم اعتماد التعديل الثالث لمعيار 802.11 في حزيران من عام 2003 وأُعطي الإسم IEEE 802.11g . يعمل هذا المعيار (شأنه شأن نظيره IEEE 802.11b) ضمن حزمة الترددات 2.4 غيغاهرتز. يستخدم معيار 802.11g نفس تقنية الترميز المعتمدة في معيار 802.11a (OFDM) مما يمكنه من بلوغ سرعةٍ قصوى لنقل البيانات تصل حتى 54 ميغابت في الثانية. لضمان التوافقية مع المنتجات العاملة وفق معيار 802.11b فإن هذا المعيار يعود إلى استخدام تقنيات الترميز CCK+DSSS (مثل تلك المستخدمة في 802.11b) عند سرعات نقل البيانات 11 و 5.5 ميغابت في الثانية في حين يستخدم ترميز DBPSK/DQPSK+DSSS عند سرعات 1 و 2 ميغابت في الثانية.

يعود الفضل إلى القبول الواسع الذي حظي به معيار IEEE 802.11g بالدرجة الأولى إلى توافقيته مع
التجهيزات العاملة وفق معيار 802.11b. يعاني هذا المعيار من نفس مشكلة سابقه 802.11b فيما يتعلق
بالتشويش (المواقع الحضرية المزدهمة) وذلك نتيجة استخدامه لنفس حزمة الترددات.

IEEE 802.11n

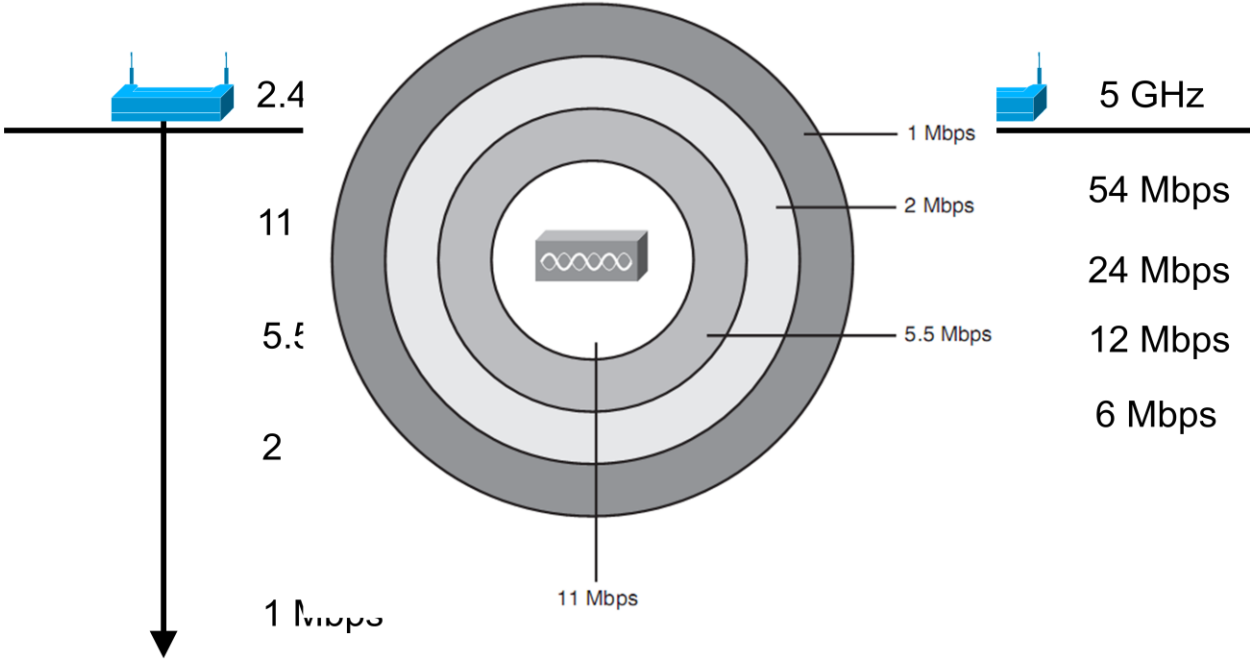
يهدف التعديل الأخير لمعيار 802.11n والمسمى IEEE 802.11n إلى الوصول إلى سرعة نظرية قصوى لنقل
البيانات تعادل 540 ميغابت في الثانية مما يجعله أسرع 40 مرة من معيار 802.11b و 10 مرات من معيار
802.11a. يعتمد المعيار الجديد على نفس التعديلات السابقة لمعيار 802.11 مع فارقٍ أساسيٍّ يكمن في
استخدام تقنية الدخل المتعدد – الخرج المتعدد (Multiple-Input Multiple-Output MIMO) والتي
تتطلب استخدام عدة رسائلٍ وعدة مستقبلاتٍ لزيادة سرعة نقل البيانات ونطاق الإرسال.
يدعي بعض الخبراء بأن تقنية MIMO ستشكل مستقبل الشبكات اللاسلكية².

ملخص بتعديلات معيار 802.11

فيما يلي ملخص مقارنة للتعديلات الأربع الأكثر أهمية لمعيار 802.11

المعيار	التردد	تقنية الترميز	السرعة القصوى لنقل البيانات	ملاحظات
802.11a	5 غيغاهرتز	OFDM	54 ميغابت / الثانية	8 قنوات غير متداخلة. لا يوجد جودة للخدمة.
802.11b	2.4 غيغاهرتز	DSSS, CCK	11 ميغابت / الثانية	14 قناة متداخلة.
802.11g	2.4 غيغاهرتز	OFDM, DSSS	54 ميغابت / الثانية	14 قناة متداخلة. متوافق مع معيار 802.11b.
802.11n	2.4 غيغاهرتز ؟	OFDM	360 / 540 ميغابت / الثانية ؟	يعتمد على معايير 802.11 السابقة بإضافة تقنية MIMO التي تستخدم عدة هوائيات لإرسال واستقبال لإتاحة قدرة أعلى لنقل البيانات عبر استخدام الترميز الفضائي.

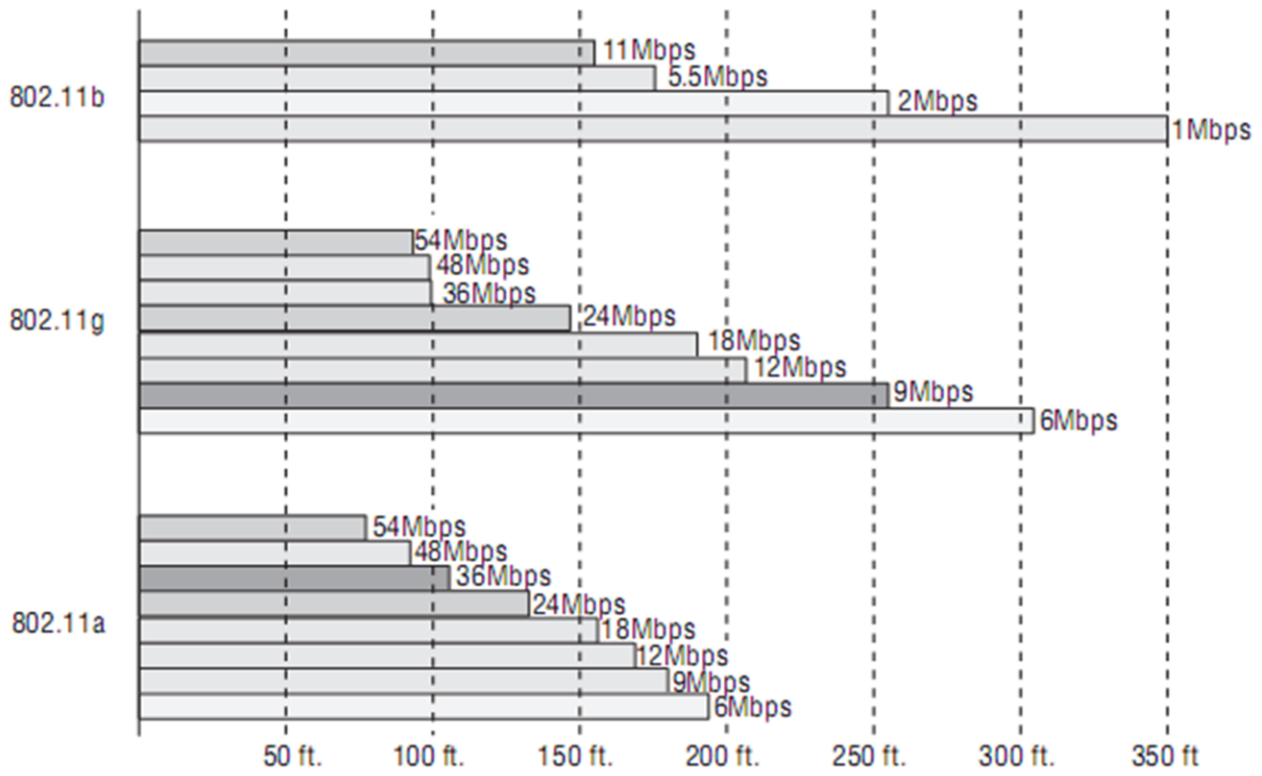
frequency Vs. distance



*

IEEE 802.11 Standards

IEEE 802.11 Standards



الفصل الخامس

Modes of 802.11 Wireless LANs

AD-HOC

هي كلمة لاتينية قديمة معناها " for this " أو " لهذا " وهي طريقة تستخدمها معايير 802.11

عندما يريد جهاز الإتصال بجهاز آخر بدون الحاجة إلي جهاز وسيط حيث يقوم أحد الجهازين بعمل

مجموعة عمل workgroup ويقوم بتحديد SSID وأسلوب الأمن و التحقق ثم يقو الآخر بطلب الإتصال

طبقا للمواصفات التي وضعها الجهاز الأول ويسمي الجهاز الذي حدد مواصفات الإرسال بالجهاز الأساسي

basic service set (BSS)



وهذه العملية تسمى independent basic service set IBSS حيث لا يعتمد الاتصال علي جهاز

وسيط ورغم سهولة هذه العملية فإنها تعاني من بعض القصور ففي حين انك تستطيع عمل شبكة من أكثر من

جهاز إلا أن الجهاز لا يستطيع الإرسال والاستقبال في نفس الوقت الامع جهاز واحد فقط وتسمى هذه

العملية Half-Duplex نظام ارسال لا يستطيع فيها المرسل ولا المستقبل الاتصال فيما بينهما في نفس

الوقت مثلما يتم مع Full-Duplex

Network Infrastructure

تعتبر عدم المركزية في اتخاذ القرارات ومعالجة العمليات في الشبكة نقطة ضعف خطيرة ولذلك فإن كل

الشبكات الحديثة والواقعية تتجه الي نظام مركزي يتم به التحكم في الشبكة وربطها وذلك عن طريق أجهزة

الشبكة كالراوترات والسويتشات أو عن طريق خدمات مركزية موجودة علي سيرفر رئيسي كخدمات

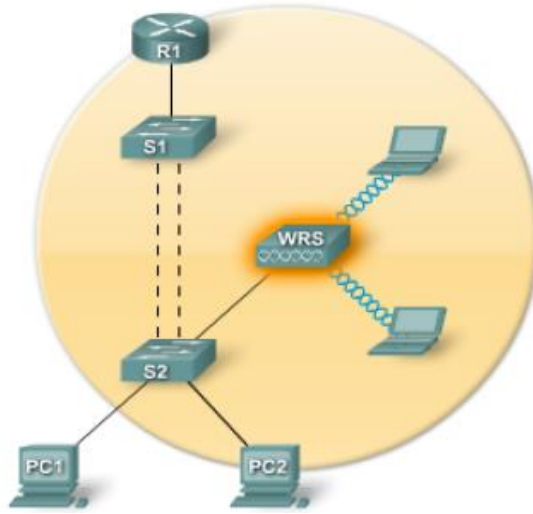
البيانات المركزية أو التوزيع المركزي لأرقام الشبكات DHCP

ولم تكن الشبكات اللاسلكية بعيدة عن هذا الواقع فبرغم أن الأجهزة اللاسلكية قادرة الإتصال ببعضها بدون

وجود وسيط AD-HOC إلا أنها مفتقرة للأمن والتوسع في عدد الأجهزة وغيرها من الميزات التي توجد في

الشبكات المركزية.

APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)

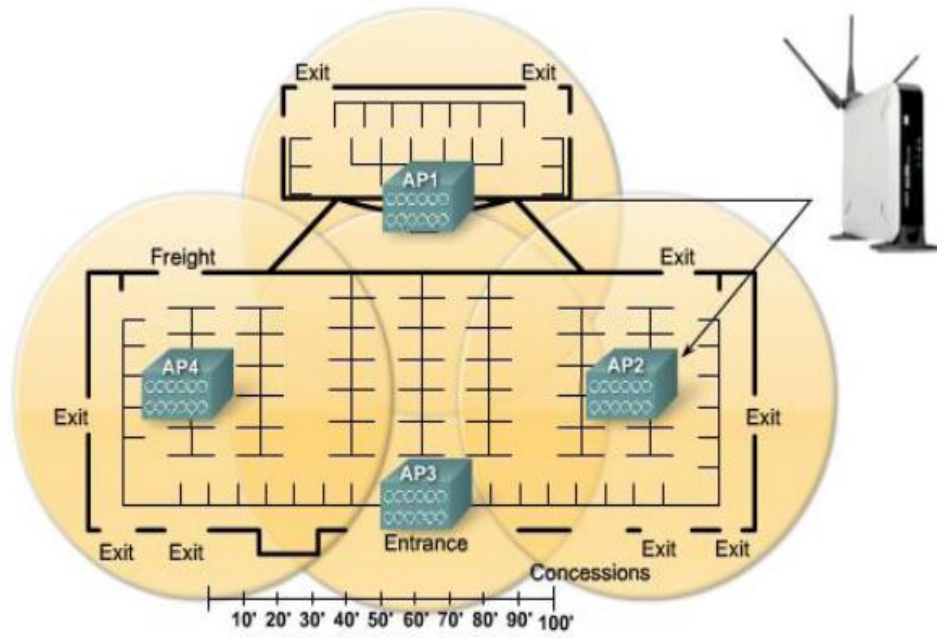




ونحن نتكلم هنا علي المركزية في الشبكة ولا نتكلم بشكل خاص عن الأكسس بوينت فهو ليس الجهاز المركزي الوحيد المستخدم في الشبكات اللاسلكية ولنكن واضحين أكثر فإن الجهاز الذي سيستخدم لعمل هذه المركزية سواء كان أكسس بوينت أو غيره سيسمي Infrastructure Device وأما الأجهزة التي ستصل بهذا الجهاز فستسمي station STA ولذلك فإن الأجهزة التي ستعتمد علي وجود جهاز مركزي فإن الحيز

الذي ستواجد فيه ويجمعها به سيسمي بمنطقة البث Basic Service Area BSA أو الخلية

اللاسلكية Wireless Cell وهي دائرية كما بالشكل

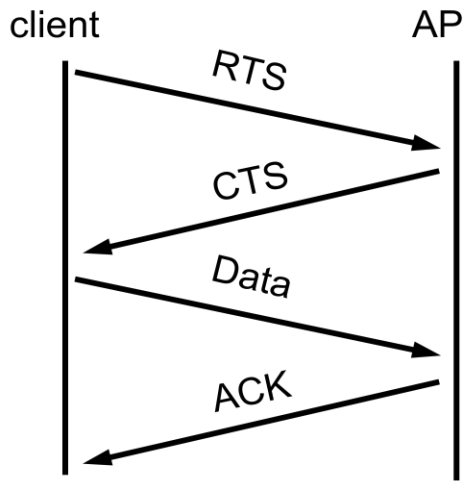


في الشبكات اللاسلكية يعمل الأكسس بوينت كنقطة مركزية لاتصال الأجهزة لاسلكيا مثلما يعمل الهب Hub والجسر Bridge في الشبكة العادية فهو يتشابه مع الهب في كونه لا يستطيع الإرسال والاستقبال في نفس الوقت حيث أنه يرسل بنمط Half Duplex أو بمعنى لاسلكي يحتوي علي مسار راديو واحد فقط يرسل و يستقبل عليه .

ويتشابه مع الجسر في أنه يرسل ويستقبل اعتمادا علي العنوان الفيزيائي للجهاز MAC Address ويختلف معه في أن الفريم اللاسلكي أكثر تعقيدا من مثيلاتها في الشبكات السلكية حيث يتكون الفريم المرسل في شبكات الإيثرنت من جزئين فقط بنا العنواف الفيزيائي للمرسل source MAC source و العنواف الفيزيائي للمستقبل destination MAC address أما في الشبكات اللاسلكية فيتكون الفريم اللاسلكي من ثلاث أو أربع أجزاء الأول عنوان المرسل و الثانية عنوان المستقبل و الثالثة عنوان الأكسس بوينت و الرابعة هي العنوان الفيزيائي لجهاز الجسر اللاسلكي

workgroup bridge المستخدم أحيانا في شبكات سيسكو و سنتكلم عنه إن شاء الله.

Most APs are use Half-Duplex to work ,meaning that the access point can only “ talk” with one device at a time “ wirelessly “ , and it uses CSMA/CA carrier sense multiple access / collision avoidance

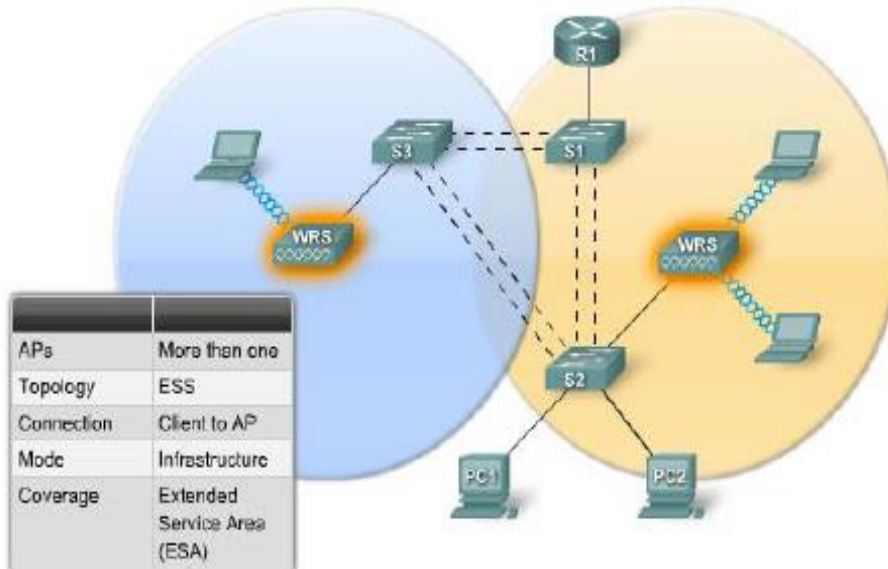


ESS extended Service Set

هو نفس للنوع السابق ولكن يمتاز هذا النمط أنه قادر علي التمدد باستخدام أكثر من أكسس بوينت و

تسمي هنا الشبكة بالشبكة الممتدة ESS extended service set

802.11 Topologies

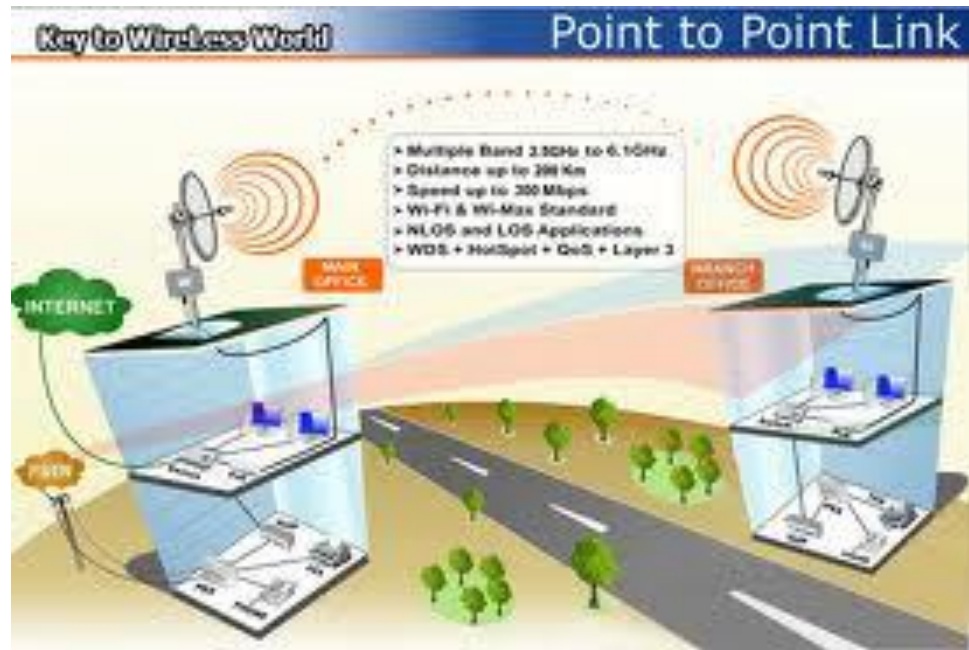


ولكي يتم الإتصال بهذه الشبكة يتم في كل أجهزتها استخدام اسم واحد فقط للشبكة SSID لتستطيع كافة الأجهزة الإتصال عبر أي من أجهزة الأكسس بوينت الموجودة كما تحتاج أيضا أن يكون هنا تداخل بين خلايا أجهزة الأكسس بوينت كما بالشكل السابق كي لا يكون عندنا مناطق ميتة Dead Zone لا تستطيع الإشارة الوصول إليها .

يتم ضبط كل خلية في الشبكة اللاسلكية الممتدة علي قناة ترددية Channel مختلفة عن جاريتها كي لا يحدث تداخل بين اجهزة الأكسس بوينت و يعطي معيار 802.11 b 802.11 b ثلاث ترددات يمكنه للنشر بين هذه الخلايا .

Point to Point mode

وهو الاتصال من نقطة إلى نقطة واحدة فقط أي مثلا من سطح عمارة لشركة إلى سطح عمارة آخر على الشارع المقابل ويعتبر اتصال فعال جدا ومفيد للشركات بشكل كبير جدا وغير مكلف.



Point to Multipoint mode

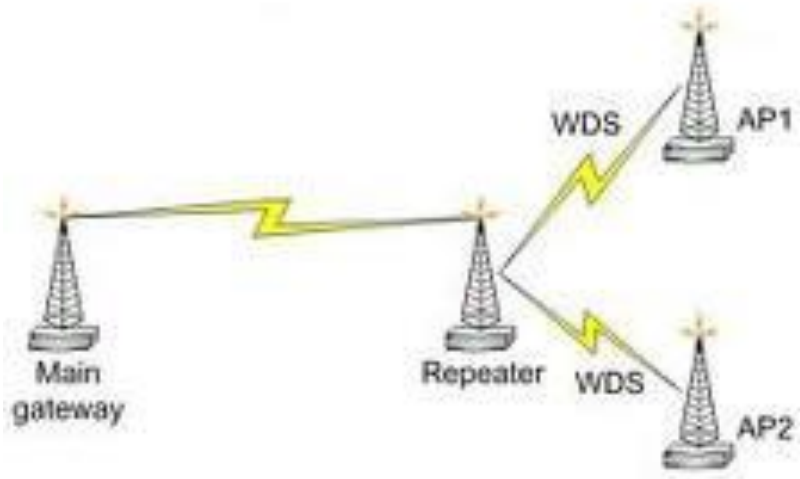
وهو يشبه إلى حد ما الوضع السابق إلا انه هنا يكون الاتصال مع أكثر من نقطة أي عدة نقاط يجب أن تقوم ببرمجة أكسس بوينت ونمكنها من الاتصال بعدة نقاط وعادة تكون من 4-6 جهة اتصال .



لاحظ هنا انه يتم برجة الاكسس بوينت على المبنى الأول حتى تتمكن من إعطاء الإشارة إلى المباني الأخرى .

Repeater mode

يستخدم هذا النوع لزيادة المسافة التي من الممكن أن تصل إليها الإشارة ويستخدم عادة في الأماكن التي يكثر فيها العوائق والحواجز الجغرافية.



WiFi-Direct

تعتبر هذه التقنية حديثة جدا تقريبا في 2010 ومن أحد إصدارات مؤسسة الواي فاي وهي تشابه قليلا في الشكل العام مع تقنية Ad hoc ولكنها تختلف في المضمون معها وعلي العكس تشابه في المضمون مع شبكات Infrastructure وتختلف معها في الشكل

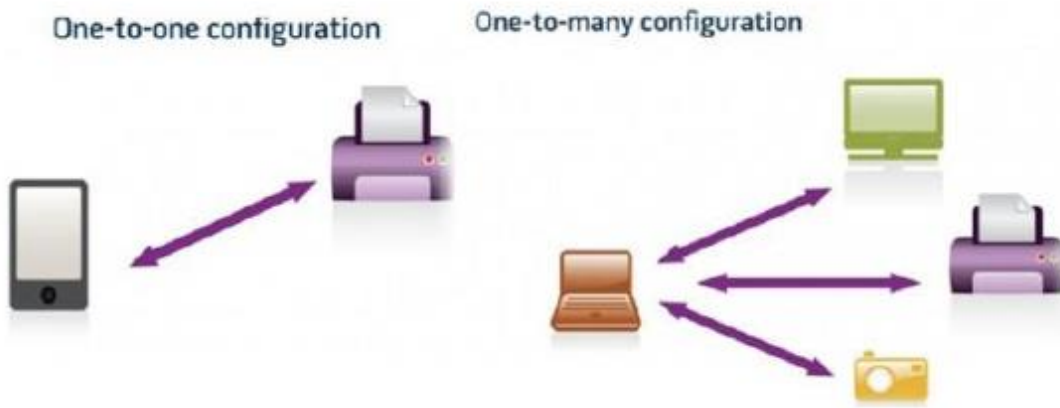
فالأجهزة التي تدعم هذه التقنية تستطيع الاتصال فيما بينها طبقا لوجود مكون إضافي بها وهذا المكون ليس هاردوير بل سوفت وير يسمى " soft Access " أي أن الجهاز سواء كان موبايل أو كمبيوتر أو طابعة أو كاميرا يستطيع التعامل كأكسس بوينت ويتصل بأي جهاز آخر به هذه الخاصية وتميز أجهزة هذا النمط في أنها تستطيع تأمين الاتصال عبر تقنية WPA2 وتم دمج تقنية WiFi Protected Setup معها لتحقيق التوثيق

عبد السلام صالح الراشدي

الأروع في هذه التقنية أن أجهزتها تستطيع الإتصال في نفس الوقت مع أكثر من جهاز اي أنها تزيد علي نمطي

Ad-Hoc و Infrastructure في أنها تتصل فيما بينها Full-Duplex مثلما تتصل اجهزة

السويتشات وليس الهب أو الأكسس بوينت



الأجهزة التي تدعم هذه التقنية قادرة علي مشاركة الإنترنت للأجهزة المتصلة بها

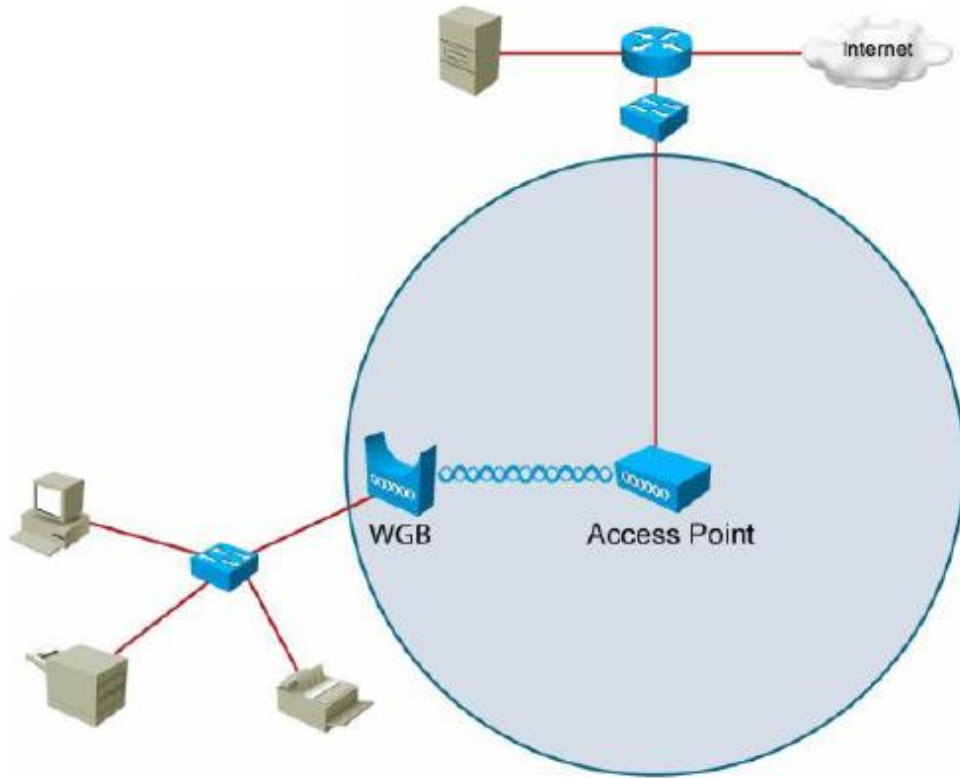
ولكي تتأكد من دعم الجهاز لهذه التقنية فابحث عن هذه العلامة



عبد السلام صالح الراشدي

WGB—Workgroup

هو جهاز لاسلكي وظيفته ربط شبكة سلكية صغيرة بشبكة لاسلكية يتعذر وصول كل أجهزة الشبكة السلكية إليها بسبب عد وجود كروت لاسلكية بها أو لعدم إمكانية وضع أكسس بوينت بها وربطه سلكيا بأجهزة الكترولر , وتكون التقنية أو الوضع الناتج عبارة عن اتصال WGB سلكيا بسويتش الشبكة السلكية ولاسلكيا بالأكسس بوينت Root AP في الشبكة اللاسلكية كما في الشكل التالي



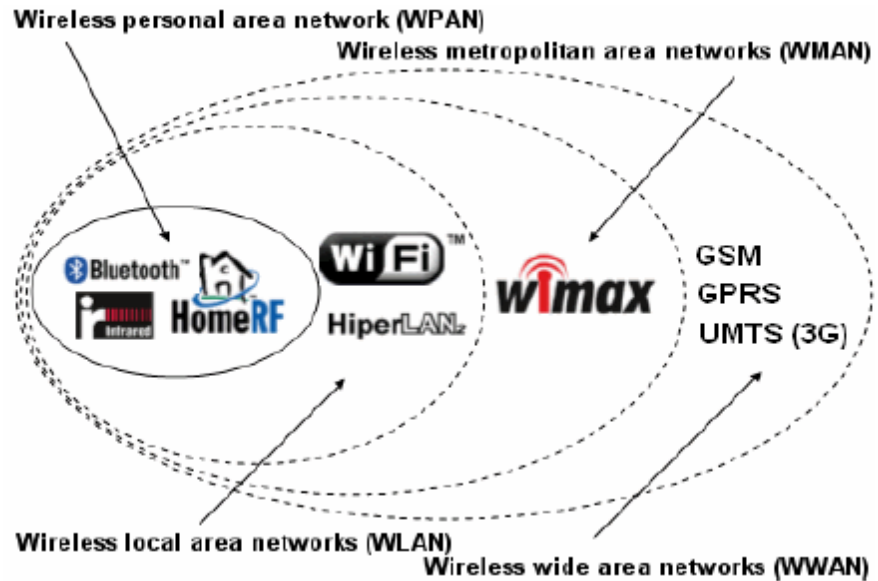
الفصل السادس

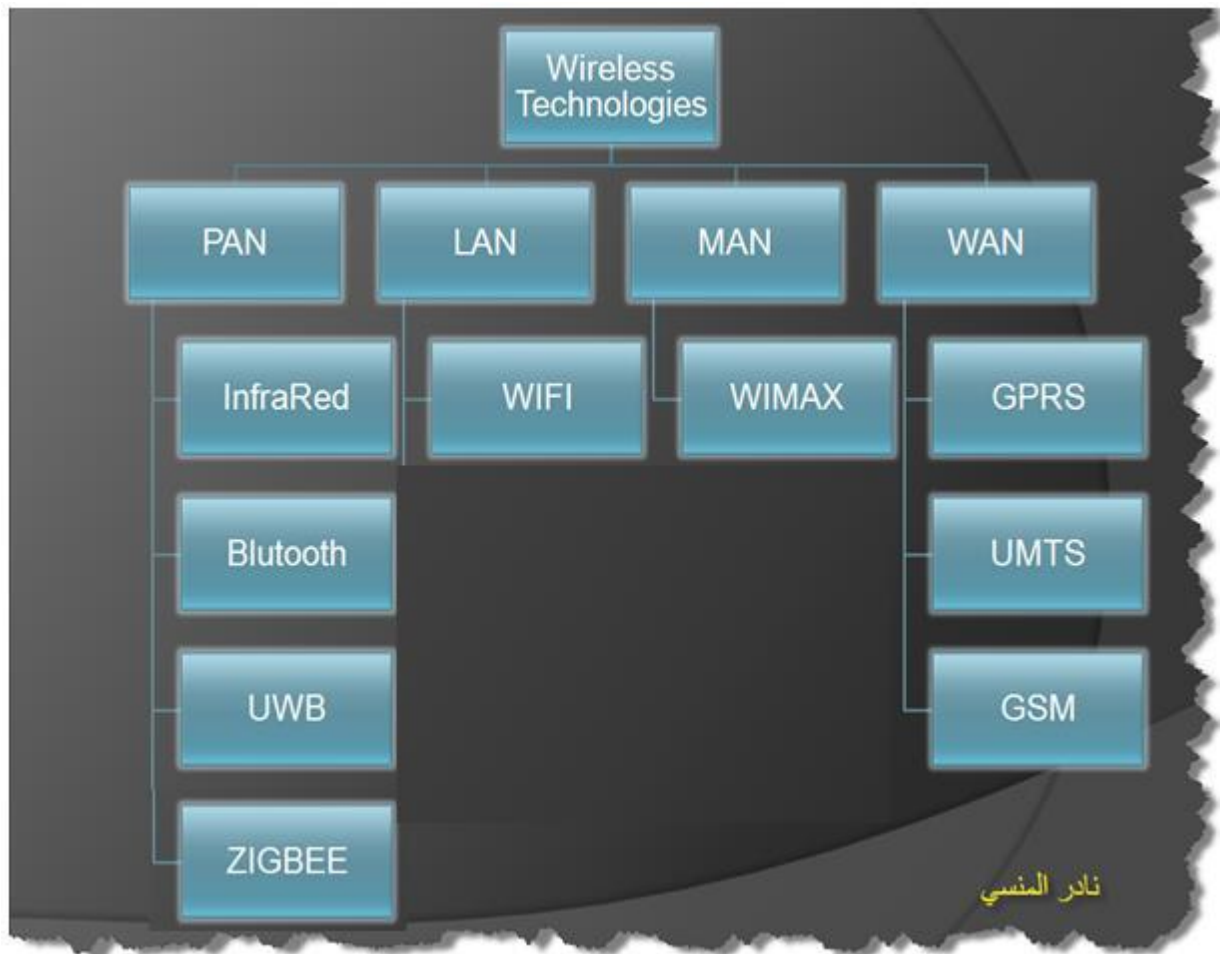
أنواع الشبكات الأسلكية

يتم تقسيم الشبكات اللاسلكية إلى أربعة أنواع كل منها يتحدد حسب المساحة التي يغطيها والتي يستخدم في

كل منها تقنية لاسلكية تتناسب مع المساحة التي تغطيها الشبكة والشكل التالي يبين بعضا من التقنيات

الشبكية اللاسلكية المستخدمة مقسمة تحت هذه الأنواع الأربعة





الشبكات اللاسلكية الشخصية (PAN (Personal Area Network)

وهي تختص بالشبكات الشخصية علي مستوي متر إلى عشرة أمتار وتختص بالأساس في اتصال جهاز الكمبيوتر لاسلكيا ببعض الأجهزة الأخرى الخدمية مثل الطابعات والأكسس بوينت والسكانر والكاميرات وأحيانا الماوس والكمبيوتر .

وتتميز هذه التقنية باستخدام إرسال لاسلكي بقدرة و طاقة محدودين لحصر حيز الإرسال في مكان صغير يستخدم في هذه الشبكات تقنيات شبك لاسلكي مثل IrDA, Bluetooth, UWB, z-wavezigbee,

تقنيات الأشعة تحت الحمراء (IRDA) Infrared Data Association



يتم استخدام تقنيات الأشعة تحت IR Infrared للاتصال المباشر line of sight عندما يكون

الجهازان علي خط واحد ولا يفصلهما اي عائق مثلما تستخدم أجهزة الريموت كنترول ورغم أن الأشعة تحت الحمراء ليست اشعة مرئية فهو يعتمد علي استخدام خواص الضوء المرئي في الإتصال ويتأثر الإتصال بما يتأثر به الضوء العادي

تقنية الإتصال اللاسلكي بواسطة البلوتوث Bluetooth



عالجت هذه التقنية مشكلة اشتراط تواجد الأجهزة علي خط نظر واحد ومشكلة تعدد الإتصال ومشكلة الأمان ومشكلة السرعة حيث تستطيع أن تحقق الإتصال بين أكثر من جهاز في نفس الوقت مع توفر الأمان الشبكي وكذلك ضمان سرعة تدفق للبيانات .

ويتم استخدام طريقة master / slave لعمل الإتصال وهي طريقة منظمة وعملية ومنطقية للغرض الذي أنشئ له هذا النظام .

تقنية البلوتوث تستخدم تردد ما بين 2.40 إلى 2.48 جيجا هيرتز وتقوم الأجهزة بتغيير التردد كل مرة في عمليات الاتصال ولذلك فمن الصعب جدا حدوث تداخل في الترددات بين الإتصالات

تقنية الإتصال اللاسلكي فائقة الإتساع UWB Ultra –wideband

يعتبر الإتصال اللاسلكي فائق الإتساع من التقنيات الأحدث في عالم الإتصالات الشبكية اللاسلكية و الأعبج أيضا فهي تستخدم موجات راديوية واسعة النطاق ذات طاقة منخفضة جدا لإرسال بيانات كبيرة جدا وهذه الميزات قد تزيح جانبا أسماء عملاقة مثل البلوتوث والواي فاي في الشبكات السلكية الشخصية

يبلغ سرعة نقل بيانات لاسلكيا تصل إلى أكثر من 480Mbps و هو هكذا أسرع عشرات المرات من معيار الواي فاي 802.11b و تتميز معداته أيضا بما يتميز به معدات البلوتوث من توافقيته و أيضا قدرته علي العمل بتكنولوجيا التشغيل و التوصيل الآلي و تتميز معداته أيضا بإمكانية ربطها بواسطة جهاز سويتش يعتمد علي تكنولوجيا UWB

الشبكات اللاسلكية المحلية (WLAN) Local Area Network

WLAN (Local Area Network)





وهي أكثر الشبكات اللاسلكية انتشارا وشيوعا وهي تعتبر الشبكات المناظرة للشبكات السلكية الشائعة وتسمى أيضا الواي فاي WI fi-- WIRELESS FIDELITY وهي خدمة الإتصال الشبكي لاسلكيا فائقة السرعة والدقة ويتم الدخول اليها عن طريق الكمبيوتر المحمول Notebook PC أو عن طريق الكمبيوتر الحبيبي Pocket Pc مثل PDA أي "المساعد الرقمي الشخصي" .

وتعتبر تقنية شبكات محلية لاسلكية wireless lan lan wireless lan ويمكنك الاستفادة من هذه الخدمة ضمن مساحة 45مترا او 100 قدم فقط وتستطيع توسيع المدى بزيادة قدرة الإشارة بواسطة هوائيات لتصل الإشارة الي عدة اميال هذه التقنية تستخدم شبكات وموجات (الراديو) لنقل البيانات عبر

الايثرو هي قادرة على اختراق الجدران والحواجز الغير معدنية وتصل سرعة نقل البيانات لاسلكيا بال-Wi

Fi من 11 الى 54 ميغا بايت في الثانية.

وتوجد في المواقع العامة مثل الفنادق والمطارات والجامعات والمطاعم وأصبحت شركات الطيران تقدم

هذه الخدمة على متن طائراتها .

الشبكات اللاسلكية لربط المدن (WMAN (Wireless Metropolitan Area Network

الواي ماكس أو WorldWide Interoperability for Microwave Access هي تكنولوجيا

لاسلكية تستخدم المعيار IEEE 802.16 لتوصي مقاييسها وتختلف عن سابقتها ان المدى الترددي

المستخدم لها مدفوع الأجر ولا بد من اصدار تراخيص لها من الجهات المختصة وتقدم غالبا بسرعات

وسرعات خدمة الواي ماكس 512 كيلوبايت , 1024 كيلوبايت , 2048 كيلوبايت

ويتم بث الإرسال عبر أبراج لاسلكية تشبه أبراج الموبايل تخدم مناطق تزيد مساحتها عن مئات الكيلومترات

ويتم استقبال الإرسال عبر هوائيات أطباق DESH علي ارتفاع ثلاثة امتار



WiMAX

Worldwide Interoperability
of Microwave Access

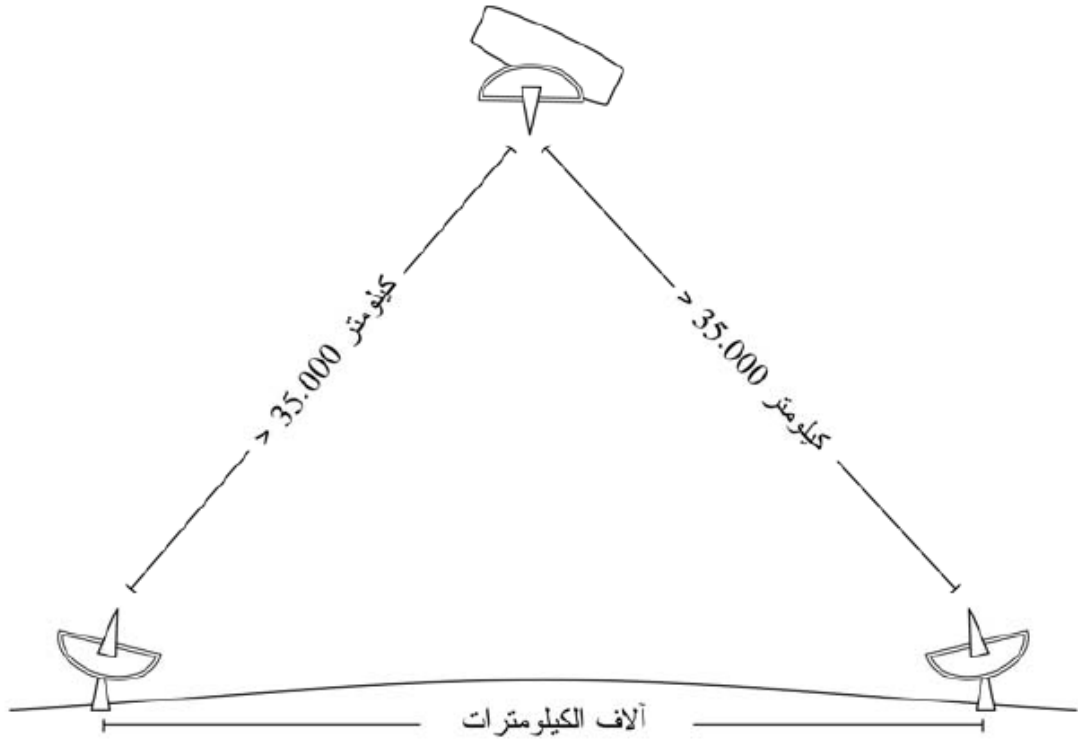
موقع الفيزياء التعليمي
www.hazemsakeek.com



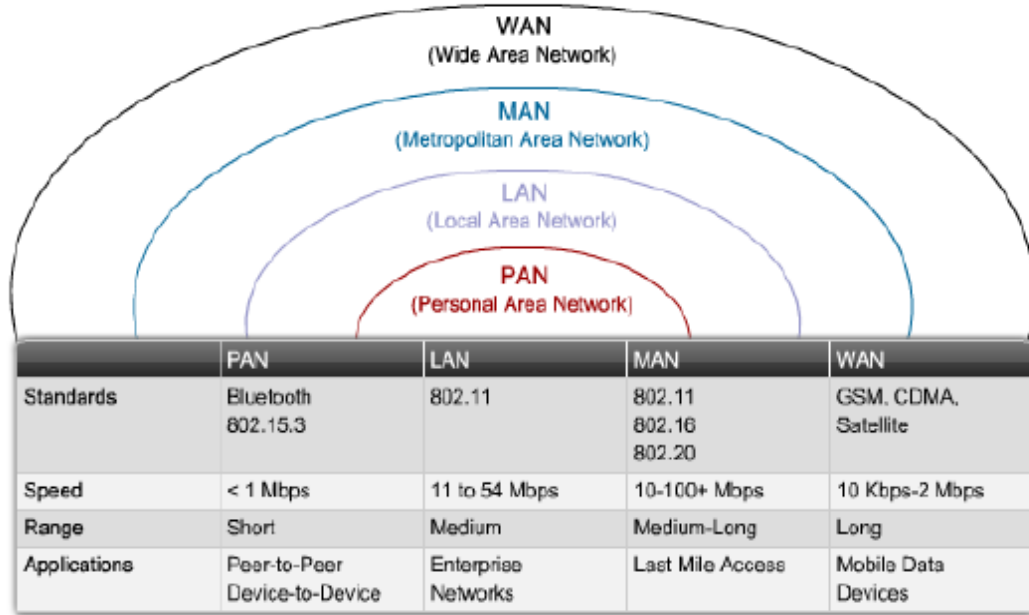
الشبكات اللاسلكية الموسعة WirelessWAN (wide area network)

بالسببة للشبكة اللاسلكية الموسعة فهي تستخدم غالبا عبر شركات الهواتف المحمولة والتي تستخدم الموجات اللاسلكية وكذلك الأقمار الصناعية والمهم فيها هو طريقة انتقال الأرسال بين عدة شبكات محلية أو مدن أو حتي شبكات فردية او شخصية شبكات فردية او شخصية





Wireless LANs



الفصل السابع

أمن الشبكات اللاسلكية

فعلى الرغم من أن مدى تغطية نقطة الولوج العادية قد لا يتجاوز عدة مئات من الأمتار إلا أنه بإمكان شخص ما يقطن في حي بعيد نسبياً الوصول إلى هذه الشبكة من خلال هوائي ذوريج مرتفع . عدا عن أنه يستحيل في حال اكتشاف مستخدم غير مخول بالولوج إلى الشبكة تفقي أثر هذا المستخدم لمعرفة موقعه الجغرافي . يمكن أيضاً لأي مستخدم أن يقوم بتجميع كافة المعلومات المنقولة عبر الشبكة اللاسلكية وتخزينها لاستخدامها لاحقاً لتوجيه ضربة احتراافية لهذه الشبكة . لذلك ينبغي عليك ألا تعتبر بأن الأمواج اللاسلكية تتوقف عند حدود المباني الخاصة بك أو بمؤسستك .

وهنا سنحاول قدر الإمكان التركيز على تأمين البيئة الشبكية اللاسلكية من أغلب المخاطر التي قد تهدده فلا يوجد أمن % 100 ولكن علينا قدر الإمكان أن نقرب من هذه النسبة بتنفيذ بعض الأمور التي ستساعد على جعل الشبكة آمنة قدر الإمكان .

أمن المعدات والأجهزة من حيث المكان

Access point , routers ,Switches

يمكن تثبيت المبدلات، المجمعات أو نقاط الولوج التي تحتوي على ثقب للتثبيت على الجدار باستخدام البراغي ينصح هنا بتركيب هذه التجهيزات على ارتفاع عال قدر الإمكان لتخفيف احتمالات لمس الأجهزة أو أسلاكها .

الأسلاك

ينبغي دوماً إخفاء الأسلاك وتثبيتها بإحكام، ويفضل دفن الأسلاك على تركها معلقة في الهواء لتتحول إلى منشئ للغسيل أو لقطعها دون قصد بسلم أو قضيب. إن تركيب الأسلاك ضمن مجار بلاستيكية سيجنبها مخاطر الحشرات والقوارض يجب دفن هذه المجاري على عمق 30سم تحت مستوى الجليد في المناطق الباردة. ننصحك هنا أيضاً بشراء مجار أكبر من الحجم الذي تحتاجه حالياً لكي تتمكن من استخدامها لتمرير أية أسلاك إضافية في المستقبل.

القدرة الكهربائية

يفضل دوماً حماية مقابس وتمديدات التيار الكهربائي ضمن خزائن خاصة، ويمكن في حال تعذر ذلك تثبيت هذه المقابس أسفل طاولة المكتب أو على الجدران مع استخدام شريط لاصق لتثبيت سلك التغذية الكهربائية في المقبس. لا تترك أية مآخذ غير مستخدمة ضمن تجهيزات أو غيرها من المقابس واستخدام شريطاً لاصقاً لإغلاق UPS عدم انقطاع التيار الكهربائي

الماء

ينبغي عليك توخي أقصى درجات الحذر لحماية تجهيزاتك من تأثيرات الماء والرطوبة. تأكد من تركيب UPS التجهيزات، بما على ارتفاع لا يقل عن 30 سم عن سطح الأرض لتجنب الفيضانات. حاول أيضاً تغطية تجهيزاتك بشكل يمنع دخول الماء والرطوبة إليها. يتوجب أيضاً عند استخدام التجهيزات في أماكن عالية الرطوبة أن تتم تهوية هذه التجهيزات بشكل ملائم للتخلص من الرطوبة. تسبب الرطوبة والحرارة المرتفعة بإتلاف التجهيزات ما لم تكن محمية في خزائن خاصة ذات تهوية جيدة.

التهديات الأمنية الأخرى للشبكة

المستخدمين غير المتعمدين

يتوافق ازدياد عدد الشبكات اللاسلكية في منطقة مكثفة بالناس مع ازدياد تواتر اتصال مستخدمي

الحواسب المحمولة بالشبكات الخاطئة.

تختار غالبية برمجيات زبائن الشبكة اللاسلكية الإتصال بأي شبكة متاحة في حال تعذر الإتصال بالشبكة

المفضلة، ليبدأ المستخدم بعد ذلك باستثمار هذه الشبكة دون أن يدري بأنه قد يرسل بذلك معلومات

حساسة إلى شبكة مختلفة. قد يستغل بعض المخربين ذلك بإعداد نقاط ولوج جديدة في المواقع الإستراتيجية

لاستقطاب المستخدمين قليلي الخبرة والتقاط معلوماتهم.

تتجلى الخطوة الأولى لتجنب هذه المشكلة في توعية المستخدمين بأهمية التأكد من الاتصال حصراً بالشبكات

المعروفة والموثوقة .

سائقو الحرب war drivers

تشق هذه الظاهرة اسمها من الفيلم الشهير "ألعاب الحرب والذي عرض في العام 1983 يهتم سائقو الحرب بإيجاد" المواقع الفيزيائية للشبكات اللاسلكية، ويقومون لذلك بقيادة مركباتهم مسلحين بحاسب وهوائي متعدد الاتجاهات لتسجيل أسماء ومواقع الشبكات التي سيجدونها. يتم دمج هذه المعلومات لاحقاً مع المعلومات التي جمعها سائقون آخرون لتحويلها إلى خريطة رسومية تظهر مواقع الشبكات اللاسلكية في مدينة ما. لا يشكل السواد الأعظم من سائقي الحرب أي تهديد مباشر للشبكة إلا أن المعلومات التي يقومون بتجميعها قد تستثمر من قبل بعض المخربين. قد يبدو من البديهي مثلاً أن يكتشف سائقو الحرب توضع نقطة ولوج غير محمية داخل مبنى هام او مكتب حكومي أو شركة ما. يمكن لأحد المخربين استغلال هذه المعلومة للوصول بشكل غير شرعي إلى هذه الشبكة. مع أنه من المفترض أن لا يتم في الأساس تركيب نقطة الولوج هذه دون حماية، إلا أن المعلومات التي نشرها عنها سائقو الحرب زادت الأمر أهمية.

Denial of service

يتوافق استخدام طيف الترددات غير المرخص مع وفر كبير في التكاليف إلا أنه يتوافق أيضاً

مع عارض جانبي سلبي يتجلى في سهولة القيام بهجمات إيقاف الخدمة (DoS) denial of service يمكن

للمخربين استغلال هذه النقطة لافترال مشاكل جملة ضمن الشبكة بسهولة فائقة لا تتعدى تشغيل نقطة ولوج

ذات استطاعة إرسال قوية، هاتف لاسلكي، جهاز إرسال فيديوي أو أي جهاز آخر يعمل بتردد 2.4

غيغاهرتز. تتعرض غالبية تجهيزات الشبكات اللاسلكية أيضاً لأشكال أخرى من هجمات إيقاف الخدمة مثل

طوفان الانفصال ARP table

نقاط الولوج المضللة

هناك نوعان من نقاط الولوج المضللة: نوع يتم إعداده بشكل خاطئ من قبل المستخدمين الموثوقين وآخر يقوم

المخربون بتركيبه بغية تجميع البيانات أو أذية الشبكة. قد يرغب أحد مستخدمي الشبكة بالحصول على

تغطية أفضل داخل المكتب أو قد يعتبر بأن التدابير الأمنية المطبقة على الشبكة اللاسلكية معقدة لدرجة

يصعب معها اتباعها بدقة. قد يقوم هذا المستخدم بتركيب نقطة ولوج رخيصة دون الحصول على إذن مسبق

ليكون بذلك قد فتح الباب أمام جميع أشكال التهديدات الأمنية الداخلية لشبكة الشركة. ننصحك بوضع

سياسة واضحة جداً حيال هذه الحالات تمنع منعاً باتاً تركيب أي نقاط ولوح ضمن شبكة الشركة دون إذن

مسبق.

يصعب التعامل مع النوع الثاني من نقاط الولوح المضللة والتي يتم تركيبها باستخدام نقاط ولوح تتمتع بقدرة إرسال مرتفعة وإعدادها تستخدم نفس معرف مجموعات خدمات للشبكة الحالية بغية تضليل المستخدمين للإتصال بهذه النقطة بدلاً من ESSID الشبكة نقاط ولوح الشبكة الأساسية. يمكنك تخفيف احتمال حدوث هذه المشكلة عبر توعية موظفيك بأهمية استخدام تقنيات التشفير المتطورة على الدوام.

المتطفلين

ذكرنا سابقاً بأن التعامل مع المتطفلين على الشبكات اللاسلكية صعب جداً.

يمكن للمتطفل مثلاً استخدام أداة مراقبة خاملة مثل برنامج Kismet لتجميع جميع البيانات المنقولة عبر الشبكة اللاسلكية من مسافة بعيدة جداً دون أن يخشى انكشاف أمره. يسهل أيضاً على هذا المتطفل تجميع البيانات غير المشفرة بشكل جيد لكسر حمايتها لاحقاً، أما يمكنه قراءة البيانات غير المشفرة مباشرة أثناء انتقالها عبر الشبكة اللاسلكية.

عبد السلام صالح الراشدي

بعض الأدوات والتقنيات التي ستساعدك على التخفيف من آثار هذه المشاكل

التحقق من الهوية Authentication

لا بد من التحقق من هوية أي مستخدم قبل تمكينه من استخدام موارد الشبكة. يتجلى الحل المثالي للتحقق من الهوية في منح آل مستخدم رمز تعريف فريد لا يمكن تغييره ولا تقمصه من قبل الآخرين، لكن تطبيق هذا الحل في الحياة العملية محفوف بالمشاكل والصعوبات.

يعتبر عنوان التحكم بالوصول إلى الناقل MAC في تجهيزات الشبكة اللاسلكية أكثر الميزات قرباً من رمز التعريف الفريد .

يتم تحديد هذا الرقم والذي يبلغ طوله 48 بتاً أثناء تصنيع أي جهاز شبكة لاسلكية أو سلكية Ethernet يمكننا عبر تفعيل وظيفة تصفية عناوين الشبكة MAC filtering ضمن نقاط وولوج الشبكة اللاسلكية التحقق من هوية المستخدم بناءً علي بطاقة الشبكة الخاصة بكل مستخدم .

تحتفظ نقطة الولوج في هذه الحالة بجدول MAC عنوان داخلي من العناوين المخولة بالوصول إلى الشبكة . ستقوم نقطة الولوج عندما يحاول مستخدم ما الاتصال بها بالبحث عن عنوان MAC لهذا المستخدم ضمن

جدول العناوين المخولة وفي حال عدم وجود هذا العنوان ضمن الجدول سترفض نقطة الولوج توصيل المستخدم بالشبكة اللاسلكية.

بعض عيوب هذه التقنية

لكن هذه الآلية لا تشكل الحل الأمثل لمشاكل التحقق من الهوية نظراً لأن إدارة جداول العناوين ضمن آل نقطة وولوج يتطلب الكثير من العمل ويتطلب الحصول على عناوين جميع MAC تجهيزات الزبائن وإدخالها ضمن جداول نقاط الولوج.

عدا عن إمكانية تغيير عنوان لجهاز ما باستخدام أدوات برمجية خاصة يمكن لمخرب ما على سبيل المثال مراقبة العناوين المستخدمة في شبكة لاسلكية معينة ليقوم بدوره بتقمص هذا العنوان وبالتالي التمكن من سيقيد في منع MAC الإتصال بالشبكة بشكل غير مشروع.

مع أن تصفية عناوين الشبكة المستخدم من غير المتعمدين أو بعض الفضوليين من الإتصال بالشبكة إلا أنه عاجز بمفرده عن صد هجمات المخربين المحترفين.

Closed network

تقوم نقاط الولوج في الشبكة اللاسلكية عادة بإرسال معرف مجموعة الخدمات . Service Set Identifier .
SSID عدة مرات في الثانية لتمكين زبائن هذه الشبكة من إيجاد الشبكة وعرض اسمها للمستخدم . لا تقوم
نقاط الولوج في الشبكات المغلقة في المقابل بإرسال معرف مجموعة الخدمات SSID وبالتالي لا بد للمستخدم
من معرفة هذا المعرف بشكل مسبق لكي يتمكن من الإتصال بنقطة الولوج، مما سيمنع الآخرين من اكتشاف
وجود الشبكة واختيارها باستخدام برمجيات تعريف الشبكة اللاسلكية.

عيوب هذه التقنية

تنطوي هذه التقنية على عدد من العيوب يتجلى أولها في كثرة الأخطاء التي ستجتم عن طلب إدخال
معرف مجموعة الخدمات SSID يدوياً من قبل المستخدم مما سيتسبب في إدخال ازدياد كبير في طلبات الدعم
الفني والشكاوى . أما أن إخفاء شبكتك عن أدوات المراقبة مثل سيحميها من الوقوع في براثن سائقي الحرب
لكنه سيخفيها أيضاً عن أعين مصممي الشبكات الأخرى مما سيحول دون معرفتهم للقنوات اللاسلكية
المستخدمة في شبكتك . قد يقوم أحد جيرانك بمسح للموقع دون أن يجد أية شبكات مجاورة وبالتالي تركيب
شبكة الجديدة للعمل ضمن نفس القناة المستخدمة ضمن شبكتك مما سيتسبب في تشويش كل من هاتين
الشبكتين على بعضهما البعض .

عبد السلام صالح الراشدي

تشفير البيانات

يعتبر التشفير أفضل أساليب التحقق من الهوية في الشبكات اللاسلكية. يمكننا باستخدام تقنيات التشفير المتطورة تحديد هوية المستخدم بدقة يصعب معها تقمص شخصيته وبالتالي استخدام نتيجة التحقق هذه لمنح هذا المستخدم الصلاحيات الملائمة للإتصال بالشبكة.

يضيف التشفير أيضاً درجة إضافية من الحماية عبر منع المتطفلين من الإطلاع على البيانات المنقولة عبر الشبكة اللاسلكية.

WEP

يمثل تشفير WEP أكثر أساليب التشفير شعبية في الشبكات اللاسلكية، وهو اختصار لعبارة الخصوصية المكافئة للشبكة السلكية Wired Equivilant Privacy والتي تدعمها جميع الأجهزة المتوافقة مع معايير 802.11 a/b/g تقريباً.

تستخدم هذه التقنية مفتاحاً مشتركاً بطول 40 بت لتشفير البيانات المنقولة بين الزبون ونقطة الولوج. ينبغي إدخال هذا المفتاح يدوياً ضمن نقطة الولوج إضافة إلى كل زبون يرغب باستخدام الشبكة اللاسلكية.

عبد السلام صالح الراشدي

لا يمكن للزبون الإتصال بنقطة الولوج في حال تفعيل ميزة تشفير WEP لا ما لم يمتلك مفتاح التشفير الملائم .

لن يمنع هذا التشفير المتطفل من الإطلاع على البيانات والعناوين MAC المنقولة عبر الشبكة لكنه لن يتمكن من قراءة المعلومات المحمولة ضمن حزم البيانات لأنها مشفرة، مما يوفر آلية معقولة للتحقق من الهوية عدا عن إضافة قسط من الخصوصية للشبكة اللاسلكية.

لا يمكن اعتبار WEP أفضل حلول التشفير المتوفرة نظراً لأنه يعتمد أساساً على مفتاح تشفير مشترك يجب تشاركه بين جميع مستخدمي الشبكة، مما سيعقد من عملية تغيير كلمة السري في حال أصبحت هذه الكلمة معروفة لسبب ما أو لآخر وذلك لضرورة تعديل إعدادات جميع الزبائن ونقاط الولوج ضمن الشبكة. أما يعني ذلك بأنه يمكن للمستخدمين المخولين بالوصول إلى الشبكة من التلصص على بيانات المستخدمين الآخرين لمعرفتهم مفتاح التشفير المشترك.

يتم اختيار مفتاح التشفير غالباً بشكل سيء مما يسهل من إمكانية اختراقه، والأسوأ من ذلك أن بعض المنتجين قد قاموا بتطبيق آليات التشفير رديء للغاية مما يجعل من بعض الشبكات المعتمدة على هذه التجهيزات عرضة للكثير من هجمات المخربين .

على الرغم من قيام بعض المنتجين بتحسين آليات تشفير WEP في العديد من التجهيزات بشكل آله عبر إضافة بعض التعديلات كزيادة طول مفتاح التشفير وتطبيق آليات تبادل أسرع إلا أن هذه التعديلات غير متوافقة مع عبد السلام صالح الراشدي

المعيار الأساسي مما يحول دون إمكانية تشغيل الأجهزة المنتجة من قبل مصنعين مختلفين مع بعضها البعض .
يمكنك تجنب بعض الثغرات الأمنية في آليات عبر ترقية برامج تشغيل جميع الأجهزة إلى أحدث إصدار
متوفر WEP .

تكمّن قوة تشفير WEP الأساسية في توافقيته العالية، حيث تدعم جميع تجهيزات الشبكات اللاسلكية آليات
تشفير WEP كطلب أساسي لتوافقها مع معايير الشبكة اللاسلكية. وعلى الرغم من أنه ليس أكثر الخيارات
المتاحة قوة إلا أنه أوسعها انتشاراً .

WPA

هو من بروتوكولات التحقق من الهوية الأخرى والتي تعمل ضمن طبقة وصلة البيانات بروتوكول الوصول المحمي
للشبكة اللاسلكية WPA Wi-Fi Protected Access أو WPA والذي صمم خصيصاً لتجاوز عيوب
سابقه بروتوكول WEP يوفر بروتوكول WPA تشفير أقوى بكثير مما يمكنه استخدام مفتاح تشفير خاص
مشترك، مفتاح خاص بكل مستخدم أو حتى شهادات SSL Certificates للتحقق من هوية كل من الزبون
ونقطة الولوج. يقوم WPA بالتحقق من الهوية باستخدام بروتوكول 802.1x القادر على الإتصال بقاعدة
بيانات خارجية مثل RADIUS . يمكن أيضاً تغيير المفاتيح دورياً وبسرعة من خلال بروتوكول. للتقليل من
. Temporal Key Integrity Protocol (TKIP)

عبد السلام صالح الراشدي

يعاني بروتوكول WPA بالمقابل عند كتابة هذه السطور من مشاكل التوافقية بين تجهيزات المنتجين المختلفين .
يتطلب هذا البروتوكول تجهيزات جديدة بالإضافة إلى أحدث إصدارات برامج تشغيل هذه التجهيزات كما
يحتاج إلى الكثير من الإعدادات .

ننصحك باستخدام هذا البروتوكول في حال أردت تركيب شبكة لاسلكية يمكنك التحكم بجميع تجهيزاتها .
يمكنك بروتوكول WPA من تجاوز مشكلة نقاط الولوج المضللة من خلال التحقق من هوية كل من الزبون ونقطة
الولوج ويمنحك أيضاً ميزات تفوق بكثير بروتوكول WEP .

لكن اعتماد بروتوكول WEP قد يشمل كابوساً في الشبكات التي تحتوي علي تجهيزات من عدة منتجين
وفي الحالات التي تكون فيها معرفة المستخدمين بمبادئ الشبكات اللاسلكية محدودة للغاية، لذلك مازال
بروتوكول WEP مستخدماً في الكثير من الشبكات حتى يومنا هذا .

WAP personal And WAP Enterprise

تعتبر هذان التقنيات من إحداه تقنيات WAP وأكثر انتشار هذه الأيام حيث يكون التعامل في WAP
Personal مع الأجهزة التي تريد أن تتصل بلاكسس بيونت ومعاً الاكسس بيونت مباشرة أما WAP
Enterprise فتستخدم بروتوكول 802.1x الذي يمكن من الاتصال بقاعدة بيانات موجود علي سيرفير
أو التحقق عن طريق البصمة أو قرنية العين وأساليب أخرى .

عبد السلام صالح الراشدي

(تعتبر تقنية طبقة المنافذ الآمنة Secure Sockets Layer والمعروفة اختصاراً باسم SSL

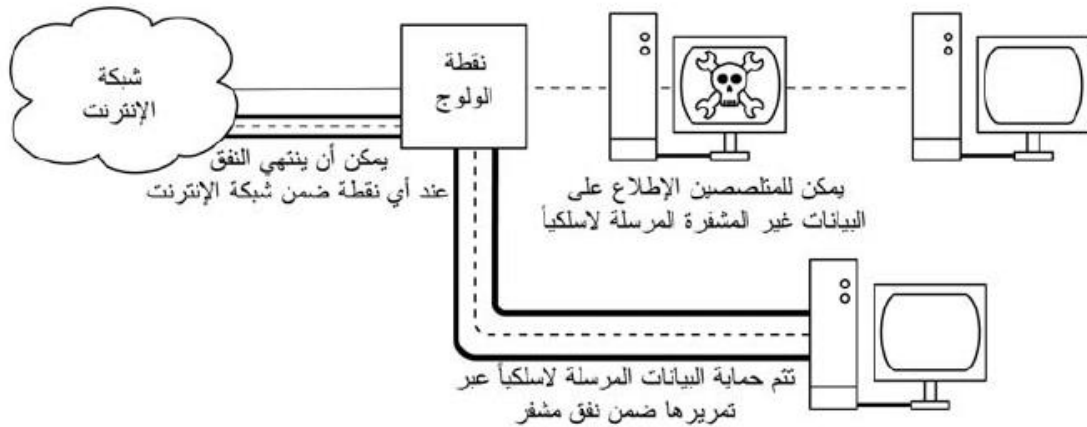
أكثر تقنيات التشفير من النهاية إلى النهاية شعبيةً في يومنا هذا .

تعتمد هذه التقنية المستخدمة في جميع خدمات الوب تقريباً على نظام التشفير المعتمد على المفتاح العام

public key cryptography إلى جانب البنية التحتية للمفاتيح العامة (PKI) public key infrastructure

لحماية البيانات المنقولة عبر شبكة الإنترنت .

إن دخولك إلى موقع على شبكة الإنترنت يبدأ بعنوانه بعبارة https . يعني بأنك تستخدم تقنية SSL .



SSH

يعتقد الكثيرون بأن بروتوكول SSH هو البديل الأمان لبروتوكول Telnet تماما كما تشكل بروتوكولات scp و sftp البدائل الأمانة لبروتوكولي ftp and rcp الي ان بروتوكول ssh ليس مجرد برووكول أمن للوصول عن بعد لجهاز ما. يستخدم هذا البروتوكول التشفير المعتمد علي المفتاح العام للتحقق من هوية الخادم البعيد وتشفير البيانات المنقولة. كما يستبدل البنية التحتية لمفتاح العام بمخزن مؤقت لبصمة مفتاح التشفير .

الفصل الثامن

بعض أشهر شهادات الشبكات اللاسلكية



شهادات سيسكو



سيسكو الشركة الاولي في الشبكات علي مستوي العالم وهي في مجال الشبكات تشبه شركة ميكروسوفت في مجال نظم التشغيل والبرامج تتكون مسارات سيسكو علي ثلاث مراتب وهي Associate ,expert ,professional, وهذه المراتب تشبه المراتب الاكاديمية في الجامعات البكالوريوس ثم الماجستير ثم الدكتوراة وأن كان هذا التشبيه فيها الكثير من النظر لكن فلنترض ذلك

فمرحلة Associate تخصص بتخريج مهندسي شبكات يستطيعون إدارة شبكة علي مستوي متوسط مثل CCNA ,CCDA اما المرحلة الاحترافية Professional فتعطيك كامل المعلومات لأدارة هذه الشبكة

علي مستوى اوسع CCIP,CCDP أما مستوى الخبير EXPERT فهو مستوى يشهد لحاملة بالخبرة
والقمة في هذا المجال مثل CCDE,CCIE وحاليا ثم ادراج مستوى علي قمة الهرم وهي Architech هذا
بشكل عام إما بشكل يخص الشبكات اللاسلكية فهناك

CCNA wireless



تؤهل هذه الشهادة و منهجها الدارس المعرفة وممارسة المهارات اللازمة لتصميم وتنفيذ ودعم ومعالجة
أخطاء الشبكات المحلية اللاسلكية وتحديد تلك الشبكات التي تخص سيسكو وذلك في المؤسسات
الصغيرة والمتوسطة وهو منهج حديث نوعا ما أطلق في صيف 2008

عبد السلام صالح الراشدي



وتعتبر هذه الشهادة بمثابة الرخصة الممنوح لك من شركة سيسكو وتشهد انك أصبحت محترف في الشبكات اللاسلكية وتستطيع الحل المشاكل الصعبة والمعقدة.

وبالطبع لابد ان تكون حاصلًا علي شهادة CCNA wireless ومن قبلها شهادة CCNA كي تستطيع دراسة

الشهادة الاحترافية CCNP wireless ولدت هذه المجموعة بعد سنة من اطلاق الترتيبات الجديدة لشركة

سيسكو في عالم الشبكات وقد كاف من المتوقع ان تكوف تسميتها CCWP علي غرار أخواتها من شهادات

سيسكو الاحترافية وظهرت سنة 2009

CCIE wireless



هي غاية المطالب و منتهي أحلام دارسي علوم الشبكات اللاسلكية ينامون ويقومون حاملين بها , ولكي بسني لنفسك بالإقتراب من امتلاكها فلا بد أن تكون ذو فهم سليم و عميق لأساسيات الشبكات اللاسلكية النظرية ومعرفة عملية تامة بأجهزتها

شهادات مؤسسة CWNP



تعتبر شهادات مؤسسة CWNP من أكثر الشهادات شيوعا في عالم الشهادات اللاسلكية فهي غير مخصصة لمنتجات شركة بعينها بل تعطيك العلم الكافي للتعامل مع إي جهاز لاسلكي قياسي .

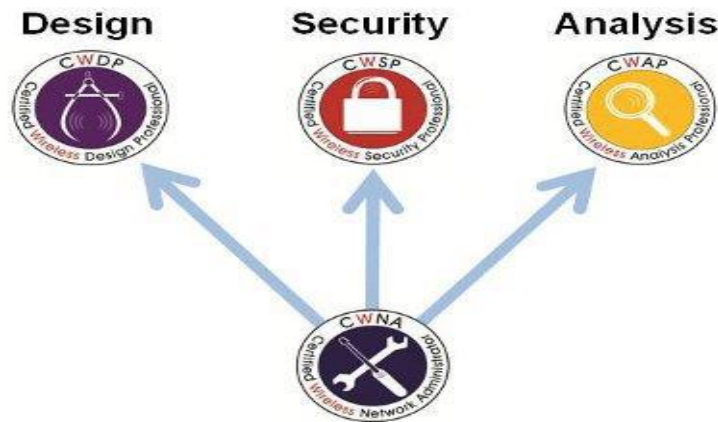
مع نهاية عام 2010 بدأت مؤسسة CWNP في ضخ دماء جديدة في جسد الشبكات اللاسلكية وذلك عبد السلام صالح الراشدي

بتدشين مسارين جديدين أحدهما يختص بتحليل أداء الشبكات اللاسلكية CWAP و الآخر يختص بتصميم

الشبكات اللاسلكية CWDP معطية لعملائها فرصة الإختيار بين ثلاث مسارات وذلك في المستوي

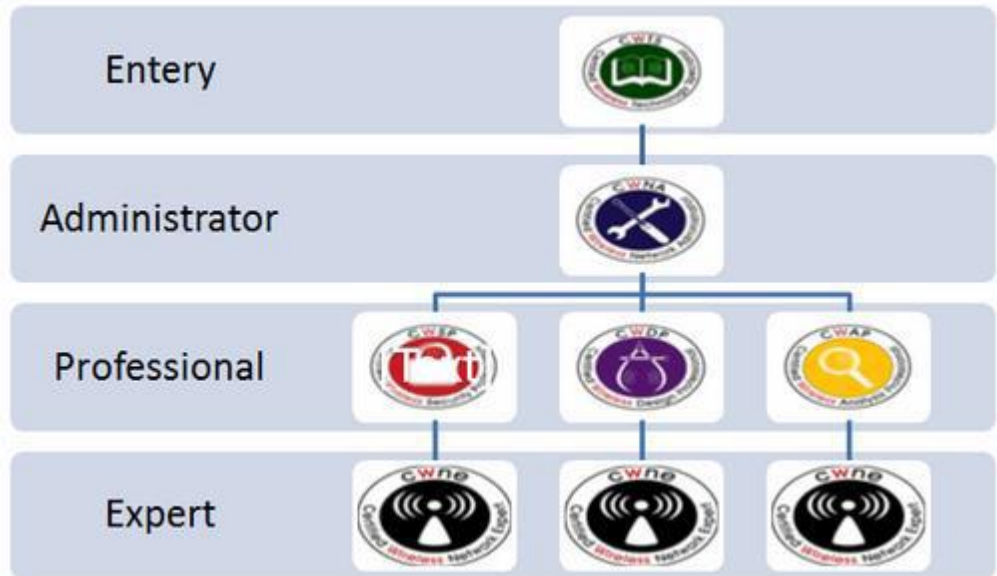
الإحترافي لشهاداتها professional level وذلك بعد أن كان هذا المستوي قاصرا فقط علي شهادة أمن

الشبكات اللاسلكية CWSP كمسار إجباري



Where will you go in 2011?

*



عبد السلام صالح الراشدي

إليكم باختصار شهادات هذا الشركه

CWTS® – Certified Wireless Technology Specialist



شهادة أخصائي الشبكات اللاسلكية في بداية السلم اللاسلكي في شهادات CWNP و تعتبر كمستوي
ابتدائي غير ملزم و تستطيع أن تتخطا إلى المستوي التالي وهي موجهة بالأساس للمبتدئين أو الأشخاص
الذين لم يسبق لهم التعامل مع اي تكنولوجيا لاسلكية .

عبد السلام صالح الراشدي

CWNA® – Certified Wireless Network Administrator



شهادة مدير الشبكات اللاسلكية هي الشهادة الأشهر علي مستوى العالم في الشبكات اللاسلكية ولم تنجح سيسكو حتي بعد أف أطلقت CCNA Wireless أو CCNP Wireless بمناهجها الأربعة في أن تزيحها عن عرشها فالشهادة بالإضافة الي عراقتها فهي غير موجهة ولا متخصصة في أجهزة شركة ما , بل تعطيك كل ما يلزمك لإدارة شبكة لاسلكية بغض النظر عن الشركة المصنعة الأجهزة وهذا ما جعلها من أحد أكبر شهادات تكنولوجيا المعلومات إنتشارا وبنظرة سريعة علي إحصائيات رواتب العاملين في تكنولوجيا المعلومات تستطيع أن تعرف مكانه هذه الشهادة.

CWSP® – Certified Wireless Security Professional



إن كافي البعض لا زال يري أن الحاجة الي الأمن المعلوماتي من قبيل الرفاهية في عالم الشبكات فلاأظنه قد تعامل مسبقا مع الشبكات اللاسلكية التي أصبحت أكثر الشبكات تعرضا لمخاطر و القرصنة مما جعل تأمين الشبكة اللاسلكية مرادفا دائما لها بل أصبح من اللازم التفكير في تأمين أي منظومة شبكية بشكل عام قبل أن تبدأ في إنشاءها ولم تكن الشركات والمؤسسات المسؤولة عن المناهج والشهادات المتخصصة في الوايرلس بعيدة عن هذا الواقع

CWDP® – Certified Wireless Design Professional



عبد السلام صالح الراشدي

الحاجة الي متخصص في تصميم الشبكات اللاسلكية أغرت CWNP في إصدار شهادة المحترف في تصميم الشبكات اللاسلكية وهذا المنهج أحد المسارين الجديدين الذين أطلقا مع بداية 2011 ولم تبدأ امتحاناته حتي لحظة كتابة هذه السطور

منهج وشهادات Wireless 5



منهج نظري ويخوض في تقنيات الشبكات اللاسلكية ولكن بتوسع أكثر في تقنيات خارج

WIFI ولكن لم ينال شهره كما نالتها الشهادات الأخرى.

الفصل التاسع

التطبيقات العملية:-

والآن أن شاء الله نبدأ في الجانب العملي بحيث نحاول قدرة المستطاع إن ننفذ ما تما تناولنا في الجانب

النظري بشكل LABS حتى تكون الصوره أوضح للقارئ حيث سوف نطبق الجانب العملي علي

حسب ما لدينا من أجهزة ومعدات .

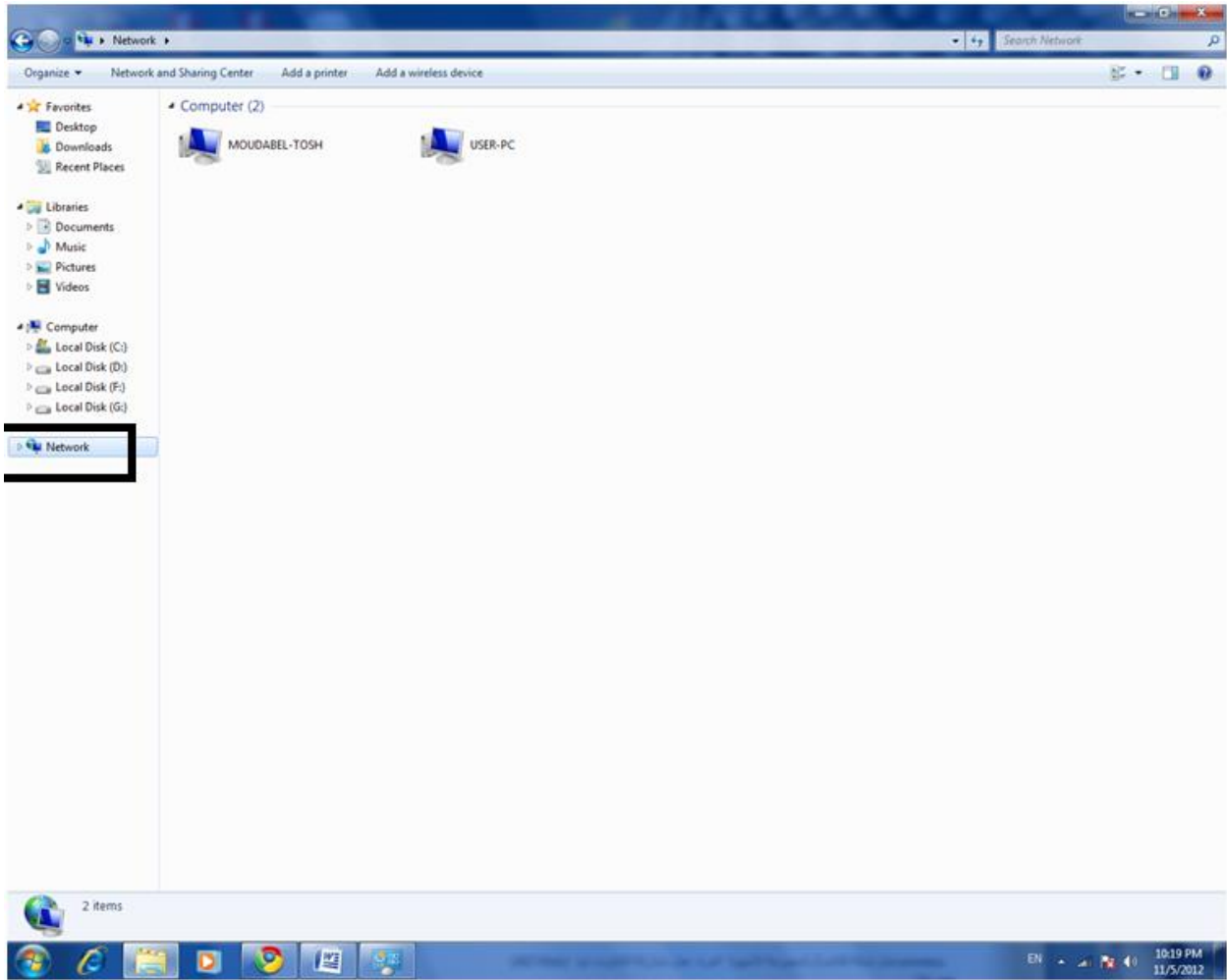
1- كيفية عمل AD Hoc

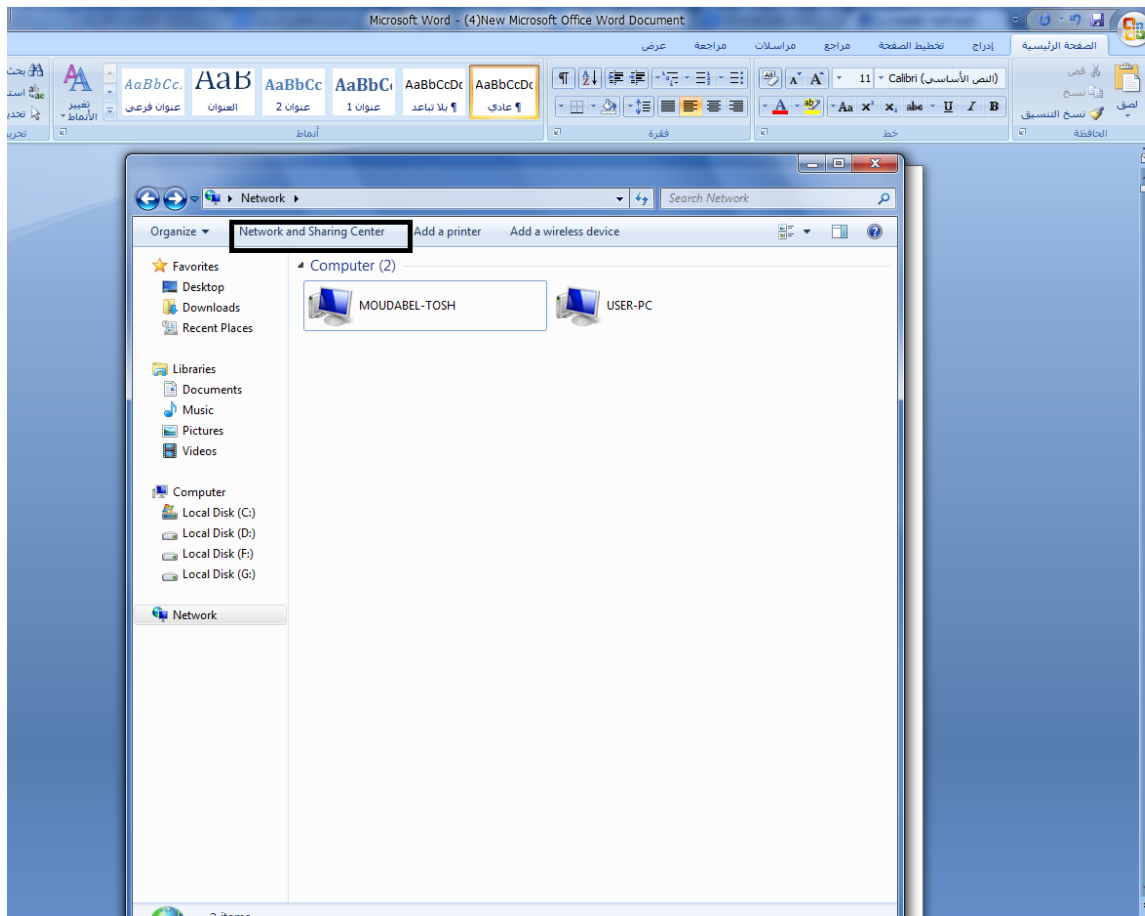
وللقيام بربط الشبكة بهذا النوع من الربط أولاً يجب علينا عمل شبكة للاتصال lan wireless

لمجموعة الأجهزة المراد عمل شبكة لاسلكية لهم ولعمل هذا أولاً نقوم بإعداد (BSS) basic service set

وهو الجهاز الذي يحدد اسم الشبكة ومستوي الأمن له وللقيام بذلك نفتح

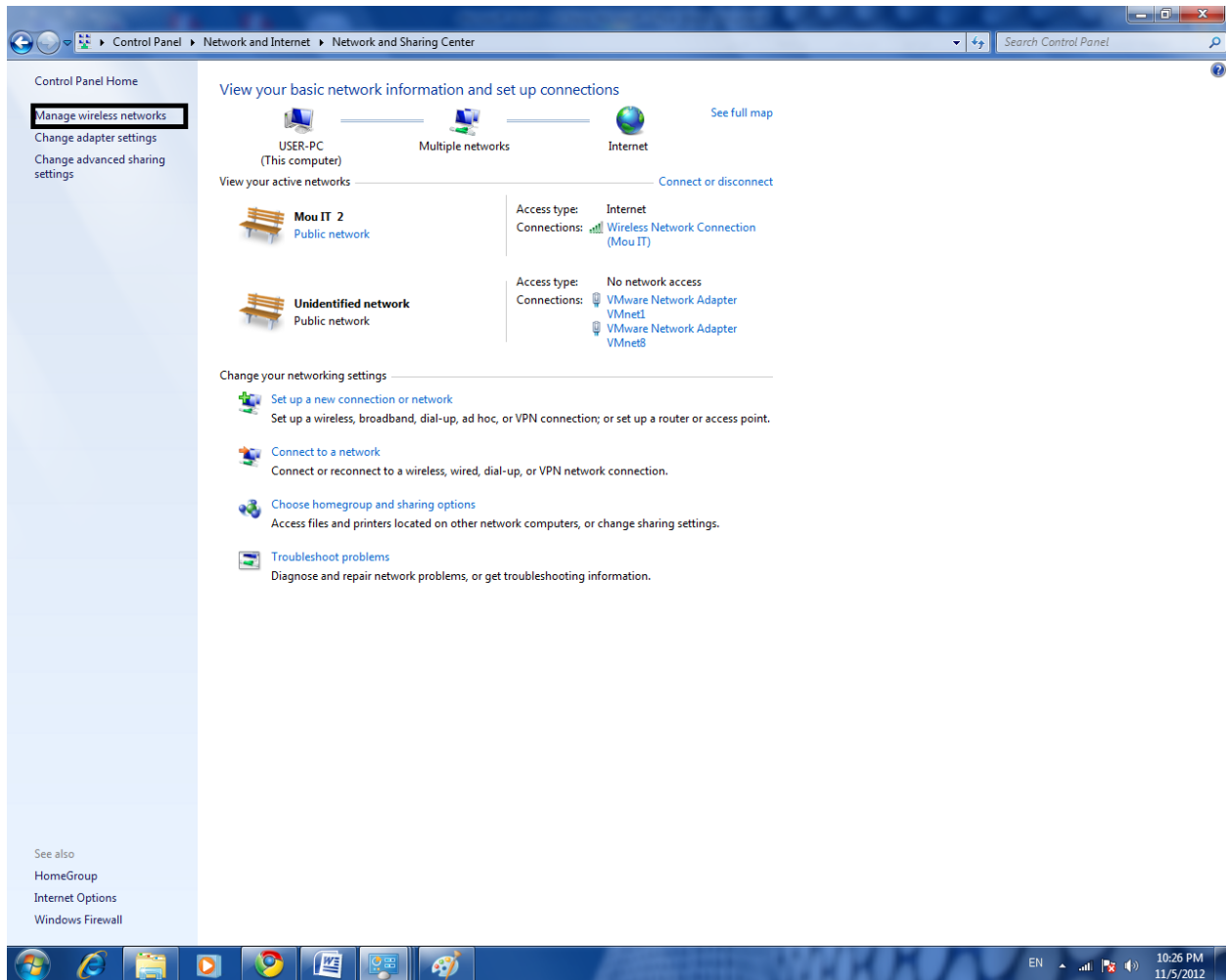
جهاز الكمبيوتر <----- network <----- center sharing and network





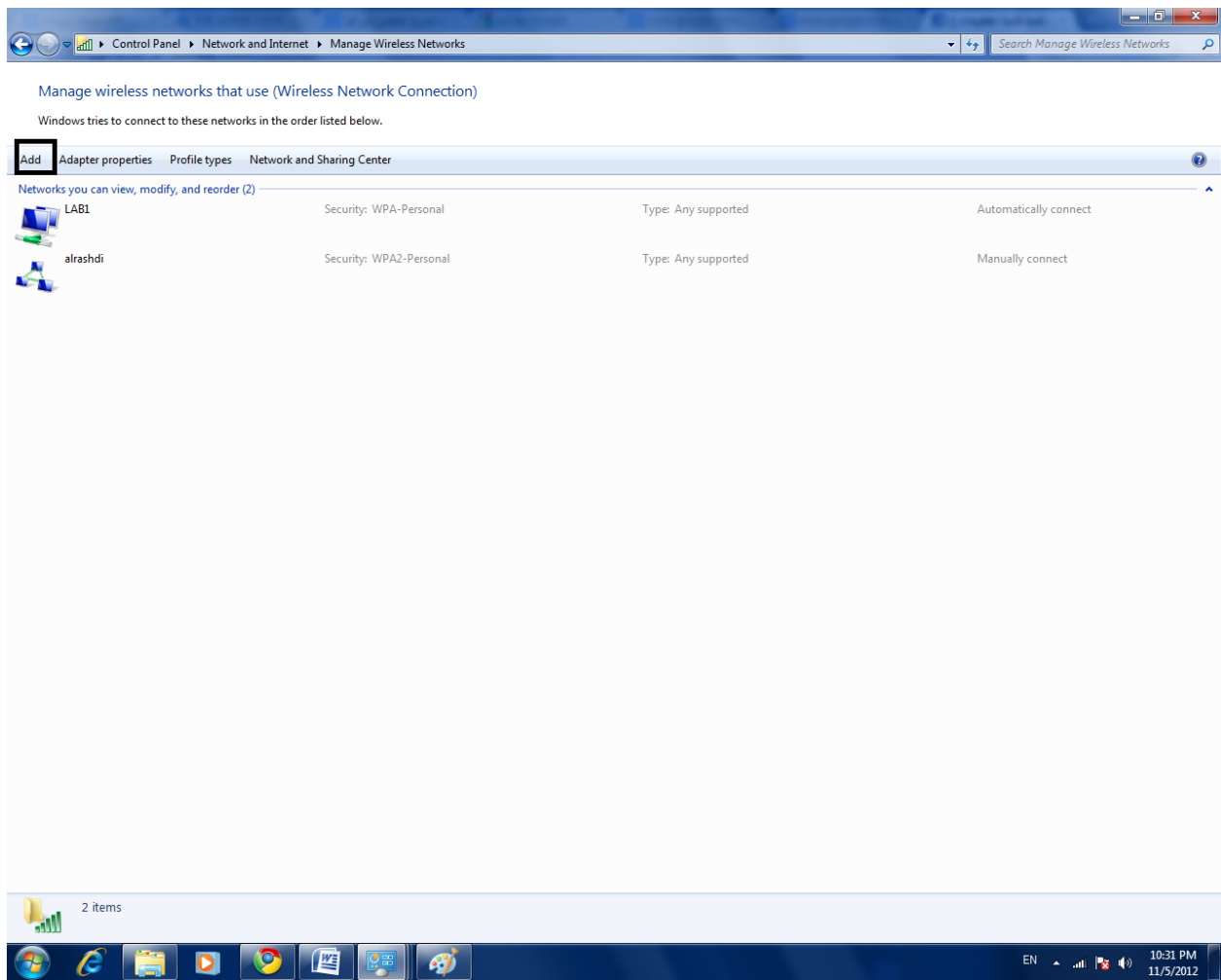
manage wireless network<-----

عبد السلام صالح الراشدي

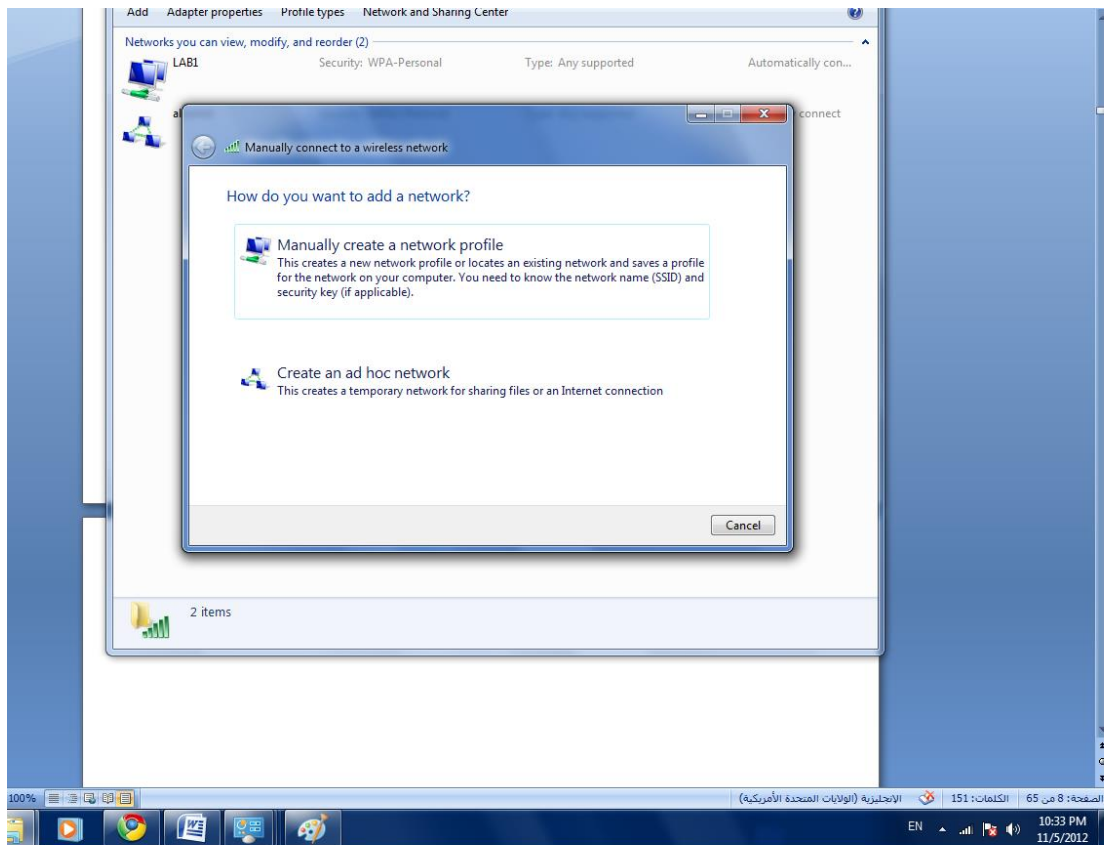


network hoc ad an create<-----Add-<-----

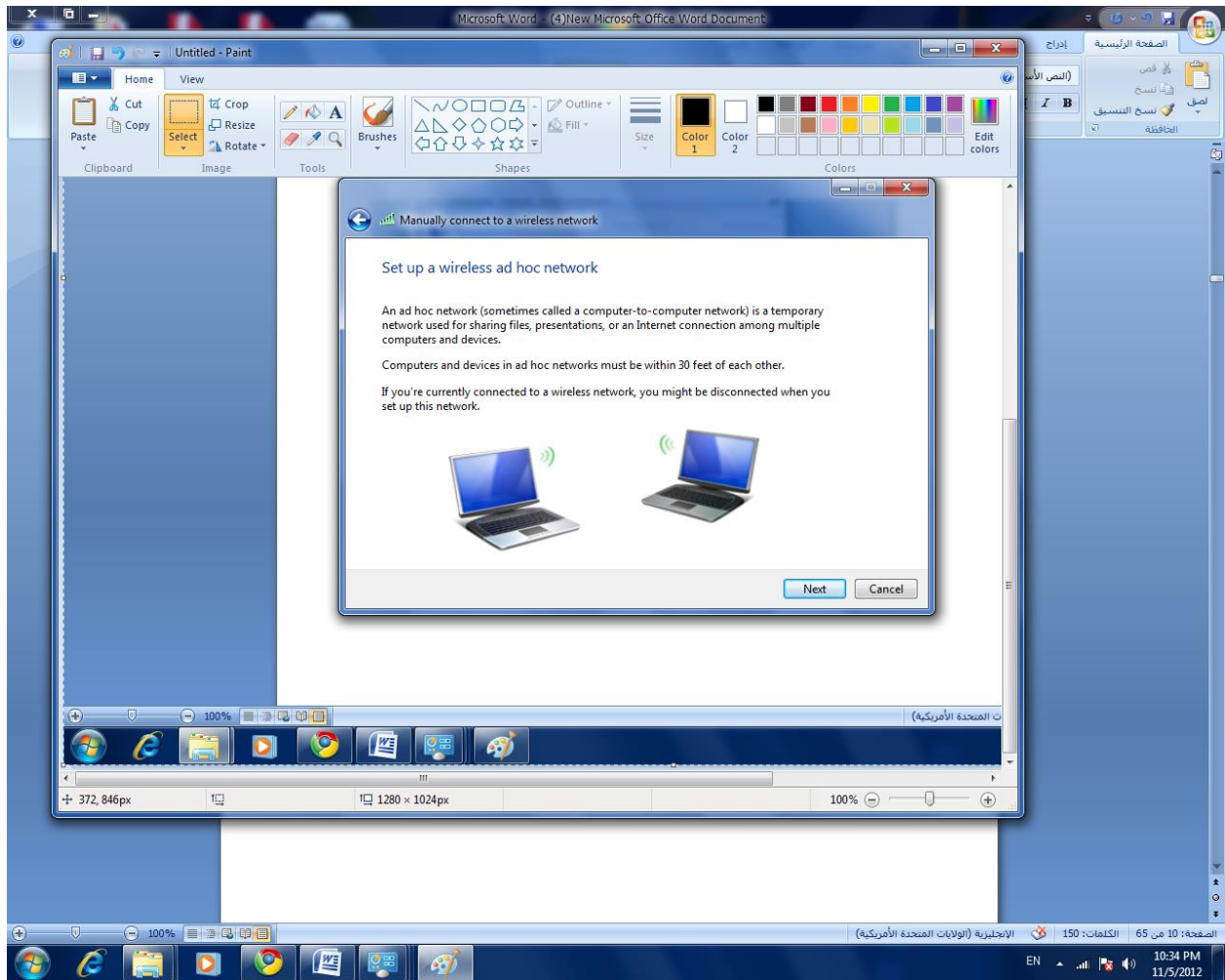
عبد السلام صالح الراشدي



عبد السلام صالح الراشدي



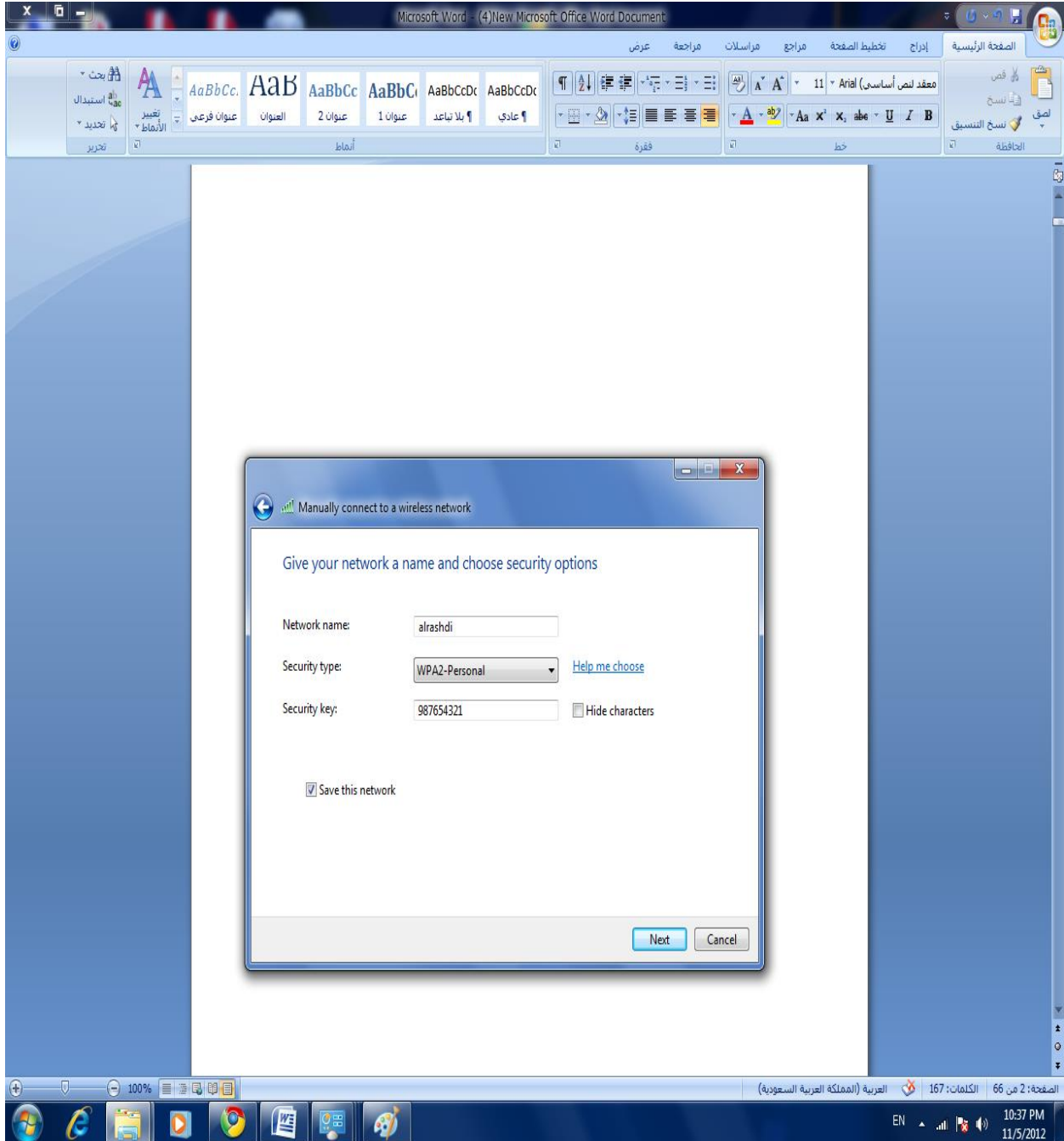
network hoc ad wireless a up set ←-----



تم تظهر واجهة الاعدادات الاخير

يتم كتابة اسم الشبكة ويتم عمل security عن طريق إدخال رقم السري للشبكة الشكل القادم

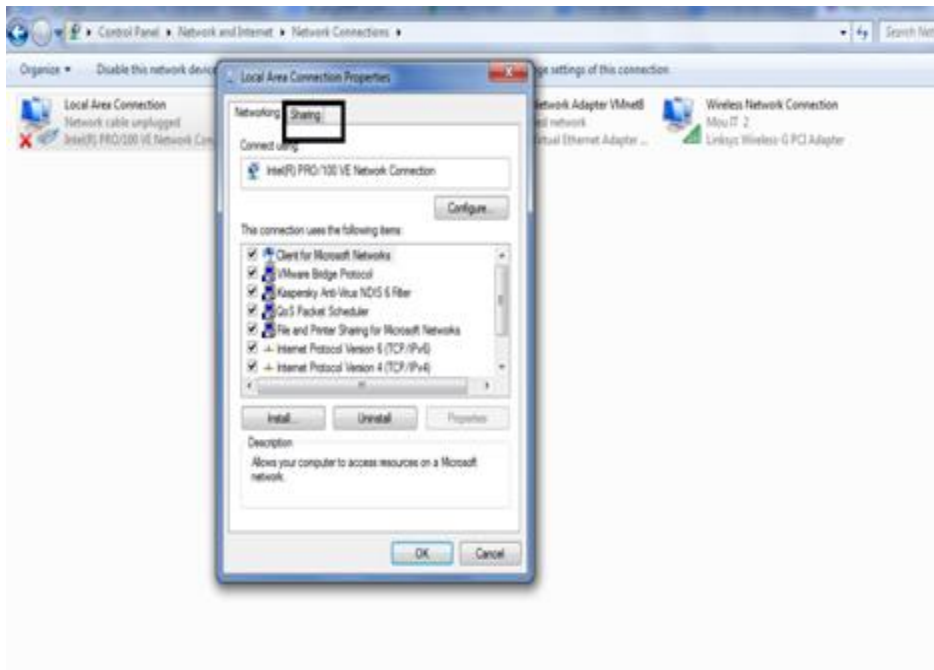
توضح هذه العملية



عبد السلام صالح الراشدي

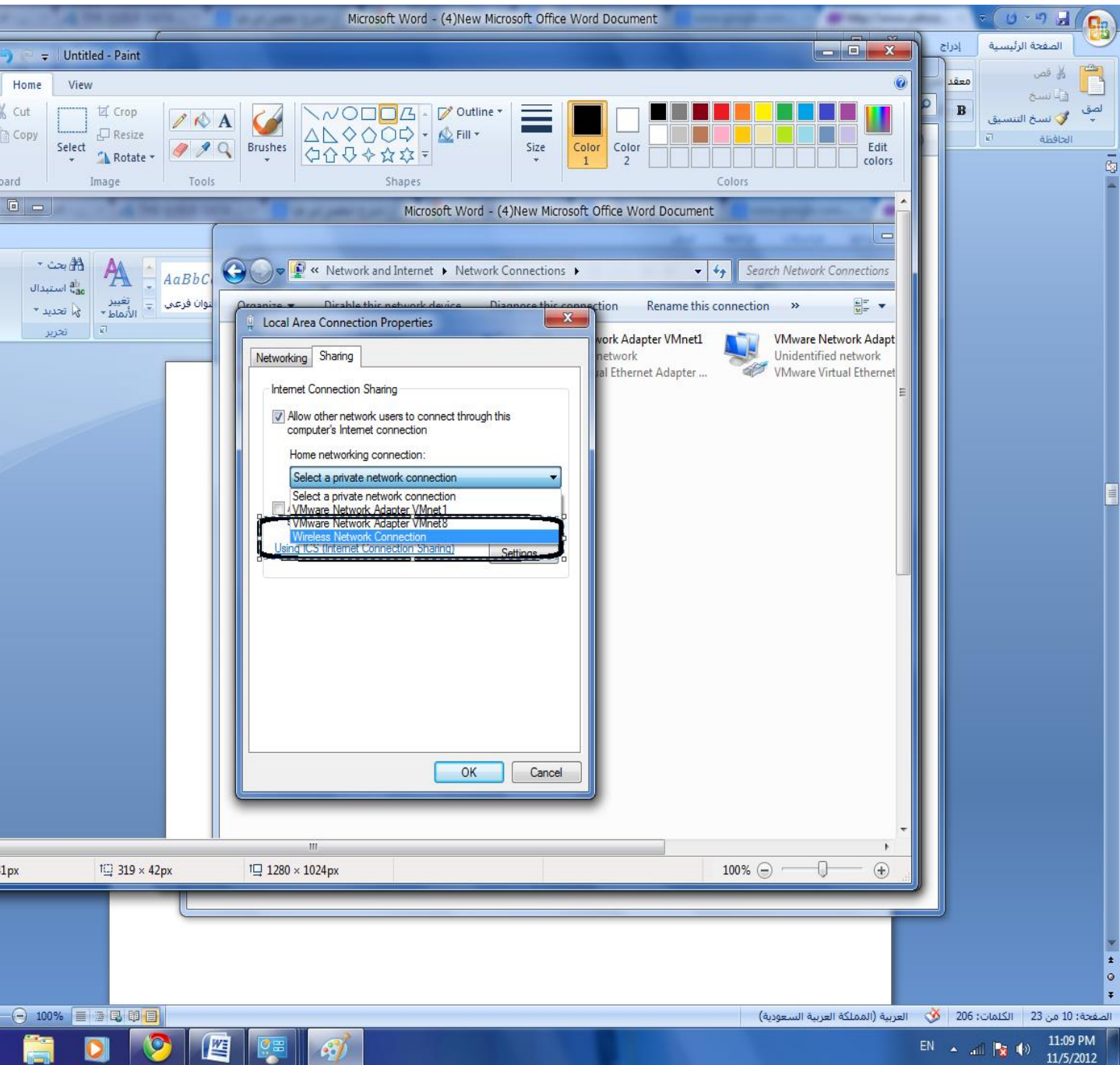
الآن أصبح لديه شبكة لاسلكية والاسم الذي سوف يظهر للجميع هو **alrashdi** وهو اسم الشبكة
الآن علي سبيل المثال أريد مشاركة أي شي ولنفترض إن لدي جهاز مثل ADSL أو جهاز واي ماكس
كما يوجد عدنا هنا في ليبيا وأريد إن أشاركه مع مجموعته من الاجهزه بحيث يستقدوا من النت جميعا
وللعمل هذا نقوم بالاتي:-

نقوم بعمل كليك يمين علي الجهاز المراد مشاركته ثم نختار **sharing** كما في الشكل الآتي



عبد السلام صالح الراشدي

يظهر لك مجموعة من الاختيارات كما في الشكل الآتي يتم اختيار



عبد السلام صالح الراشدي

يتم اختيار المشاركة عن طريق wireless تقوم باختيار network wireless

conecction لان الشبكة مربوط بشبكة لاسلكية

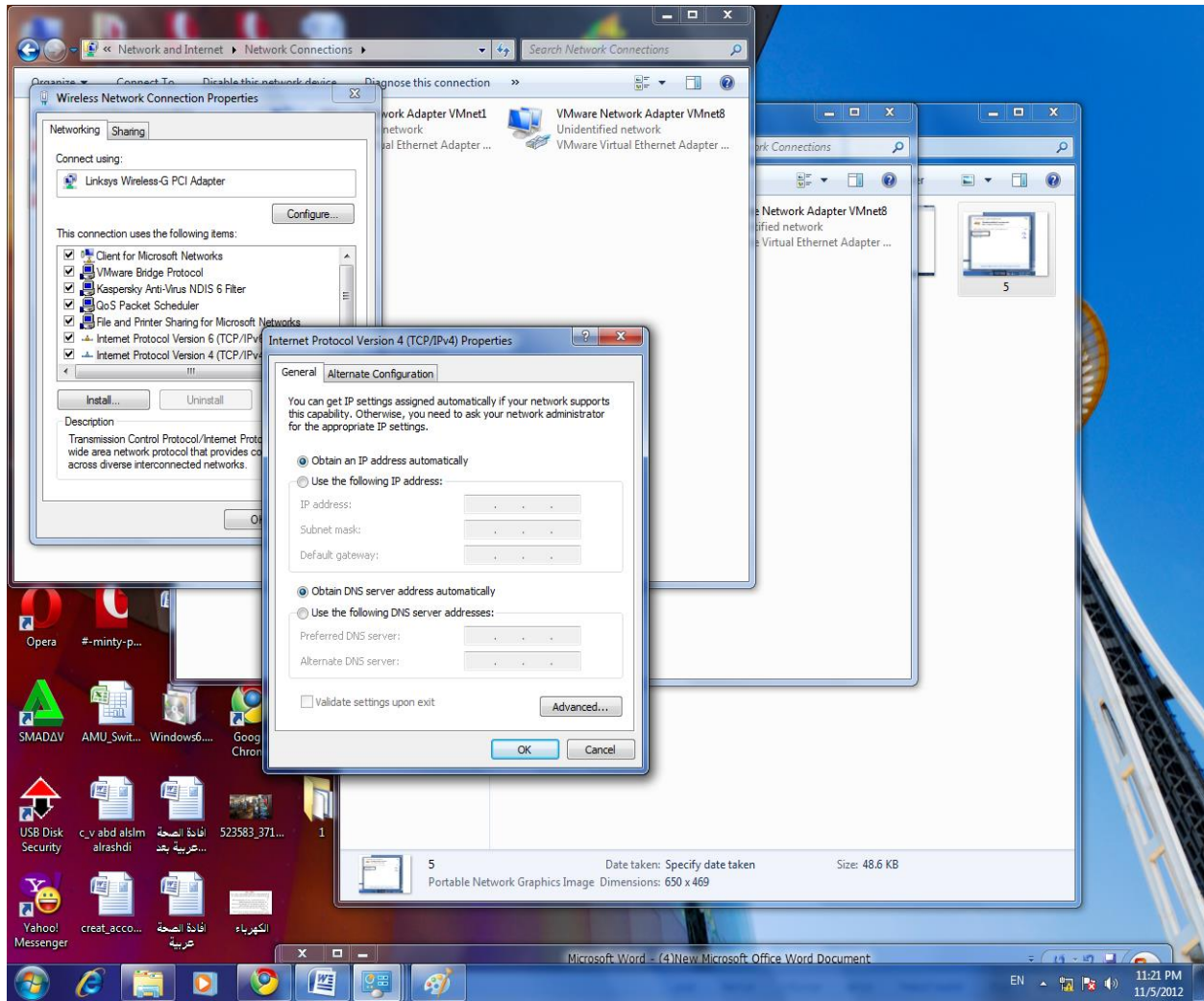
اما إذا أردنا المشاركة عن طريق الكابل نقوم باختيار Local area network

بعدها تلقائي يتم إعطاء IP للكروت اللاسلكي .

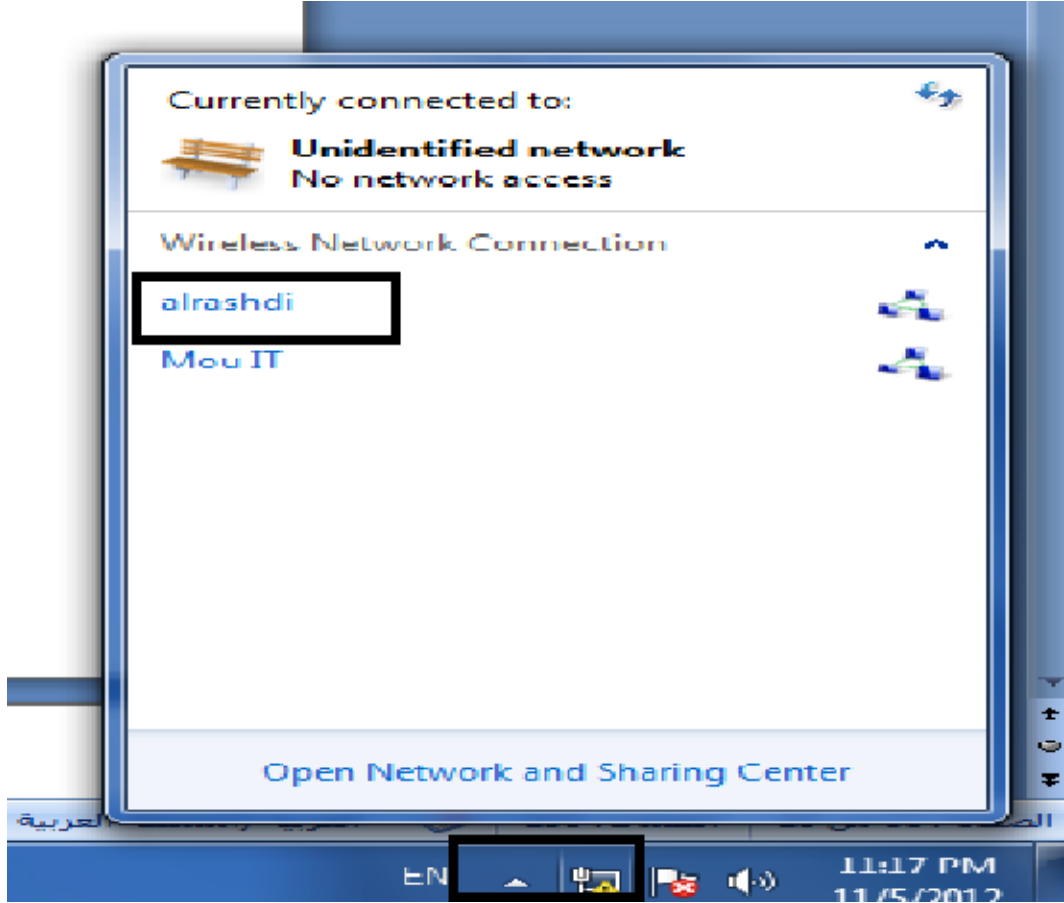
تم تقوم بعمل disconnect ثم connect للبرامج واي ماكس حتى يتم تفعيل المشاركة معا باقي الاجهزه

الآن نأتي للخطوة الاخيره بالنسبة لأجهزة التي تريد الحصول علي الانترنت

اولا نناكد ان كرت الشبكة يحصل علي أي بي عن طريق DHCP كالاتي



الخطوة الاخيره هي الاتصال بشبكة الاسلكية معا كتابة الرقم السري للشبكة



وألان إن شاء الله كل الاجهزه سوف تقوم بمشارك الانترنت

-2 Network Infrastructure (Access point)

أآن سوف نعلم سوا كيفة ربط مجموعه أجهزه لاسلكية عن طريق Access point وسوف نستخدم في

هذا Lab Access point من نوع Linksys من شركة Cisco كما في الشكل التالي



يتم عمل اعدادات للاكس بيونت بطريقتين

الاولي-: عن طريق توصيل الكابل مباشرة بالاكسس بيونت (Console) عن طريق كابل الشبكات

RJ45 وهو الأصح والأفضل كما في الشكل التالي



عبد السلام صالح الراشدي

معا ملاحظة إن هناك أخطاء يقع فيها الكثير فعندما يريدون الدخول علي الاعدادات الاكسس بيونت يضع الكابل علي بورت WAN

او internet وهذا خطأ كبير كما في الشكل التالي



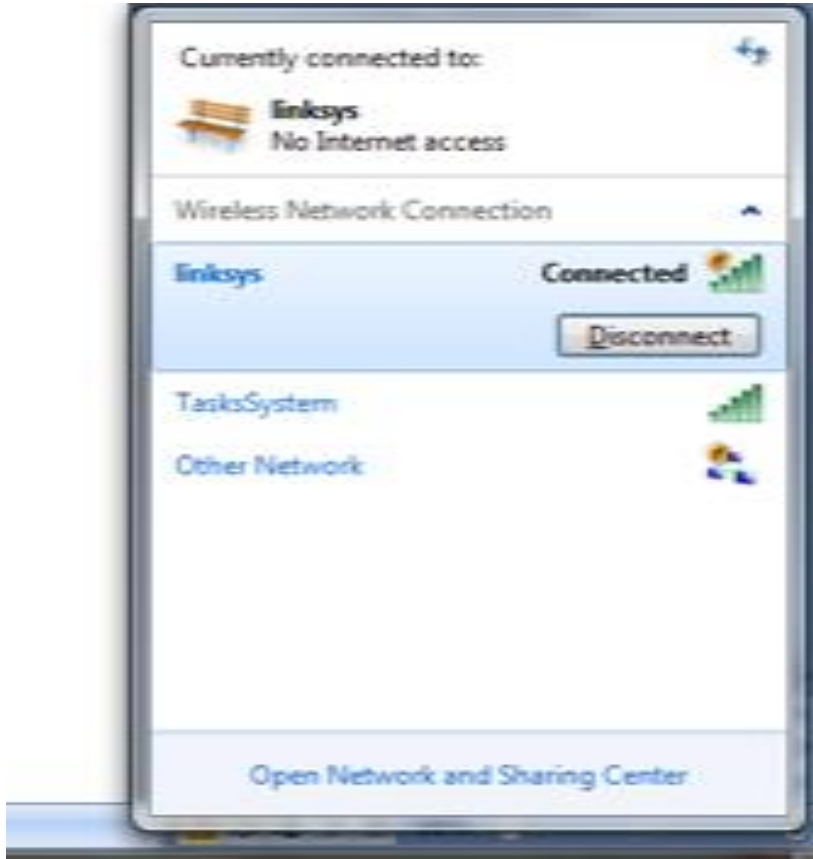
عبد السلام صالح الراشدي

ثانيا : -وهو الدخول علي الإعدادات للاكسس بونت عن طريق جهاز غير متصل مباشرة بالاكسس

بيونت (Telnet)

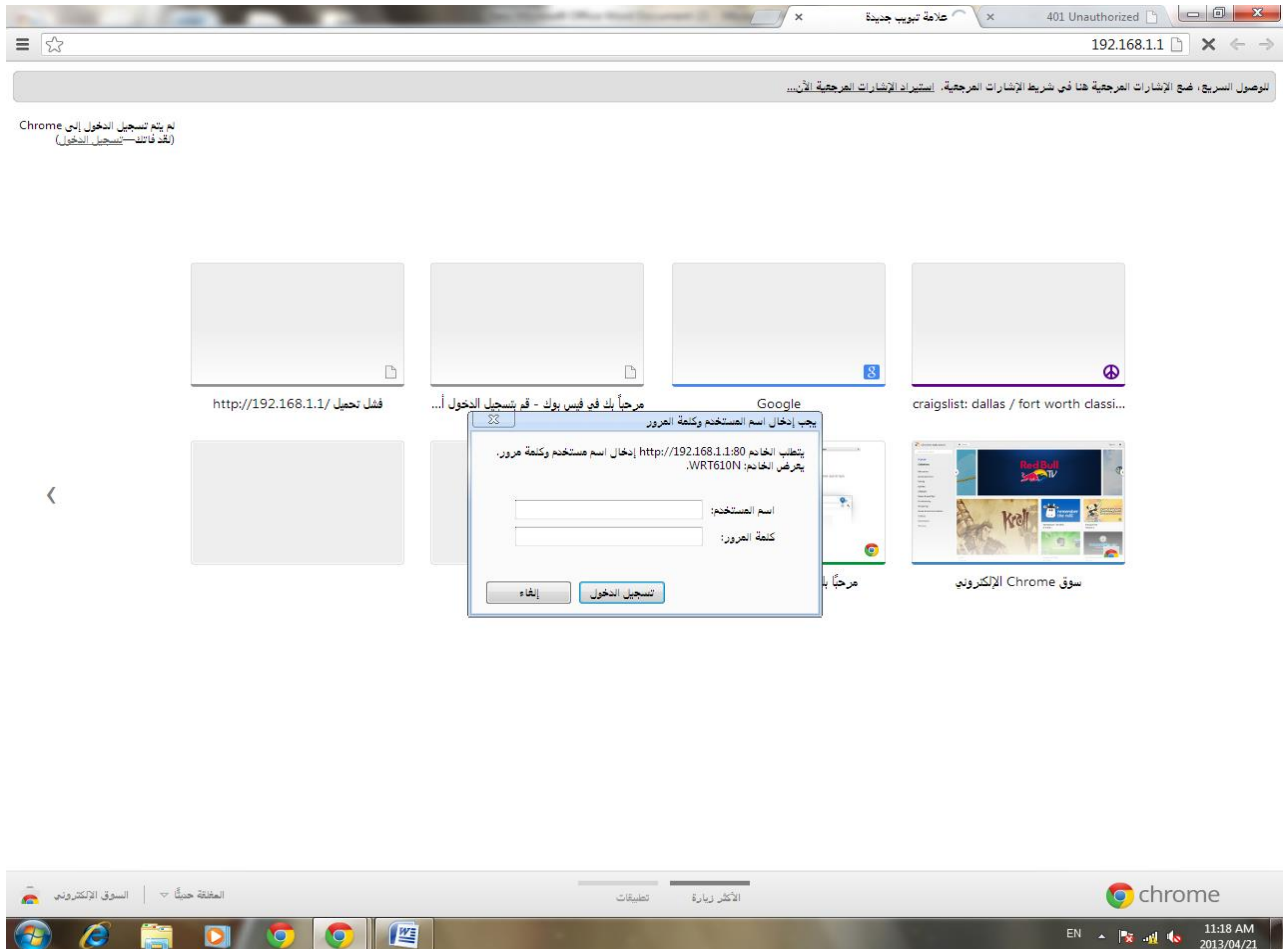
و للدخول على إعدادات الاكسس بونت يجب علينا اولا الاتصال بالاكسس بونت حيث يظهر اسم

الاكسس البيونت الافتراضي وهو نفس اسم الشركة Linksys كما في الشكل التالي



ثانياً يجب معرفه IP Address وعادة يتم كتابته في الاسفل ويبدأ مثلا 192.168.1.1 أو 192.168.0.1

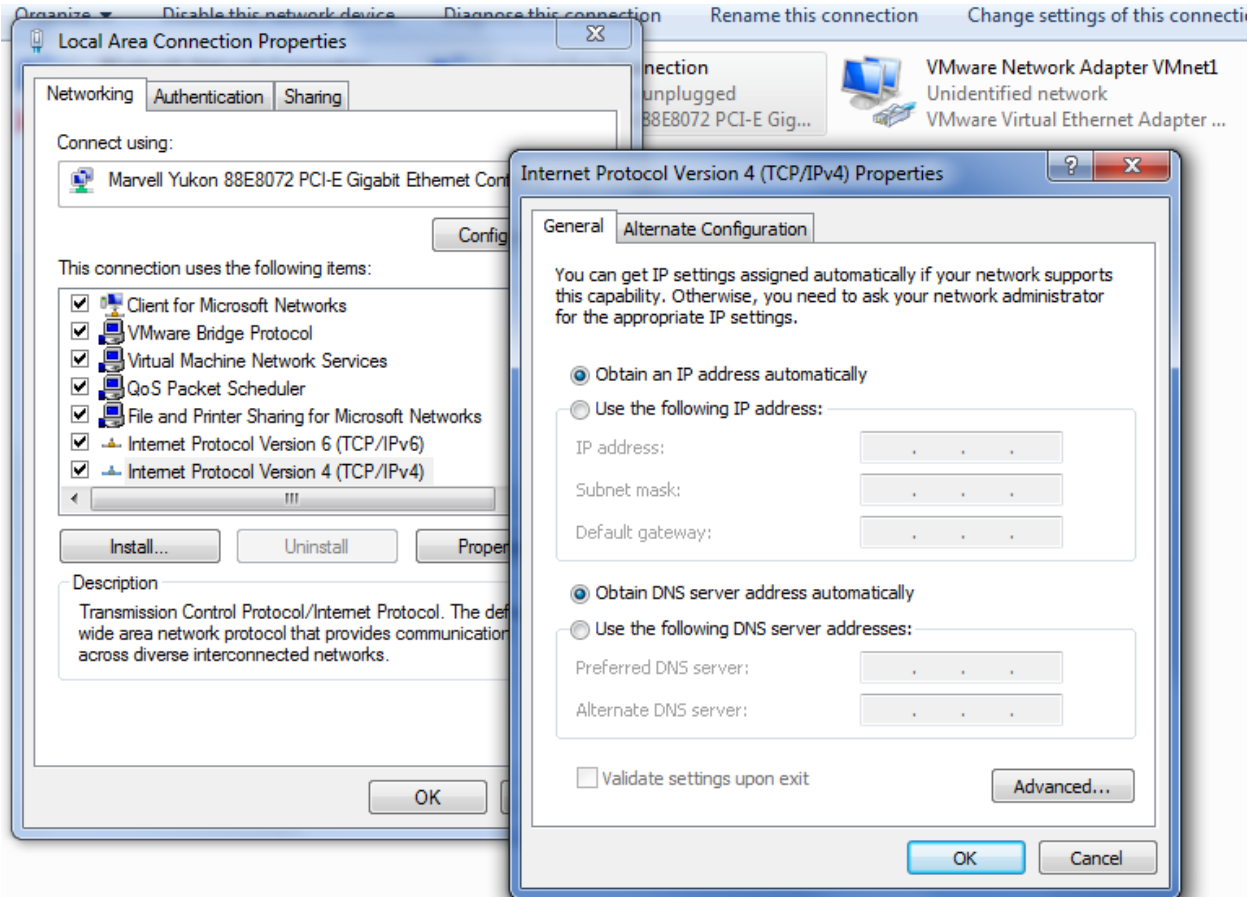
فنقوم بدخول علي أي Internet explorer كما في الشكل الآتي



عبد السلام صالح الراشدي

rfg

معاً ملاحظة ان نجعل كرت الشبكات يأخذ IP من DHCP



عبد السلام صالح الراشدي

وبعد ذلك يطلب منك إدخال اسم المستخدم وكلمه المرور بالنسبه اسم المستخدم في غالب تكون

admin اما بالنسبة للكلمة المرور فأحيانا 1234 وأحيانا كلمة admin في هذا الأक्स بوينت كلمة

المرور admin

بعد كتابة واسم المستخدم admin كلمة المرور admin تظهر لنا النافذة التالي

Basic Setup 192.168.1.1

خيارات

عدم الترجمة مطلقاً من اللغة الانجليزية الترجمة لا فهل تريد ترجمتها؟ الانجليزية

Setup

- Setup
- Wireless
- Security
- Storage
- Access Restrictions
- Applications & Gaming
- Administration
- Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Language

Select your language: English

Internet Setup

Internet Connection Type: Static IP

Internet IP Address: 10 . 0 . 0 . 99

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 0 . 0 . 2

DNS 1: 8 . 8 . 8 . 8

DNS 2 (Optional): 8 . 8 . 4 . 4

DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Network Setup

Router Address

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

URL Address: http://WRT610N.com

DHCP Server Setting

DHCP Server: Enabled Disabled

Start IP Address: 192 . 168 . 1 . 100

Maximum Number of Users: 50

IP Address Range: 192 . 168 . 1 . 100 to 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 8 . 8 . 8 . 8

Static DNS 2: 8 . 8 . 4 . 4

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Time Settings

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

Help...

EN 11:26 AM 2013/04/27

عبد السلام صالح الراشدي

سوف تظهر عدة قوائم كما في الشكل السابق سوف تتكلم على القوائم التي سوف نحتاج اليها في تكوين

هذا الشبكة والقوائم هي

Setup

تحتوي على عدة قوائم من أهمه **basic setup** التي من أهمه

Internet setup اذا كان لديك انترنت وتريد جميع الاجهازه المتصل بالاكسس بينت تدخل

على انترنت فتقوم بكتابه IP Address الجهاز الذي سوف يدخل على النت اما يدويا او عن طريق

DHCP

Network setup

فهي IP Address امتاع الاكسس بيونت وتستطيع تغييره

DHCP Server setup

وفيه يتم تفعيل او عدم تفعيل خدمة الحصول على IP Address من DHCP ايضا يتم تحديد المدى IP

Address الذي سوف يخدمه الاجهازه أي مثلا سوف يقوم بتحديد المدى IP Address يبدأ مثلا من

192.168.1.50 وينتهي 192.168.1.200

عبد السلام صالح الراشدي

كما في الشكل التالي

The screenshot shows the 'Basic Setup' page of a router's web interface. The browser address bar shows '192.168.1.1'. The page is in Arabic, with a navigation menu at the top and a sidebar on the left. The main content area is divided into sections: Language, Internet Setup, Optional Settings, Network Setup, DHCP Server Setting, and Time Settings. The 'Internet Setup' section is currently selected, showing 'Static IP' configuration. The 'Router Address' section shows the IP address '192.168.1.1'. The 'DHCP Server Setting' section shows the DHCP server is 'Enabled'. The 'Time Settings' section shows the time zone is '(GMT-08:00) Pacific Time (USA & Canada)'. The Windows taskbar at the bottom shows the system clock as 11:26 AM on 2013/04/27.

Setup

Setup | Wireless | Security | Storage | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Language

Select your language: English

Internet Setup

Internet Connection Type: Static IP

Internet IP Address: 10 . 0 . 0 . 99

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 0 . 0 . 2

DNS 1: 8 . 8 . 8 . 8

DNS 2 (Optional): 8 . 8 . 4 . 4

DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings
(required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Network Setup

Router Address

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

URL Address: http://WRT610N.com

DHCP Server Setting

DHCP Server: Enabled Disabled

Start IP Address: 192 . 168 . 1 . 100

Maximum Number of Users: 50

IP Address Range: 192 . 168 . 1 . 100 to 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 8 . 8 . 8 . 8

Static DNS 2: 8 . 8 . 4 . 4

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Time Settings

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

أما القوائم الثانية فهي **Wireless** وفيها مجموعة قوائم أيضا منها

Basic setup wireless

تتكون من جزأين جزءاً خاص IEE 802.11 A التي تستخدم كما ذكرنا سابقاً تردد 5 GHz

أما الجزء الثاني وهو الذي سوف نركز عليه فيخص IEE 802.11 G,B والذي يستخدم تردد 2.4 GHz

نستطيع من هذا القوائم تغيير اسم الاكسس بيونت من الاسم الافتراضي الي أي اسم نريده

أيضا نستطيع الغاء خاصية broadcast للاكسس بيونت حيث لن تظهر اسم الاكسس بيونت للاجهازه

المحيطة والشكل التالي بوضوح الصورة أكثر

Wireless

Setup

Wireless

Security

Storage

Access
Restrictions

Applications &
Gaming

Administration

Status

Basic Wireless Settings

Wireless Security

Wireless MAC Filter

Advanced Wireless Settings

Wireless Configuration

Manual WPA-PSK Protected Setup™

[Help...](#)

5GHz Wireless Settings

Network Mode:

Network Name (SSID):

Radio Band:

Wide Channel:

Standard Channel:

SSID Broadcast: Enabled Disabled

2.4GHz Wireless Settings

Network Mode:

Network Name (SSID):

Radio Band:

Wide Channel:

Standard Channel:

SSID Broadcast: Enabled Disabled

Save Settings

Cancel Changes

Wireless security

حيث يعتبر من أهم الأشياء التي يجب علينا القيام بها وهي حماية الألكسس بيونت من الدخول الغير مسرح به و باختيار نظام التشفير والحماية حيث كل شي شخص يريد الدخول علي الألكسس بيونت يجب التحقق منه عن طريق كلمة السر وبتالي حماية الشبكة من الدخول الغير مصرحة بيه

أيضا يتم فيها اختيار نوع التشفير مثلا Wep ,WPA WPA2 WPA personal WPA security enterprise

وسوف نختار في هذا المثال WPA 2 personal

Wireless

Setup Wireless Security Storage Access Applications & Administration Status
Restrictions Gaming

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

5GHz Wireless Security

Security Mode: Disabled

2.4GHz Wireless Security

Security Mode: WPA2-Personal

Encryption: WPA2-TKIP or WPA2-AES

Passphrase: abcd@2013

Key Interval: 3000 seconds

Help...

Save Settings

Cancel Changes



حيث يتم ادخال كلمة المرور التي من الافضل ان تكون معقدة وصعبة التخمين

Wireless Mac filter

حيث تعتبر أكثر أنواع الحماية وثوقا حيث يسمح فقط للأجهزة التي يتم تخزين MAC Address امتاعها في الأكسس بيونت بدخول والاتصال بالشبكة اللاسلكية فقل ان يتم الاتصال بالأكسس بيونت فان الأكسس بيونت تقوم بالبحث علي MAC Address الجهاز الذي يريد الاتصال به فاذا وجدا هذا MAC فسوف يسمح له بالاتصال بالشبكة .

لمن لا يعرف MAC Address فهو عنوان فريد للكروت الشبكات بحيث لا يتكرر هذا الرقم في جميع انواع

كراوات الشبكات في العالم ويتكون من 48 bit 24 للشركة المصنع 24 تعطي IEEE

Wireless

- Setup
- Wireless
- Security
- Storage
- Access Restrictions
- Applications & Gaming
- Administration
- Status

- Basic Wireless Settings
- Wireless Security
- Wireless MAC Filter
- Advanced Wireless Settings

Wireless MAC Filter

Access Restrictions

MAC Address Filter List

Enabled Disabled

Deny PCs listed below from accessing the wireless network.

Permit PCs listed below to access the wireless network.

Wireless Client List

MAC 01:	04 20 2C C9 83 0	MAC 17:	00 00 00 00 00 00
MAC 02:	00 0E 18 21 3C 4	MAC 18:	00 00 00 00 00 00
MAC 03:	0C 03 0F 4D 84 0	MAC 19:	00 00 00 00 00 00
MAC 04:	00 00 00 04 07 9	MAC 20:	00 00 00 00 00 00
MAC 05:	00 01 18 71 88 8	MAC 21:	00 00 00 00 00 00
MAC 06:	00 00 00 00 00 0	MAC 22:	00 00 00 00 00 00
MAC 07:	00 0C 82 98 79 8	MAC 23:	00 00 00 00 00 00
MAC 08:	00 00 00 00 00 00	MAC 24:	00 00 00 00 00 00
MAC 09:	00 00 00 00 00 00	MAC 25:	00 00 00 00 00 00
MAC 10:	00 00 00 00 00 00	MAC 26:	00 00 00 00 00 00
MAC 11:	00 00 00 00 00 00	MAC 27:	00 00 00 00 00 00
MAC 12:	00 00 00 00 00 00	MAC 28:	00 00 00 00 00 00
MAC 13:	00 00 00 00 00 00	MAC 29:	00 00 00 00 00 00
MAC 14:	00 00 00 00 00 00	MAC 30:	00 00 00 00 00 00
MAC 15:	00 00 00 00 00 00	MAC 31:	00 00 00 00 00 00
MAC 16:	00 00 00 00 00 00	MAC 32:	00 00 00 00 00 00

Save Settings

Cancel Changes



Administrations

ومن أهم قوائمها Management حيث نستطيع من خلالها تغيير اسم المستخدم وكلمة المرور حيث من المهم تغييرهم حتي لا يتسني لاحد الدخول علي الأكسس بيونت وتغيير اعدادتها لان كلمة المرور واسم المستخدم معلومة لجميع لأنها افتراضية

The screenshot displays the Linksys WRT610N router's administration interface. The browser address bar shows the URL 192.168.1.1/Management.asp. The page title is "LINKSYS by Cisco" and the firmware version is 1.00.00 B18. The navigation menu includes Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration, and Status. The Administration section is active, showing the Management page. The Management page is divided into several sections: Router Access, Local Management Access, Remote Management Access, Upnp, and Backup and Restore. The Router Access section includes fields for Router Password and Re-Enter to Confirm. The Local Management Access section includes checkboxes for Access via HTTP and HTTPS, and radio buttons for Access via Wireless (Enabled/Disabled). The Remote Management Access section includes radio buttons for Remote Management (Enabled/Disabled), checkboxes for Access via HTTP and HTTPS, radio buttons for Remote Upgrade (Enabled/Disabled), and a field for Allowed Remote IP Address. The Upnp section includes radio buttons for Upnp (Enabled/Disabled) and checkboxes for Allow Users to Configure, Allow Users to Disable Internet Access, and Internet Access. The Backup and Restore section includes buttons for Backup Configurations and Restore Configurations. The page footer shows the Cisco logo and the text "Save Settings" and "Cancel Changes".

آخر القوائم التي سوف نتكلم عليها هي **status**

وهي لا يتم فيها تكون أعداد ولكن تكون خاصة بعرض حالة ووضع الاكسس بيونت وتتكون من 3

قوائم

Router

وتعرض معلومات عن Router من حيث MAC Address الوقت الحالي لاكسس بيونت معلومات عن IP

Address من حيث

Internet IP address

Subnet mask

Default gatewayDNS

Status

- Setup
- Wireless
- Security
- Storage
- Access Restrictions
- Applications & Gaming
- Administration
- Status

- Router
- Local Network
- Wireless Network

Router Information

Firmware Version: 1.00.00 B18 Aug 16, 2008
Firmware Verification: 6e777e6306991f968cfd63824683acc
Current Time: Mon, 29 Apr 2010 03:45:24
Internet MAC Address: 00:23:69:14:C9:2F
Server Name : WRT610N
Host Name:
Domain Name:

[Help...](#)

Internet Connection

Connection Type: Static
Internet IP Address: 10.0.0.99
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.0.1
DNS1: 8.8.8.8
DNS2: 8.8.4.4
DNS3:
MTU: 1500

Refresh



Local network

وتحتوي بيانات على Ip Address الألكسس بيونت و subnet mask و Mac Address

ايضا تحتوي بيانات على DHCP من حيث التفعيل وعدم التفعيل وبداية ونهاية رنج IP Address

The screenshot displays the Linksys WRT610N router's status page. The page is titled "LINKSYS by Cisco" and "Simultaneous Dual-Band Wireless Router WRT610N". The firmware version is 1.00.00 B18. The page is divided into several sections:

- Status:** A navigation menu with options: Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration, and Status. Below this, there are sub-sections: Router, Local Network, and Wireless Network.
- Local Network:** This section displays the following information:
 - Local MAC Address: 00:13:89:14:C9:2E
 - Router IP Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
- DHCP Server:** This section displays the following information:
 - DHCP Server: Enabled
 - Start IP Address: 192.168.1.100
 - End IP Address: 192.168.1.149A button labeled "DHCP Client Table" is visible below this section.

The Cisco logo is visible in the bottom right corner of the page.

wireless network

وتحتوي بيانات علي كل من Access point , Name Mac Address , Mode ,

نوع واسم وعنوان الاكسس بيونيت ورقم القناة المستخدمة في عملية الاتصال

Status

[Setup](#) [Wireless](#) [Security](#) [Storage](#) [Access Restrictions](#) [Applications & Gaming](#) [Administration](#) [Status](#)[Router](#) | [Local Network](#) | [Wireless Network](#)

5G Wireless Network

MAC Address: 00:13:8F:14:C9:31
Mode: Mixed
Network Name (SSID): Backup_media
Radio Band: Wide - 40MHz Channel
Wide Channel: 26
Standard Channel: 26
Security: Disabled
SSID Broadcast: Disabled

[Help...](#)

2.4G Wireless Network

MAC Address: 00:13:8F:14:C9:30
Mode: Mixed
Network Name (SSID): LAB
Radio Band: Standard - 20MHz Channel
Wide Channel: N/A
Standard Channel: 1
Security: WPA2-Personal
SSID Broadcast: Enabled

الخاتمة

في نهاية هذا الكتاب أتمن من الله إن يفيد هذا الكتاب المسلمون جميعا وان تعم الفائدة الجميع وان أسف إذا حدث مني أي تقصير أو خطأ وأتمن من الله أن يساعدني في مواصلة تجميع وتوليف الكتب حتى يتسنى للقارئ الفهم الصحيح والبسيط لكل ما له علاقة بتقنية المعلومات وعلم الحاسوب وأخيرا اريد أن اشكر كل من كان له الفضل عليا في أي شيء وأي معلومة وأي مساعدة وأتمن إن يجزه الله عني كل خير والسلام علي خير خلق الله محمد صلي الله علي وسلم .