تقريب الشبكات اللاسلكية

تصدر كل شهر عربي عن موقع Wireless4arab.net

العدد الأول

المحرم 1434

تقرأون في هذا العدد

- نظرة علي AP 1240
- تقنية Cisco CleanAir
- انشاء Out door AP
- IEEE 802.11C
- تأمين الشبكات اللاسلكية بـ WEP
- برنامج CISCO WCS
- شهادة CWTS

نادر المنسي

مقدمة

السلام عليكم و رحمة الله و بركاته

في عام 2003 قرأت كتاب للمهندس محمد حمدي غانم عن لغة الفيجوال بيسك و الذي قام بترجمته و لقد حفزني هذا الكتاب – خصوصا مقدمته التي تعتبر "أم المقدمات " بالنسبة لمقدمات الكتب التي قرأتها في حياتي – للكتابة و لترجمة العلوم و اخترت مجال الشبكات بعدها ليكون مجال دراستي و عملي

و في عام 2007 بدأت أول كتاباتي بترجمة كتاب عن كابلات الشبكات سميته "هندسة و فن تمديد كابلات الشبكات " و ذلك عبر منتدي الواحة

و في عام 2009 بدأت بكتابة أول كلماتي عن الشبكات اللاسلكية بترجمة منهج CWTS

و في عام 2010 بدأت بالكتابة في مدونتي" تقريب علوم الشبكات للناطقين بلغة الضاد" و التي حولتها الي مدونة تخص فقط الشبكات اللاسلكية و بدأت بمشروع ضخم لترجمة منهج CCNA Wireless قد أنتهي منه نهاية 2012 ان شاء الله

و في عام 2011 دعاني المهندس أيمن النعيمي لكتابة مقال شهري في مجلته المباركة NetworkSet

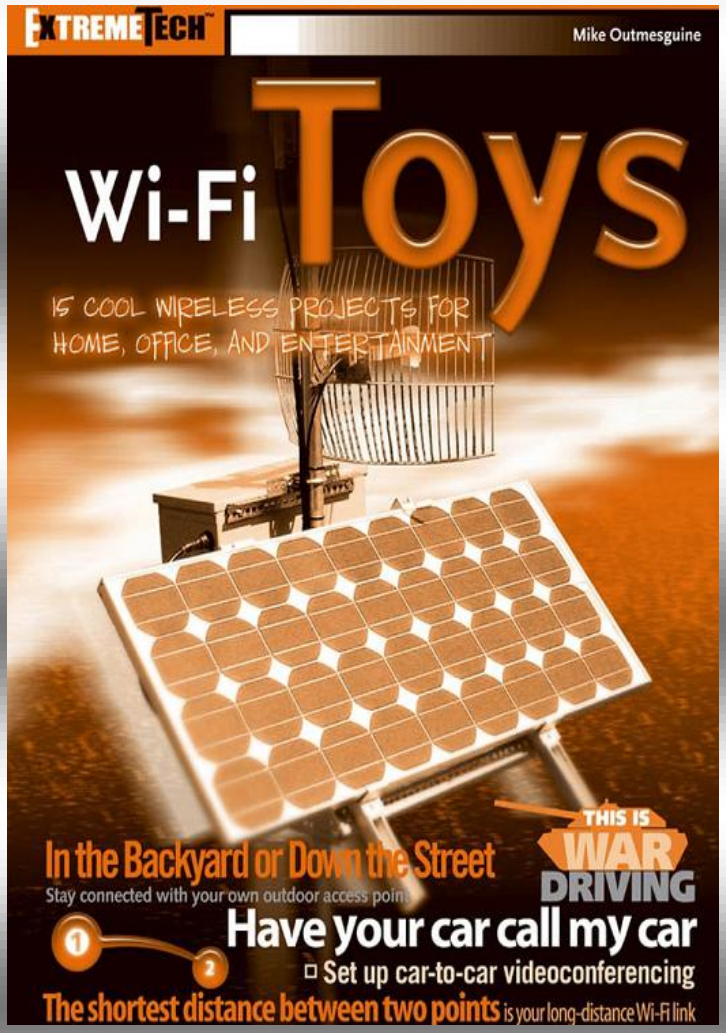
و الأن و بعد استخارة ربي قررت أن أبدأ بمشروع جديد شخصي بحت كمدونتي و هو عمل مجلة شهرية تختص بالشبكات اللاسلكية و هي لن تكون مجلة بالشكل المعروف بل كراسة شهرية أجمع فيها ما كتبته في المدونة بشكل مبوب و مرتب

و اعذروا تقصيري في التصميم و اللغة

أسأل الله أن يوفقنا للعمل بما يرضيه و لما يرضيه و أن يوفقنا للسداد في الإعتقاد و القول و العمل

نادر المنسي

2012-12-9



رحلتي مع كتاب

15 Cool Wireless Projects for Home Office and Entertainment

كتاب نوعا ما قديم فالإصدارة التي بين يدي الآن منذ سنة 2004 و هو زمن سحيق جدا بالنسبة لعمر الشبكات اللاسلكية الحديثة

و يشرح الكتاب بشكل عملي خمسة عشر مشروعا لاسلكيا تؤهلك عند اتمامها لتكون فنيا متمرسا في انشاء الشبكات اللاسلكية سواء كانت الشبكات تخص المنزل أو الشركات أو المؤسسات الكبيرة و الكتاب لا يخوض مباشرة في عمل المشروع بل يقوم اولا بتقديم نظرية مفيدة و مهمة و لا غني عنها

الكتاب يتكون من خمس أبواب كل باب يختص بفئة متشابهة من المشاريع و الباب مقسم الي 15 فصل كل فصل يختص بمشروع واحد

Part I: Building Antennas

الباب الأول يختص بمشاريع انشاء الهوائيات و كل ملحقاتها من الكابلات و الموصلات و اختبار عملها و يتكون هذا الباب من أربع فصول

Chapter 1: Building Your Own Wi-Fi Antenna Cable

الفصل الأول أو المشروع الأول فيختص بإعداد كابل الهوائي و يبدأ هذا الفصل بالكلام عن التردد و الطول الموجي و النطاقات الترددية غير المرخصة unlicensed و القنوات الترددية channel المسموح بها في هذا النطاق و لأن الكتاب قديم فهو يتكلم فقط عن النطاق الترددي 2.4 GHz ذو 11 قناة

يبدأ بعدها في الكلام عن انواع الأجهزة اللاسلكية مثل الأكسس بوينت و غيرها ثم يتكلم عن الكابل المحوري coaxial و الموصلات و ذلك لأنها المستخدمة في الشبكات اللاسلكية للربط بين الهوائي و هذه الأجهزة و يشرح طريقة حساب الفقد في الكابل

يبدأ بعدها في مشروعه و هو يتمثل في تجهيز كابل جديد و قبسه في موصل ليكون جاهزا لربطه بهوائي أو جهاز مع صور تبين مراحل عمل الكابل و المعدات المستخدمة فيه

الشبكات الخارجية اللاسلكية لها طبولوجية تختلف وعا ما عن الشبكات اللاسلكية الداخلية و هنا في هذا الفصل يقوم بشرح كيفية انشاء هذه الشبكة مع شرح مبسط عن بعض ما يخص هذه الشبكات مثل POE و Line of sight و تأريض الشبكات مع بيان لإعدادات IP

Chapter 9: Building a Solar-Powered Wireless Repeater

سيحاول هنا الكاتب ايجاد وسيلة أخري لتوفير الطاقة لمعدات الشبكة اللاسلكية و ذلك باستخدام الطاقة الشمسية و يقوم بشرح وحدات الخلايا الشمكسية و كيفية عملها و معدات تحويل الطاقة المترددة و المستمرة و كيفية تركيب الخلايا و الهوائيات و اتصال الخلايا بأجهزة الشبكة

Chapter 10: Creating a Free Wireless Hotspot

سيتيح هذا الفصل فهم طريقة عمل شبكة انترنت لاسلكية مثل تلك المخصصة في المقاهي و المطارات مع توسيعها و طريقة استخدام بعض البرمجيات التي تتحكم في هذه الشبكة مثل NoCat و هي برمجيات قديمة تشبه حاليا الميكروتيك

Chapter 11: Playing Access Point Games

هنا سيحول الكاتب الشبكة اللاسلكية الي متعة بجعلك قادرا علي توسيعها عبر اتصالها بأكثر من أكسس بوينت علي مسافات

Part IV: Just for Fun

هذا الباب سيأخذك الي ما هو بعد الممكن ليجعلك تصنع مشاريع لاسلكية غير اعتيادية

Chapter 12:Wi-Fi Your TiVo

TIVO جهاز يشبه مسجلات الفيدو أو DVD و يقوم هنا الكاتب بشرح كيفية اتصاله لاسلكيا بالشبكة اللاسلكية ليصبح و كأنه سيرفر ملتيميديا

Chapter 13: Create a Long-Distance Wi-Fi Link

سنستطيع مع هذا الفصل توسيع الشبكة اللاسلكية لتغطية مساحات أكبر و ذلك باستخدام هوائيات مخصصة و تقليل فقد الإشارة و سيقوم الكاتب بتعريفك ببعض المفاهيم الرياضية مثل Fresnel Zone و التي ستطبقها عمليا و نظريا و رياضيا في هذا الفصل

Chapter 14: Deploy a Car-to-Car Wireless Video Link

هذا الفصل من اروع فصول هذا الكتاب لأنه دمج عدة تقنيات فيه أهمها هي نقل الصوت و الفيديو عبر الشبكة اللاسلكية ثانيها النقل المتحرك للإشارة اللاسلكية الحاملة للفيديو بين اكثر من جهة متحركة

Chapter 15:Making a Dynamic Wireless Digital Picture Frame

هنا سيتخطي الكاتب الممكن و يختم كتابه بمشروع رائع بعمل شاشة لاسلكية بمكونات لابتوب قديم , الأمر لا يحتاج سوي الشجاعة فقط ☺

في النهاية وجب أن نعرف أن الكتاب يصدر عن مؤسسة Wiley Publishing و من تأليف Mike Outmesguine و هو متخصص في الإلكترونيات و عمل لعشر سنوات في القوات الجوية الأمريكية كمتخصص في الكترونيات طائرات B-52 و حضر حرب الخليج ثم تفرغ لتأسيس و إدارة مؤسسة TransStellar, Inc.

اصنعها بنفسك

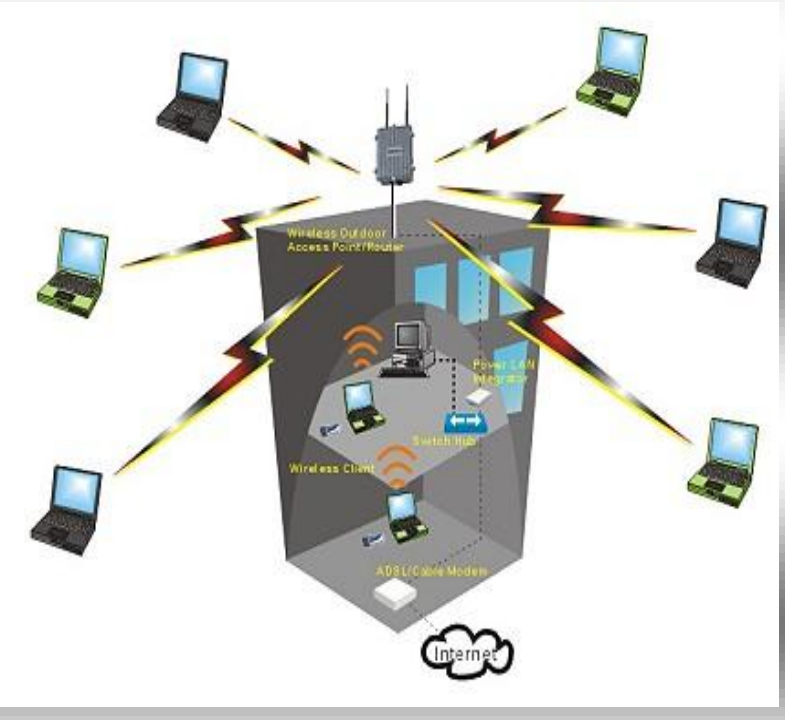
عمل أكسس بوينت خارجية

ما رأيكم أن نقوم بعمل محطة لاسلكية منخفضة التكاليف بدلا من مد الكابلات التي تتعرض للتلف نتيجة الحرارة في الصيف و الأمطار في الشتاء و حوادث القطع المتعمد , الأمر لن يحتاج الكثير فسنقوم بإيهام الأكسس بوينت العادية أنها أكسس بوينت خارجية و سنهديها صاري و غطاء بلاستيكي و هوائي و دعها هي تقوم بالباقي

سنختار أكسس بوينت عادية جدا تعمل بنفس المعيار المنتشر في منطقتك و يعتبر 802.11b أشهر هذه المعايير لكن لابد أن يكون هوائي الأكسس بوينت قابل للتركيب و الإزالة removable antenna و ذلك لتوصيل الهوائي به و يفضل أن يكون الأكسس بيونت معه معدات POE , و سنتستخدم جهاز DWL-900AP+ من ديلينك و هو جهاز قديم نوعا ما و أظنه متوفر و قياسي

قبل أن تقوم بتركيب الأكسس بوينت ستقوم بإعداده ليقوم بمهمة النشر الخارجي للإشارة و هذه الإعدادت تتمثل في اسم الشبكة SSID و الحماية و التشفير و اعداد القنوات و اعدادات IP و تستطيع أن تستخدم طريقة المعالج ان لم يكن معد مسبقا يفضل في البداية أن تقوم بتغيير كلمة سر المدير الإفتراضي للجهاز ثم قم بترقية نظام تشغيل الأكسس بوينت

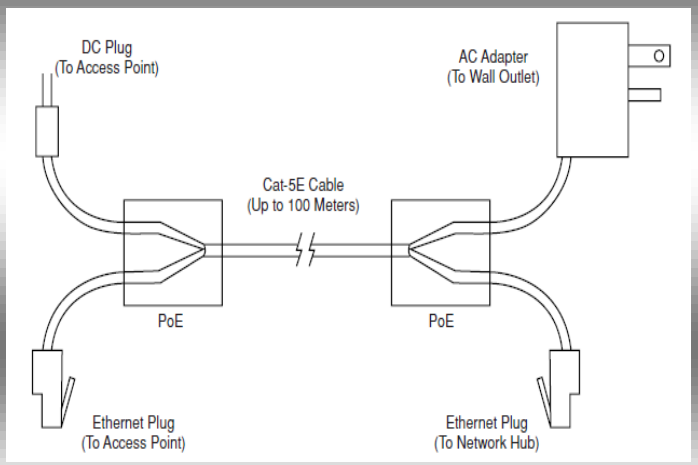
بعدها ستقوم بعمل حماية و تشفير لشبكتك بالشكل الذي تحبه و أبسطه هو استخدام WEP و تستطيع زيادة تأمينها باستخدام WPA و باستخدام Media Access Control (MAC) filtering و ضبط اعدادات LAN بالشكل الذي يتناسب مع شبكتك و تبقي اعدادات ثانوية قد تراها مهمة مثل امكانية رؤية SSID و الطاقة و السرعة ثم قم بحفظ إعدادات و تصديرها و كل تلك الخطوات أصبحت شائعة بالشكل الذي يجعل سردها اضاعة للوقت ثم بعدها قم باختبار عمل الأكسس بوينت مع لابتوب



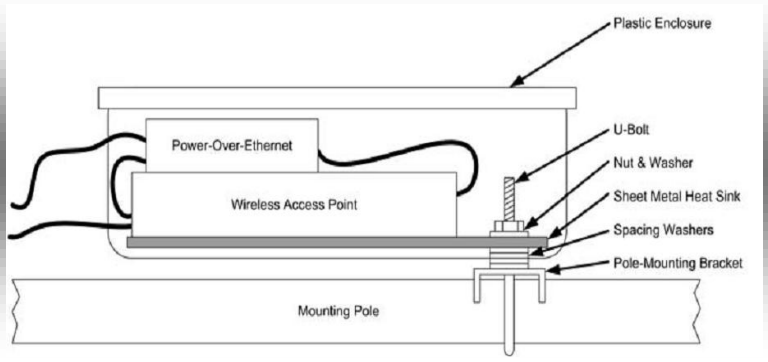
حل مشكلة الطاقة

و لها أكثر من وجه للتوصيل اسهله هو استخدام كابل من السويتش يوفر الطاقة و البيانات الي الأكسس بوينت مباشرة كما هو الحال مع سويتشات سيسكو 3750 و منها و هو المستخدم هنا و هو استخدام وحدتين POE أحدها لتجميع الكهرباء مع البيانات و تكون بالقرب من مصدر الطاقة و البيانات تخرج 48 VDC و أخري بجوار الأكسس بوينت لتوزيع الكهرباء و البيانات بقيمة 5 VDC مع اتصالهم عبر كابل ايثرنت عادي لا يتعدي 100 متر

و تكمن فكرة POE هو ان كابل الإيثرنت يتكون من ثماني اسلاك أربع منها تحمل البيانات و الأربع غير مستعملة و سيستخدمها POE لنقل الطاقة و يعتبر بروتوكل IEEE 802.3af هو المسؤل عن انشاء هذه التقنية

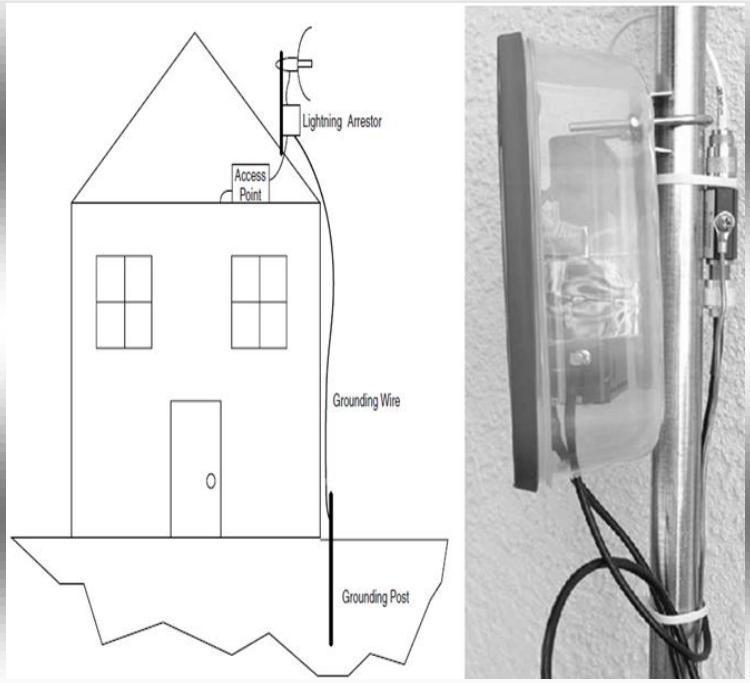


و سيتم وضع الأكسس بوينت مع POE في صندوق معدني أو بلاستيكي لحماية الجهاز من العوامل الجوية علي أن تراعي طبعا فتحات لتوصيل كابلات POE و الهوائي



الحماية من صواعق البرق

صواعق البرق أحد أكبر المخاطر التي تعاني منها الشبكات اللاسلكية و ذلك لأن البرق يقوم بتأيين الهواء حول الهوائي مما ينقل الكهرباء من الهواء اليه ثم الي أجهزة الشبكة ليدمرها تماما و في حال ضرب الهوائي نفسه فإنه سيدمره أيضا و لذلك يتم استخدام مانع صواعق lightening Arrestor ثم تأريضها بكابلات نحاسية قطر 8 gauge و تركيبها



يجب أن تراعي نوع الكابل المتصل بالهوائي و طريقة التوصيل و شكل الموصل و ستجد كل ذلك علي جهاز التأريض و مواصفات تأريضه مع اتمام تغليفه كي لا يتأثر بالعوامل الجوية

بروتوكولات و معايير

IEEE 802.11C

يعتبر هذا البروتوكول التعديل اللاسلكي للبروتوكول المعروف IEEE 802.D الصدمة الثانية أن IEEE 802.D هو الإسم البروتوكولي من IEEE لبروتوكول STP Spanning Tree Protocol

و يستخدم هذا البروتوكول من قبل مطوري أجهزة الأكسس بوينت حيث لوحظ في بداية عمل الشبكات اللاسلكية أن معايير 802.11 تختص فقط باتصال الأجهزة بالأكسس بوينت و غير قادرة علي تحديد كيفية الإتصال علي نطاق أوسع بين ألأكسس بوينت و بعضها لدعم عمليات Roaming مثلا

اذن فالمعيار اللاسلكي IEEE 802.11c هو النسخة اللاسلكية من IEEE 802.1D الخاص بشبكات الإيثرنت و المعروف اصطلاحيا بـ STP و الذي طور بشكل فعال في 2004 و كمان أن STP 802.1D يقوم بمنع Loops في الشبكة و استخدام أقصر مسار فإن 802.11C يختص بهذا الأمر في الشبكات اللاسلكية و تسمي هذه العمليات Wireless Bridging أو Access Point Bridging

و لأن الكلام انتهي في هذا البروتوكول الي هنا فلنشرح شيء عن مجموعة بروتوكولات STP

فمثلما يتم مع باقي بروتوكولات الشبكات فإن منظمة IEEE تقوم بعمل بروتوكول عام يصلح للتعامل مع كل الشركات ثم تقوم كل شركة بتطوير في هذا البروتوكول أو استحداث بروتوكول شبيه و يؤدي نفس المهمة و قد لا يتعامل فقط الا مع منتجاتها

Cisco Proprietary

قامت سيسكو بتطوير أكثر من بروتوكول لمواجهة Loop مثل PVST و +PVST و +Rapid PVST , فأما بروتوكول Per-VLAN spanning tree protocol (PVST) فيقوم بالعمل من خلال VLAN واحدة متعاملا مع كل منها كوحدة و شبكة مستقلة مستخدما بروتوكول سيسكو القديم ISL trunking protocol و الذي يسمح بانتقال البيانات بين VLANs , و أما بروتوكول Per-VLAN spanning tree protocol plus (PVST+) فقام بدعم بروتوكول IEEE 802.1Q trunking و هو يعمل بنفس طريقة PVST الا أنه غير مدعوم من أي أجهزة غير سيسكو , و أما Rapid per-VLAN spanning tree protocol (rapid PVST+) فهو مبني علي معيار IEEE 802.1w لأنه أسرع في استجابة الشبكة له convergence من STP الأساسي 802.1D

IEEE Standards

معايير IEEE أعرق و اقدم من معايير سيسكو و يستطيع أي مصنع أي يبني عليها و هي STP و RSTP و MSTP

فأما معيار Rapid spanning tree protocol (RSTP) فقد قدم في سنة 1982 كتعديل لـ (802.1D standard) و هو من اسمه يقدم convergence اسرع و من بعد 2004 تم دمجه في STP اي عندما تجد كلمة STP تأكد أنها RSTP

و أما Multiple STP (MSTP) فهو يمكن STP من التعامل مع أكثر من VLAN و قد كان لسيسكو دور في تطوير هذا البروتوكول

شهادات لاسلكية

تغييرات في شهادة أخصائي مبيعات الشبكات اللاسلكيةCWTS

تعتبر شهادة أخصائي الشبكات اللاسلكية Certified Wireless Technology Specialist ®CWTS من مؤسسة CWNP من الشهادات التي تؤهل حاصبها للعمل في مجال مبيعات الشبكات اللاسلكية و رغم أن مؤسسة CWNP تجهز هذا المنهج كأساسيات غير ملزمة لتراكاتها التي تبدأ من المستوي CWNA الا أن هذا المنهج كاف جدا لفهم الكثير جدا عن الشبكات اللاسلكية التي تعمل علي معايير IEEE 802.11

و لقد بدأت هذه الشهادة باسم Wireless # برقم PW0-50 ثم قامت في 2009 بتغيير جذري في الشهادة و تم تسميتها بالإسم الحالي CWTSبرقم PW0-70 ثم قامت بتغير الهدف من الشهادة بجعلها مخصصة لأخصائي مبيعات و ما قبل المبيعات في الشبكات اللاسلكية

في 2012 تم تغيير آخر في الشهادة برقم PW0-71 و سيكون امتحانها متوفر في نوفمبر 2012 و سينتهي التعامل مع منهج PW0-70في نهاية 2012

علي عكس التغيير السابق في الشهادة و الذي كان جذريا حيث نقل الشهادة من شهادة عامة في الشبكات اللاسلكية الي شهاذة خاصة بالواي فاي فقط ., فإننا نجد هذا التغيير الجديد لا يتعرض للخطوط العريضة للمنهج و إنما عدل قليلا في نسبة كل باب في الإمتحان كذلك تعديل بسيط في مسمي الباب الأخير كما تري

Subject Area	% of Exam
Wi-Fi Technology, Standards, and Certifications	25% ~~15%~~
Hardware and Software	20% ~~25%~~
Radio Frequency (RF) Fundamentals	20%
Site Surveying and Installation	10%
Applications, Support, and Troubleshooting	15%
Security & Compliance Monitoring	10% ~~15%~~
Total	100%

التغييرات زصلت لبعض ملامح المنهج و التفاصيل البسيطة فعند تصفحك للمنهج الجديد و مقارنته بالقديم نجد الآتي

تم إضافة طبولوجية BSA, IBSS في باقي الطبولوجيات الموجودة في الواي فاي مثل ,BSSID, SSID, BSS, ESSو ذلك في فصل خصائص تكنولوجيا الواي فاي

وجدت CWNPأن كل الكتب التي تطرحها الشركات بخصوص منهج CWTS أنهم يضيفون بعض التنويهات و الشرح عن بروتوكولات OSI فقامت بإضافته الي المنهج

كانت بعض الكتب تتجاهل حذف CWNP لطبولوجيات الوايرلس

مثل WWAN WPAN WLAN WMAN و تضعها في الكتب التي تشرح CWTA و الذي كان موجودا في الشهادة القديمة wireless # فقامت المؤسسة بالتراجع عن هذها الحف و أضافته في في المنهج الجديد

تم حذف الأجزاء الخاصة بأنواع مستقبلات الإشارة اللاسلكية CF, SD Devicesو ذلك لقدمها و تم استبدالها بجزء عن كروت Half Mini PCI

تم إضافة جزء عن الهوائيات الخارجية و الداخلية الخاصة بربط ألأكسس بوينت

تم إضافة أجزاء عن وحدة الوات و أجزاء عن كيفية قياس الإشارة RSSI , SNR

تم استيراد بعضا من المفاهيم الموجودة في المنهج العلوي CWNA الخاص بخصائص الإشارة مثل Frequency Wavelength Amplitude Phaseو المعوقات مثل Free space path loss

تم تنظم جزء Interference و تحديده بالتداخلات الناتجة عن أجهزة الواي فاي و الناتجة عن أجهزة لا تنتمي للواي فاي

تم حذف الأجزاء الخاصة بالطيف المنتشر مثل OFDM و حذف الجزء الخاص بـHR/DSSS

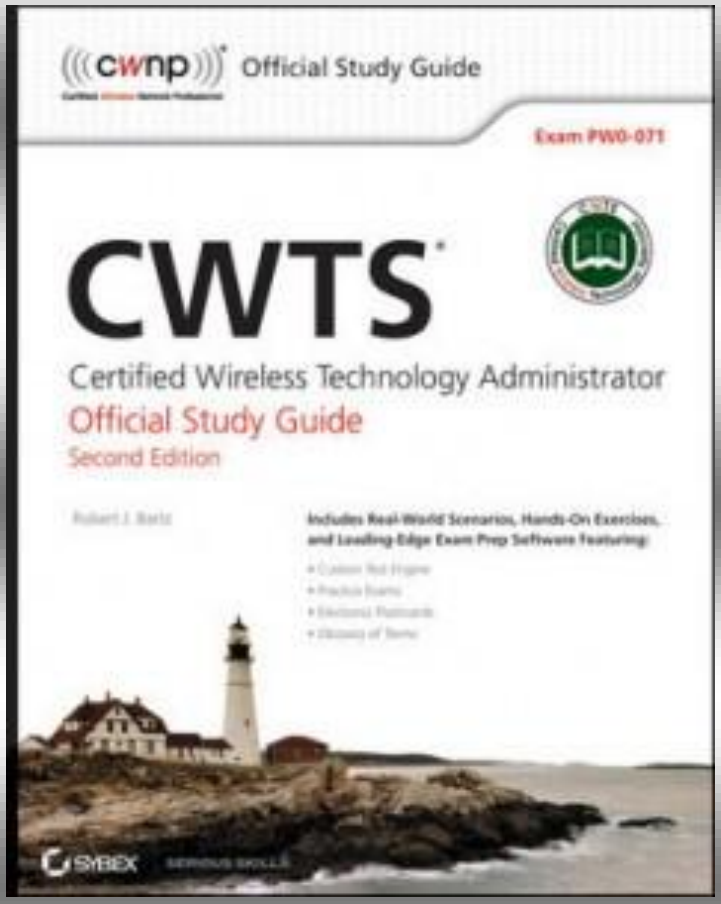
تم اضافة جزء خاص بمراقبة الشبكات اللاسلكية و إدارتها

تم اضافة معلومات عنinfrastructure redundancy

تم حذف الجزء الخاص بـDevice upgrades

تم حذف فصل كامل كان يتكلم عن عوائق تركيب أجهزة الشبكات اللاسلكية

و هذا هو الكتاب المعتمد لشرح هذا المنهج



أمان الشبكات اللاسلكية

WEP

و تقنية أمنية encryption algorithmهي خوارزمية تشفير بيانات و تم IEEE 802.11للشبكات اللاسلكية التي تعمل طبقا لمعيار اطلاقها في سبتمبر من عام 1999 كوسيلة لحماية خصوصية البيانات التي تنتشر عبر الشبكات اللاسلكية و يعتبر data confidentiality بذبك أو و سيلة لتأمين الشبكات اللاسلكية

و علي الرغم من أن عرش هذه التقنية الأمنية قد هدد بالزوال بعد ظهور المعيار 802.11i و تطويره من قبل Wi-F Alliance بإسم Wi-Fi Protected Access (WPA) الا أن الكثيرين لازالوا يستخدمونه في أجهزتهم بل ان المصنعون لازالوا يضعونه كأحد وسائل الحماية في أنظمتهم رغم أنه سهل الكسر و الإختراق

الرزمة اللاسلكية

802.11 Header		
BSS ID	Initialization Vector (IV)	Destination Address
Logical Link Control		
Sub Network Access Protocol Header		
Data		
Integrety Check Value (CRC32)		

تشفير WEP

لتشفير Encryption البيانات اللاسلكية يستخدم WEP خوارزمية تدقيق stream cipher تسمي Ron's Code 4 RC4)لتوليد بيانات مشفرة Key system و يعتبر RC4 خوارزمية متماثلة symmetric algorithm أي أن الكود المستخدم في التشفير عند المرسل هو نفسه المستخدم في فك التشفير عند المستقبل

و ينقسم كل Key system الي جزئين أولهما هو WEP Key و هو رقم التشفير الذي تدخله في الجهاز و الثاني هو initialization vector (IV) و هو رقم عشوائي خاص بعملية التشفير و طوله هنا 24 bit و يتم اضافته بشكل عشوائي الي WEP Key لتمويه Key System الذي ينقسم الي ثلاث أنوع و هم 64-bit WEP و 128-bit WEP و 256-bit WEP

فأما 64-bit WEP الذي يسمي أيضا (WEP-40) لأنه يحتوي علي 10 byte سداسي عشر hexadecimal , 0-9) A-F) كل بايت يحتوي علي 4 bits اي في النهاية 40 bit يتم اضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل الي 64-bit WEP

لكن الكثير من الأجهزة تجبرك علي إدخال خمس بيانات من النوع ASCII و هي بدورها تحول كل بيان حرف أو رقم الي ثمانية بت لتصل في النهاية الي 40 bit

فأما 128-bit WEP الذي يسمي أيضا (WEP-104) لأنه يحتوي علي 26 byte سداسي عشر hexadecimal (0-9 , A-F) كل بايت يحتوي علي 4 bits اي في النهاية 104 bit يتم اضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل الي 128-bit WEP

و أما النظام الثالث يسمي 256-bit WEP system و يسمي أيضا (WEP-232) لأنه يحتوي علي 58 byte سداسي عشر hexadecimal (0-9 , A-F) كل بايت يحتوي علي 4 bits اي في النهاية 232 bit يتم اضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل الي 256-bit WEP

و يتم التوزيع طبقا لنفس العملية الحسابية

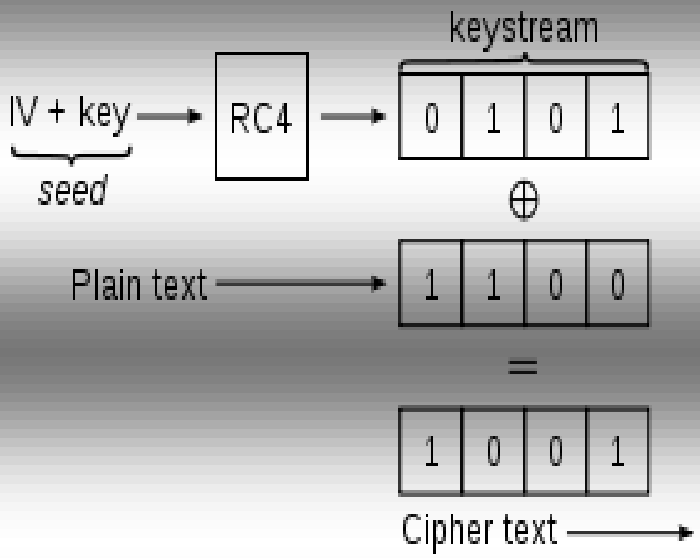
(HEX × 4 bits = WEP key) + IV = 256-bit WEP System

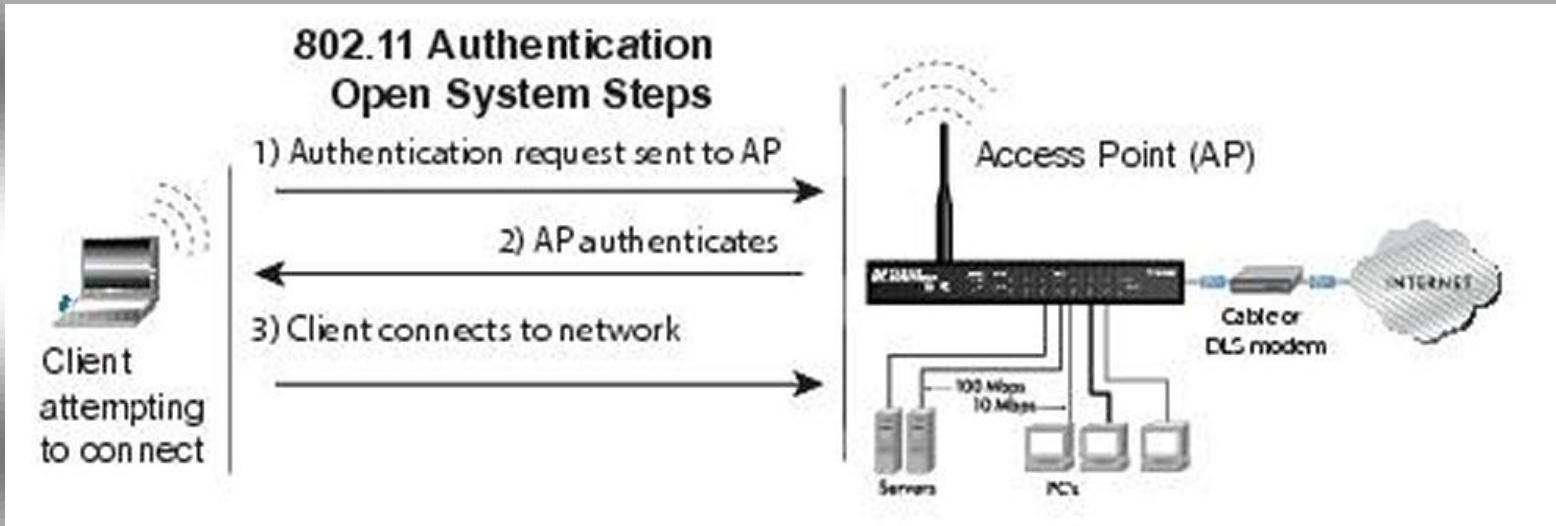
و يتم جمع IV مع Key ثم اضافة خوارزمية تدقيق خوارزمية تدقيق stream cipher تسمي RC4 لينتج Keystream ثم جمعها بطريقة XOR مع plain text ليخرج لنا في النهاية كود التدقيق

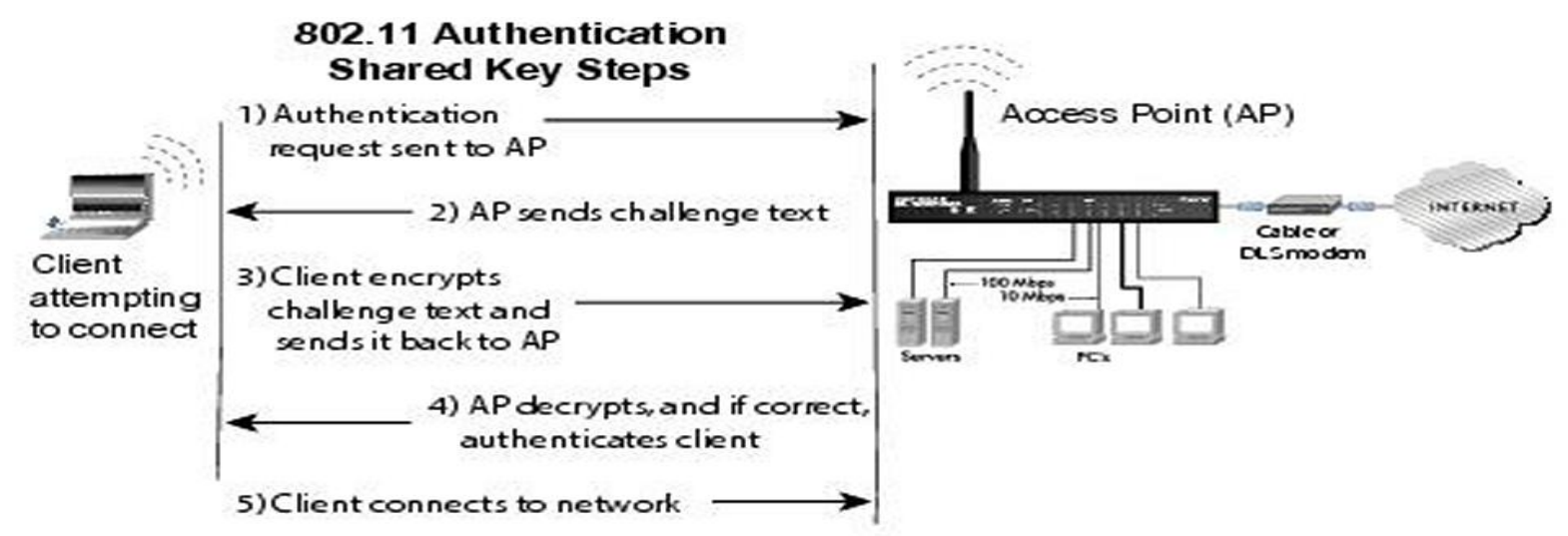
توثيق WEP

يتم استخدام نوعين من التوثيق Authentication مع WEP هما Open System و Shared Key

أما Open System authentication فلا يحتاج مستقبل الإشارة أن أي ترخيص لإستقبالها و يستطيع أي أحد أن يدخل الي الشبكة عبر الأكسس بوينت بما يسمي عملية الإرتباط Associate و يستخدم هنا WEP فقط في تشفير البيانات المرسلة كي لا تري من الأشخاص خارج الشبكة



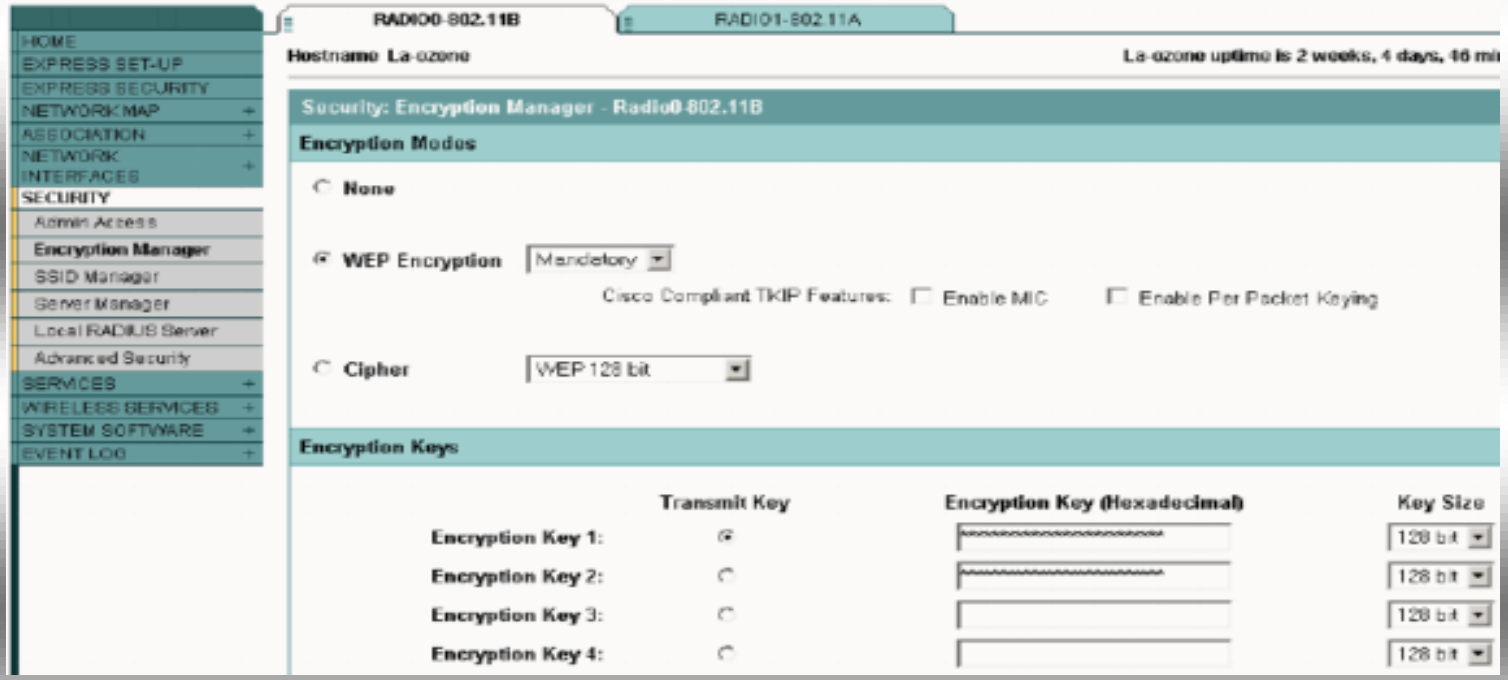




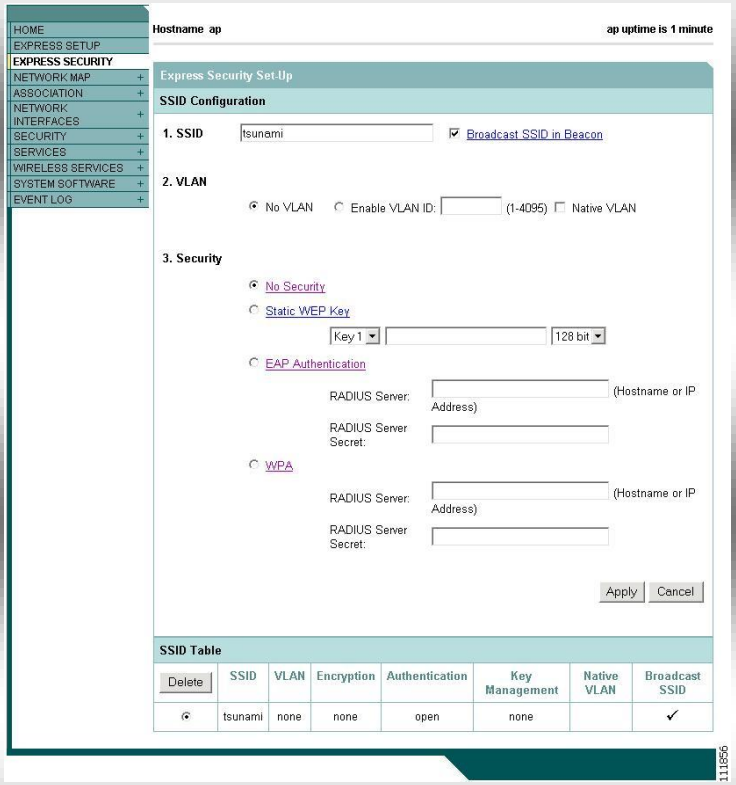
و أما Shared Key authentication فيتم استخدام مفتاح WEP للتوثيق و التشفير علي أربع خطوات أولها يقوم الكلاينت بإرسال طلب توثيق لدخول شبكة الأكسس بوينت يقوم بعدها الأكسس بوينت بالرد برسالة غير مشفرة تسمي clear-text challenge يقوم الكلاينت بعد استلام الرسالة بتشفيرها باستخدام مفتاح WEP ثم يرسلها للأكسس بوينت يقوم الأكسس بوينت بعد استلام الرسالة ثم اذا نجح في فك تشفيرها decrypt باستخدام مفتاح WEP فيتم السماح للجهاز بالولوج للشبكة

Shared Key authentication أوثق و أكثر أمانا فأنت مخطيء ان كنت تظن أن هناك فرق بين الإثنين في مستوي الأمان و أن فكلا من الطريقتين سهل اختراقها أو أن أحدهما فقط أسهل من الأخري فباستخدام برامج التقاط و تحليل الإشارة لرسالة clear-text challenge ايابا و ذهابا من الكلاينت أي قبل و بعد التشفير يتم معرفة خوارزمية التشفير و فك رموزه أي أن في كل الأحوال WEP ضعيف و قد قمت بنفسي –نادر– بكسر أكسر من شبكة لاسلكية تستخدم هذا النظام و بسهولة

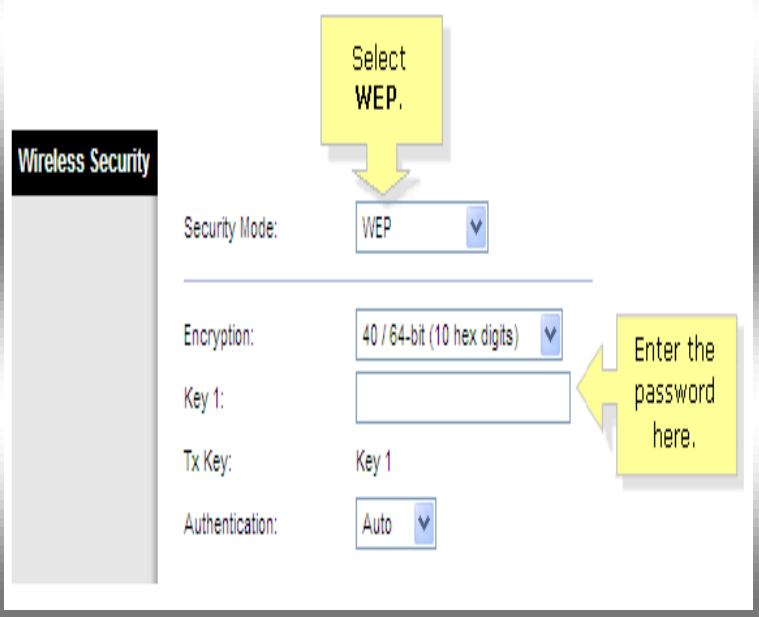
و هذه هي صفحة إعداد WEP لتأمين الأكسس بوينت من سيسكو



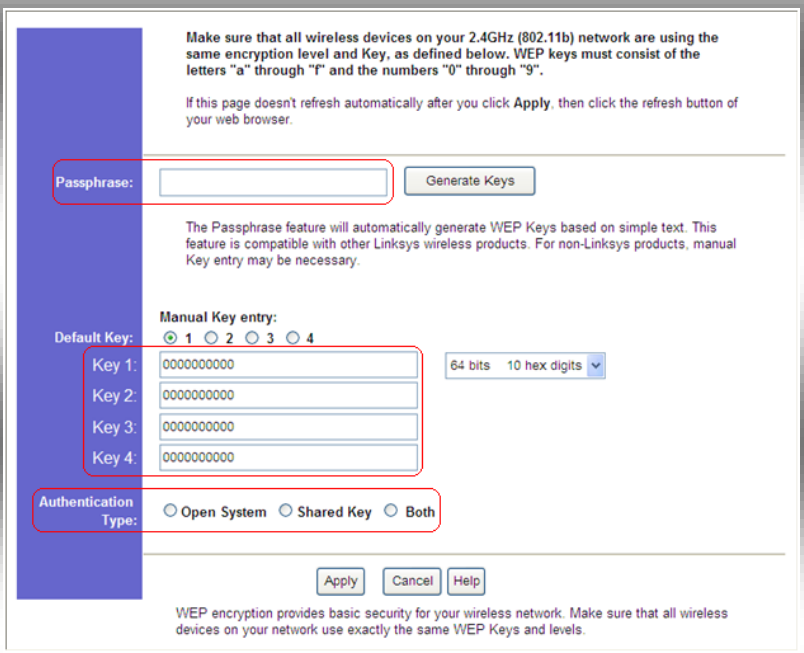
و هذه أكسس بوينت أخري من سيسكو و تري اختلافات في طريقة العرض



و كما تري فانك تستطيع توليد أكثر من مفتاح لإستخدامهم و كل مربع نصي يحتوي علي مفتاح يسمي Slot و هو مهم هنا لفهم طريقة عمل الكود في نظام CISCO IOS الذي سنشرحه في الخطوة التالية بإذن الله تعالي , و هذه هي جزء من صفحة أكسس بوينت من لينكسيس



و في بيئة لاسلكية كاملة منم لينكسيس يستطيع الأكسس بوينت بنفسه بإقتراح توليد مفاتيح كما تري في هذا النوع



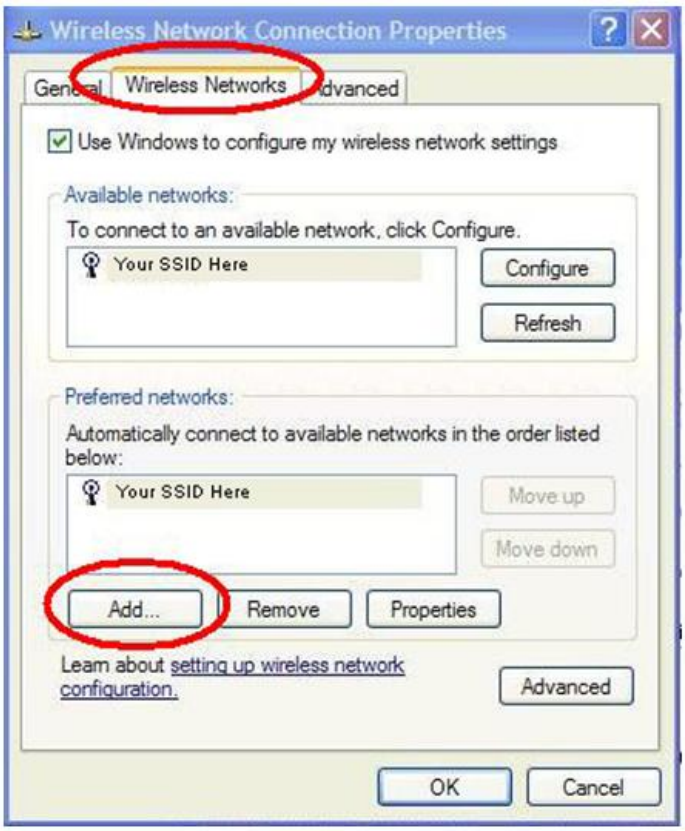
و المثال التالي يوضح كيفية تأمين الأكسس بوينت من نوع Aironet 1200 من سيسكو و سنقوم إعداده و الدخول عليه مثل أي راوتر أو سويتش من سيسكو

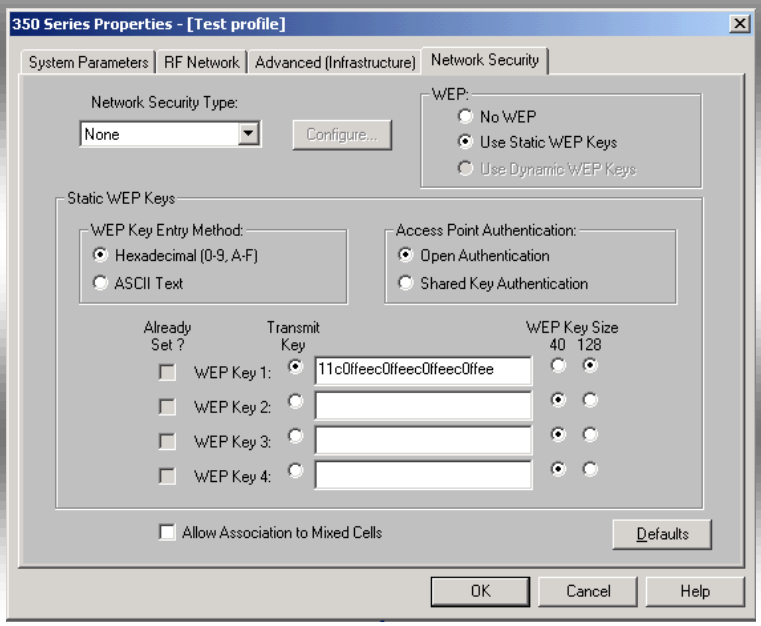
و في وضع الإعداد conf t سنقوم بالدخول الي الواجهة interface dot11radio 0 و التي تعني هنا أننا سنقوم بتشفير الإتصال اللاسلكي عبر 802.11b الذي يعمل بالتردد 2.4 GHz في حين لو أردت أن تقوم بتشفير الإتصال اللاسلكي عبر 802.11a الذي يعمل بالتردد 5 GHz ستقوم بالدخول الي الواجهة interface dot11radio 1

سنقوم بتوليد المفتاح الثالث من نوع WEP بطول 128 bit اي 26 حرف و هم 12345678901234567890123456 رقم أو حرف سداسي عشر و ذلك في الشبكة VLAN 22

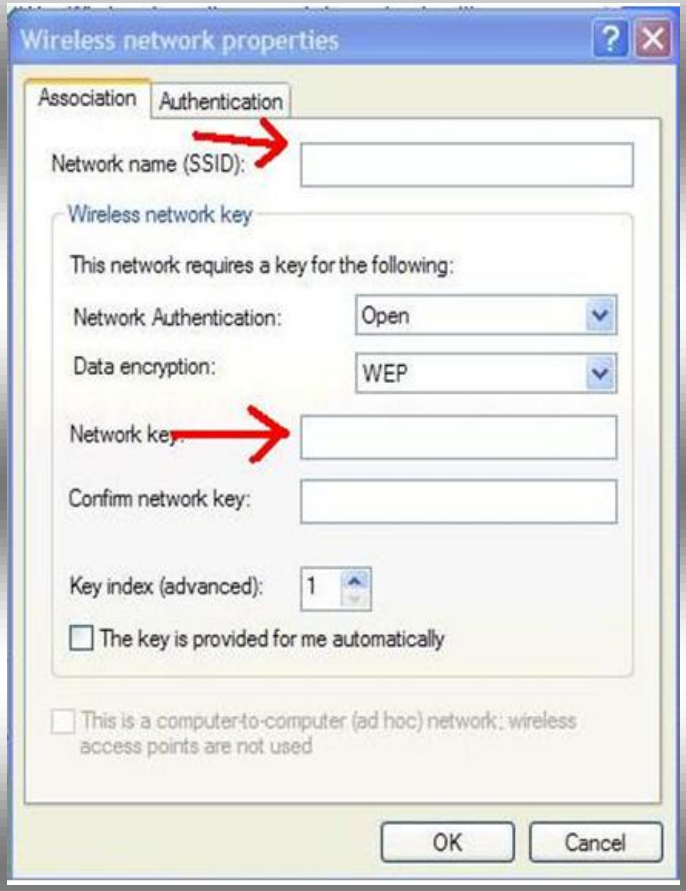
```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-ssid)# end
```

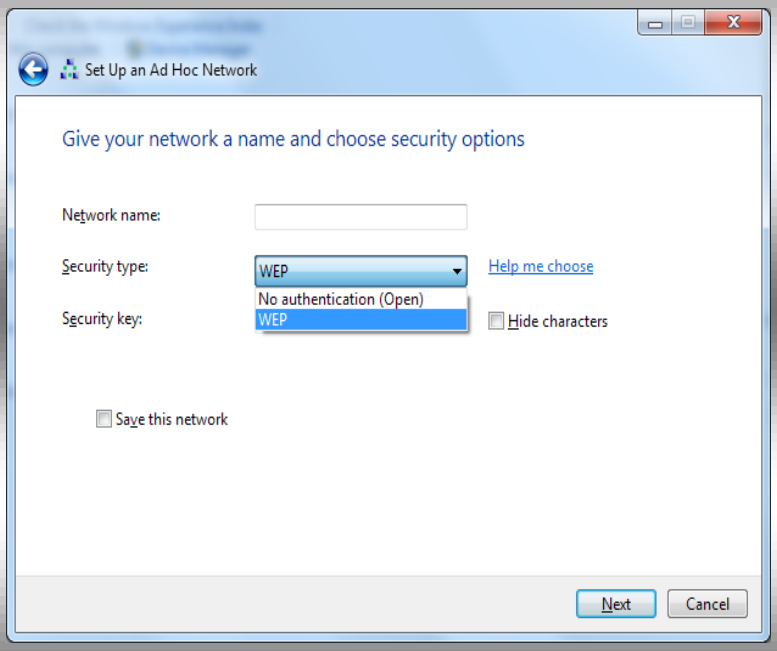
و في Client و اذا كنت تستخدم برنامج Aironet Client Utility (ACU). من سيسكو فستكون هذه الصفحة التي ستضبط بها الاعدادات لإلتقاط الوايرلس





أما اذا كنت ستقتصر علي WZC و هو البرنامج الإفتراضي في ويندوز فستكون الطريقة في ويندوز سفن بالدخول الي Setup a New Connection or Network ثم هكذا





و في اكس بي ستدخل علي *Network Connections* ثم هكذا

و في لينكس فأحيانا يكون لكل شيخ – توزيعة – طريقة حتي أنه في التوزيعة الواحدة مثل UBUNTU يختلف التطبيق ما بين KDE و Unity و Gnome فما بالك بالتوزيعات المبنية علي كور واحد مثل Debian المبني عليها backtrack و GOS و Sabily و غيرها و ما بالك بالإختلاف بين التوزيعات المختلفة مثل Ubuntu و Fedora بل ان تحديث و ترقية اللينكس من اصدارة الي أخري قد يغير من برنامج الإعداد اللاسلكي

و تستطيع الإعداد من خلال سطر الأوامر terminal

```
sudo ifdown wlan0
sudo ifconfig wlan0 essid TheCafe key abcabc1234
sudo ifup wlan0
```

و عموما هذا برنامج الإعداد في اوبنتو و الذي تدخل عليه من Network Setting

عيوب WEP

طرق التشفير التي تعتبر بدائية تستخدم خوارزمية خطية Linear Checksum أي أن تسلسل التشفير معكوس تسلسل فك التشفير بالضبط كأنك تقوم بتغليف علبة هدايا و هذه هي أسوأ عيوب WEP

كذلك في طرق التشفير يستخدم مفتاح أساسي Key و في WEP يتم اضافة بيانات عشوائية IV اليه كي لا يستطيع أحد فهم طريقة التشفير و تسمي البيانات العشوائية 24 bit و رغم أن هذه بيانات عشوائية يصعب توقعها الا أنها بيانات أي plain text مقروءة بالإضافة الي أنها ليست بالطول الكافي فيمكن تكرار نفس IV بعد ارسال 5000 باكت و لهذا عند استخدامك برنامج air crack في لينكس توزيعة دبيان و ما يشبهها تلاحظ أنك عند استخدام أمر كسر الباكت aircrack-ng أنه ينبهك الي الإنتظار بعد قراءة 5000 باكت أو مضاعفاتها اذا لم يكن قادرا بعد علي الكسر و عموما لا يستغرق هذا الأمر كله أكثر من نصف ساعة

```
                              Aircrack-ng 1.1

                    [00:00:06] Tested 1705777 keys (got 156 IVs)

   KB    depth   byte(vote)
    0  255/256   1B(    0) 78(    0) 7A(    0) 7B(    0) 7C(    0)
    1   33/ 34   C0(  512) DF(  256) 04(  256) 06(  256) 07(  256)
    2  110/  2   6B(  256) C5(    0) C9(    0) CC(    0) CE(    0)
    3   76/  3   8C(  256) 8E(  256) 96(  256) 98(  256) 9B(  256)
    4    1/  4   66(  768) 81(  512) E1(  512) 75(  512) FD(  512)

Failed. Next try with 5000 IVs.
```

و يعتبر أول من أثبت امكانية كسر WEP هو العالم الإسرائيلي Adi Shamir بمساعدة آخرين و هم Scott Fluhrer, Itsik Mantin في August 2001 أي لم يكن WEP قد أتم عامه الثاني بعد ثم تباري العلماء و المتخصصون بعدهم ببهدلة WEP و كسره في أقل وقت

كذلك بمجرد معرفة WEP Key فإنك تستطيع ولوجها و مشاركة الآخرين بنفس KEY علي عكس بعض تقنيات التشفير الأخري التي حتي و إن عرفت Key فلابد من وسيلة لتوثيق دخولك الشبكة

تخطي العيوب

تم تطوير WEP في السنوات الأخيرة و ادخال تحسينات عليه من قبل Agere Systems و ذلك عبر تخطي عيوب IV و سمي بعدها باسم WEP Plus الا أن ظهور WPA قد حد من انتشاره

كذلك ظهر تحسين آخر سمي بـ Dynamic WEP و هو مزج بين تقنيتي 802.1X و EAP Extensible Authentication Protocol و قام بتعيير دوري في WEP Key و لكن هذا التحسين حصري فقط لشركة 3COM

برمجيات لاسلكية

CISCO Wireless Control System

الفائدة الأساسية لأجهزة الكنترولر في الشبكات اللاسلكية هو إدارة و متابعة أجهزة الأكسس بوينت التي قد يصل عددها الي المئات و هنا لن نستطيع أن نتحكم في هذه الأجهزة بكنترولر واحد و سنحتاج لتوزيع أكثر من كنترولر و هنا تعود مشكلة عدم المركزية في إدارة الكنترولر و لحل هذا الأمر يتم استخدام سيرفر خاص بإدارة الشبكات اللاسلكية من سيسكو يسمي CISCO Wireless Control System اذن فهو أحد أدوات سيسكو لإدارة الشبكات اللاسلكية

و لدي سيسكو بعض البرمجيات الأخري مثل

Cisco Configuration Assistant (CCA)

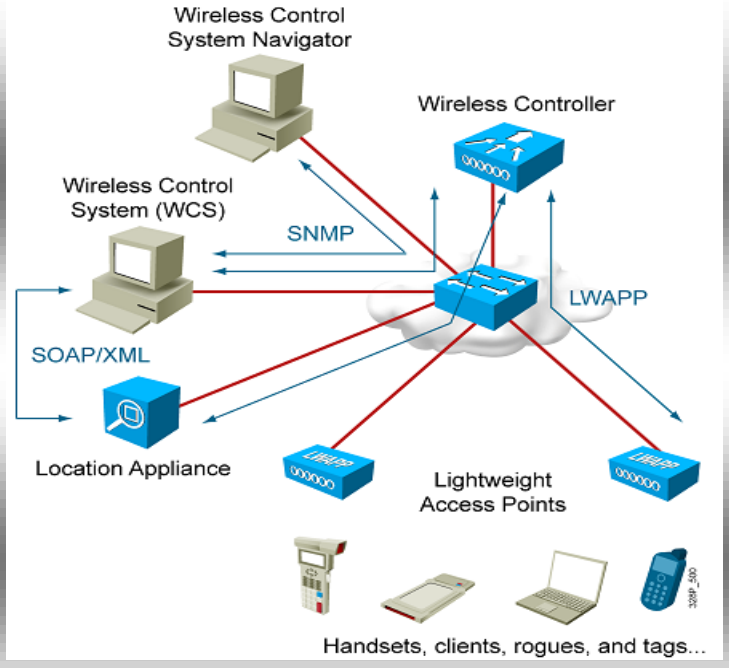
Cisco Wireless Control System

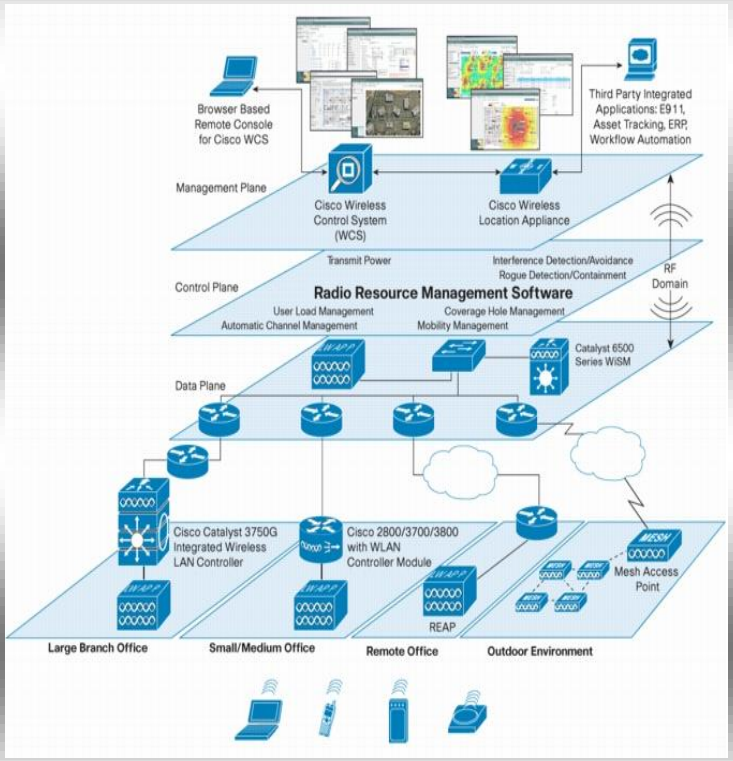
Cisco Wireless Control System Navigator

Cisco Wireless Location Appliance

Network Control System

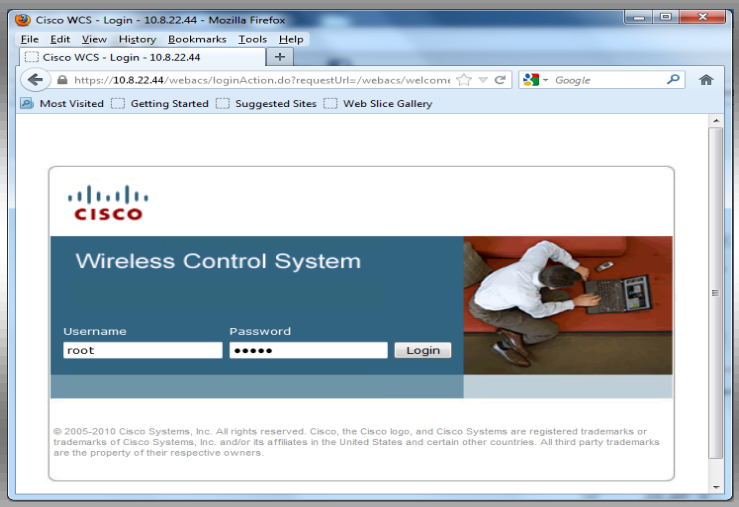
Cisco Prime Network Control System Series Appliances





و هو برنامج يتم تحميله علي سيرفرات تعمل علي ويندوز 2003 أو Linux Red Hat لإدارة العشرات من أجهزة الكنترولر التي تدير بدورها مجتمعة المئات من الأكسس بوينت و في الشبكات الكبري العملاقة يتم التحكم في أكثر من WCS بواسطة برامج أخري تسمي Cisco Wireless Control System Navigator و التي تدير ما يقرب من 30,000 اكسس بوينت

و يعتبر WCS برنامج تعتمد إدارته للشبكة اللاسلكية علي واجهة ويب تشبه تلك المستخدمة في الكنترولر أو SDM و يستطيع أن يدير ما بين 500 الي 2500 أكسس بوينت طبقا لنوع الرخصة التي يدعمها



تحميل و إعداد WCS

تتواجد نسخ WCS علي نمطين أحدهما يخص ميكروسوفت و الآخر يخص لينكس بتوزيعة ريد هات سيرفر فأما نسخة ويندوز فتحتاج ويندوز سيرفر علي الأقل 2003 سيرفر مع امكانيات جهاز تناسب السيرفر و أما نسخة لينكس فهي المعتمدة في الشبكات الكبري و لذلك فلابد أن يكون السيرفر الذي ستنزل عليه النسخة ذات امكانيات معقولة لسيمح بالتحكم في 300 أكسس بوينت عبر 250 كنترولر

و لم أحب أن أنقل لكم مواصفات الهاردوير للجهاز مفصلا لأن النسخ تتغير و يتغير معها متطلبات الجهاز و يفضل أن تتابعها بنفسك من علي موقع سيسكو www.cisco.com/g/wireless علما بأن نسخة الويندوز هي التي تدعم في امتحان و منهج ccna wireless

و للحصول علي WCS فلابد أن يكون لديك حساب علي سيسكو ثم تقوم بالدخول الي الصفحة المخصصة للبرنامج و تستطيع أن تستخدم نسخة دعائية من سيسكو لإدارة 10 أكسس بوينت لمدة شهر

و لأن WCS يعتمد علي مزيج من بيئة Apache Web Server و بروتوكول Network Management Protocol SNMP و الجافا فإنه لابد من السماح للبورتات التي تخص هذه التطبيقات في الفايروول او الراوتر و الجدول التالي يبين هذه البورتات

من الأشياء المهمة أيضا هو عدم تحميل برمجيات أو تفعيل خدمات تعطل هذه البورتات فنجد مثلا أن هناك مشاكل عند عمل WCS علي جهاز به IIS لأنه يقوم بتأمين الإتصال عبر تعطيل البورت 80

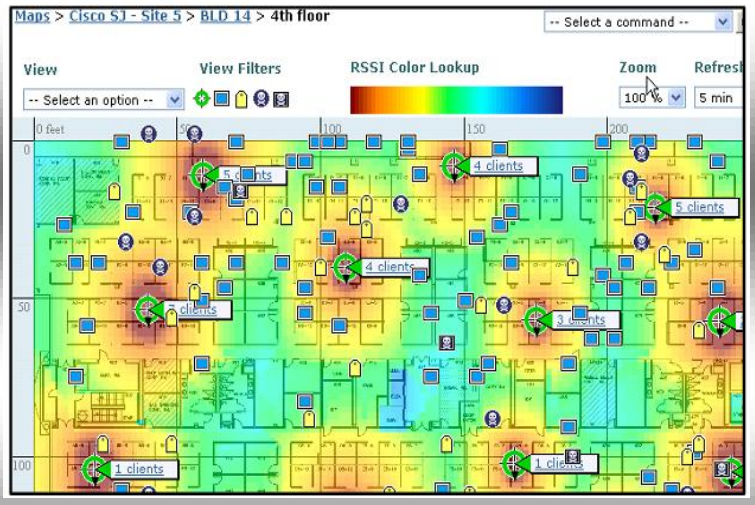
و لدي سيسكو رخصتين لبرنامج WCS هما Cisco WCS و Cisco WCS Location فأما Cisco WCS **فيقوم** بتصميم و تخطيط و إدارة و مراقبة و صيانة الشبكات اللاسلكية و أما Cisco WCS Location فيقوم بتعقب أجهزة الأكسس بوينت و بيان حالة الترددات الراديوية في الشبكة اللاسلكية و توفير المعلومات التي تخص أجهزة الشبكة اللاسلكية

Port Name	Port Number
Advent Net	2000
Database	1315
FTP	21
HTTP Connector	8456
HTTP Connector Redirect	8457
HTTP	80
HTTPS	443
RMI	1299
TFTP	69
Trap	162
Web Container	8009

أنواع WCS

يتم تقسيم أنواع WCS طبقا لعدة عوامل فعند تقسيمها طبق للخصائص الإدارية المدمجة في البرنامج فإن لدينا نوعان من WCS أحدهما WCS Base و الآخر WCS Base + Location

و كذلك يتم تقسيم WCS طبقا لنوع الرخصة التي حمل علي أساسها و هي خمس رخص تسمي WCS SKU Families Five كل رخصه لها خصائصها من حيث عدد الأكسس بوينت التي يدعمها و هل ستدعم العمل علي سيرفر واحد Single-Servere License أو رخصة متعددة Enterprise License و هذه الرخص هي التالية



	License	50	100	200	500	1000	2000	2500	Total
Single Server	WCS-APBASE 50	50							50
	WCS-APBASE 100		100						100
	WCS-APBASE 500				500				500
	WCS-APLOC 50	50							50
	WCS-APLOC 100		100						100
	WCS-APLOC 500				500				500
Enterprise	WCS-ENT-1000		100	200 x 2	500				1000
	WCS-ENT-2500				500 x 3	1000			2500
	WCS-ENT-10000 Includes Cisco WCS Navigator					1000 x 2	2000 x 4		10.000
	WCS-ENT-50000 Includes Cisco WCS Navigator							2500 x 20	50.000

Single Server Licenses:

- Up to 500 APs, one license file per PAK
- Available as Cisco WCS base or Cisco WCS location
- License families WCS-STANDARD-K9 and WCS-LOC-UPG-K9 support 50,100, 500 APs; license family WCS-WLSE-UPG-K9 supports 50, 100, 500, 1000 and 2500 APs

Enterprise Licenses:

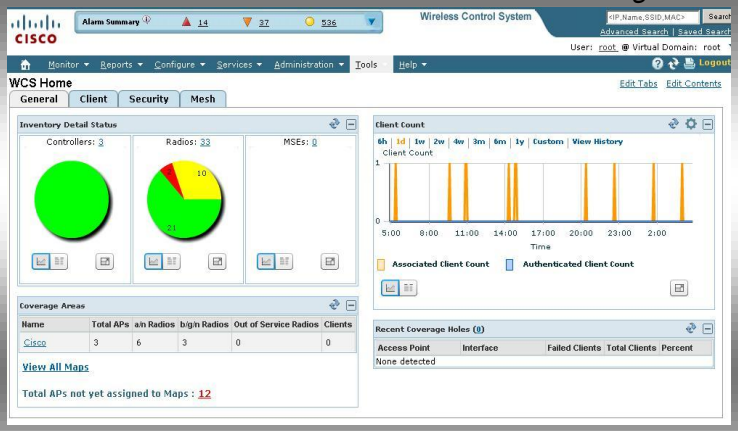
- For 500 or more APs, multiple license files linked to a single PAK certificate, deployable on one or multiple servers
- Always includes location Cisco WCS Navigator included in 10,000 and 50,000 versions
- Cisco WLC code 4.1 and later required

و لزيادة فاعلية فيتم استخدام جهاز خاص لهذا الأمر هو CISCO Location Server و هذا الجهاز يتم ربطه مع WCS و هذه مقارنة بين الثلاث طرق لاستخدام WCS

Features	Benefits
Cisco WCS with Location + Cisco Wireless Location Appliance	
Real-time tracking Up to 2500 clients simultaneously View a store location history RF fingerprinting for high accuracy (<10 meter 90%; <5 meter 50%)	Asset management Inventory management Network modeling & capacity planning Security Third-party API
Cisco WCS with Location	
On-demand tracking Single device RF fingerprinting for high accuracy (<10 meter 90%; <5 meter 50%)	Rogue location Device tracking Troubleshooting
Cisco WCS Base	
On-demand tracking Single device "Closest AP" for basic location	Easily determine device proximity Understand WLAN associations

Cisco Spectrum Intelligence

يتم فتح WCS باستخدام وضع IP في المتصفح لتخرج لنا شاشة البداية مثل هذه



CISCO WCS Base

يقوم هذا الإصدار بالأساس بمراقبة أجهزة الأكسس بوينت و التحكم فيها و كشف وجود الأجهزة الدخيلة و ذلك عبر واجهة مرئية و مخططات تبين المناطق التي فيها مستوي شدة الإشارة و تستطيع من هذا الإصدار إدارة و إعداد كل الأجهزة في الشبكة مثل الكنترولر و الأكسس بوينت و اصدار التقارير الخاصة بها

Location + CISCO WCS Base

هو إصدار يحمل نفس مواصفات الإصدار WCS Base إلا أنه يزيد عليه بخصائص تعقب أماكن الأجهزة بميزات أكبر حيث يقوم بتعقب الأجهزة التي توجد في حيز الشبكة و استخدام مستشعرات محللات الطيف CISCO Spectrum Expert Sensor حيث يقوم بتعقب هذه الأجهزة بعد طرق هي RF Closest AP و RF Triangulation و RF Fingerprinting كل منها يتفاوت في طريقة التتبع و مدي فاعليته

و هذه الصورة تبين استخدام Location علي خرائط WCS

فأما القائمة Configure فتحتوي علي خيارات لإضافة أجهزة الكنترولر و الأكسس بوينت

و اما القائمة Administrator فتحتوي علي إعدادات الولوج للسيرفرو التي تستطيع تغييرها من Administrator>Logging , كذلك تستطيع تعديل الولوج باستخدام AAA و ذلك من خلال الخيار الفرعي لإضافة مستخدم Administrator>AAA> Add user أو تعديل جروبات من Administrator>AAA>Groups , و لمشاهدة المستخدمين الذي دخلوا الي السيرفر Administrator>AAA> User>Audit

من الأشياء الجميلة أيضا في القائمة Setting هي امكانية اعداد السيرفر لإرسال بريد الكتروني في أحداث معينة مثل دخول أو خرو أو تغير في الشبكة أو غيرها و ذلك من هنا Administrator>Setting>Mail Server

و اما التبويبات فهي General و Client و Security و Mesh و AP و Tags

فأما General فيعطي معلومات ع التغطية و عدد Client

و أما Client فيعطينا معلومات عن أجهزة الأكسس بوينت التي بهه عدد أجهزة مرتبط بها و كذلك معلومات عن هذه الأجهزة

و أما Security فيعطينا بيانات عن الأجهزة المخترقة للشبكة او غير المسموح بها في حيز الشبكة

و أما Mesh فيختص ببيانات مثل SNR لنقاط الربط بين الأجزاء الأساسية للشبكة

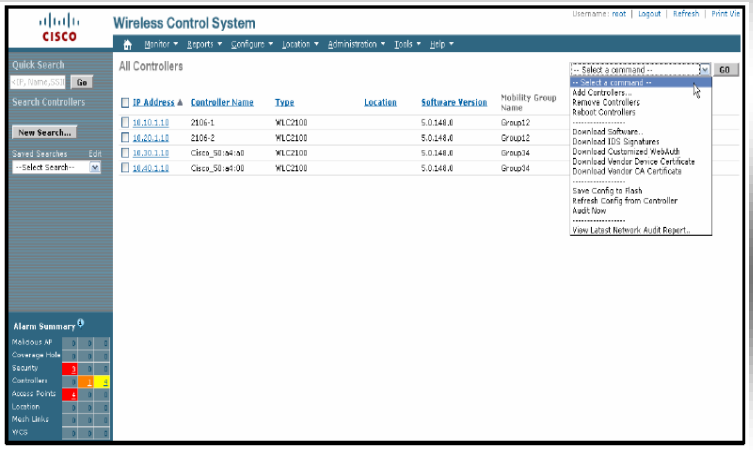
أهم شيء بعد فتح البرنامج هو إدخال رخصة البرنامج و ذلك في السطر العلوي Help\licensing و بدون هذه الخطوة لن تستطيع أن تدير أو تدرج اي كنترولر في البرنامج

خيارات WCS

عند فتح واجهة WCS فإننا نري عدة تبويبات و قوائم موضوعة بشكل أفقي **فأما القوائم فهي Monitor و Report و Administration و Configure و Mobility و Tools ثم Help** , و لكل هذه القوائم خيارات أخري ثانوية

إضافة الكنترولر الي WCS

لإضافة اجهزة الكنترولر الي WCS سيتم استخدام القائمة Configure و التي من خلالها ايضا تستطيع ان تدير أجهزة الأكسس بوينت المرتبطة بها , قم بالذهاب الي Configure>Controller و ستجد قائمة Select Commandاختر منها Add Controller ثم GO



ستظهر لك صفحة قم بكتابة بيانات الكنترولر كما تراها مثل IP و Subnet , كذلك تستطيع أن تضيف أكثر من كنترولر في المرة الواحدة و ذلك بإستخدام ملفات CSV , و بنفس الطريقة تستطيع أيضا التعامل مع الأكسس بوينت

تقنيات لاسلكية

Cisco® CleanAir™

في الشبكات اللاسلكية التي تستخدم ترددات مجانية مشتركة ISM تتشارك الأجهزة اللاسلكية جميع المدي الترددي و لا أفضلية لشبكة أو جهاز أو نظام علي آخر فقد تري فرن المايكروويف يعمل في نفس النطاق الترددي الذي يعمل عليه الراوتر اللاسلكي و يتشارك معهم أيضا نفس النطاق الهاتف اللاسلكي Cordless Phone و هنا تحدث التداخلات و التي قد تؤثر علي انتقال الإشارة عند اتحاد القناة الترددية و هو ما يسمي co-channel interference بالضبط كأنك تقوم بوضع أكثر من جهاز علي سويتش عدد منافذه قد تتعدي عدد هذه الأجهزة مما يجعل حتمية فصل جهاز عن الشبكة ليتصل الآخر

و لمراقبة هذا الطيف الترددي يتم استخدام تقنية محلل الطيف الذكي Spectrum intelligence (SI) و التي تعمل علي مراقبة الأجهزة اللاسلكية التي تطلق موجات لاسلكية في نطاق الشبكة و ذلك يتم عبر استخدام برمجيات أو أجهزة تحليل الطيف spectrum analyzers

و في الشبكات اللاسلكية تزداد أهمية محلل الطيف حيث أنه يقوم تحديد مصادر الإشارات الغير مرغوب فيها و التي مصدرها أجهزة لا تعمل في شبكات الواي فاي و عمل حماية تلقائية للشبكة Self Healing

في عام 2011 قامت سيسكو بخطوة غير مسبوقة و هي تطوير تقنية تضاهي عمل محلل الطيف و هي تقنية CleanAir هي بإختصار تقنية تجعل الشبكة قادرة علي كشف monitoring التداخلات الراديوية Radio interference و ذلك عبر دمج شريحة داخلية built chipsets في الأكسس بوينت و التي تجعل هذا الجهاز قادرا تلقائيا علي مراقبة المحيط الراديوي للأكسس بوينت و

كشف مصدر التداخلات و كأنه محلل طيف مدمج spectrum analyzer في الأكسس بوينت , هذه التقنية لم تضعها سيسكو في كل أجهزتها بل بعض أجهزة الأكسس بوينت و التي من المعروف استخدامها في الشبكات غير الصغيرة أو المنزلية

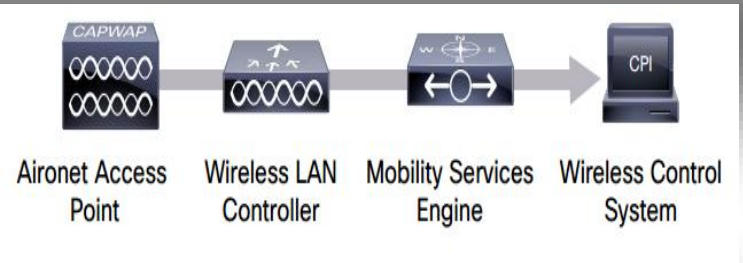
Spectrum Analysis Engine (SAgE)

و قد قامت سيسكو بتطوير خط كامل من الأكسس بوينت يسمي Aironet 3500 series مدعم بشريحة الكترونية خاصة لهذا الغرض ASIC (application-specific integrated circuit) chipset قادرة علي تجميع و تحليل الطيف اللاسلكي و تقوم هذه الأكسس بوينت بتقديم خدمة الإتصال اللاسلكي في نفس وقت أداء مهمة تحليل الطيف و مراقبته علي نفس القناة الترددية و هذا يقلل عدد الأكسس بوينت في الشبكات الضخمة حيث يخصص دائما اكسس بوينت للقيام بمهمة التحسس Sensor

تؤكد سيسكو أن تقنية CleanAir تعتبر نظام و ليست خاصية فهي تشبه بشكل ظاهري برنامج سيسكو الرائع Cisco Spectrum Expert الا أن CleanAir تعتمد علي هاردوير و سوفتوير لا يتوفران الا عبر شريحة ASIC و يسمي

ذلك intelligence silicon-level و هو القلب النابض لهذا النظام أو كما تطلق عليه سيسكو محرك محلل الطيف Spectrum Analysis Engine (SAgE) ASIC

من الخصائص الجميلة في CleanAir هو وجود radio resource management (RRM) حيث يقوم الأكسس بوينت الذي يدعم هذه التقنية بتغيير القناة التي يعمل عليها تلقائيا عند شعوره بوجود تداخلات co-channel interference علي قناته التي يعمل عليها

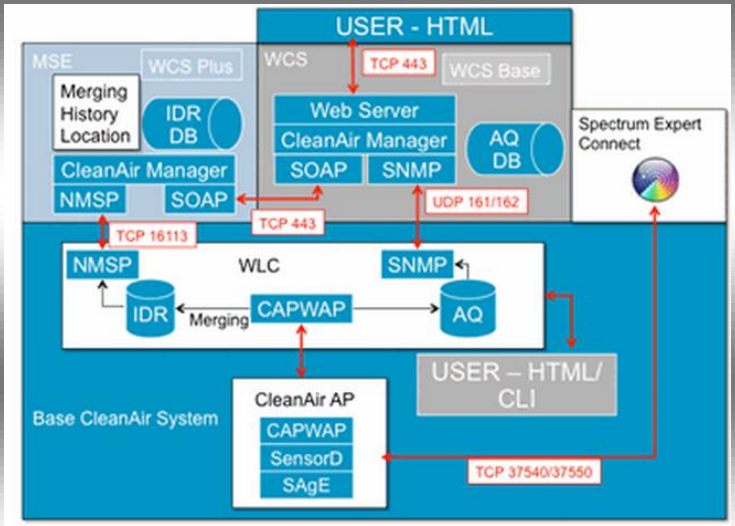


مكونات دعم CleanAir

لكي نستطيع التعامل مع هذه التقنية لابد أن تحتوي شبكتك اللاسلكية علي معدات أساسية و هي

- CleanAir capable APs are Aironet 3502e, 3501e, 3502i, and 3501i
- Cisco WLAN Controller (WLC) running version 7.0.98.0
- Cisco Wireless Control System (WCS) running version 7.0.164.0
- Cisco Mobility Services Engine (MSE) running version 7.0

و تقوم هذه البرمجيات بعمل قاعدة بيانات للأجهزة اللاسلكية سواء كانت تعتمد علي الواي فاي أم أن ترددها مغايرة مثل الهواتف و الكاميرات و الحواسيب و تحدد أماكن تواجدها و تتعقب تحركها خلال الشبكة اللاسلكية , و هذا رسم تخطيطي لبيان كيفية تفاعل أجزاء هذا النظام مع بعضه



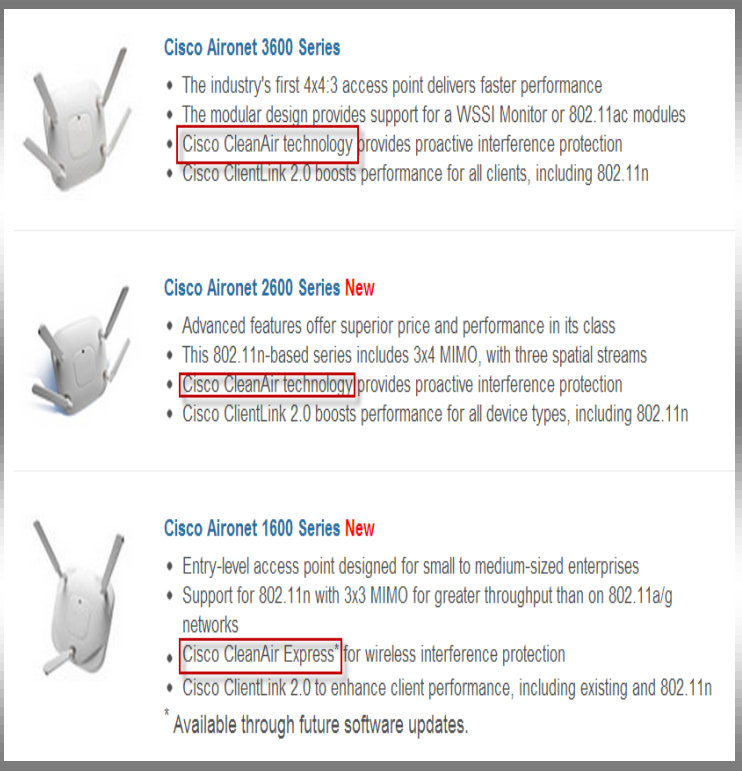
و رغم أن وجود Mobility Services Engine (MSE) يعتبر اختياريا الا أنه يزيد من فعالية CleanAir و يضيف امكانيات أخري له تراها في هذا الجدول و الذي يقارن بين شبكة تعتمد علي وجود Cisco Mobility Services Engine (MSE) و أخري لا تعتمد عليه

	CleanAir APs with Wireless Controller Only	CleanAir APs with Wireless Controller and Mobility Services Engine
Rogue Mitigation	✓	✓
Detect Interferers	✓	✓
Classify Interferers	✓	✓
Mitigate Interferers	✓	✓
Maintain Air Quality	✓	✓
Detect Layer 1 Exploits	✓	✓
System wide Interferer Details and Event Correlation	×	✓
Zone of Impact and Interferer Notification	×	✓
Track and Trace Interferers and Layer 1 Exploits	×	✓
Track and Trace Rogues	×	✓
Security Penetration and DoS attack Mitigation	×	✓

CleanAir AP

تعتبر أهمية الأكسس بوينت في كونها هي الواجهة الأولي لجمع البيانات عن التداخلات الراديوية للأجهزة اللاسلكية التي لا تعتمد علي الواي فاي non-Wi-Fi interference sources و يقوم الكنترولر بتجميع هذه البيانات من كل أجهزة الأكسس بوينت المتصة به و يعطيها لسيرفر WCS حيث يقوم بتحليلها و ترتيبها و عرضها لمدير النظام علي هيئة بيانات أو مخططات

في البداية لابد أن تكون الأكسس بوينت تدعم هذه التقنية و سيسكو تعرض ذلك في خصائص الأكسس بوينت علي صفحتها كما تري



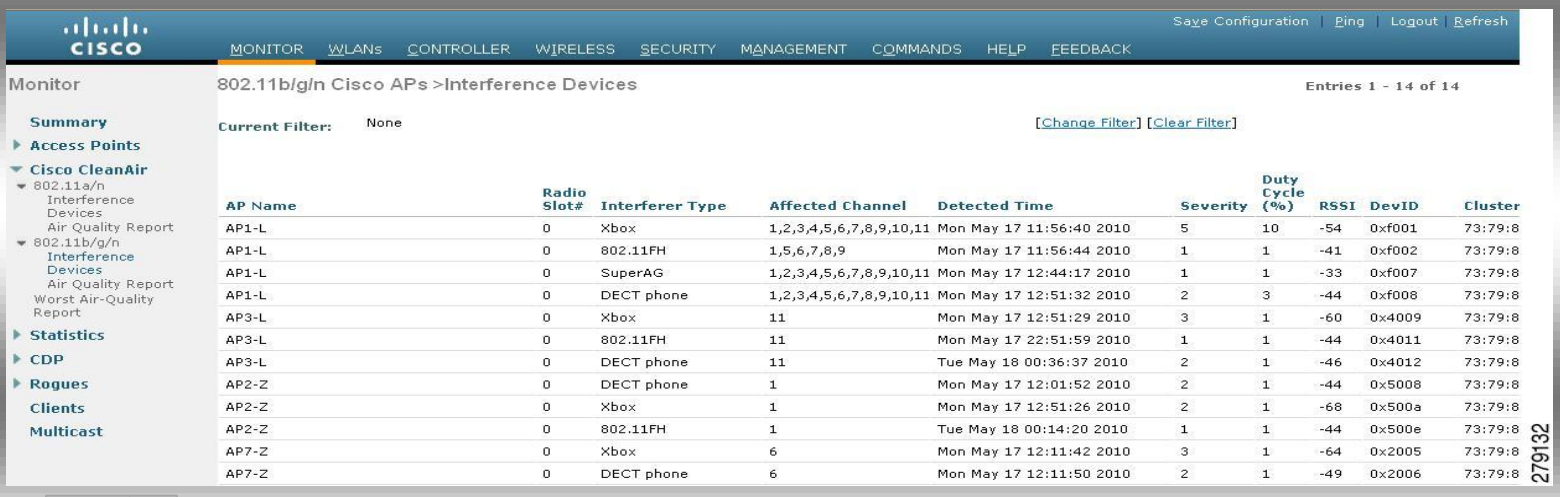
و كما تري فإن كل أكسس بوينت يدعم اصدار معين أو جيل من أجيال ClientAir و هذه مقارنة بين هذه الإصدارات

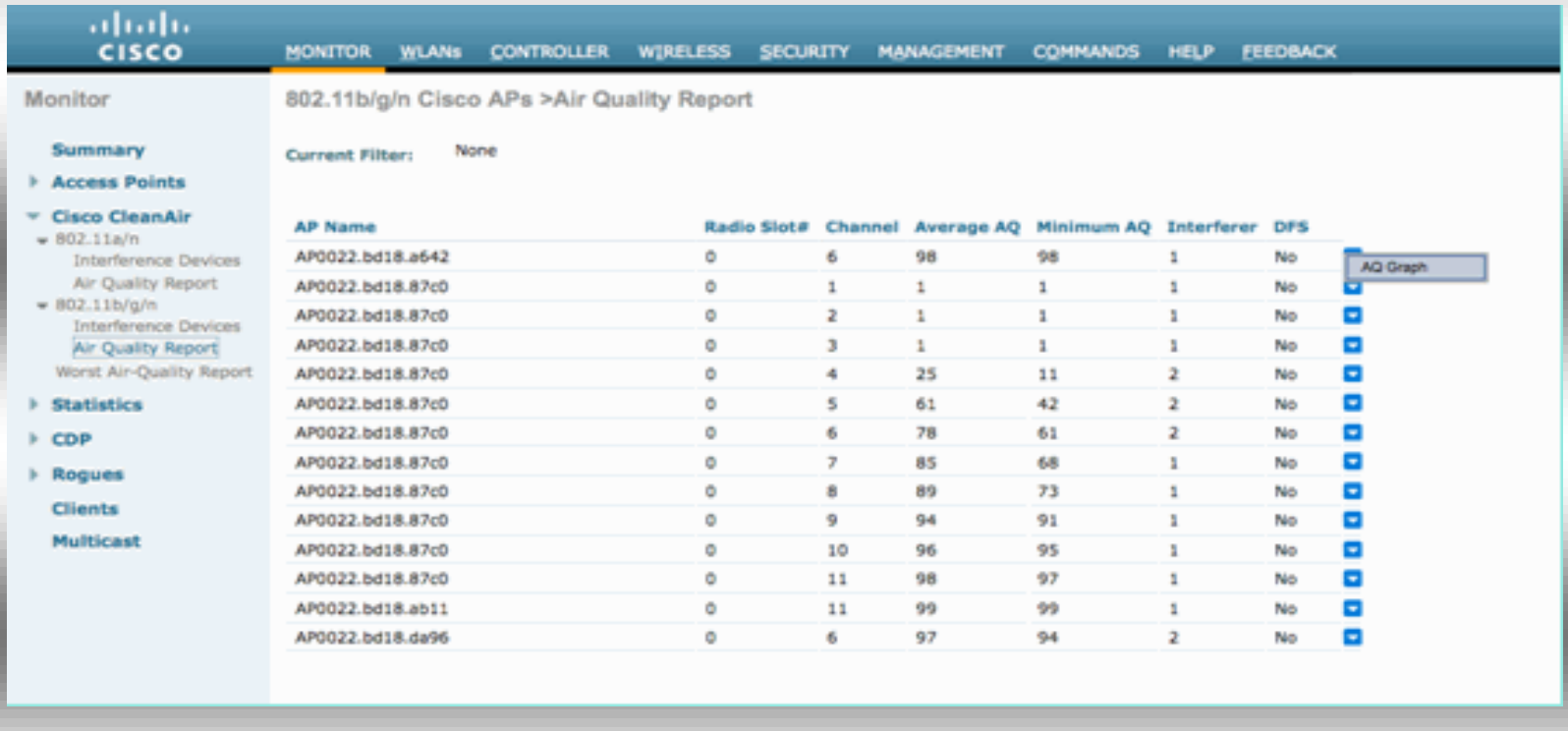
Spectrum Intelligence			
	CleanAir Express*	CleanAir	CleanAir with WSSI
Access Point	1600*	2600 or 3600	3600 with WSSI Module
Detection	■	■	■
Classification	■	■	■
Mitigation	■	■	■
Location	■	■	■
Performance Optimized		■	■
Top Impacts and Severity List		■	■
Alert Correlation		■	■
Air Quality Index		■	■
Zone of Impact		■	■
Off Channel Scanning			■
Predictive Intelligent Channel Switching			■

* Planned for future support

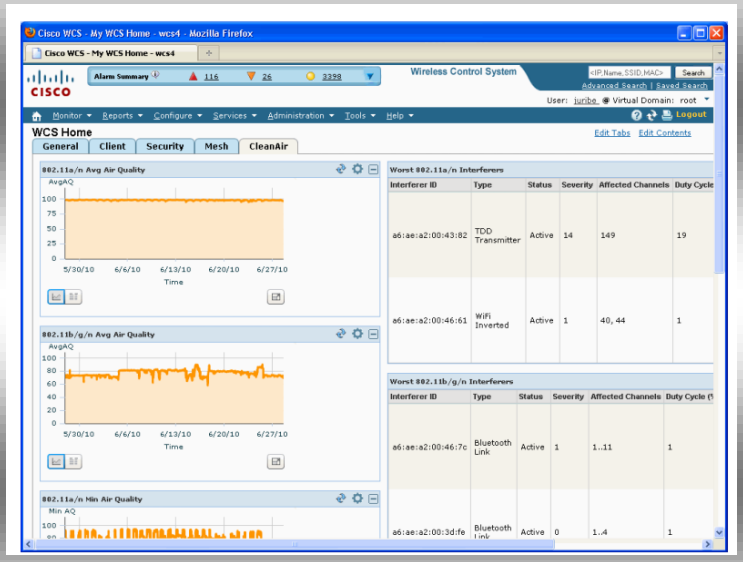
المعلومات اتي يعطيها CleanAir

يعطي CleanAir نوعين من البيانات أولهما IDR (Interference Device Report) يخص المصادر التي تطلق الموجات الراديوية و تؤدي للتداخل و يشبه التقارير التي يصنعها برنامج Cisco Spectrum Expert و تستطيع أن تشاهده من خلال الكنترولر و به الكثير من العوامل و البيانات عن خصائص هذه الأجهزة و ما تطلقه من تداخلات





و تستطيع أن تشاهد هذين النوعين من التقارير عبر واجهة WCS و بشكل بياني أجمل



Spectrum Configuration:

WLC – AP

```
CAPWAP msg: CAPWAP_CONFIGURATION_UPDATE_REQUEST = 7
payload type: Vendor specific payload type (104 -?)
vendor type: SPECTRUM_MGMT_CFG_REQ_PAYLOAD = 65
```

AP-WLC

```
Payload type: Vendor specific payload type (104 -?)
vendor types: SPECTRUM_MGMT_CAP_PAYLOAD = 66
              SPECTRUM_MGMT_CFG_RSP_PAYLOAD = 79
              SPECTRUM_SE_STATUS_PAYLOAD = 88
```

Spectrum data AP – WLC

```
CAPWAP: IAPP message
IAPP subtype: 0x16
data type: AQ data – 1
main report 1
worst interference report 2
IDR data – 2
```

معدات لاسلكية

Cisco Aironet 1240AG

كنت أتمني أن آخذكم في جولة مع الأكسس بوينت Cisco 1250 Aironetو معياره اللاسلكي الرائع 802.11 n و لك سآخذكم في جولة مع Cisco Aironet 1240AGو هو يشبهه في الإعدادات مثل غالب أجهزة الأكسس بوينت من سيسكو و التي تستطيع أن تعمل مع الوضعين Standalone و Lightweight

فأما الوضع lightweight أو ما يسمي Controller-Based فيستخدم في الشبكات التي تعتمد علي أجهزة كنترولر للتحكم في الشبكة اللاسلكية لكثرة عدد الأكسس بوينت مما يحتاج لمركزية في التحكم بها و لا تستطيع أن تعمل بدونه و أما الوضع Standalone أو autonomousفهو الوضع العادي للأكسس بوينت و الذي يستخدم في الشركات الصغيرة و البيوت حيث يقوم الأكسس بوينت بأداء كل مهام الشبكة بدون الحاجة لجهاز آخر يتحكم فيه

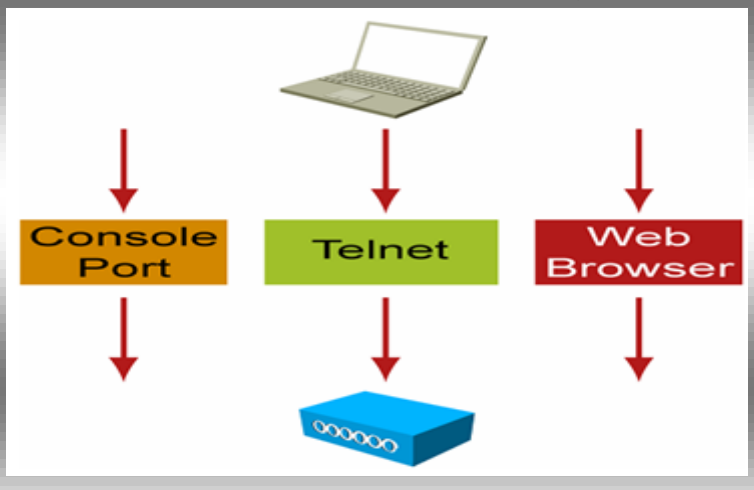
و نظرا لإحتمالية زيادة عدد الأكسس بوينت و لجوء الشركات لزيادة اعتمادها عليه فإنها قد تحتاج الي تغيير أجهزتها Standalone الي Lightweightو هذا يتطلب ميزانية جديدة و لهذا عملت سيسكو علي ايجاد وسيلة لتحويل الأكسس بوينت من الوضع Standalone الي Lightweightبدون الحاجة لتغيير الأجهزة

سنتعامل الآن مع Cisco Aironet 1240AGفي وضع Standalone APو هذا الوضع في بسيسكو يتم إدارته و الإتصال به بثلاث طرق هم Web Browser و Telnet و Console Port

فأما Console Portفيحتاج الي كابل rollover للإتصال بالطريقة التي نعرفها و التي تتطابق مع الطريقة التي تتصل بها بأجهزة الراوترات و السويتشات و نحتاجه عند بداية التعامل مع الأكسس بوينت و يكون enable passwordالإفتراضية هيcisco

أما Tellnet فيحتاج أن يكون للأكسس بيونت IP اي انه وضع تعامل مع الأكسس بوينت قد تم إعدادها مسبقا و كلمة السر الإفتراضية هي cisco

و web browserو هو اسهلهم و أكثرهم شيوعا و المستخدم في الغالبية العظمي من أجهزة الأكسس بيونت من خارج سيسكو أيضا و يكون الباسورد الإفتراضي هو Cisco

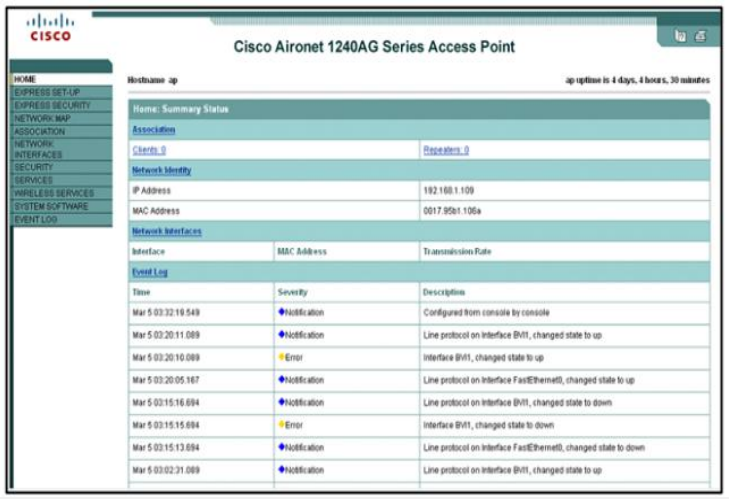


الصفحة الرئيسية لCisco Aironet 1240AG

بمجرد اتصال الأكسس بوينت بالشبكة فإنها تبحث عن سيرفر DHCP فإن لم يجد أو لم يستطع الحصول علي IP فهناك طريقة أخري بإستخدام Cisco Aironet IP setup Utilities و التي ليس مجالها الآن

سنتعامل في هذا الفصل مع أكسس بوينت من سيسكو من نوع Cisco Aironet 1240AG series Access Point و ستجد غالب الأجهزة الأخري تحتوي علي نفس الإعدادات تقريبا

عند دخول الصفحة الرئيسية للأكسس بوينت تظهر الصفحة الإبتدائية التالية



في هذه الصفحة ستجد معلومات مختصرة عن اهم ما يخص هذا الأكسس بوينت مقسمة الي أجزاء

فالجزء الخاص بـ Network identify يعرض معلومات عن عنوان IP و MAC

و الجزء الخاص بـ Network Interfaces يعرض مختصر للواجهات الشبكية للأكسس و عنوان MAC و كذلك سرعة تدفق البيانات لكل واجهة

و أما Event Log فتعرض الملاحظات و الأخطاء التي مر بها الأكسس بوينت اثناء عمله مع تصنيفها و وجود وصف مختصر لكل منها

Express Setup

قم بالدخول الي Express Setup لنقوم بعمل بعض الإعدادات الأساسية للأكسس بوينت

و تري في هذه الصفحة الأتي

Host Name : اسم الأكسس بوينت و هو أمر لا يؤثر في مجريات عمل الشبكة , و يظهر اسم الأكسس بوينت في أعلي كل صفحة بجوار Hostanme

Cofiguration Server Protocol : هل ستستخدم سيرفر DHCP أم ستدخل بيانات IP يدويا

IP Adderess : عنوان IP للأكسس بوينت و بالطبع لابد أن يكون ضمن الشبكة الخاصة بك

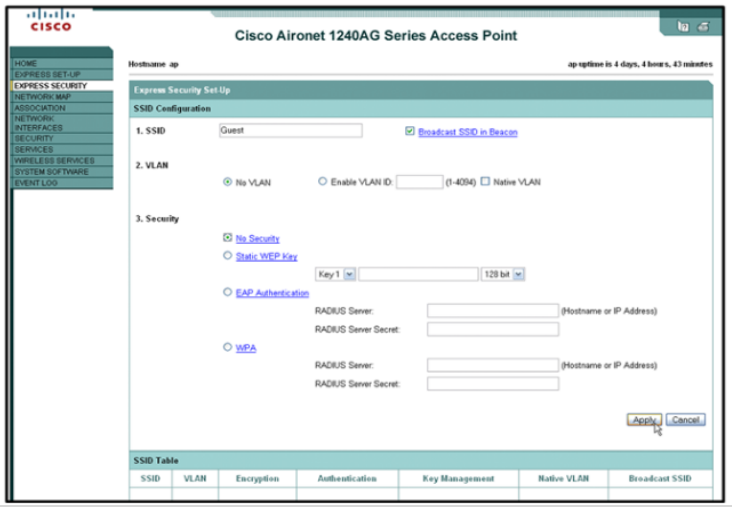
IP Subnet Mask : قناع الشبكة

Default Gateway : الراوتر أو المكان الذي ستأخذ من الإنترنت

SNMP Admin Community : هو اسم مدير مجال Simple Network Management Protocol و الذي سيقوم بإدارة الأكسس بوينت

Express Security

قم بعدها بالدخول الي Express Security لنبدأ بالتعامل مع اعدادات سريعة لتأمين الشبكة اللاسلكية المتصلة بالأكسس بوينت



يعتبر SSIDهو عنوان الشبكة التي ستظهر للمستخدمين و هو اختصار Service Set Identifersو تستطيع أجهزة الأكسس بوينت من سيسكو ان يكون لها اكثر من SSID و هنا في AG 1240تستطيع عمل 8 SSID يتم تفعيلهم علي كل الواجهات اللاسلكية Interfacesالمتوفرة في الأكسس بوينت و تراهم في الجدول في أسفل الصفحة

في كثير من الحيان تجد أن هناك SSID افتراضية و غالبا ما تكون tsunamiفي أجهزة سيسكو الا انه في نسخ نظام التشغيل للأكسس بوينت CISCO IOS Software Release 12.3(4)JA و الأحدث منها فإنه لا يوجد SSID الإفتراضية و للذلك يجب ان تضعها قبل البدء في عمل الأكسس بيونت

يساعدك تعدد SSID عند استخدامك للشبكات الظاهرية VLAN في شبكتك اللاسلكية و هنا تستطيع ان تضع لكل VLAN عنوان SSIDخاص بها

و اليك هذه الملاحظات المهمة الخاصة بهذا الجهاز عند اعداده بواسطة Express security

- لن تستطيع التعديل في SSID و لكنك تستطيع حذفهم
- لن تستطيع أن تضع SSID لأحد المعيارين 802.11 aأو 802.11 gفقط و لكن يتم تفعيل SSIDعلي المعيارين و لكي تستطيع التعديل في ذلك قم بالدخول علي security SSID Manager
- لن تستطيع اعداد أكثر من authentication server و لعمل ذلك قم بالدخول لصفحة Security Server Manager
- لن تستطيع عمل اكثر من مفاتيح عديدة لـ WEP و لكنك تستطيع القيام بذلك من صفحة Security Encryption Manager

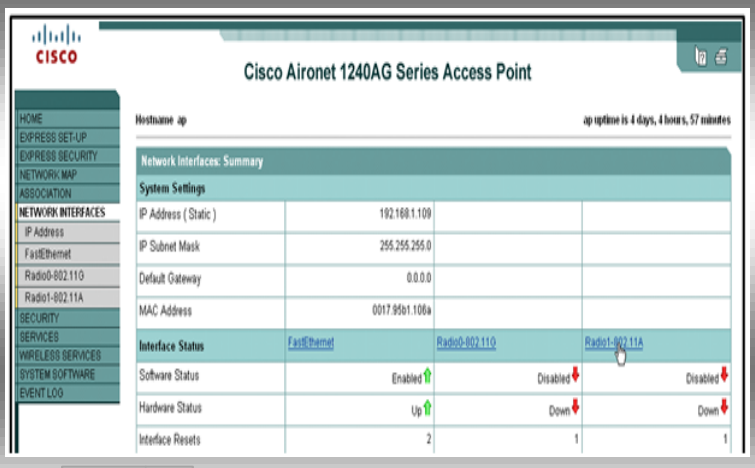
و الكثير من الأشياء التي لن تسعفك فيها صفحة Express Security

Network Interfaces

و الجزء الخاص بـ Network Interfaces يعرض الواجهات الشبكية للأكسس بوينت فمن المعروف أن اي جهاز شبكي يحتوي علي واجهات للإيثرنت أو fasteathernet أو serial و يزيد عليها واجهات لاسلكية يعبر عنها بكل معيار لاسلكي متوفر في الأكسس بوينت مثل 802.11 802.11n 802.11g 802.11b وكما تري من اسم a الأكسس بوينت AG 1240فإن لها واجهتين لاسلكيتين هما Radio 802.11a و802.11g

قم بالدخول علي Network Interfaces لتري معلومات عن الواجهات عنوان MAC و كذلك سرعة تدفق البيانات لكل واجهة و الكثير من المعلومات الأخري

يظهر لنا في أول الصفحة System Setting و فيه عنوان الأكسس بوينت IP و MAC و عنوان الراوتر



Interface Status : و فيه تجد معلومات عن حالة الهاردوير من و السوفتوير الخاصة بتلك الواجهات من حيث تفعيلها أو تعطيلها

Receive/Transmit Status : حالة البيانات المرسلة و المستقبلة من تلك الواجهات مثل كمية البيانات و عدد الباكت و الباكت المتجاهلة و الأخطاء و غيرها

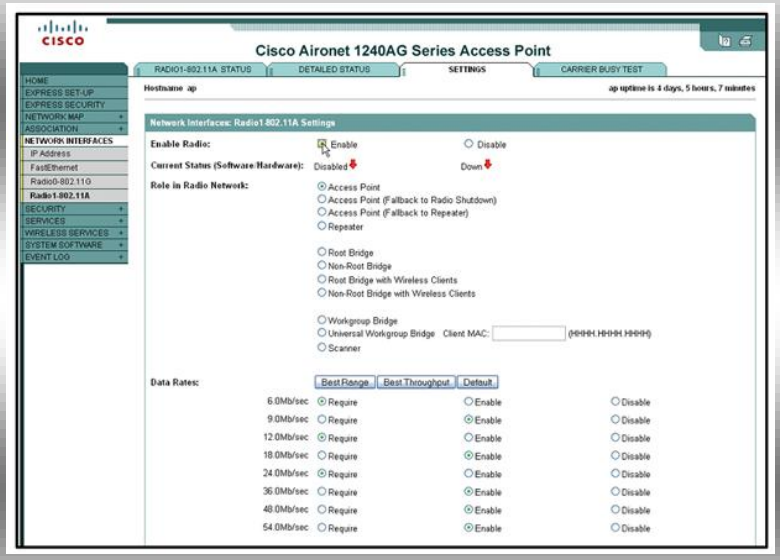
Receive			
Input Rate Timespan	5 minute	5 minute	5 minute
Input Rate (bits/sec)	5000	0	0
Input Rate (packets/sec)	5	0	0
Time Since Last Input	00:00:00	never	never
Total Packets Input	1216436	0	0
Total Bytes Input	120465406	0	0
Broadcast Packets	1155257	0	0
Total Input Errors	0	0	0
Overrun Errors	0	0	0
Ignored Packets	0	0	0
Throttles	0	0	0
Transmit			
Output Rate Timespan	5 minute	5 minute	5 minute
Output Rate (bits/sec)	5000	0	0
Output Rate (packets/sec)	3	0	0
Time Since Last Output	00:00:00	never	never
Total Packets Output	51915	0	0
Total Bytes Output	5587761	0	0
Total Output Errors	0	0	0
Last Output Hang	never	never	never

في البداية تكون الواجهات اللاسلكية Radio 802.11a و Radio 802.11g غير مفعلة و لتفعيلها قم بالدخول علي أي منها بالضغط علي اسمها في جدول Interface Status و لنأخذ مثلا Radio 802.11a و تظهر لك الصفحة التالية بها العديد من التبويبات قم بالدخول علي التبويب Setting ثم قم بتفعيل هذا المعيار الراديوي من الخيار enable

ستجد بعض الخيارات الأخري مثل Data Rates و التي تستطيع من خلالها تغيير معدل نقل البيانات للأكسس بوينت في حدود تحت الحد الأعلي المسموح به

و من الخيارات أيضا التي ستجدها Roles in Radio Network و التي تحدد طبيعة عمل الأكسس بوينت مع المعيار A802.11

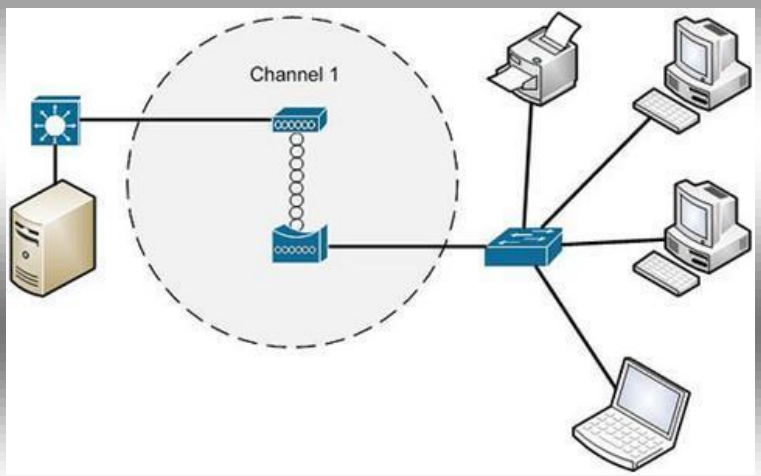
و Radio Roles هي الوظائف التي يستطيع أن يقوم بها الجهاز الشبكي اللاسلكي و هذه الوظائف تختلف من جهاز الي آخر و من شركة الي أخري ففي حين تشرح مناهج CWNP الوظائف الأساسية فقط تقوم مناهج CISCO اللاسلكية بالتوسع في شرح هذه الوظائف وهذا ناشيء عن أن أجهزة سيسكو اللاسلكية قادرة علي العمل في وظائف فرعية للشبكة اللاسلكية سنعرفها الآن بإذن الله تعالي و تستطيع اختيار الوظيفة التي تريدها للجهاز من صفحة اعدادته



Access point Role

هنا سيلعب الأكسس بوينت دور الوسيط لتمرير البيانات بين أجهزة الشبكة اللاسلكية و هو الشكل الطبيعي و الإفتراضي للأكسس بوينت كجهاز اتصال و ربط لاسلكي

Repeater access point Role



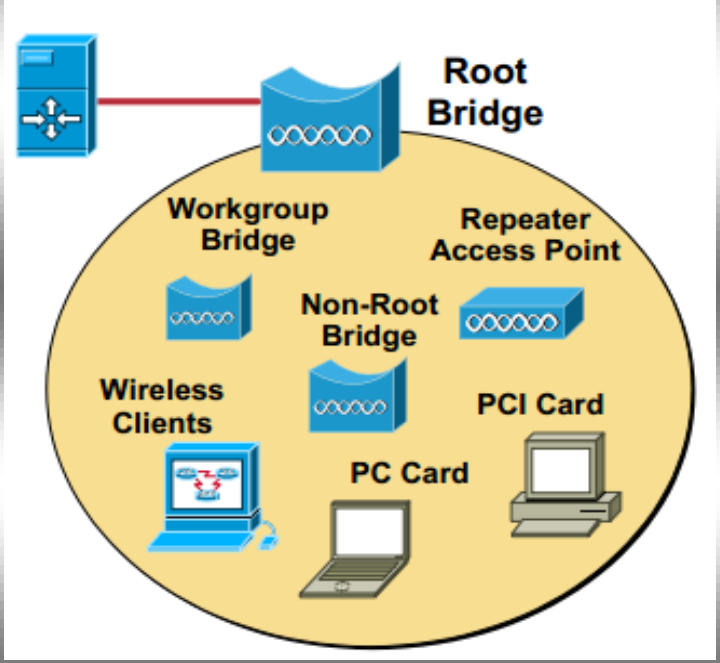
سيلعب هنا الأكسس بوينت دور مقوي الإشارة مع تعطيله لمخارج الإيثرنت في الجهاز أي أنه يربط فقط بين الشبكات اللاسلكية ودور جهاز المقوي أو المكرر, Repeater هو إيصال الإشارة الي أقصي مكان ممكن أن تصله ولذلك فإن هذا الجهاز يسمي أيضا بعدة أسماء توحي

بطبيعة عمله مثل wireless range extender و booster و expanderفغالب شبكات الوايرلس في العالم تعاني من وجود نقاط ميتة dead zone و هي مناطق لا تستطيع الأكسس بوينت تغطيتها أما لقصور في الأكسس بوينت أو لبعد هذه المناطق أو لوجود عوائق تعوق الإشارة

و لا توجد في سيسكو أجهزة Repeater خاصة و لكن يتم تحويل وضع الأكسس بوينت أو الجسر الي وضعrepeater

أهم شيء لابد أن تفهمه أن جهاز Repeater ليس جهاز ربط بل مجرد ناقل للإشارة و مقوي لها و أحيانا مقوي لمعدل نقل البيانات Data Rateو يعمل علي نفس قناة لأكسس بوينت الذي يقوي اشارتها

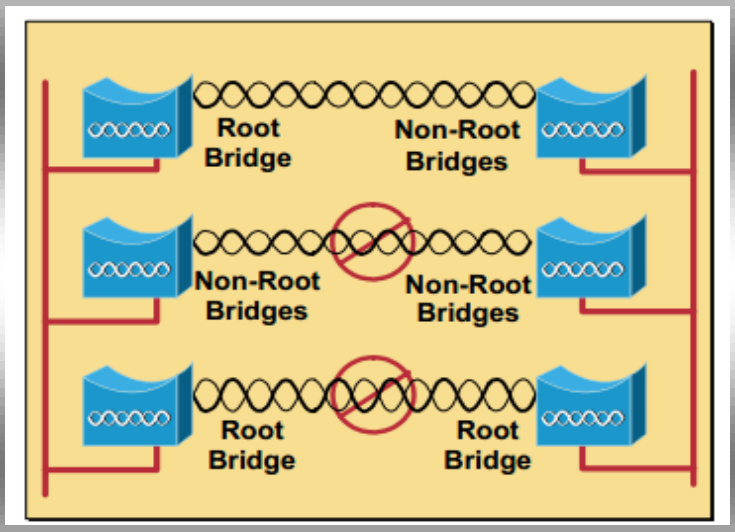
Root bridge with clients Role



هنا سيلعب الجهاز دور الجسر اللاسلكي الجذري ليربط بين شبكتين لاسلكيتين أو شبكة سلكية و لا سلكية مع امكانية استخدامه كأكسس بوينت ليسمح بالأجهزة بالإتصال به

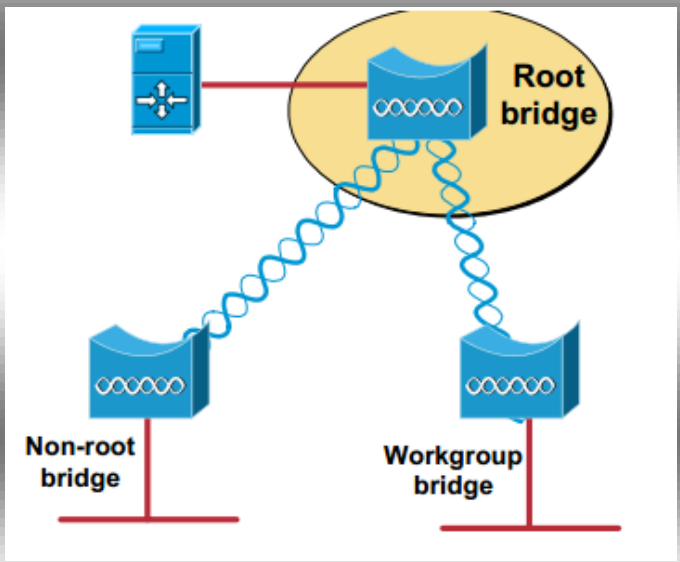
Root Bridge

هو وضع اتصال لاسلكي للجسر يقوم علي اساسه بالإتصال بأجهزة الجسور الأخري شرط أن لا تكون في نفس الوضع أي أنه لا يجوز أن تكون هناك في الشبكة اللاسلكية الواحدة سوي جسر واحد فقط في Rootو يستطيع الجسر اللاسلكي في وضع Rootالإتصال مع كل الأجهزة اللاسلكية عدا التي الجسور التي تعمل في نفس وضعه و هو Rootكما بالشكل التالى



Root bridge without clients Role

لن يتم السماح بإتصال العملاء بهذا الجهاز و سيستخدم فقط كجسر بين الشبكات سلكية أو لاسلكية و سيلعب دور الجهاز الأول أو الجذر في الشبكة الاسلكية و لن يسمح لغيره بهذه الوظيفة

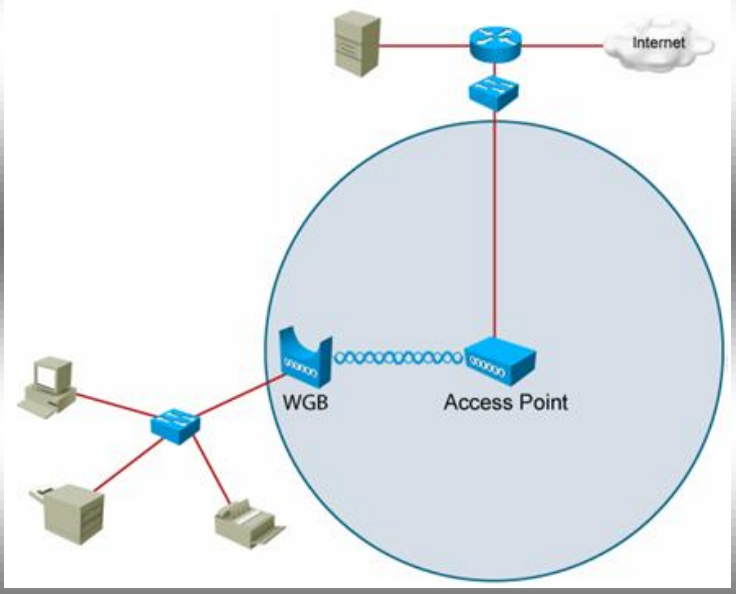


و أجهزة Non-root bridgeبشكل عام هي أجهزة الجسور التي تتصل بالجسر الجذري Root Bridges و لا تستطيع الإتصال مع مثيلاتها الا اذا كان الجهاز Non root الآخر متصل بجهاز جذري Root Bridge

Non-root bridge with clients Role

سيقوم بالإتصال بالجهاز الجذري لينقل الإشارة الي باقي الشبكة السلكية أو اللاسلكية و لا يسمح بإتصاله بجهاز آخر من نفس وظيفته ولكنه سيعمل كأكسس بوينت

WGB Workgroup bridge Role



هنا سيصبح الجهاز البوابة اللاسلكية للشبكة المحلية السلكية لتتصل بشبكة لاسلكية أخري أي كأنه كارت لاسلكي مشترك للشبكة

و تتعامل أجهزة الأكسس بوينت مع WGB علي أنه جهاز Clientفلا تستطيع أجهزة الكمبيوتر الإتصال به مباشرة لاسلكيا اطلاقا و لكنه يستطيع الإتصال بأكثر من جهازأكسس بوينت و يستطيع أكثر من جهاز WGB الإتصال بأكسس بوينت واحد و لا مجال أيضا لربط جهاز WGB مع جهاز آخر يعمل في وضع WGB

لا يقتصر اتصال WGB مع الأكسس بوينت في الوضع الطبيعي لها بل يستطيع الإتصال بها في وضع المكرر Repeater و يستطيع الإتصال أيضا بأجهزة الجسور العادية Bridges

Access Point Root (Fallback to Radio Island) Role

سيعمل كجهاز جذري يربط بين شبكتين و سيقوم بالربط اللاسلكي في حال فشل الجهاز في الإتصال سلكيا

Access Point Root (Fallback to Radio Shutdown) Role

عندما يفقد الجسر اللاسلكي اتصاله بشبكة ما سلكيا يقوم بقطع الإتصال اللاسلكي عن الأجهزة المتصلة به و علي الأجهزة المتصلة اختيار جهاز آخر للإتصال بالشبكة

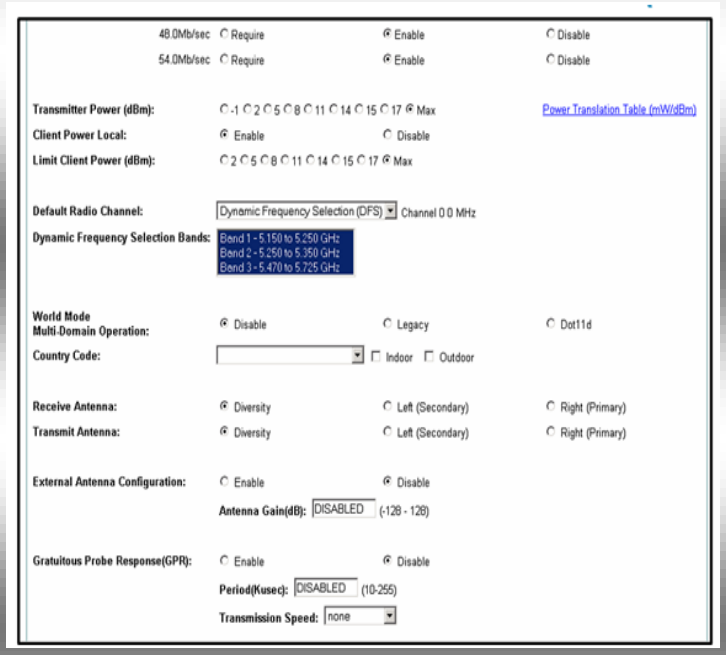
Access Point Root (Fallback to Repeater) Role

عندما يفقد الجسر اللاسلكي اتصاله بشبكة ما سلكيا يقوم بالتحويل الي وضع المقويRepeater

Scanner

هذا الخيار متوفر فقط عندما يتم الإعتماد علي جهاز WLSE في الشبكة و هنا لن يقبل الأكسس بوينت أي اتصال من client بل سيقوم بتجميع الإشارات و يرسلها الي WDS AP لتحليلها و هذه مقارنة بين هذه الأنواع من حيث قابليتها للإتصال ببعضها

Role	Associates to:				Accepts Associations from:					STP
	Root AP	Root BR	Repeater AP	NR BR with Clients	Wireless Clients	Wired Clients	NR BRs	WGBs		
Root AP					✓	✓		✓		Disabled
Repeater AP	✓	✓	✓	✓	✓			✓		Disabled
Root BR			✓	✓	✓	✓	✓	✓		Settable
NR BR without Clients		✓		✓		✓	☆ ✓			Settable
NR BR with Clients		✓	✓	✓	✓	✓	☆ ✓	✓		Settable
Work Group Bridge	✓	✓	✓	✓		✓				Disabled



و باقي الخيارات ستجدها في الأسفل و هي

Transmit Power : تحديد مستوي القدرة للإشارات الراديوية و اليت من خلالها تستطيع توسيع و تضييق مساحة انتشار الإشارة

Default Radio Channel: يسمح هذا الخيار باختيار القناة يدويا أو اليا حسب القناة الشاغرة في الشبكة

Receive/Transmit Antenna : تحديد أي من اهوائيات التي تستخدم للإرسال أو للإستقبال او استخدام خاصيةdiversity

External Antenna Configuration : تفعيل الهوائيات الخارجية لتوسيع نطاق الشبكة