المختصر في أمن الشبكات اللاسلكية

م نادر المنسي

امن الشبكات اللاسلكية

السلام عليكم و رحمة الله و بركاته

الحمد لله و الصلاة و السلام علي محمد و اله و جميع صحبه أما بعد

فهذا كتيب تكلمت فيه بإختصار – مجمعا و مترجما و مؤلفا – عن أحد الأبواب المهمة في عالم الشبكات اللاسلكية و هو أمن الشبكات اللاسلكية من سيسكو و هذا الباب مهم لدارسي CCNA Wireless و يعتبر مقدمة وافية لمن يريد أن يدرس منهج CWSP من CWNP أو منهج الأمن اللاسلكي في مسار CCNP Wireless

و لمن لا يعلم فإن غالب ما أكتبه يمر بأربع مراحل

أولها هو نشر ما يكتب علي هيئة مقالات و تدوينات عبر موقعي تقريب الشبكات اللاسلكية للناطقين بالعربية wireless4arab.net أو مجلة networkset أو مجلة تقريب الشبكات اللاسلكية

و المرحلة الثانية هي أن أقوم بتجميع كل ما يخص موضوع معين و أنشره ككتيب صغير و هو مثل ذلك كتيب السرعات في عالم الشبكات الذي نشرته منذ أيام و مثل كتيب الأكسس بوينت و شبكات موفرات الخدمة

و المرحلة الثالثة و هي عندما يكتمل باب كامل و ينشر علي هيئة كتاب خاص بنفسه مثل هذا الذي بين أيديكم الآن و كتاب برنامج مراقبة الشبكات اللاسلكية WCS و مثل كتاب السويتشنج الذي سينشر قريبا هنا ان شاء الله

و أما المرحلة الأخيرة فهي عندما عندما يكتمل الكتاب فأنشره كاملا مثل كتاب wireless 4X1 و هندسة و فن تمديد كابلات الشبكات و كتاب CCNA Wireless الذي انتهيت منه تقريبا و سينشر في القريب العاجل ان شاء الله تعالي

و هذه المراحل تضمن لي و لكم التنقيح المستمر في الكتاب و أخذ اراؤكم في مادته العلمية و الأدبية و لهذا فإني فقير الي توجيهاتكم و اراؤكم العلمية و الأدبية و الفنية في ما أنشره عبر موقعي أو من خلال البريد

و فقنا الله و اياكم الي الإخلاص و العلم العمل

نادر المنسي

2013/3/19

naderelmansi@gmail.com

الأمن والمنطق في الشبكات اللاسلكية

أذكر أن أحد زملائي حكي لي يوما عن محاولة هكر الدخول الي جهازه و لما كانت طريقة إتصاله بواسطة خدمة Dial Up فلم يكن لديه خيار حينها إلا أن يقوم بغلق إتصال الإنترنت ثم إعاداة الإتصال مرة أخري ليقوم موفر الخدمة بتغيير IPالخاص به و هكذا فهم صديقي ساعتها أن تغيير هذا الأيبي سيمنع من دخول الهكر لديه ، فصديقي قام بالتمويه بدون استخدام برمجيات و ذلك بفهمه لبروتوكول IP الموجود ضمن طبقةNetwork

و سواء نجحت هذه الطريقة أم لا إلا أن تفكير صاحبي و تطبيقه لهذا الفعل يدل عن فهم – عن قصد أو غير قصد – لتأمين الشبكة طبقا لطبقات الشبكةOSI

ما أقصده من ذكري لهذا الأمر تثبيت و إقرار أن مدي فهمك لبروتوكولات طبقات الشبكة مساعدا رئيسيا لإستراتيجيات التأمين

و من المعروف أنه كلما نزلت في سلم طبقات OSI كلما كان تأمينك للشبكة أعلي و لا شك أن أكبر تأمين للشبكة هو فصل الطاقة نهائيا عن الجهاز المصاب و بهذا فأنت ستنجح بنسبة 100% في تأمين الشبكة و ستفشل بنفس النسبة من الدخول ايضا علي شبكتك "علي و علي أعدائي ☺"

و هذه الطريقة تعتبر تأمين طبقا للطبقة الأولي الفيزيائية

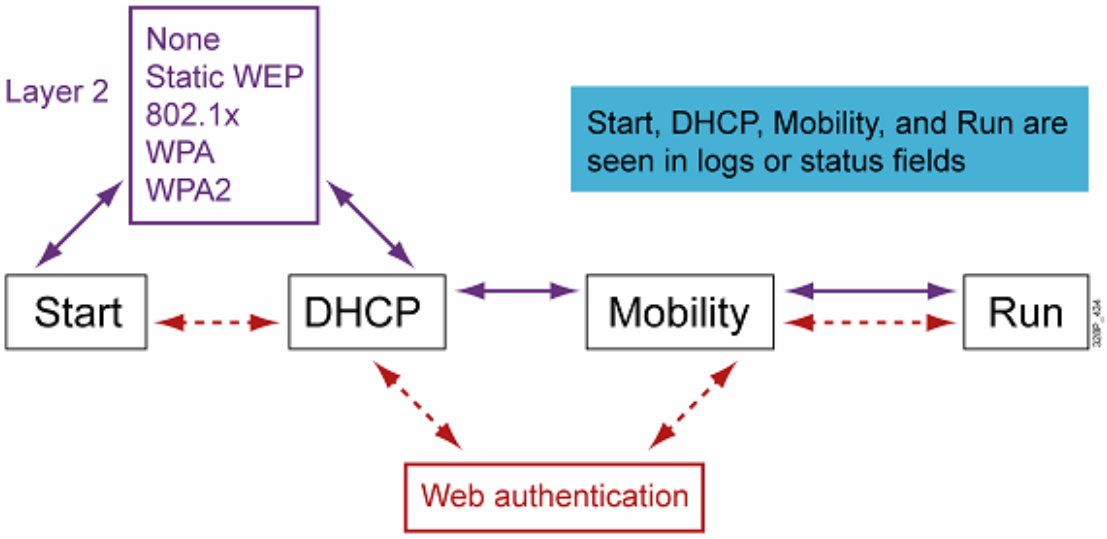
و منا أيضا من يؤمن منظومته برمجيا في "الطبقة السابعة " و ذلك بواسطة برمجيات مضادات الفيروسات أو عن طريق استخدام حجب SSID كما في الشبكات اللاسلكية

و منا من يؤمنه في طبقة session و ذلك بإغلاق منافذ port يعلم مسبقا أن أحدهم يستغلها لإختراقه

و صاحبي أمن شبكته طبقا لطبقة الشبكة

و هناك أجهزة و برمجيات تؤمن الشبكة بإستخدام أكثر من مستوي مثل برمجيات ISA و أجهزة الفايروول مثل PIX و Bluecoat

و من البديهي جدا قبل أن تبدأ في تأمين أي شبكة هو أن تتعرف علي احتياجاتها الأمنية و أن تقوم بعمل سياستك الأمنية بحيث لا يتعارض بعض مكونات الشبكة مع البعض الآخر بالضبط مثلما تفعل في group policy في نظم تشغيل ويندوز فالأمن في الشبكات اللاسلكية من سيسكو – كغيرها – هي عملية منطقية logic تمر بأربع مراحل تعبر عنها هذه الصورة



كما تري فإن هذه المراحل تمر بكافة طبقات بروتوكول OSI من قاعه المادي physical الي قمته التطبيقية Application

Start : هي خطوة تحتل طبقيتن من OSI فتمثل الطبقة الأولي Layer 1 physical في تفعيل الكارت اللاسلكي و من ثم ارسال الإشارة و بداية الإتصال بين الجهاز و الشبكة ثم يعني اختيار المستخدم للشبكة اللاسلكية للإتصال بها و من ثم انتظار قبول طلبه و هنا تبدأ الطبقة الثانية Layer2 Data Link فلو كانت الشبكة بلا تأمين open سيقوم الجهاز بالإنتقال للخطوة الثانية تلقائيا DHCP و ان كانت الشبكة مؤمنة ببروتوكولات layer2 security مثل WEP , IEEE 802.1x, WPA, WPA2 سيحتاج المستخدم الي ادخال معاملات التأمين كي يستطيع أن يدخل للخطوة التالية و هي DHCP

DHCP : هي المرحلة الثانية و التي يبدأ معها التعامل مع الطبقة الثالثة Layer 3 Network حيث سيحتاج جهازك الي IP للولوج الي خدمات الشبكة اللهم الا إذا كانت شبكتك تدعم الولوج عبر توثيق الويب web authentication

أي لابد من إدخال باسورد و كلمة مرور كأنك تدخل علي واجهة إدارة الأكسس بوينت هنا لن تستطيع الشبكة أن تكمل ولوجك للشبكة الا بإدخال بياناتك المطلوبة و بهذا تكون انتهيت من طبقة Layer 4 Transport و تحقق مع هذه الخطوة بروتوكولي TCP\IP

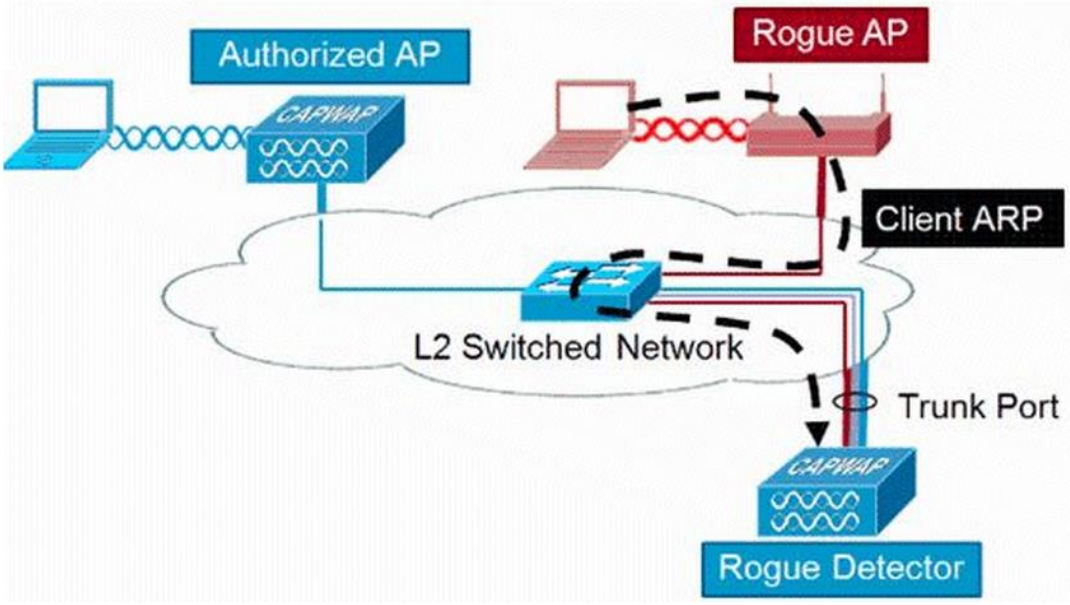
Mobility : بعد تلقيك بيانات IP و TCP تبدا الشبكة في عقد أول جلسة ولوج و اختبار و تبادل بيانات السرعات و هذه هي مهمة الطبقة الخامسة Session

Run : هنا يبدأ الجهاز بالعمل فعليا ضمن الشبكة و تبدا عملية استقبال و ارسال البيانات و تشفيرها في طبقة Layer 6 Presentation و بمجرد أن يقوم الجهاز بالتصفح أو بنقل البيانات فإنه يتم عمليات OSI بالطبقة السابعة Layer 7 Application

Wireless threats

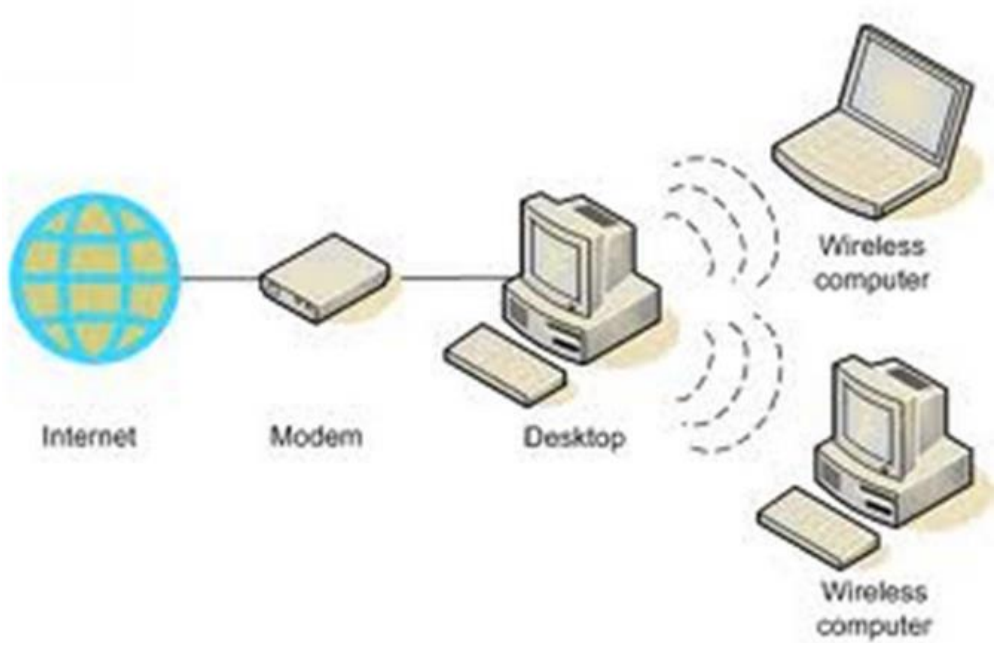
نظرا لخصوصية الشبكات اللاسلكية فإن المخطر الأمنية التي تعاني منها تختلف عن تلك التي توجد في شبكات الإيثرنت و قد تكون الشبكة اللاسلكية هي بوابة المخترق الي الشبكة السلكية نظرا لسهولة الوصول اليها ، سنتكلم هنا عن المخاطر الأمنية التي تخص الشبكات اللاسلكية وحدها

Rogue AP and Rogue Clients



تعتبر الأكسس بوينت الدخيلة أو أجهزة الكمبيورت الدخيلة هي الإختراق الأمني الشائع في الشبكات اللاسلكية و هو يحدث ذلك الإختراق نتيجة وجود هذه الأجهزة في حيز اشارة الشبكة اللاسلكية مما يسمح لها بالتقاط اشارتها

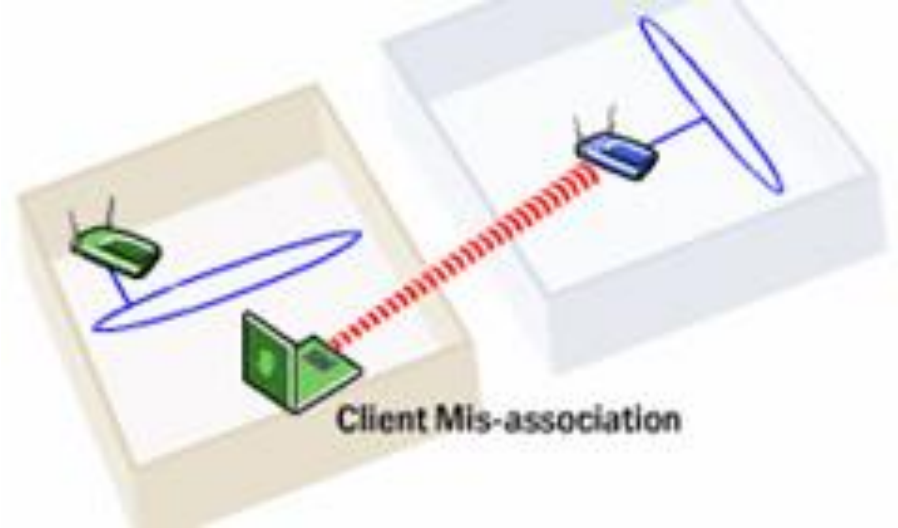
AD HOC Network



عندما يقوم شخص باستعمال جهاز في العمل و يتصل بالشبكة السلكية بعمله و نفس الوقت يمكن الإتصال اللاسلكي بجهازه فإنه يفتح بابا لآخرين لإمكانية التحايل و الإتصال لاسلكيا بجهازه بما يسمي بشبكة الند للند و بذلك يجعل من نفسه بوابة لإختراق الشبكة

اذن فمن الأفضل عند الإتصال بأي شبكة هو تعطيل منافذ الإتصال الأخري الموجودة خصوصا اللاسلكية مثل الواي فاي و البلوتوث حتي لا يستخدمها الآخرون في غفلتنا للولوج للشبكة

Client misassociation



من الإعدادات الإفتراضية في اتصالك بالشبكات اللاسلكية هو تمكين اتصالك اللاسلكي بأي شبكة قمت بالإتصال بها مسبقا و في كثير من الأحيان لا يقوم أصحاب الشبكات اللاسلكية بتغيير SSID الإفتراضي للأكسس بوينت مما يجعل امكانية اتصالك بشبكة بنفس الإسم في مكان آخر و بدون وجود توثيق أمر وارد و بدون علمك و هذا من الأساليب التي يتبعها المخترقون بما يسمي فخاخ الشبكات اللاسلكية حيث يهيء لك الأمر للولوج لشبكته ثم يقوم هو بالعبث بجهازك

Wireless attack

جميع المخاطر السابقة كانت لك اليد العليا في ايجادها و السماح للآخرين باختراقك باستخدام ثغرات صنعتها أنت و لا يقع فيها غالبا الا المبتدئون في عالم اللاسلكي و لا يعول عليها المخترقون كثيرا فهم مستعدون للمعركة الأم و هو الإختراق الكامل و بدون وجود ثغرة يسببها المستخدم فكثير منا عاني من اختراق شبكته اللاسلكية رغم التأمين الشامل لها و هذا يرجع ليس لغفلتك و أنما لقوة و خبرة من اخترقك و لعلك استخدمت يوما أحد أساليب الإختراق اللاسكية و التي يتم تصنيفها الي نوعين هما Passive Attack و Active Attack

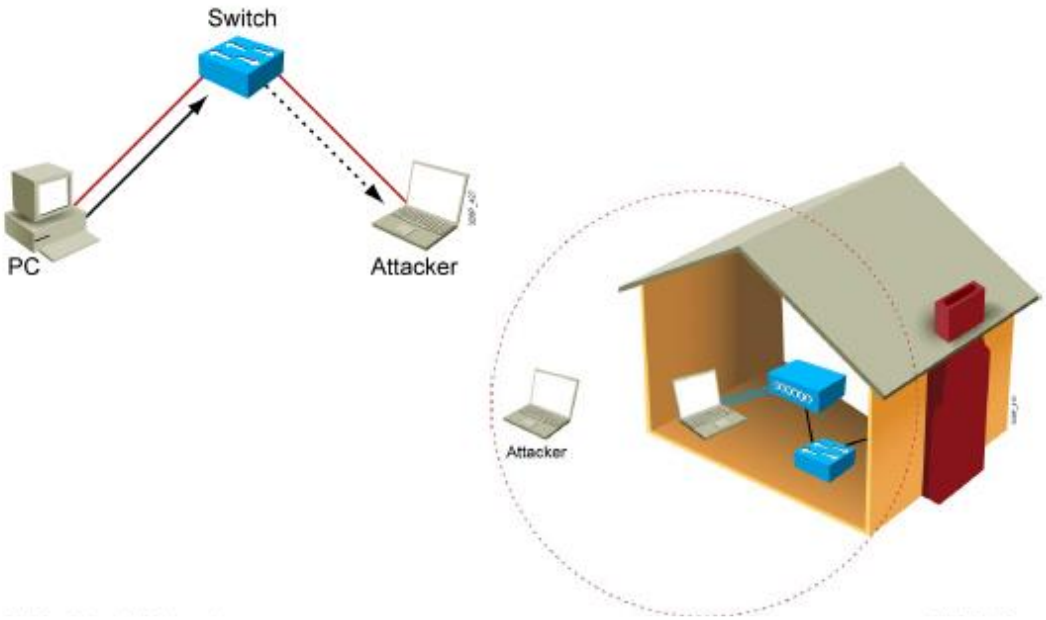
passive attack

فأما passive attack فيتم باستخدام برمجيات تقوم بالتقاط capture فريمات الشبكات اللاسلكية probes ثم يقوم بتحليلها analyzing و ذلك بناء علي بعض المعطيات المسبقة مثل نوع التشفير و رقم القناة و نوع المعيار اللاسلكي و ذلك لبعض الوقت ينقص أو يزيد طبقا لمستوي الأمن و التشفير في الشبكة ليقوم بعدها بإعطائك باسورد الشبكة

Active Attack

و أما Active Attack فيتم استخدامه عند فشل الطريقة السابقة و ذلك في الشبكات الكبيرة التي تستخدم معدات مركزية و طبولوجيات غير معتادة تعتمد علي أجهزة كنترولر و سيرفرات توثيق و هنا فإن الحل هو انتحال شخصية أحد أجهزة الشبكة باستخدام Rogue AP او man-in-the-middle و هو من الخروقات الأمنية التي لا يجيدها الا الخبراء جعلنا الله و اياكم منهم بدون ضراء مضرة و لا فتنة مضلة

Authentication –Encryption

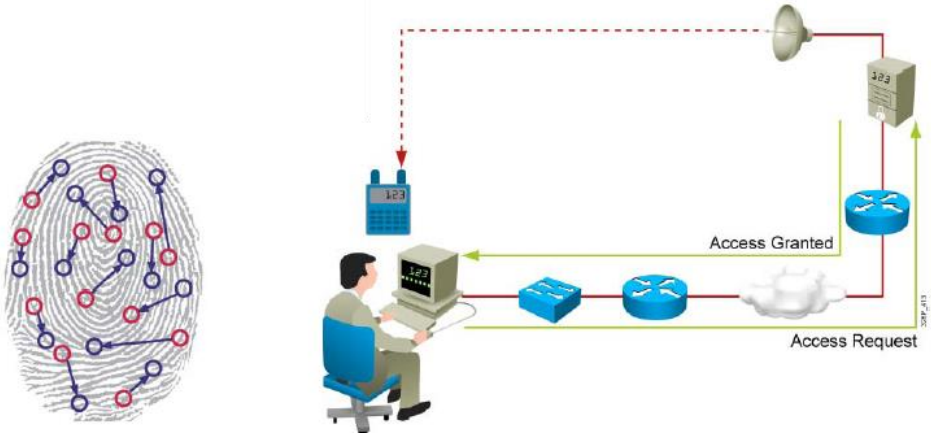


تأمين المعلومات هو أحد أهم مقاصد الشبكات و الحاجة الي تأمين الأنظمة الشلكية أمر مهم و في الشبكات اللاسلكية أمر بالغ الأهمية و لا غني عنه ، فلكي تقوم بمحاولة اختراق الشبكات السلكية فأنت تحتاج الي اتصال سلكي بالسويتش ثم التقاط البياناتcapture الي الجهاز و هذا يعني ضرورة وجود اتصال مباشر بالشبكة ، أما الشبكات اللاسلكية فالأمر اسهل فبمجرد وجودك في حيز اشارة الأكسس بوينت و يكون ارسالها عير مشفر Encrypted و لا يحتاج لتوثيق authenticated فتستطيع حينها الولوج للشبكة

Authentication

في الحياة الواقعية يعتبر Authentication هي عملية ايجاد شيء مطابق لشيء و في الشبكات اللاسلكية تستخدم للتأكد من صلاحية و سماحية دخول شخص أو جهاز الي الشبكة و في كلا الحالتين لن ينجح توثيق دخول الجهة الي الشبكة الا اذا استطاع أن ينشيء اتصال عبر الطبقة الثانية Data Link Layer 2 بها و ذلك عبر جهاز سويتش في الشبكات السلكية أو أكسس بيونت في الشبكات اللاسلكية و في بعض الأحيان عبر الطبقة الثالثة Network Layer3 عبر تخصيص IP صالح له

Authentication User



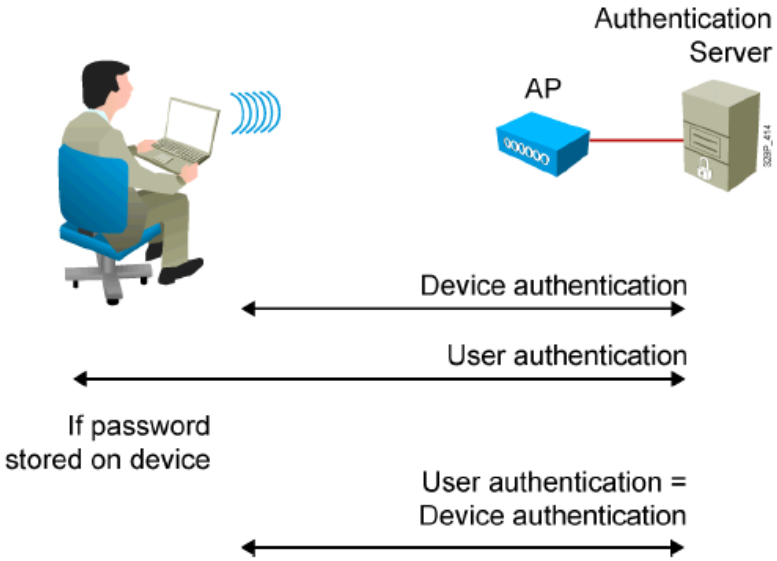
و يتم توثيق دخول المستخدمين في الأنظمة الأمنية بأحد تلك الأشياء

أولها التوثيق باستخدام شيء تعرفه Something you know مثل كلمة المرور Password و هي الطريقة الشائعة للتوثيق و لكن يعيبها ضرورة الحفظ

ثانيها التوثيق باستخدام شيء تملكه Something you have مثل استخدام كروت الولوج الذكيةSmart Card

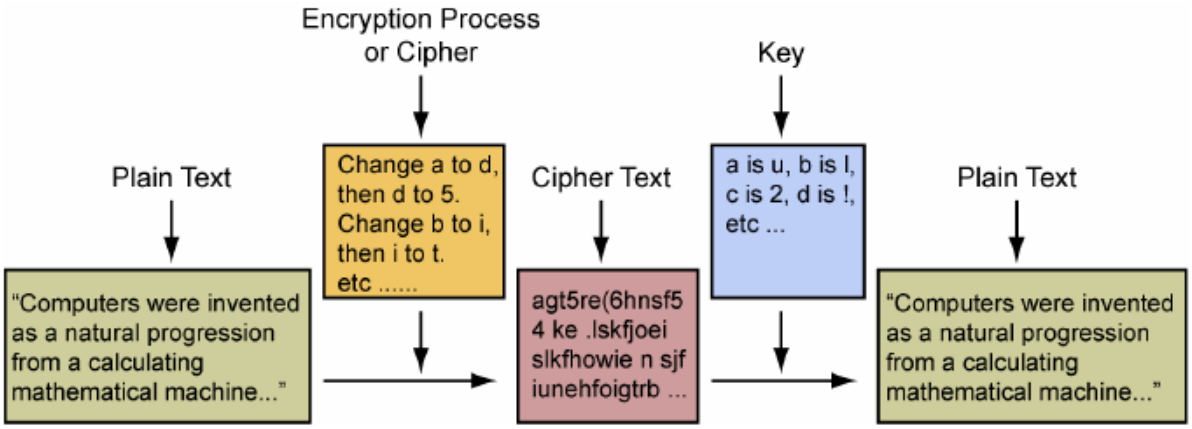
ثالثا التوثيق باستخدام جزء منك something you are مثل بصمة الإصبع fingerprint أو قزحية العين

Authentication Devices



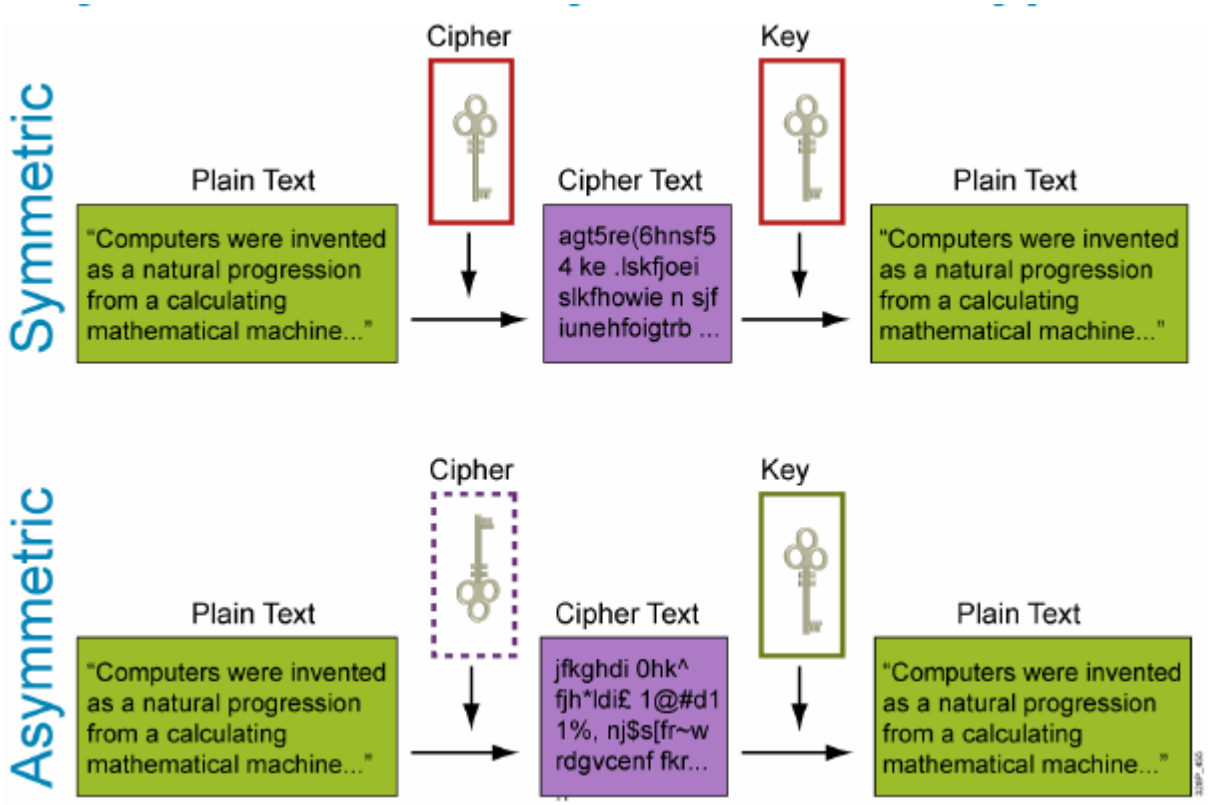
الطرق السابقة تستخدم لتوثيق دخول الأشخاص و لكن ماذا عن توثيق دخول الأجهزة للشبكة و ذلك لضمان عدم دخول الأجهزة الغير مرغوب فيها للشبكة ، و يتم استخدام Signature لتوثيق الأجهزة طبقا لمواصفات كل جهاز بغض النظر عن الشخص الذي يدخل و هذا من عيوبه

Encryption



التشفير Encryption هو عملية تحويل البيانات المفهومة Plaintext الي بيانات غير مفهومة unreadable باستخدام سلسلة تشفير Cipher و ذلك لضمان وصول البيانات الي الأشخاص أو الأجهزة التي تملك مفاتيح التشفير key لعمل العملية العكسية المسماة فك التشفيرDecrypt

أنواع التشفير



و للتشفير نوعان هما Symmetric وAsymmetric

Symmetric encryption

فأما Symmetric encryption فتتم عملية التشفير باستخدام سلسلة تشفير cipher معاكسة للمفتاح Key المستخدم في عملية فك التشفير فبذلك تكون عملية التشفير encryption معاكسة تماما لعملية فك التشفير decryptionو هذه العملية بسيطة و سريعة و لذلك فكسرها سهل و سريع أيضا و تستخدم في الأنظمة التي يكون فيها وقت التشفير أهم من قوة التشفير

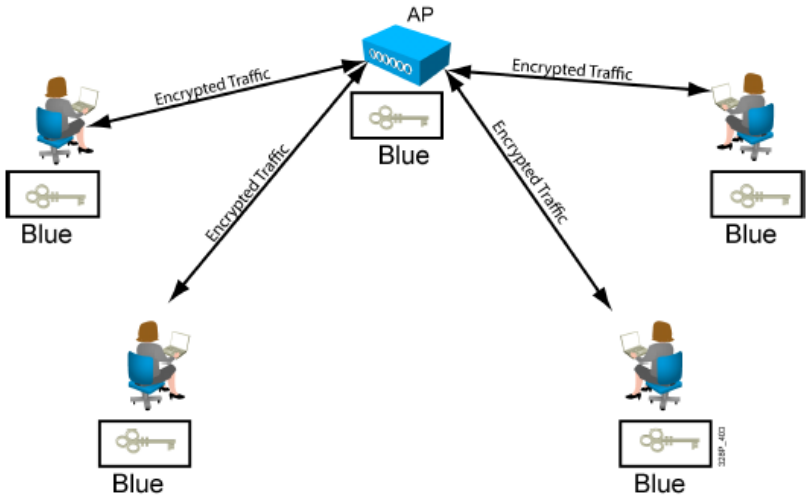
Asymmetric encryption

و أما Asymmetric encryption فتتم عملية التشفير باستخدام سلسلة تشفير cipher مختلفة عن Key مفتاح المستخدم في عملية فك التشفير و كل منهما لا يصلح الا للعملية التي صنع لأجلها و تستخدم هذه الطريقة عندما يكون قوة التشفير أهم من وقت التشفير

Key Management

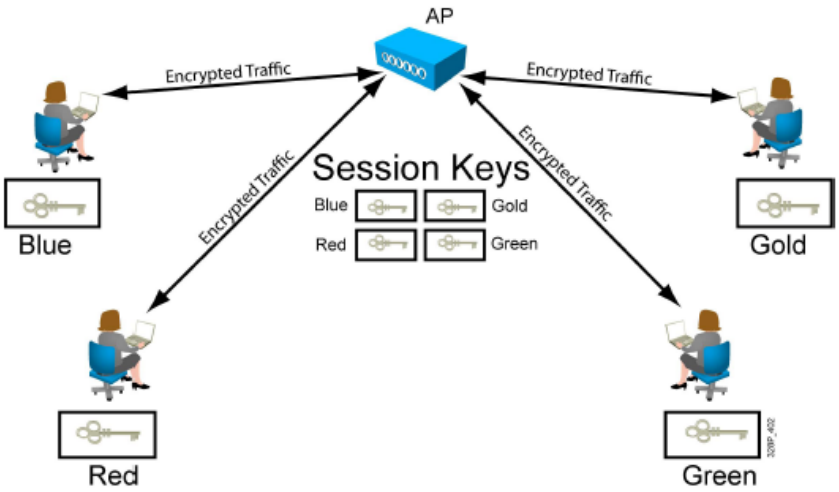
تتم استخدام طريقتين لعملية فك التشفير أحدهما Common Key أوIndividual

Common Key



هنا سيستخدم كل مستخدم مفتاح ولوج خاص به و هذا الأمر يصلح للشبكات الكبيرة حيث يكون الأمن أهم و يكون لكل مستخدم صلاحيات و لكن يعيب هذا الأمر احتياجه لإعدادات و أجهزة أخري و يأخذ وقت أكبر لمعالجة كم طلبات التوثيق و التشفير

Individual Keys



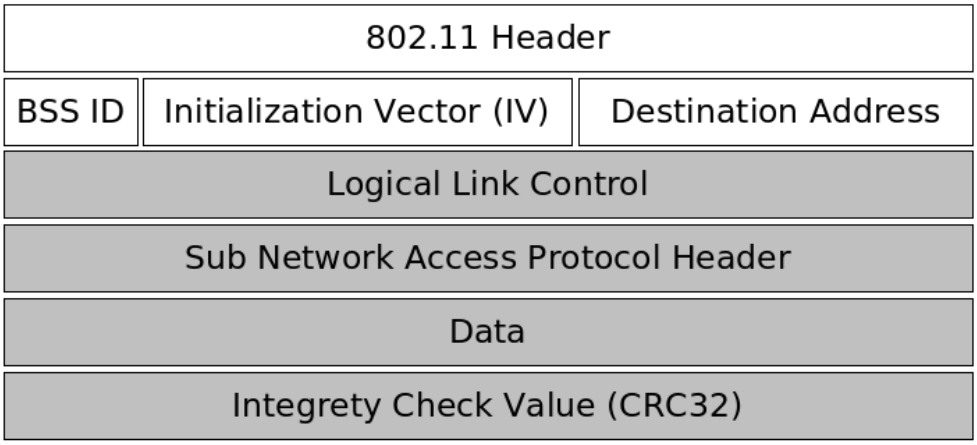
هنا سيستخدم كل مستخدم مفتاح ولوج خاص به و هذا الأمر يصلح للشبكات الكبيرة حيث يكون الأمن أهم و يكون لكل مستخدم صلاحيات و لكن يعيب هذا الأمر احتياجه لإعدادات و أجهزة أخري و يأخذ وقت أكبر لمعالجة كم طلبات التوثيق و التشفير

Wired Equivalent Privacy (WEP)

هي خوارزمية تشفير بيانات encryption algorithm و تقنية أمنية للشبكات اللاسلكية التي تعمل طبقا لمعيار IEEE 802.11 و تم اطلاقها في سبتمبر من عام 1999 كوسيلة لحماية خصوصية البيانات data confidentiality التي تنتشر عبر الشبكات اللاسلكية و يعتبر بذلك أول 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



الشكل السابق هو شكل رزمة الوايرلس Wireless Packet و يتكون كما تري من جزئين أولهما غير مشفر و هو الجزء الغير مظلل في الشكل و هم

- 802.11 Header و هي مقدمة الرزمة و التي تعبر عن الشبكات اللاسلكية غير مشفرة
- BSS ID Basic Service Set Identifier و هو العنوان الفيزيائي للأكسس بوينت AP MAC
- IV initialization vector رقم عشوائي يتم اختياره من قبل المرسل و المستقبل و يرسل بشكل غير مشفر مع الباسورد أو WEP Key و هو نقطة الضعف في WEP

باقي أجزاء الباكت و هي التي تحتوي علي البيانات و غيرها يتم تشفيرها Encrypted

تشفير WEP

لتشفير Encryption البيانات اللاسلكية يستخدم WEP خوارزمية تدقيق stream cipher تسمي Ron's Code 4 (RC4لتوليد 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 غند المستقبل

و ينقسم كل Key system الي جزئين أولهما هو WEP Key و هو رقم التشفير الذي تدخله في الجهاز و الثاني هو (IV) initialization vector 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 و256-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

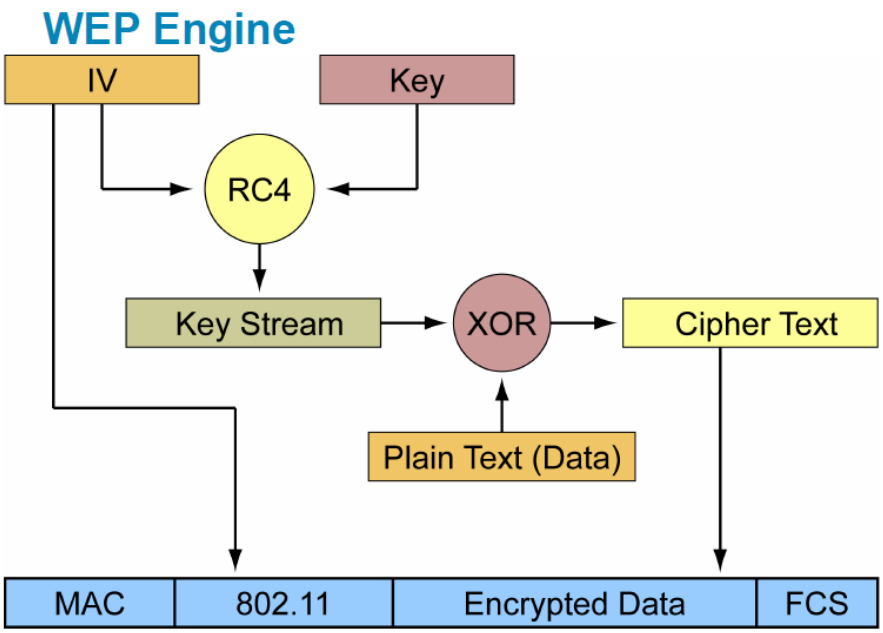
فأما 128-bit WEP الذي يسمي أيضا (WEP-104) لأنه يحتوي علي 26 byte سداسي عشر hexadecimal (0-9 , A-F) كل بايت يحتوي علي 4 bits اي في النهاية 104 bit يتم اضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل الي 128-bit WEP

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

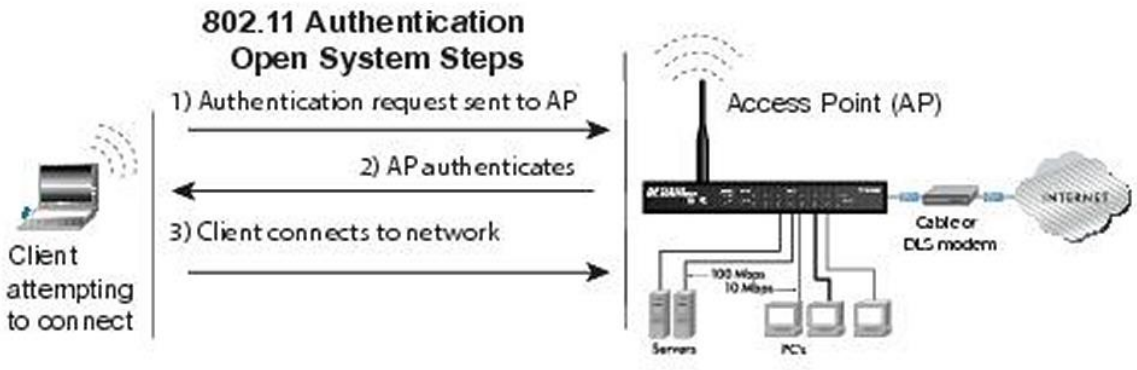
و يتم جمع IV مع Key ثم اضافة خوارزمية تدقيق خوارزمية تدقيق stream cipher تسمي RC4 لينتج Keystream ثم جمعها بطريقة XOR مع plain text ليخرج لنا في النهاية كود التدقيق



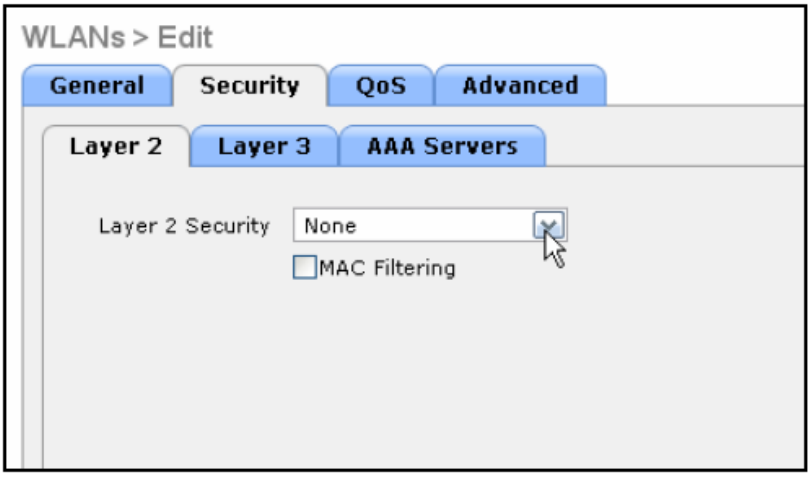
توثيق WEP

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

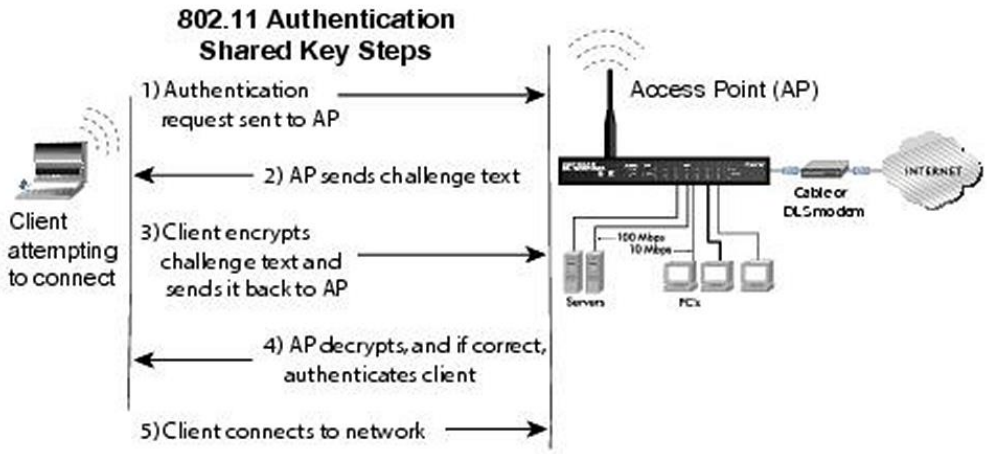
أما Open System authentication فلا يحتاج مستقبل الإشارة أن أي ترخيص لإستقبالها و يستطيع أي أحد أن يدخل الي الشبكة عبر الأكسس بوينت بما يسمي عملية الإرتباط Associate و يستخدم هنا WEP فقط في تشفير البيانات المرسلة كي لا تري من الأشخاص خارج الشبكة



و تستطيع تعميم هذا الأمر علي كل الأجهزة في شبكتك باستخدام الكنترولر هكذا WLAN > Edit > Security settings



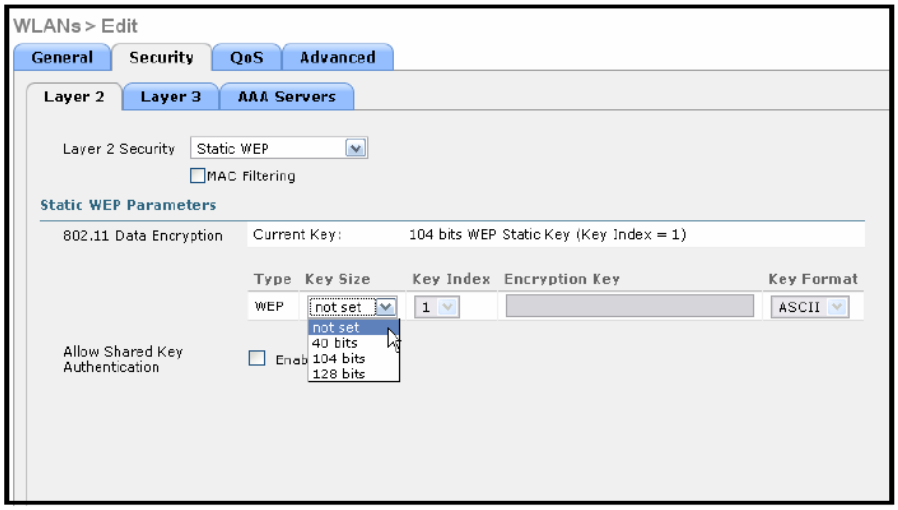
و أما Shared Key authentication فيتم استخدام مفتاح WEP للتوثيق و التشفير علي أربع خطوات أولها يقوم الكلاينت بإرسال طلب توثيق لدخول شبكة الأكسس بوينت يقوم بعدها الأكسس بوينت بالرد برسالة غير مشفرة تسمي clear-text challenge يقوم الكلاينت بعد استلام الرسالة بتشفيرها باستخدام مفتاح WEP ثم يرسلها للأكسس بوينت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



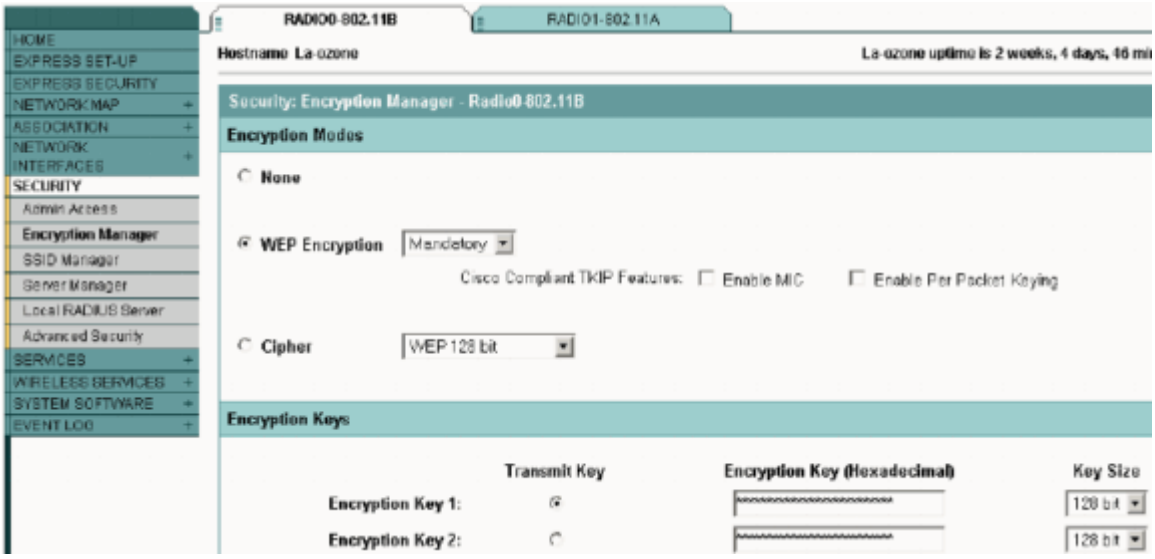
ان كنت تظن أن هناك فرق بين الإثنين في مستوي الأمان و أن Shared Key authentication أوثق و أكثر أمانا فأنت مخطيء فكلا من الطريقتين سهل اختراقها أو أن أحدهما فقط أسهل من الأخري فباستخدام برامج التقاط و تحليل الإشارة لرسالة clear-text challenge ايابا و ذهابا من الكلاينت أي قبل و بعد التشفير يتم معرفة خوارزمية 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

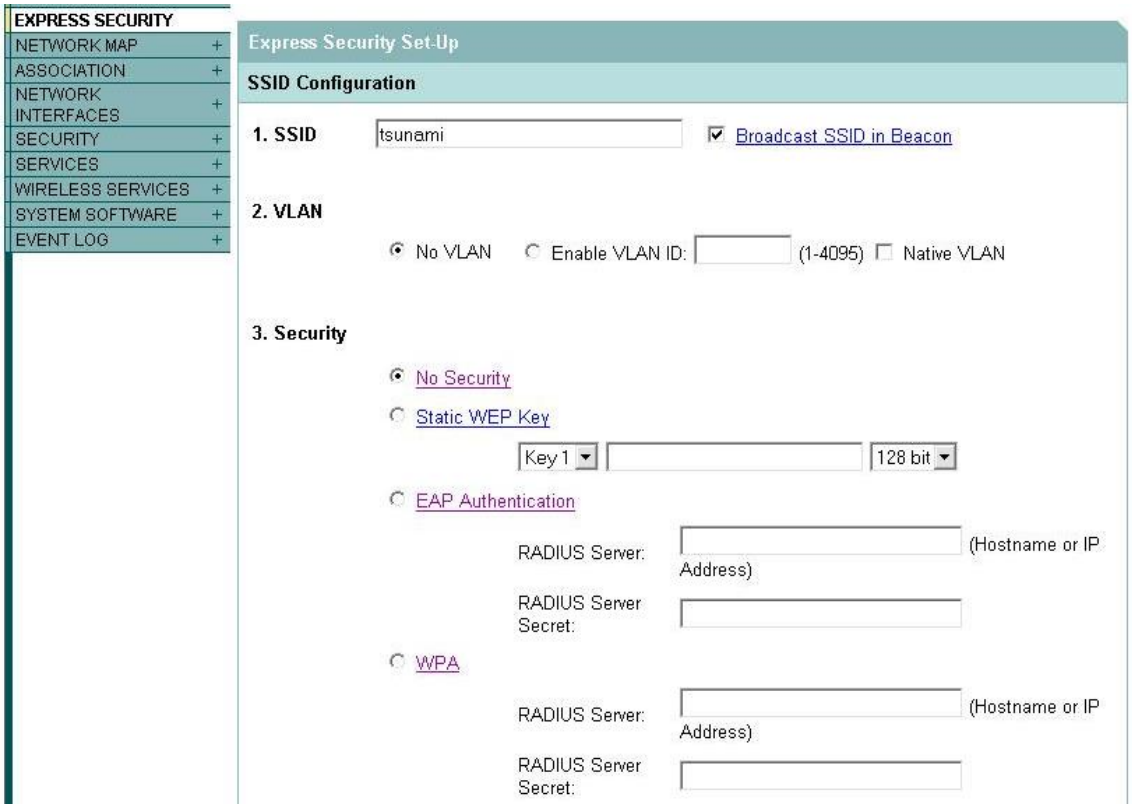
و هذه صفحة الكنترولر الخاصة بهذا النوع من التوثيق و الوصول اليها عن طريق WLAN > Edit > Security settings



و هذه هي صفحة إعداد WEP لتأمين الأكسس بوينت من سيسكو Aironet APs التي تعمل علي نسخة Cisco IOS Software

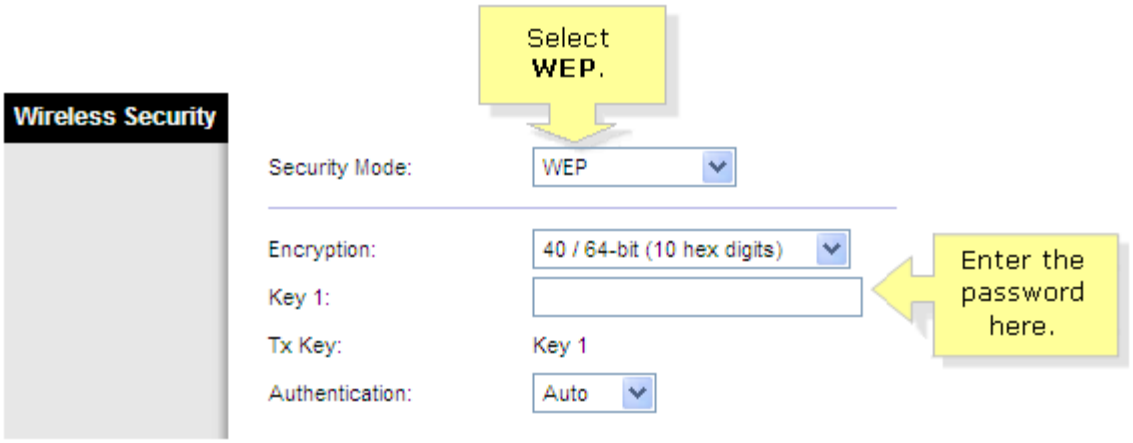


و هذه أكسس بوينت أخري من سيسكو و تري اختلافات في طريقة العرض

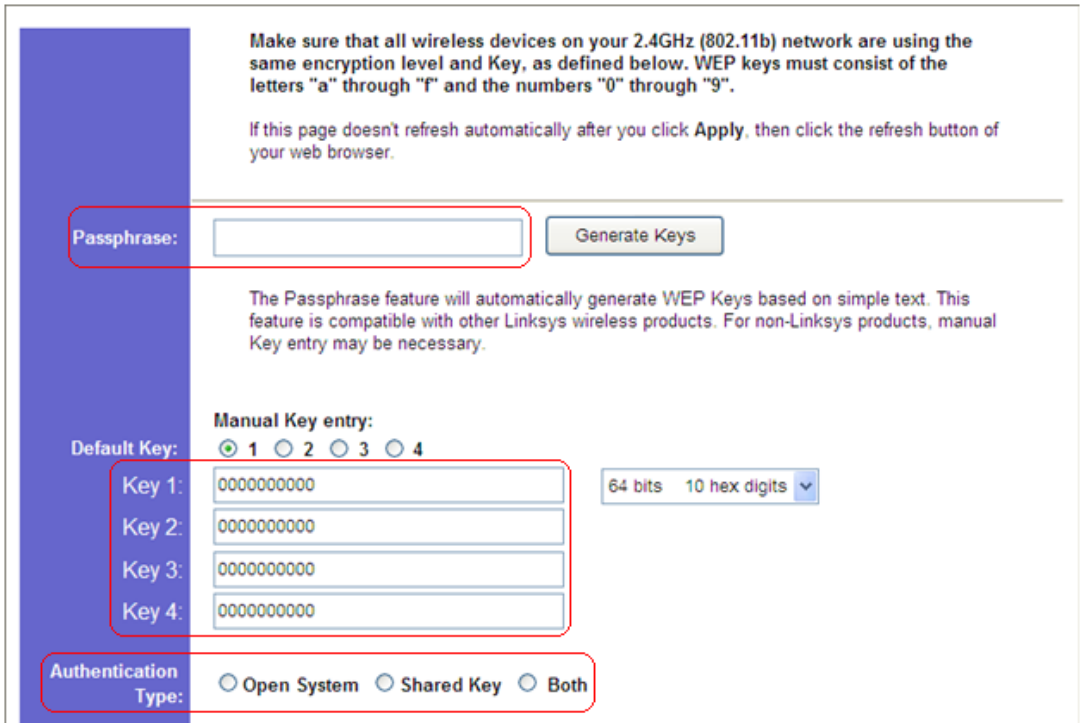


و كما تري فانك تستطيع توليد أكثر من مفتاح لإستخدامهم و كل مربع نصي يحتوي علي مفتاح يسمي Slot و هو مهم هنا لفهم طريقة عمل الكود في نظام CISCO IOS الذي سنشرحه في الخطوة التالية بإذن الله تعالي

و هذه هي جزء من صفحة أكسس بوينت من منتجات لينكسيس



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



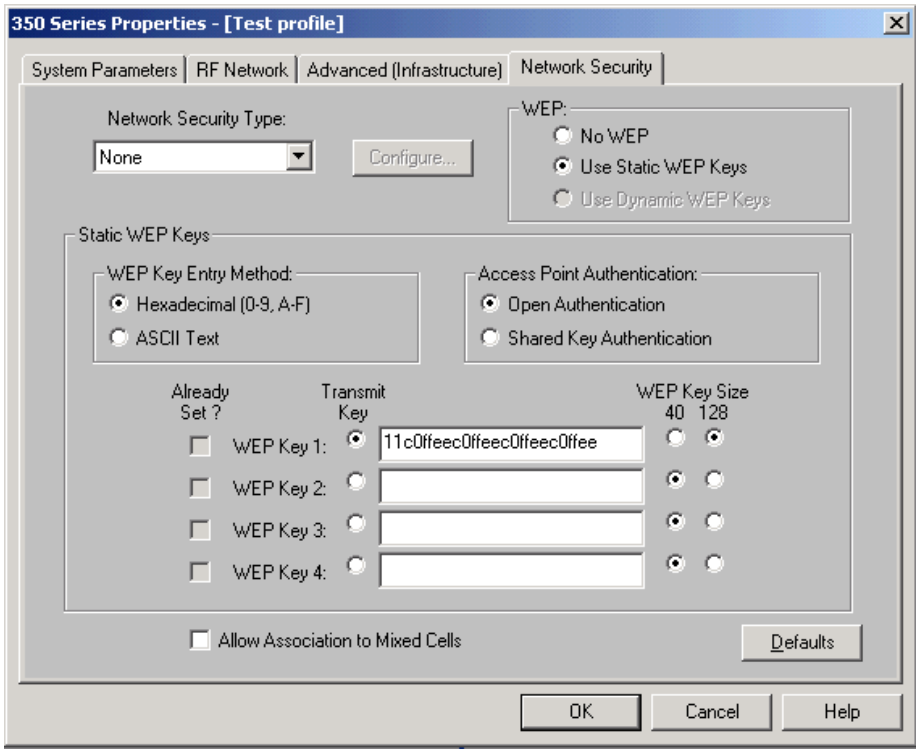
و المثال التالي يوضح كيفية تأمين الأكسس بوينت من نوع Aironet 1200 من سيسكو و سنقوم إعداده و الدخول عليه مثل أي راوتر أو سويتش من سيسكو

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

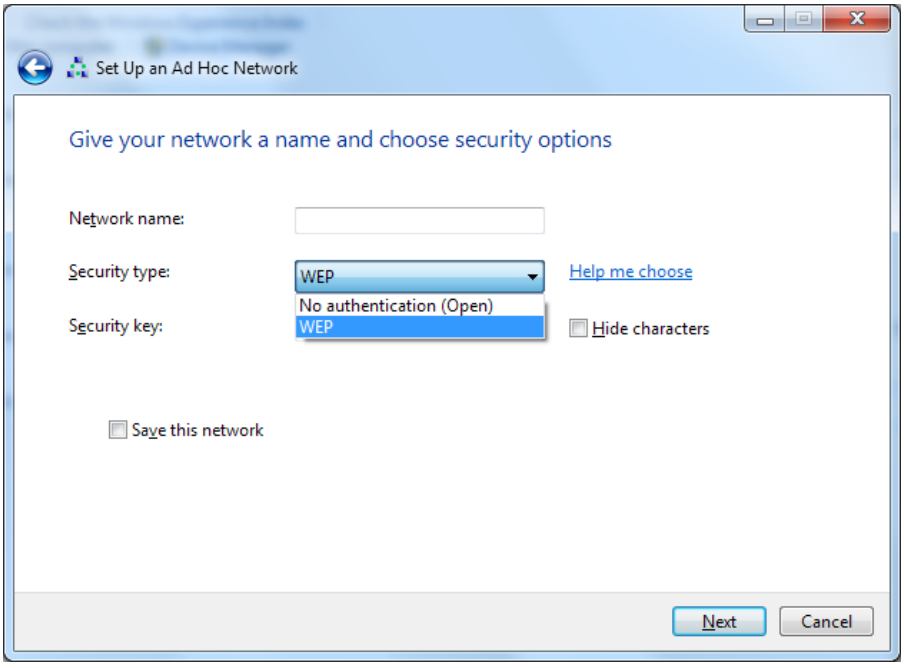
سنقوم بتوليد المفتاح الثالث من نوع WEP بطول 128 bit اي 26 حرف و هم 12345678901234567890123456 رقم أو حرف سداسي عشر و ذلك في الشبكة VLAN 22

```
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
```

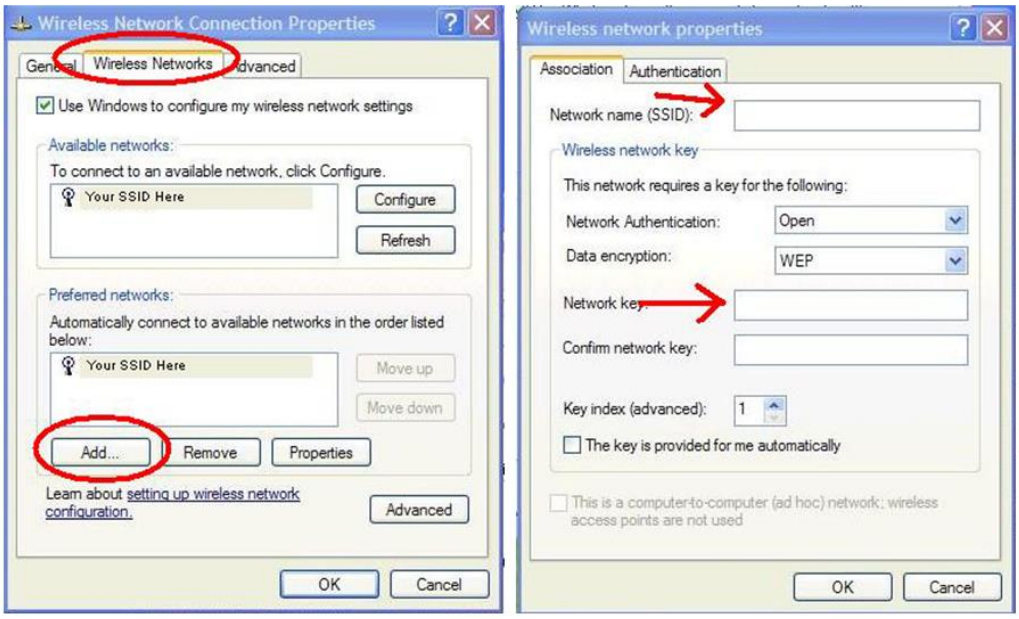
و في Client و اذا كنت تستخدم برنامج Aironet Client Utility (ACU). من سيسكو فستكون هذه الصفحة التي ستضبط بها الاعدادات لإلتقاط الوايرلس



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

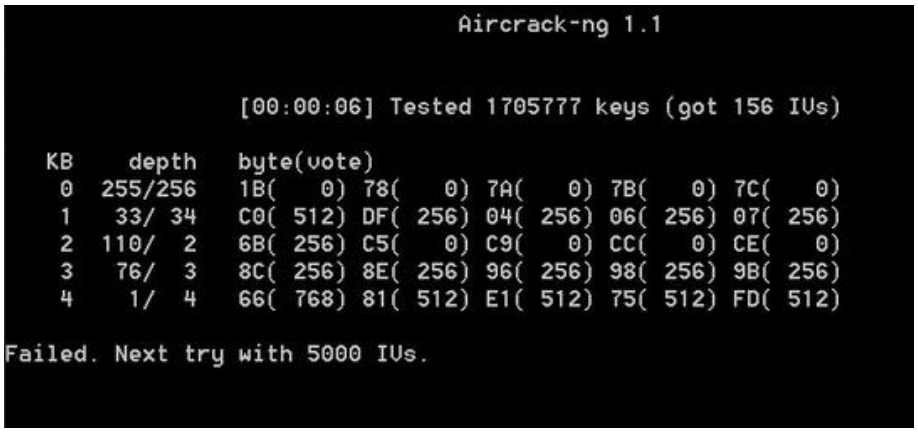
و تستطيع الإعداد من خلال سطر الأوامر terminal

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

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 plain text أي 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



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 Extensible EAP Authentication Protocol و قام بتعيير دوري في WEP Key و لكن هذا التحسين حصري فقط لشركة 3COM

IEEE 802.11i/WPA2

عرفنا مدي ضعف تقنية التشفير Wired Equivalent Privacy (WEP) و لهذا قامت مؤسسة Wi-Fi و جمعية مهندسي الكهرباء و الإلكترونيات IEEE بالعمل سويا لاستبداله بمعيار أكثر أمانا و خرج الي النور جيلين الأول يخص Wi-Fi و هو Wi-Fi Protected Access (WPA) و الثاني يخص IEEE و يسمي IEEE 802.11i/WPA2

فأما Wi-Fi Protected Access (WPA) فقد قامت منظمة الواي فاي بإطلاقه في 2003 بغرض سرعة استبدال المعيار القديم WEP و هو النسخة الأولية draft للمعيار الأحدث **Wi-Fi Protected Access II (WPA2)** و الذي يسمي أيضا IEEE 802.11i

و أما IEEE 802.11i/WPA2 فهو كما ذكرنا المعيار الأحدث و الأعقد و قد أطلق في 2004 و لهذا فإنه يسمي أيضا IEEE 802.11i-2004 و كل أكسس بوينت التي أنتجت بعد 2003 تستطيع أن تتعامل مع WPA مباشرة أو بترقية برامج تصنيعها firmware

مميزات WPA

تكمن فكرة WPA في استخدام Temporal Key Integrity Protocol (TKIP) و ذلك لتغيير مفاتيح تشفير بطول 128-bit بشكل اوتوماتيكي لكل Packet علي عكس WEP الذي يستخدم مفاتيح تشفير بطول 40-bitأو 104-bit تدخلها في الأكسس بوينت و الجهاز الذي سيستخدم الشبكة و الذي يستخدم تقنية RC4 و تم بعدها تعديل بنيته ليعتمد علي AES encryption

يحتوي أيضا WPA علي تقنية تسمي Micheal و هي تقنية فحص للرزم MIC message integrity check و هي البديلة لتقنية CRC cyclic redundancy check المستخدمة في WEP و هذه التقنية هي التي مكنت WPA من منع إختراقه بحجب عملية capturing التي تستخدم في أخذ نسخ من الرزم المرسلة و تحليلها لإختراق الشبكة و رغم قوة MIC الا أنه استبدل ايضا في WPA2 بوسيلة أكثر قوة

WPA Authentication Modes

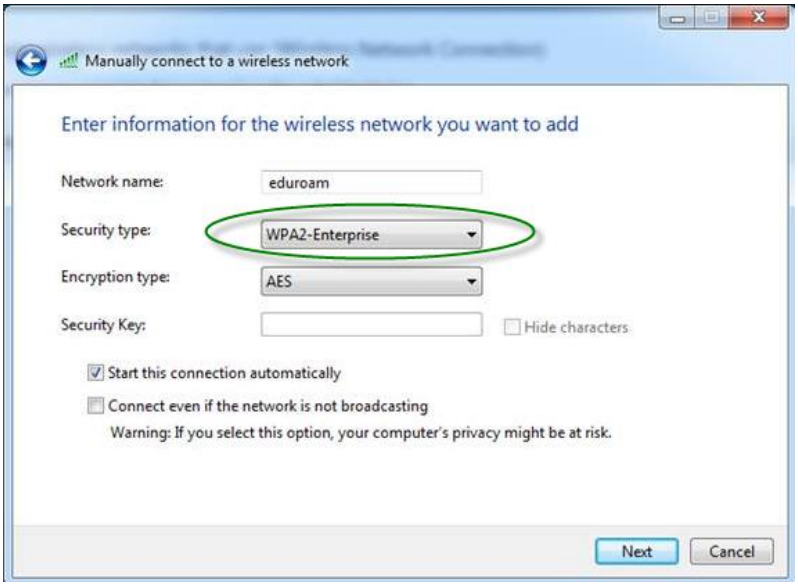
Enterprise (802.1X Authentication)	Personal (PSK Authentication)
Authentication server required	Authentication server not required
RADIUS used for authentication and key distribution	Shared secret used for authentication
Centralized access control	Local access control
Encryption uses TKIP, AES optional	Encryption uses TKIP, AES optional

لدينا نوعان للتوثيق هما (WPA Personal) و (WPA Enterprise)

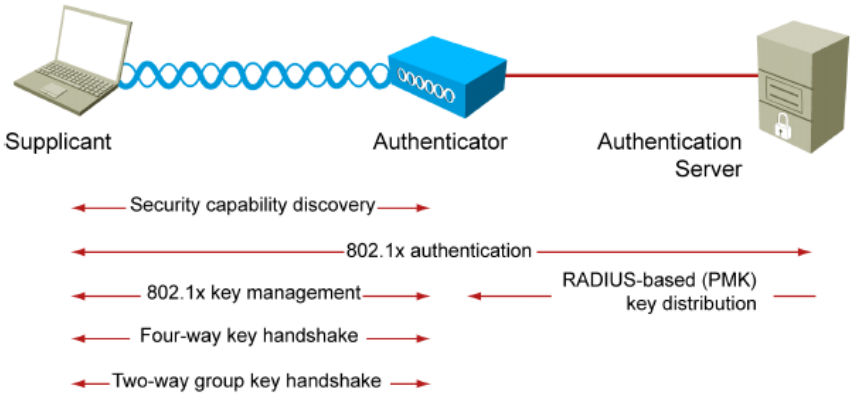
WPA Personal

في WPA Personal يتم بإستخدام مفتاح متفق عليه بين الجهاز و الأكسس بوينت (WPA- pre-shared keys (PSK و هو المستخدم غالبا في الشبكات الخفيفة SOHO مثل المنازل حيث يعتبر استخدام RADIUS server خيار غير عملي و لهذا فإن WPA يشبه WEP في كونه يسمح بإستخدام pre-shared key (PSK) كمفتاح مشترك بين client و access point

WPA Enterprise



و أما (WPA Enterprise) فيتم بإستخدام سيرفر مركزي ببروتوكولات توثيق 802.1X/EAP أو بأي نوع EAP مثل (Transport Layer Security) EAP-TLS أو (Protected EAP) PEAP EAP-TTLS أو EAP [Microsoft Challenge Handshake Authentication Protocol] MS-CHAP v2 أو غيرها

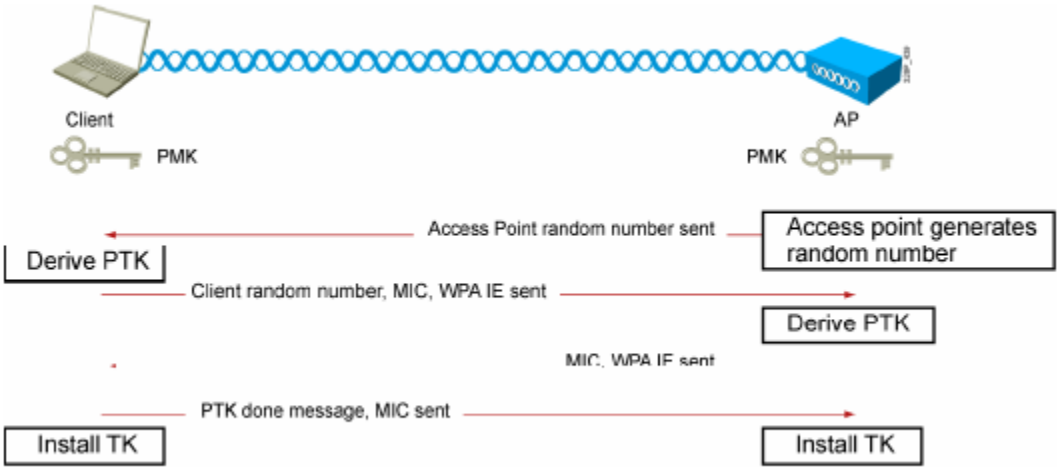


كما هو الحال مع بروتوكلات التوثيق يتم استخدام فريمات التراسل (probe request, probe response) بين الجهاز و الأكسس بوينت الا أن الإختلاف يكمن في أنه لابد أن يتوافق الأكسس بوينت و الجهاز علي هذه العملية أمنيا ثم يستكمل خطوات توثيق 802.1X و عند استكمالها يقوم السيرفر بإرسال master key الي الأكسس بوينت و التي أخذها مسبقا من الجهاز الطالب للإتصال و لهذا يسمي المفتاح Pairwise Master Key (PMK)

ثم يتم بعدها عملية تراسل رباعي four-way handshake و التي يتم منها توليد مفتاح آخر يسمي Pairwise Transient Key (PTK)

ثم يبدأ بعدها مرحلة جديدة من التراسل تسمي two-way group key handshake يحدث تراسل مشفر بواسطة Group Transient Key (GTK), بين client و authenticator

Unicast Keys: Four-Way Handshake



يتم التراسل بين الأكسس بوينت عبر أربع خطوات تسمي four-way handshake ينتج بعدها مفتاح جديد Pairwise Transient Key (PTK) يؤكد عملية الإتصال و التي بدأت عبر مفتاح Pairwise Master Key (PMK)

لعملية التراسل WPA four-way الرباعي عدة فوائد أهمها

- تأكيد مفاتيح PMK بين Supplicant و Authenticator
- توليد المفاتيح المؤقتة pairwise temporal keys
- توثيق معاملات التأمين المتبادلة

قبل أن تحدث عملية التراسل الرباعي WPA four-way handshake لابد أن يتم توليد pairwise master key كنتيجة لعملية توثيق 802.1X بين client و server authentication ثم تتوالي الخطوات التالية

أولا يقوم AP بإرسال رقم عشوائي Nonce الي Client يستخدم لجلسة واحدة فقط one session

ثانيا بهذا الرقم العشوائي و باستخدام أيضا PMK يقوم Client بتوليد مفتاح لتشفير البيانات التي سترسل الي AP و يتم استخدام دالة تسمي pseudo-random function (PRF) و ذلك لحساب PTK كدالة في الأرقام العشوائية المتولدة في Client و AP و في MAC و في PMK أو المفتاح المشترك و يتم حماية الفريم المرسل بواسطة frame check sequence (FCS) بواسطة تقنية MIC (message integrity check) و ذلك للتأكد من أن الفريم لم يتم اعتراضه

ثالثا يقوم الأكسس بوينت بعد تلقيه nonce بإرساله مرة اخري الي Client بنفس السياسة الأمنية المستقبل بها و يقوم أيضا الأكسس بوينت بإرسال group key و بهذا يكون هناك توثيق بين الأكسس بيونت و الجهاز

رابعا يتم تأكيد أن المفاتيح قد تم ارسالها و العملية جاهزة للتراسل

بمجرد الحصول علي المفتاح المؤقت PTK بطول 64 bit فإنه يتم تقسيمه الي خمس مفاتيح

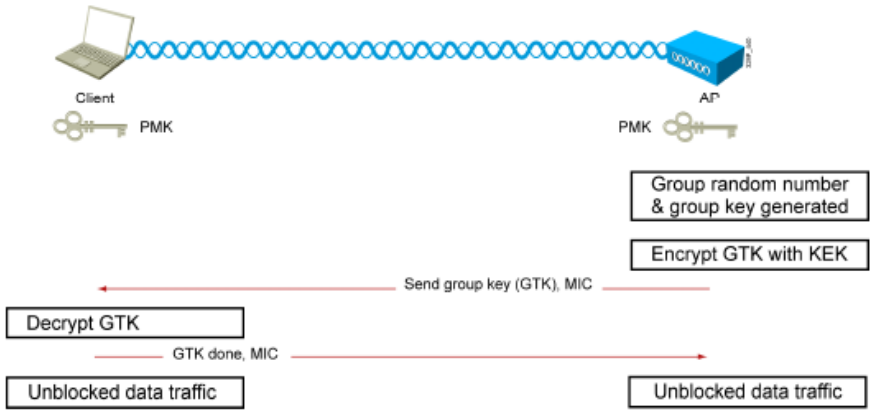
الأول بطول 16-byte و يسمي EAP over LAN-Key Encryption Key و يختصر لـ EAPOL-KEK و يستخدم في تشفير أي بيانات إضافية مرسلة الي Client

الثاني بطول 16 byte و يسمي EAPOL-Key Confirmation Key و يختصر لـ KCK و يستخدم لحساب MIC

الثالث بطول 16 byte و هو Temporal Key TK و يستخدم لتشفير و فك تشفير unicast data Packets

الرابع و الخامس كل منهما بطول 8 byte و هما Michael MIC Authenticator و احدهما يستخدم لحساب MIC المرسل مع البيانات المرسلة مع الأكسس بوينت و الآخر مع Client

Group Key Handshake



يستخدم (Groupwise Transient Key) GTK لمنع الجهاز من استقبال أي رسائل من الأكسس بوينت و يتم ذلك عبر التراسل الثنائي two-way handshake بهذا السيناريو

أولا يقوم الأكسس بوينت بإرسال GTK جديد لكل الأجهزة في الشبكة و يتم تشفيرها بإستخدام KEK و حمايتها باستخدام MIC

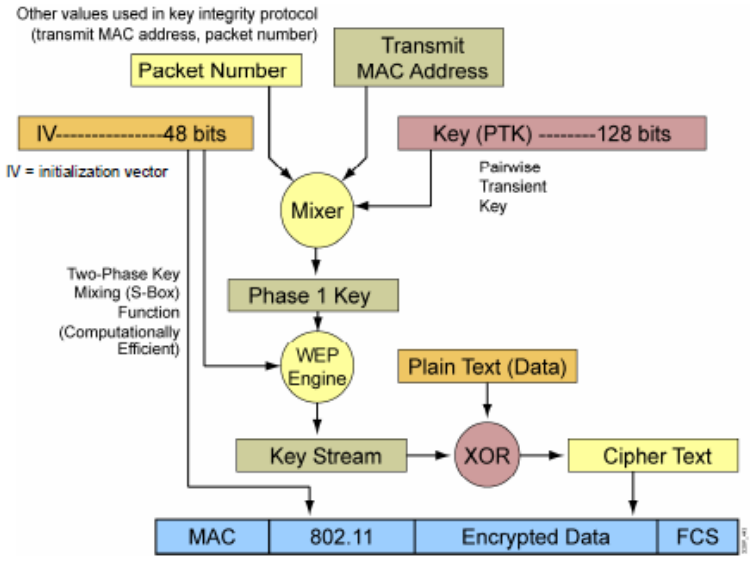
ثانيا تقوم هذه الأجهزة بالإستجابة لـ GTK و الرد علي الأكسس بوينت

و يكون (Groupwise Transient Key) GTK بطول 32 bytes مقسمة الي ثلاث مفاتيح

الأول بطول 16 byte و هو TK Temporal Key و يستخدم لتشفير و فك تشفير unicast data Packets

و الثاني و الثالث كل منهما بطول 8 byte و هما Michael MIC Authenticator و احدهما يستخدم لحساب MIC المرسل مع البيانات المرسلة مع الأكسس بوينت و الآخر مع Client

WPA Encryption



كما أن WPA قد دعم عملية التوثيق authentication بشكل كبير فإنه أيضا فد قام بتحسين التشفير encryption أيضا بشكل رائع حسن و ذلك عبر نظامين هما AES و TKIP

أما AES فهو نظام جديد أقوي من نظام التشفير RC4 المستخدم مع WEP و لكنه يحتاج الي الكثير من الطاقة بالإضافة الي ضرورة دعم الجهاز لهذا النوع من التشفير

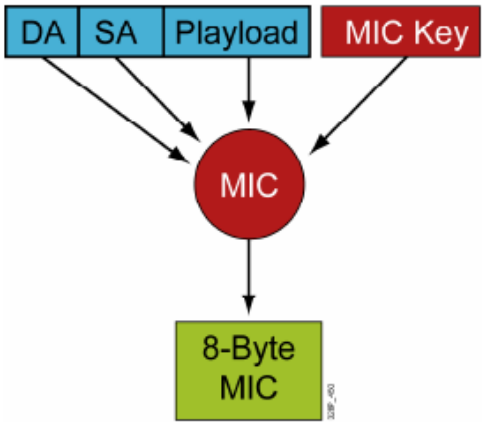
و أما **TKIP** و هو اختصار **Temporal Key Integrity Protocol** فهو بروتوكول لا زال يستخدم تقنية RC4 و هي الخيار الإفتراضي لل WPA الا أن به تحسينات عن الذي يستخدم مع WEP حيث أنه يستخدم مفاتيح بطول 128 bit بعد أن كان يستخدم مفاتيح بطول 40-bit مع WEP

أما العيب الثاني الذي تخطاه WPA هو IV initialization vector فمن المعروف أن المفتاح يتم مزجه مع المفتاح الرئيسي بواسطة عملية XOR كما بالشكل السابق و لأن IV في WEP قيمة محددة لا تتغير و غير مشفرة فإنه و باستخدام بعض برامج بتحليل Packets تستطيع أن تكشف قيمة IV و من ثم تكسر هذا التشفير و ذلك في غضون ساعات قليلة

أما في WPA فتغيرت هذه العملية كذلك أصبح IV بطول 48 bit و ليس بطول 24 bit كما كان في WEP و هذا يحتاج 280 تريليون محاولة لكسره أي ما يساوي محاولات تتم في 645 سنة

كذلك يتم عمل عملية مزج mixer لكل مفتاح PTK مع عنوان الجهاز MAC مع رقم كل باكت مخرجا لنا مفتاح متغير لكل باكت ثم مزج ذلك مع IV ليتم تشفير البيانات المرسلة بها و بهذا فإنه بالإضافة لصعوبة كسر هذا التشفير فإنه الأكسس بوينت يستطيع اكتشاف عملية الإختراق بواسطة عنوان الجهاز المرسل مع مفتاح التشفير

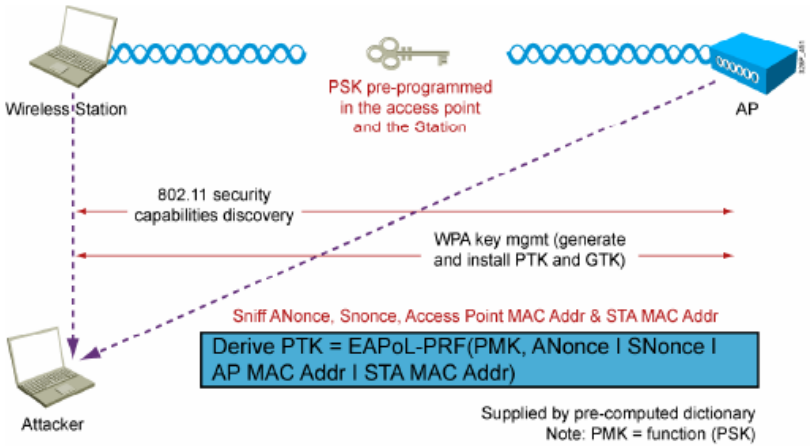
Message Integrity Check



التعديل الآخر في WPA هو استخدام تقنية تسمي Message Integrity Code تختصر الي MIC أو Michael حيث يتم وضع بعض bits القليلة الي الباكت قبل تشفيرها و ذلك لمراقبة مدي سلامة ارسال الباكت

802.11i

الآن لدينا في WPAمفاتيح أطول و IV أطول و مزج فعال و كذلك تقنية MIC للتأكد من سلامة وصول الباكت الا أن عملية التراسل الرباعي الموجودة في WPA PSK المدعوم افتراضيا في شبكات SOHO تغري بالإختراق و ذلك عبر عمل عملية فك الإرتباط deauthentication و من ثم انتحال شخصية أحد أجهزة الشبكة ، و ان كان هذا الأمر أصعب بكثير مما يتم في WEP الا أنه يحدث و هذا ما دعا الخبراء الي الإنتقال الي WPA2



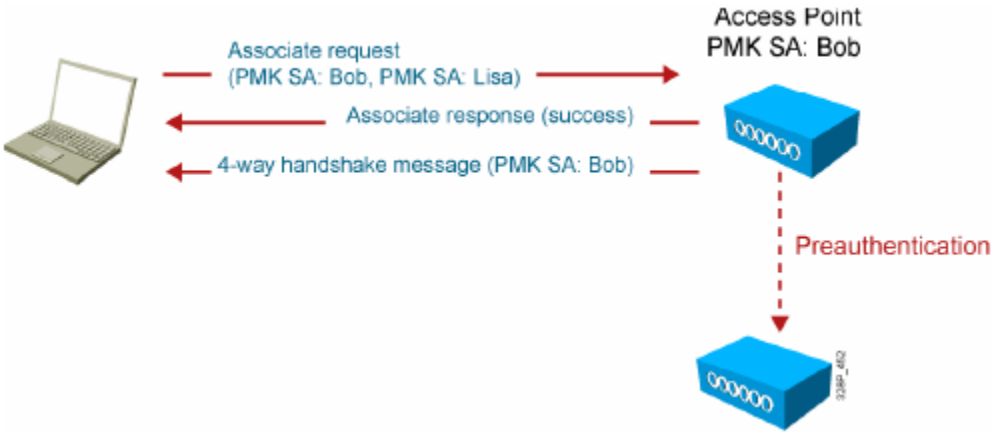
WPA2 مبني علي 802.11i و انتهي منه في 2004 و يدعم بروتوكولات التوثيق المركزي 802.1X و يستبدل تقنية تشفير RC4 بالجيل الثاني من طرق التشفير AES الذي أطلق من قبل National Institute of Standards and Technology (NIST) والذي يستخدم عمليات مزج تسمي Rijndael algorithm و يعلو بالتأمين بإستخدام IV لكل بلوك مرسل و يستخدم أيضا طلايقة التأكد من وصول الباكت MIC مثلما يفعل WPA

و هذه مقارنة بين **WPA**, **WPA2**, **802.11i**

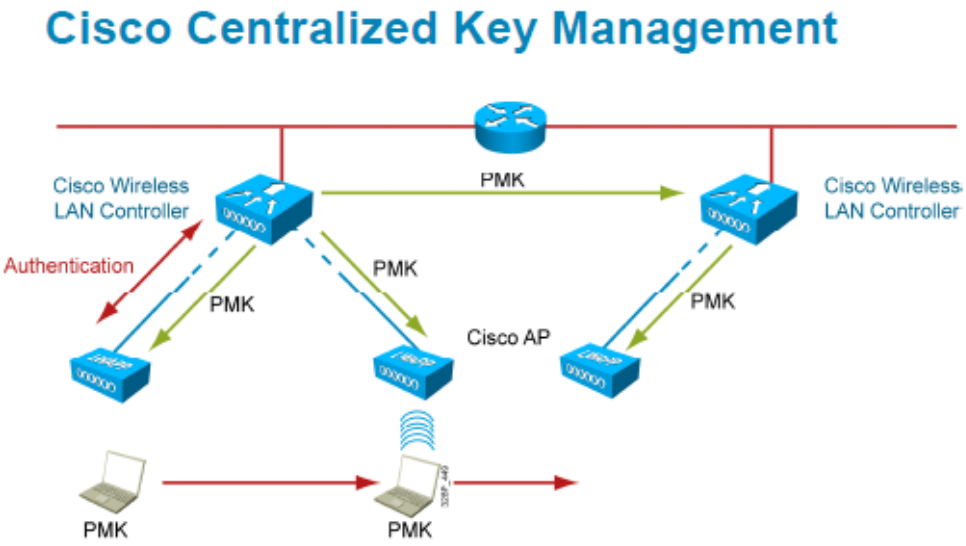
WPA	WPA2	802.11i
SOHO	Enterprise	Enterprise
802.1X authentication/PSK	802.1X authentication/PSK	802.1X authentication
128-bit RC4 w/ TKIP encryption cipher	128-bit AES encryption cipher	128-bit AES encryption cipher
Ad hoc not supported	Ad hoc not supported	Allows ad hoc
Test devices for compliance	Test devices for compliance	No test, specification

تطوير سيسكو الخاص بـ WPA

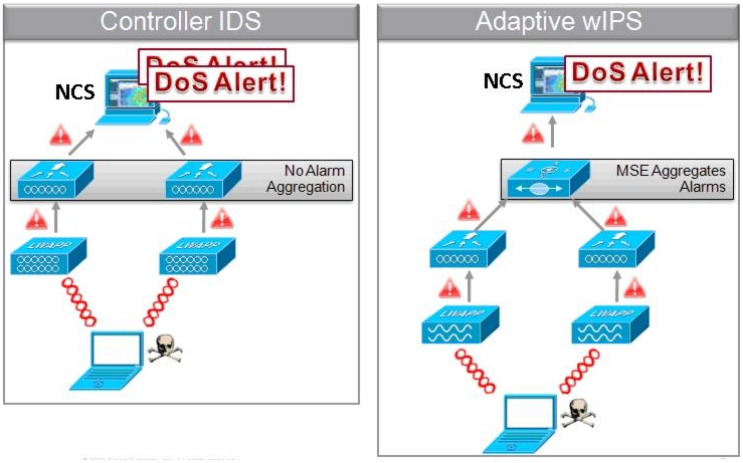
دائما سيسكو لها لمساتها في أي تقنية ومن هذه اللمسات الرائعة key caching حيث يتم حفظ مفاتيح الولوج عند خروج الأجهزة من الشبكة وذلك عبر تثبيت قيمة SA لكل جهاز وعند رجوعه الي حيز الشبكة يستطيع الدخول مرة أخري بدون الحاجة الي إعادة التوثيق



كذلك قامت سيسكو بتطوير WPA بعمل مركزية لمفاتيح الولوج تسمي Cisco Centralized Key Management حيث يقوم الكنترولر بإدارة عمليات الربط association كما يحدث في 802.1X حيث يقوم الكنترولر بدور الموثق authenticator و ليس الأكسس بوينت فبمجرد ارتباط الأكسس بيونت بالكنترولر يتم توثيقه في أقل من 100 مللي ثانية و يحدث نفس الأمر عند رجوعه مرة أخري في حال ابتعاده حيث يحدث تخزين caching لمفتاح PMK



Wireless IDS/IPS

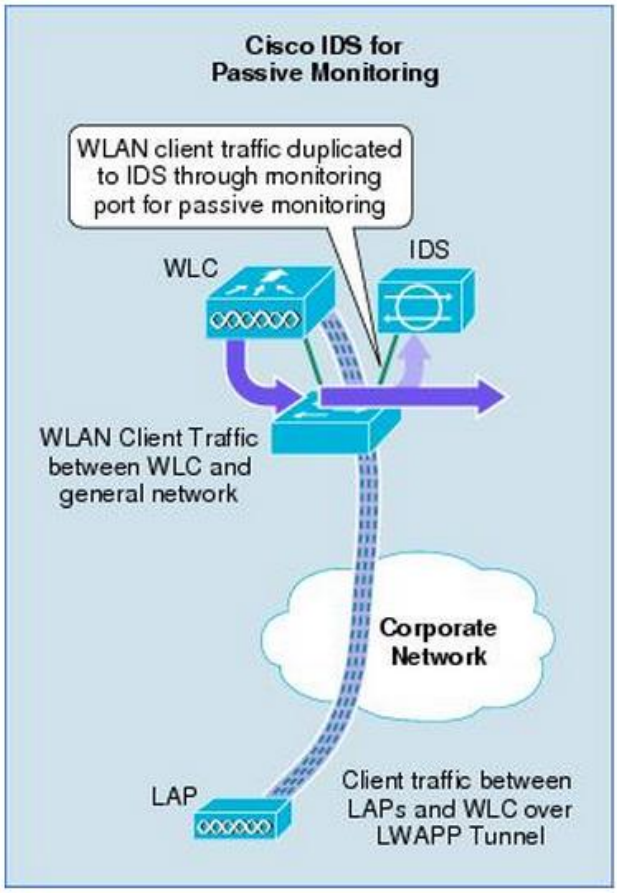


تعتمد الأنظمة علي سيناريوهين لحمايتها من خطر الإختراق أولهما هو الكشف Detection و الثاني هو المنع prevention و الشبكات اللاسلكية ليست بعيدة عن هذه الأنظمة فهي تستخدم سيناريو Intrusion Detection Systems IDSs للكشف عن هذه المخاطر بدون استباق اعتراضها و تستخدم Intrusion Prevention System IPS لإعتراض المخاطر استباقيا

Wireless IDS

من الخصائص الرائعة في البروتوكول اللاسلكي LWAPP أنه يحتوي رسائل راديوية إدارية Radio Resource Management PRM بين الأكسس بوينت و الكنترولر لمراقبة المحيط الراديوي للشبكة و اختبار التداخلات Interference و الحمل علي الشبكة Traffic Load

تتلخص فكرة Intrusion Detection Systems IDSs بأن يقوم الأكسس بوينت الذي يعمل في الوضع العادي Local كل فترة لمدة 30 ms بمراقبة القنوات الأخري في الشبكة لتحديد المخاطر التي توجد في هذه القنوات و التي تتمثل في تواجد أكسس بوينت غريبة Rogue AP أو اتصالات Ad Hoc و يقوم أيضا سيرفر WCS بتوضيح أماكن الأكسس بوينت التي لا تنتمي للشبكة و يعبر عنها علي خرائط WCS بـ External Known أو Internal Known



و الي هنا تبدأ عملية Intrusion Prevention System IPS حيث بعد أن يقوم الأكسس بوينت بإخبار الكنترولر الي ما وصل اليه ليقوم باتخاذ اللازم من تعريف مدير الشبكة أو اتخاذ القرار بناء علي السياسة الأمنية التي تم دمجها به

في المواقع المتباعدة Branch – remote و التي تعتمد مصادر بياناتها علي المراكز الرئيسية يتم استخدام طريقتين للتأكد من وجود أجهزة أكسس بوينت دخيلة هما Rogue Location Discovery Protocole RLDP و Rogue detector

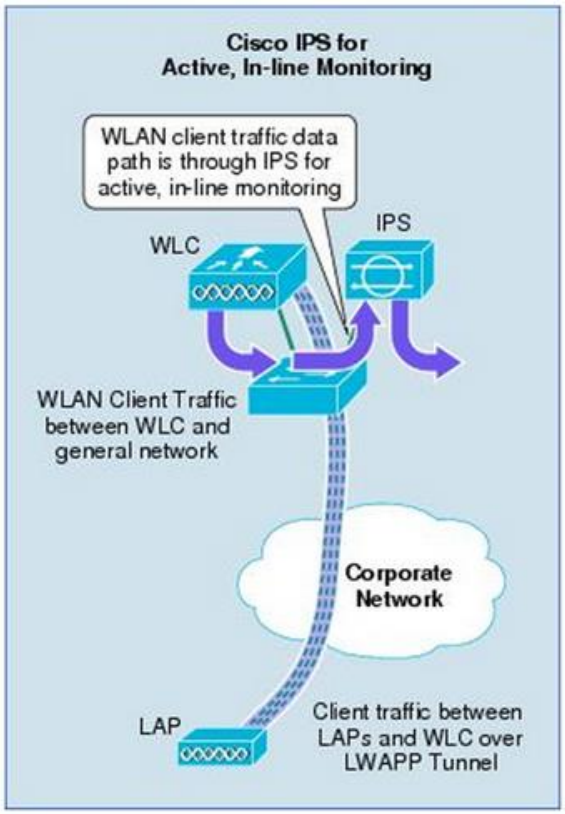
فأما RLDP فهو بروتوكول يقوم بحث أكسس بوينت من الموجودين بالشبكة "المخبر ☺ " بالإتصال بالأكسس بوينت الدخيل ثم ارسال بياناته الي الكنترولر ثم يقوم الكنترولر باستضافته في الشبكة و هذا يتم عندما لا يكون الإتصال بالأكسس بوينت الدخيل يتطلب كلمات مرور أو تشفير

أما في حالة أن الإتصال مشفرا بالأكسس بوينت الغريب فإننا سنحتاج أداة أخري أو جهاز آخر في الشبكة و هو Rogue Detectors و يستخدمه الكنترولر لمراقبة رسائل Address resolution Protocol – ARP المتبادلة بين الأكسس بيوت الغريب و الأجهزة التي تحاول الإتصال به و التي تساعد علي معرفة MAC للجهاز الدخيل و الذي بواسطته نستطيع منعه من الولوج للشبكة

يقوم أيضا الكنترولر في المساعدة علي كشف وجود اتصالات Ad Hoc في الشبكة حيث يقوم بالإيعاز الي الجهاز الذي تم الإتصال به بفك اتصاله بهذه الأجهزة عبر فريمات disassociation

اذن فإن IDS هو نظام أمني يسمح بالكشف عن بعض المخاطر الأمنية و لكن بدون اعتراضها و يترك التصرف لأجهزة أخري

Wireless IPS



هناك مخاطر لا تستطيع الشبكة أن تكتشفها مثل تلك التي تنشأ عن اخطار الإختراق من داخل الشبكة نفسها عندما يقوم جهاز أو مستخدم في الشبكة بمحاولة الوصول الي مصادر غير مصرح له بها

في هذه الحالة يتم استخدام Intrusion Prevention System IPS و ربطه بالكنترولر ليقوم بفلترة كل طلبات الإتصال بالشبكة و كذلك كل طلبات خدمات الشبكة

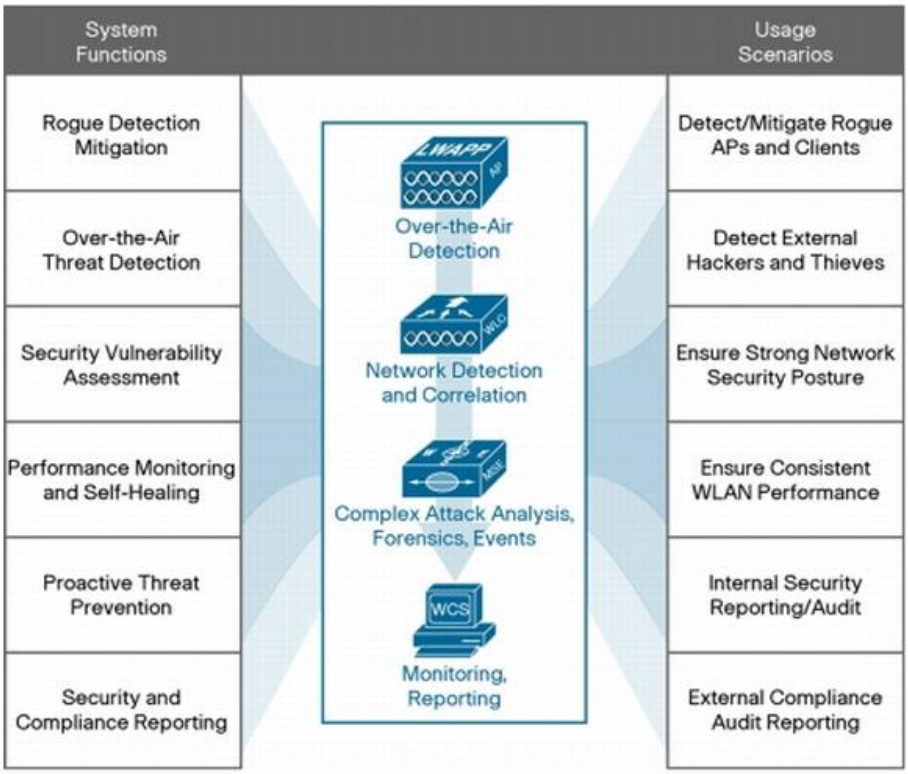
يتكون WIPS من ثلاث مكونات أساسية هي Sensor و Server و Console و هذه المكونات قد تتحد أو تتفرق الي اكثر من ثلاث

أما Sensor فهو الذي يقوم بدور المتحسس للمحيط الراديوي و يتم ذلك عبر أكسس بوينت تلعب دور detector

و أما server فيقوم بتحليل كل المعلومات التي يلتقطها sensor

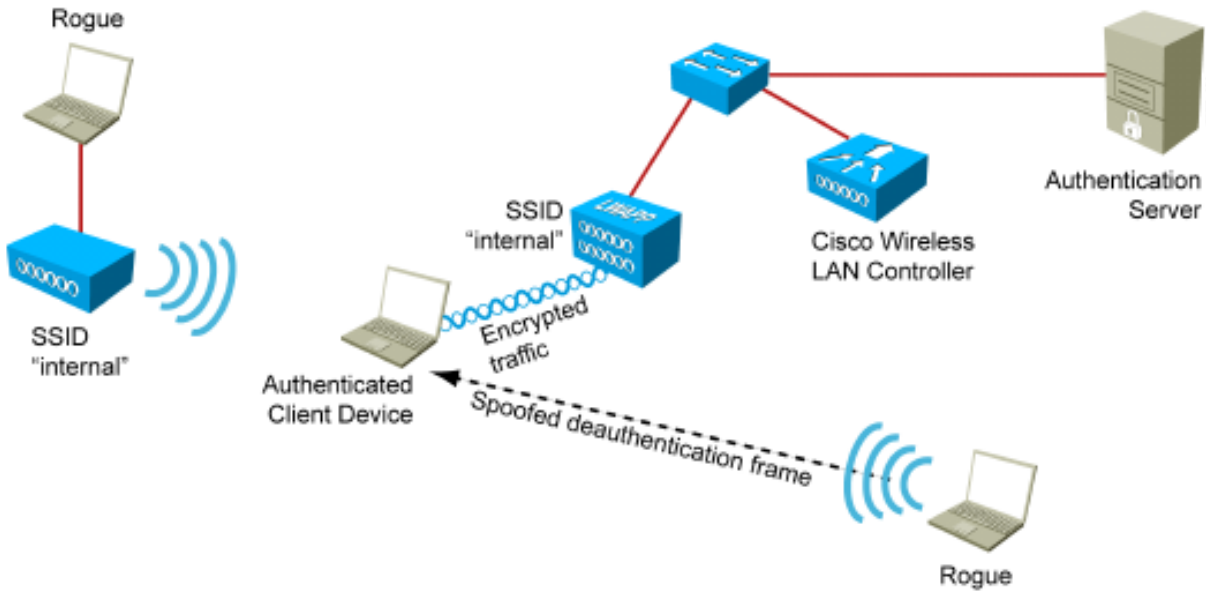
و أما Console فهي الأداة أو الواجهة التي يقوم بها المدير بإتخاذ القرار بناء علي تحليل Server

و لدي سيسكو منظومة خاصة بها تسمي Cisco® Adaptive Wireless IPS و الذي يعبر عنها هذا الشكل



و تستطيع أن تستنتج المكونات الثلاث من الشكل السابق حيث يقوم الأكسس بوينت بدور المستشعر و MSE بدور السيرفر و WCS بدور الواجهة التي تعطي التقارير في حين يتشارك الكنترولر دور المستشعر و السيرفر

Management Frame Protection : MFP

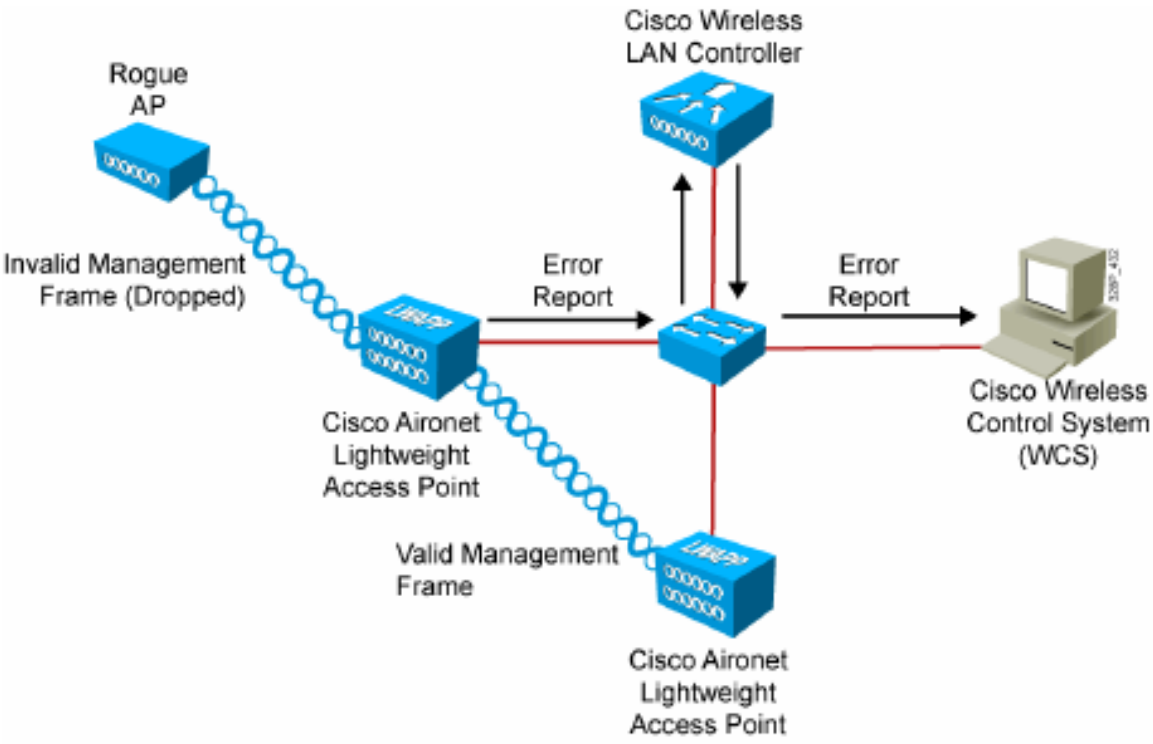


رغم أن المؤسسات التي تنظم بروتوكولات و معايير الشبكات مثل IEEE و WIFI تتضافر لإخراج معايير أكثر تشددا و ذكاء لطرق توثق و تشفير الولوج للشبكات اللاسلكية فإن هناك ثغرات كثيرة و خطيرة تأتي من قبل الفريمات الإدارية للشبكات اللاسلكية Wireless Management Frames مثل authentication/deauthentication, association/disassociation, beacons, probes

حيث أن هذه الفريمات يتم ارسالها بدون أي تأمين حتي و إن كنت تستخدم أقصي درجات التأمين و التشفير و التوثيق مثل Wi-Fi Protected Access [WPA], WPA2, VPN و هذا يعني أن أي هاكر يستطيع أن يتعرف علي ما تحمله هذه الفريمات ان استطاع أن يلتقطها و يحللها بوساطة برنامج Air Crack علي سبيل المثال

و سيسكو لم تكن بعيدة عن هذا الواقع فقد قامت بواسطة جهازها الرائع Cisco Wireless LAN Controllers (WLCs) بحماية و تأمين هذه الفريمات بطريقة أطلقت عليها MFP- Management Frame Protection و صنفتها الي صنفين Infrastructure MFP و Client MFP

Infrastructure MFP



يسمي هذا النوع بهذا الإسم لأن الأكسس بوينت هو المنوط به تبادل الرسائل و الفريمات للتأكد من صلاحية الأجهزة للدخول في الشبكةو لا يحتاج التأكيد من خلال client

و هنا يقوم الكنترولر بتوليد صبغة خاصة Signature لكل شبكة لاسلكية SSID يتم وضعها في الفريم الإداري Management Frame و يتم تبادلها في صيغة معقدة تسمي integrity check (MIC) message و عند أي اعتراض لهذا الفريم يتم اكتشافه

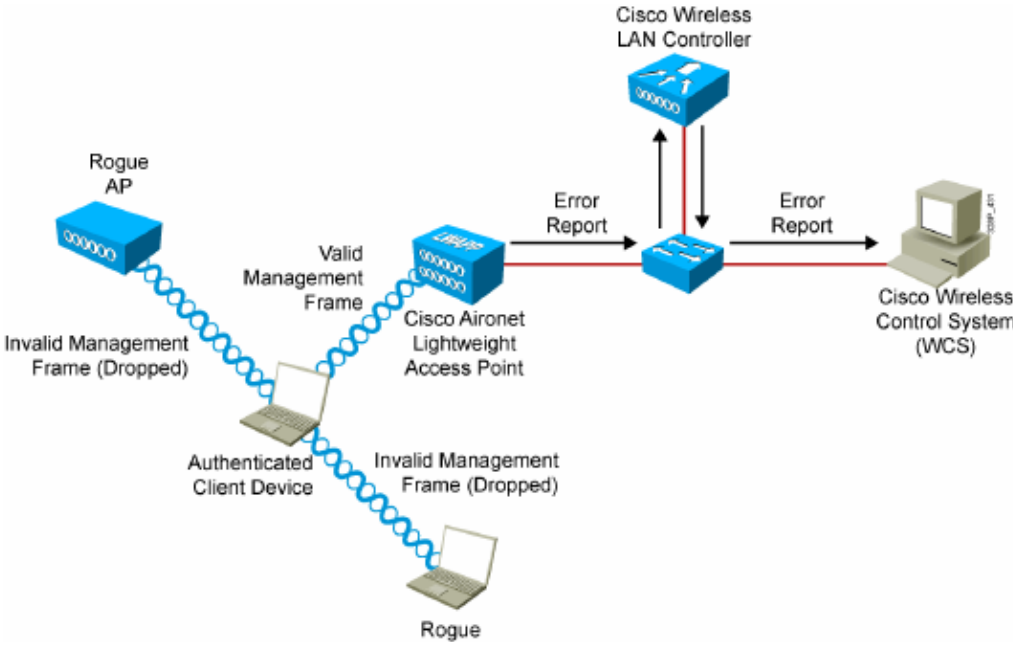
و عندما يكتشف الكنترولر أي أكسس بوينت لا يتم ارسال فريماته بهذه الطريقة فإنه يقوم علي الفور بوصمه كأكسس بوينت غريب أو دخيل Rogue AP

و عندما يستقبل الأكسس بوينت فريم MFP لا يعلم مصدره فإنه يقوم بإرسال نسخة الي الكنترولر ليأخذ منه مفتاح التعامل مع هذا الفريم و يكون السيناريو احد هذه الثلاث

- اذا كان أن BSSID أو ما يعرف بـ MAC غير معروفة من الكنترولر فإن الكنترولر يقوم بإرسال فريم الي الأكسس بيونت يخبره أن الجهاز الذي يتصل بك غير معروف مما يجعل الأكسس بوينت يرفض طلب هذه الجهاز

- اذا كان أن BSSID أو ما يعرف بـ MAC معروف من الكنترولر و لكن MFP معطلة و الفريم لا يرسل بالصيغة integrity check (MIC) message فإن الكنترولر يعيد الفريم مرة أخري للجهة التي أتي منها ليقوم بتصحيح شكل الفريم بالصيغة MIC و بالتشفير MFP
- اذا كان أن BSSID أو ما يعرف بـ MAC معروف من الكنترولر و الفريم مرسل بالصيغة message integrity check (MIC) بالتشفير MFP فإن الكنترولر يقوم بإرسال المفتاح الي الأكسس بوينت عبر قناة مشفرة AES-encrypted LWAPP management tunnel

Client MFP



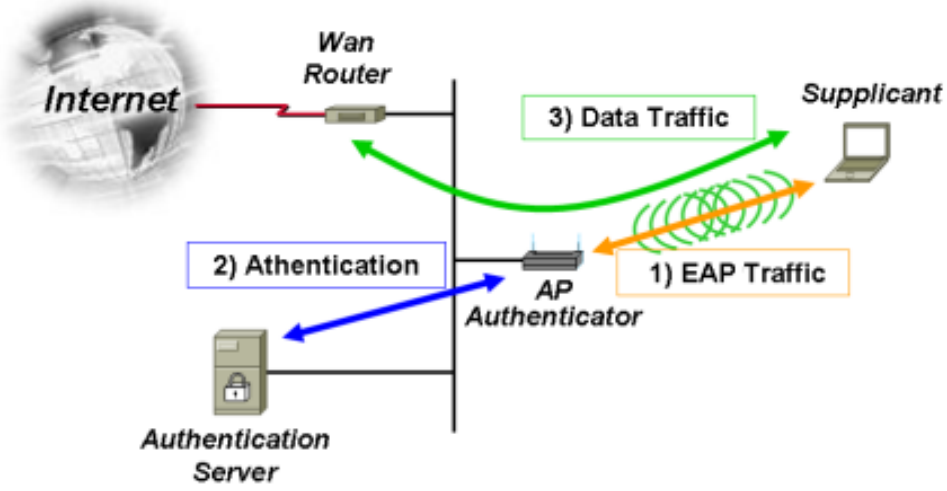
من المخاطر الشائعة في الشبكات اللاسلكية هي AP Impersonation أو Spoof AP MAC و يقوم فيها المخترق بانتحال صفة أكسس بوينت في الشبكة عبر استخدام نفس MAC للأكسس بوينت و يقوم بإرسال فريمات إدارية الي أجهزة في الشبكة مثل deauthentication و disassociation و هي فريمات يرسلها الأكسس بوينت الي الأجهزة لفصلها عن الشبكة لإجبارها مرة أخري علي الإتصال بالأكسس بوينت أو عمل اختراقات DoS

مع Client MFP يتم تأمين ارسال الفريمات الإدارية بين الأكسس بوينت و الأجهزة و لهذا فإن كلا من الأكسس بوينت و الأجهزة يستطيعان كشف و ايقاف أي محاولة لإنتحال صفة اي طرف في الشبكة أو اي محاولة للهجوم عبر DOS

في هذه الطريقة يتم تأمين الفريمات الإدارية ذات الوجهة الواحدة Unicast Frame مثل deauthentication و disassociationو Probe Response حيث يتم اسقاط أي فريم لم يتم حمايته بطريقة MFP و يتم ابلاغ الكنترولر عنه لوصمه كدخيل

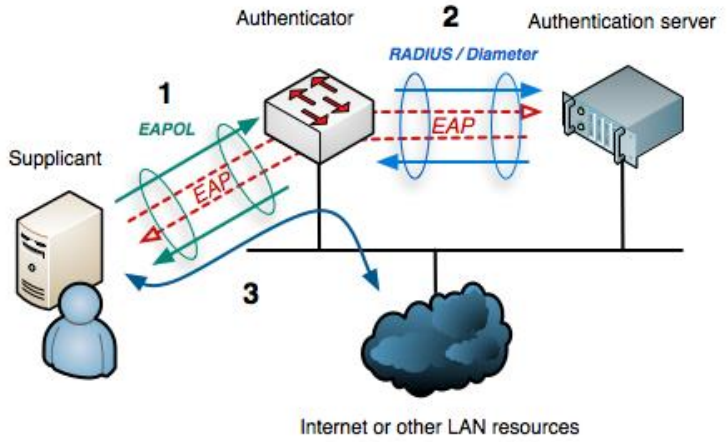
و لتستطيع دعم هذه الطريقة فلابد أن تعمل الأجهزة تحت مظلة تقنية سيسكو Cisco Compatible Extensions v5 مع استخدام تقنيات تشفير WPA2مع Temporal Key Integrity Protocol (TKIP) أو AES-Counter CBC-MAC (AES-CCMP6)

Centralizing WLAN Authentication 802.1X



من القصور الذي يعاني منه تأمين الشبكات اللاسلكية هو عمل مقتاح ولوج موحد لكل المستخدمين في الشبكة و في حال تم معرفة هذه المفتاح فإن الشبكة هنا يكون قد تم اختراقها و هنا ظهرت الحاجة الي عمل تعددية لمفاتيح الولوج للشبكة بحيث يكون لكل مستخدم مفتاح خاص به و هذا يحدث بشيئين أولهما فصل التوثيق authentication عن التشفير encryption و ثانيهما عمل مركزية لتوليد و و تخزين هذه المفاتيح و هذا بالضبط ما سنتكلم عنه وهو 802.1X و هو أحد بروتوكولات IEEE المستخدمة في عمليات الأمن و التي اشتهرت بشكل واسع في الشبكات اللاسلكية

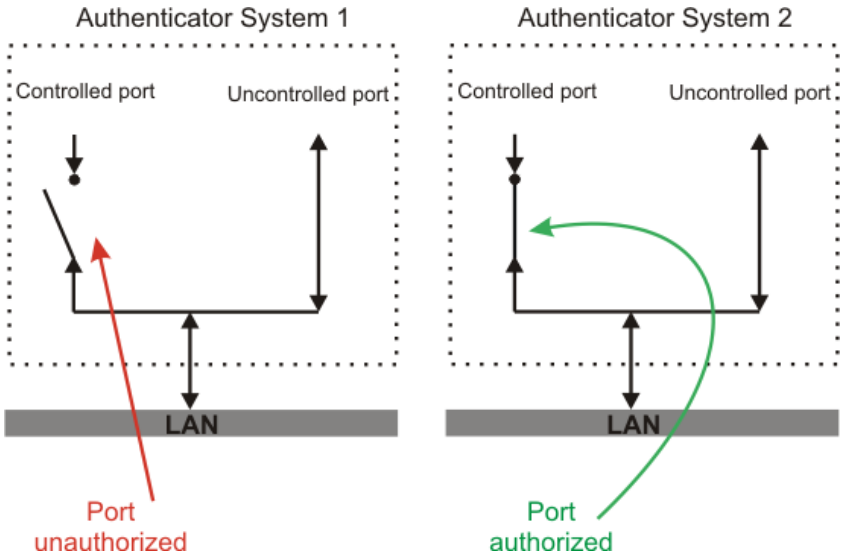
و يتكون نظام 802.1X من ثلاث أجزاء هم Supplicant و Authenticator و Authentication server



أما Supplicant فهو الجهاز الذي يريد الولوج للشبكة

و Authenticator الواجهة التي سيتم الولوج للشبكة عبرها مثل السويتش أو الأكسس بوينت

و Authentication server فهو الجهاز الذي سيشرف علي كل عملية ولوج للشبكة عبر أليات مخزنة فيه



في هذا النظام سيكون هناك اتصال فيزيائي بين Supplicant و Authenticator و رغم هذا فلن يتم السماح بارسال أو استقبال الفريمات الا بعد أن يتم توثيق الدخول بواسطة Authentication server و لهذا تسمي هذه العملية "port"-based authentication لأنها تعتمد بالأساس علي السماح أو حجب ولوج الأجهزة رغم اتصاله فيزيائيا عبر بورت السويتش

8021.X over Wireless

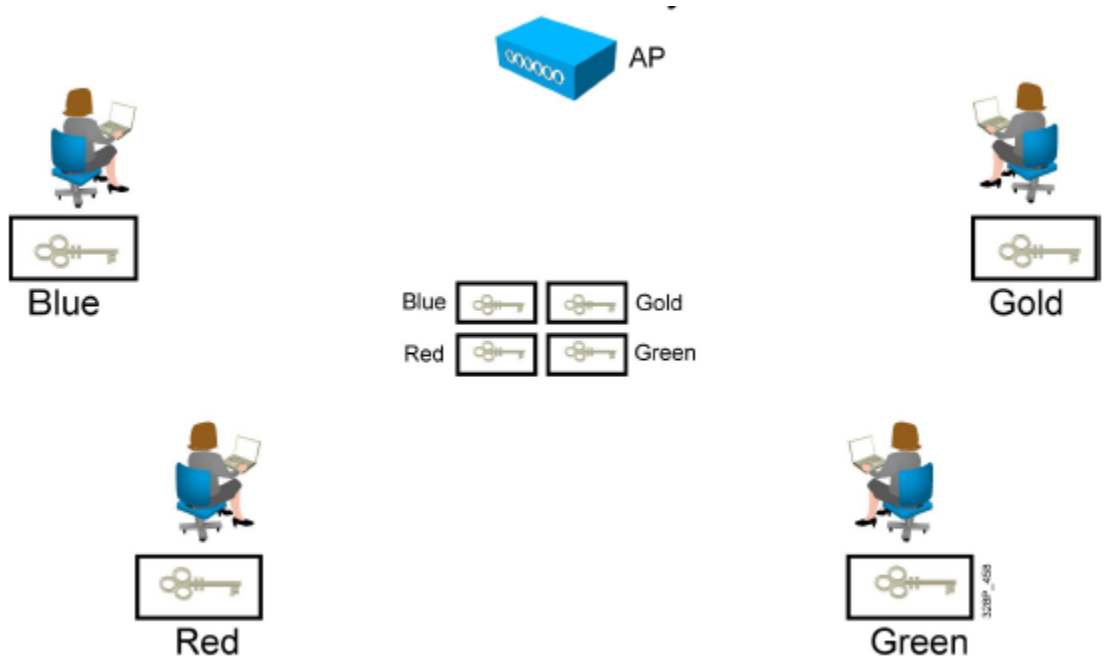
في الشبكات السلكية يعتبر authenticator هو السويتش أما في الشبكات اللاسلكية فهو الأكسس بوينت و في هذه الحالة فإن توثيق طلبت الولوج سيتم علي مراحل في عملية open authentication

سيقوم supplicant بإرسال طلب توثيق authentication request و ينتظر الرد authentication response فإن جاء بالموافقة سيقوم بطلب الإرتباط بالشبكة association request و سينتظر الرد association response

حتي هذه اللحظة فإنك لم تنجح في فتح قناة اتصال بالشبكة اللاسلكية فإن ما قمت به يشبه وصل كابل الشبكة بالسويتش و لكنك لم تستطيع بعد الإتصال بالشبكة لأن السويتش لم يسمح حتي الآن بالإتصال بالشبكة لأن سيرفر التوثيق لم يبحث طلبك بعد و الذي سيكون هنا RADIUS و عندما سيجد أن الجهاز الذي يطلب الولوج ذو بيانات صالحة فإنه يقوم بافيعاز للأكسس بوينت بفتح الطريق له للدخول للشبكة

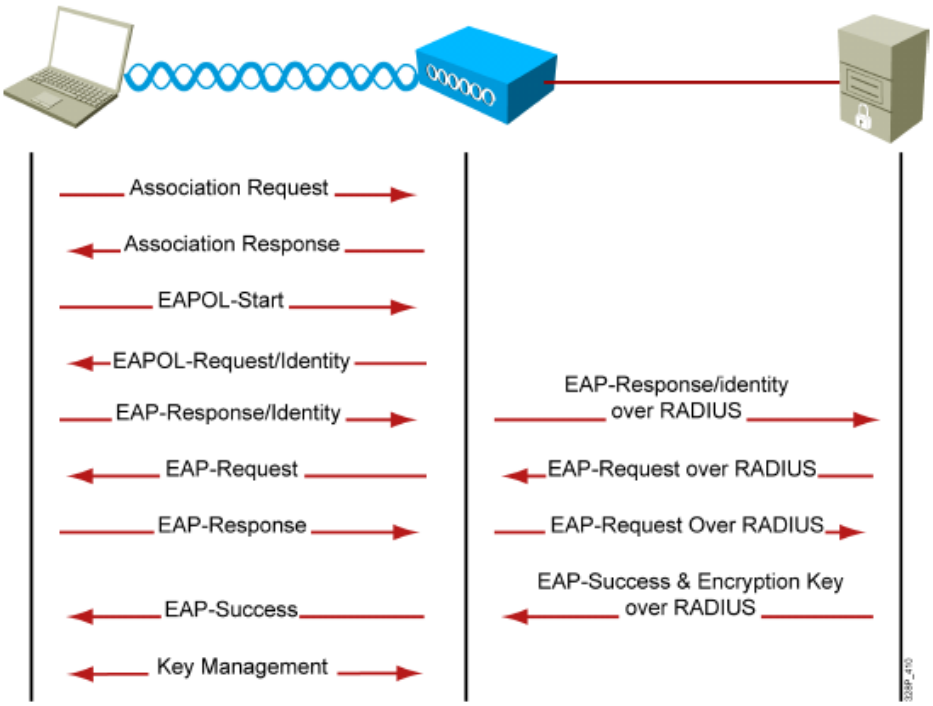
ملحوظة : في الشبكات الصغيرة لا يتطلب الأمر وجود ثلاث جهات Supplicant و Authenticator و Authentication server كل منها جهاز مختص بل نستطيع أن تدمج عمل سيرفر RADIUS في الأكسس بوينت –ان كان يدعم ذلك –

Unique Encryption Keys



في 802.1X يتم توثيق كل جهاز supplicant بشكل مستقل و تستفيد الشبكات اللا سلكية من ذلك بإضافة دعم إضافي للتشفير بعمل مفتاح فريد WEP key لكل جهاز و لكل عملية اتصال session عبر سيرفر RADIUS و في كل مرة يخرج الجهاز ثم يدخل الشبكة اللاسلكية يقوم السيرفر بتكرار هذه العملية و لهذا تطلق علي WEP key اسم session keys

Extensible Authentication Protocol –EAP

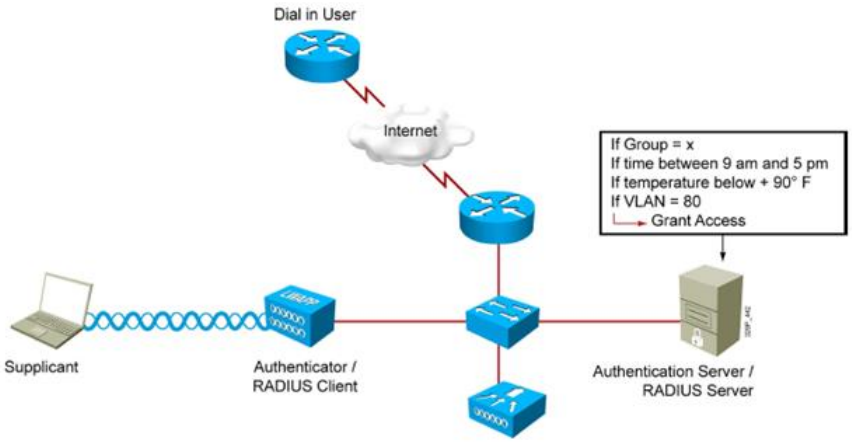


هو بروتوكول صمم من قبل منظمة Internet Engineering Task Force (IETF) لحل مشكلة في الإتصال بشركات موفرات الخدمة Dial-in ISPs بموائمة استخدام أكثر من جهة لأكثر من طريقة توثيق مثل Handshake Authentication Protocol (CHAP) أو Password Authentication Protocol (PAP) و لذلك فالفريم الخاص به يحتوي علي خانة عن "authentication type" لتلائم نوع التوثيق

و يستخدم ثلاث رسائل لبيان حالات الطلب request, response, success, failure و له أنواع عديدة كل منها يلائم خطة أمنية معينة مثل, LEAP (Lightweight EAP), EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) , PEAP (Protected EAP), EAP-TLS (EAP-Transport Layer Security).

و شرح كل هذه الأنواع سنتكلم عنه بإذن الله بالتفصيل عندما نصل الي منهج أمن الشبكات اللاسلكية في CWNP و CISCO

عمل سيرفر توثيق للشبكة اللاسلكية بواسطة RADIUS



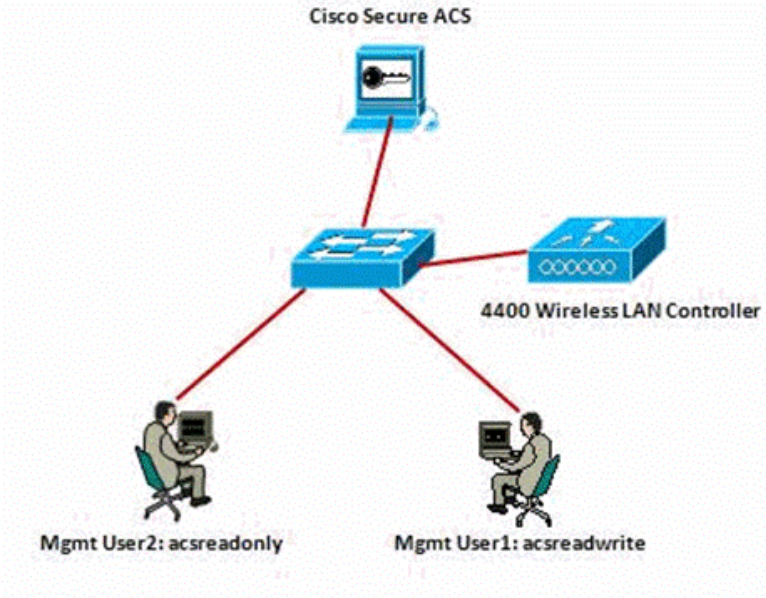
هو نظام يعمل ببروتوكولات الطبقة السابعة application layer ضمن نظام client/server لولوج شبكة ما طبقا لشروط محددة و يوظف في برنامج لأداء هذه المهمة و يسمي سيرفر التوثيق المركزي Remote Authentication Dial In User Service (RADIUS)و يشبه في ذلك نظلم Active Directory بالويندوز و هو بكل حال جزء من النظام الأمني الثلاثي(AAA) authentication, authorization, accounting

كانت بدايته في 1991 من قبل مؤسسة Livingston Enterprises ثم انتقلت تبعيته الي هيئة الإنترنت Internet Engineering Task Force (IETF)ليصبح مقياسا عالميا يعمل به في شبكات ISP و الشبكات اللاسلكية و الإيثرنت و غيرها من الشبكات التي يتطلب الولوج اليها عمل حسابات للمستخدمين

و بالطبع فإنه يفضل التعامل مع برنامج سيسكو Cisco Secure Access Control Server (ACS) كسيرفر RADIUSلعمل قاعدة بيانات للمستخدمين و التحكم بهم

و يتم الإتصال بين – network access server (NAS) و الذي يعتبر الكنترولر – و RADIUS server طبقا لبروتوكول(UDP) User Datagram Protocol

و سنقوم هنا بشرح طريقة تأمين شبكة لاسلكية بإستخدام Wireless LAN Controller (WLC) و Access Control Server (Cisco Secure ACS)و بذبلك يتم عمل بيئة AAA لإدارة الولوج للشبكة اللاسلكية و سنستخدم المعدات و البرمجيات التي في الشكل التالي



Cisco Secure ACS Configuration

بالنسبة لبرنامج ACS فإنه يتم تحميله من موقع سيسكو و يتم إعداده الا علي ويندوز 2003 سيرفر و سنقوم بعمل المستخدمين التاليين

Username – acsreadwrite

Password – acsreadwrite

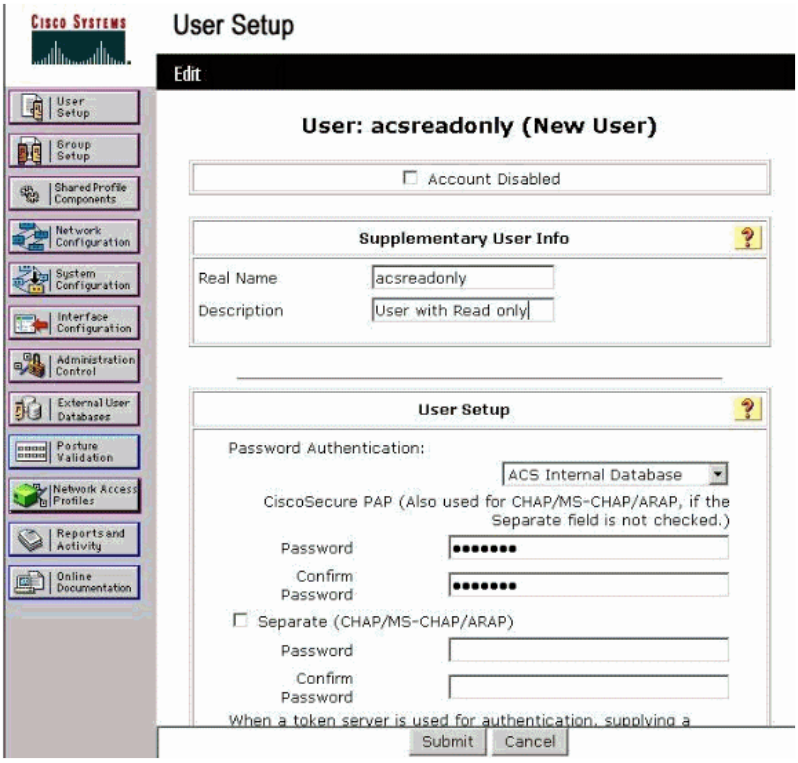
Username – acsreadonly

Password – acsreadonly

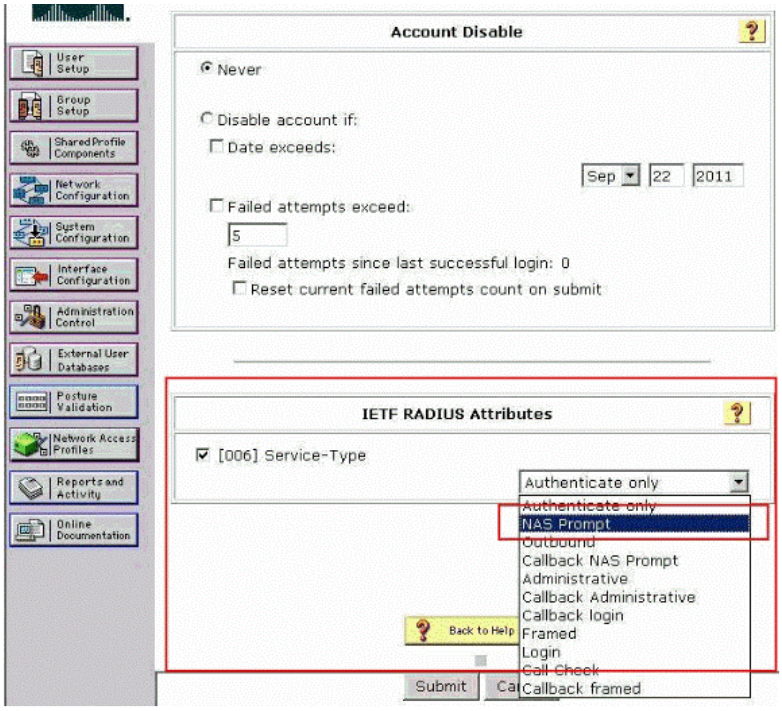
سنتبع الخطوات التالية

أولا سنضيف الكنترولر أولا كـ AAA Client الي RADUIS Server و ذلك من خلال Network Configurationو الضغط علي Add Entry ثم ادخال بيانات الكنترولر كما بالشكل

بعد ذلك سنقوم بعمل مستخدمين بصلاحيات read-write للمدراء و read-only للمستخدمين

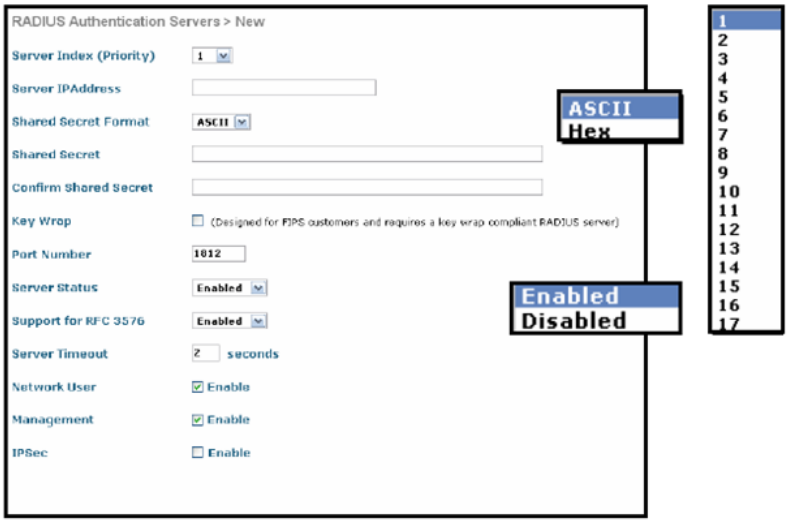


و في أسفل الصفحة نختار صلاحية المستخدم



WLC Configuration

لإعداد الكنترولر للتعامل مع سيرفر التوثيق قم بالدخول للصفحة Security > AAA > RADIUS3 > Authentication



Server Index (Priority) : يستطيع الكنترولر أن يتعامل مع 17 سيرفر توثيق RADIUS و يتم مناداتهم حسب الترتيب

Server IP Address : عنوان السيرفر

Shared Secret Format : عمل كلمات المرور بالصيغة ASCII أو hexadecimal

Shared Secret/Confirm Shared Secret : ادخال كلمة المرور مع التأكيد

Key Wrap : التشفير بشكل أقوي بنظام(Advanced Encryption Standard) AES

Port Number : بورت الإتصال

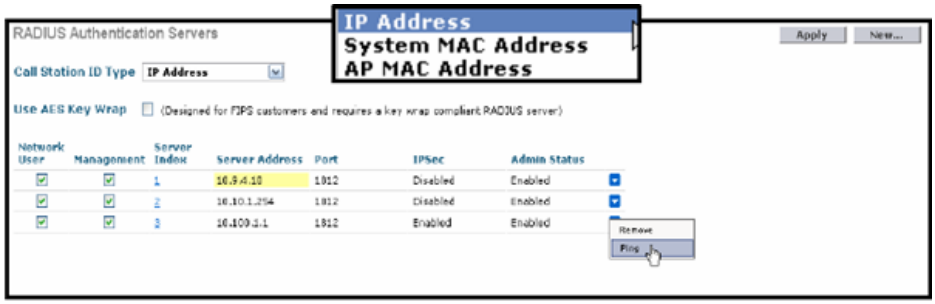
Server Status : تفعيل أو تعطيل السيرفر

Support for RFC 3576 : تفعيل البروتوكول تحسين أداء السيرفر

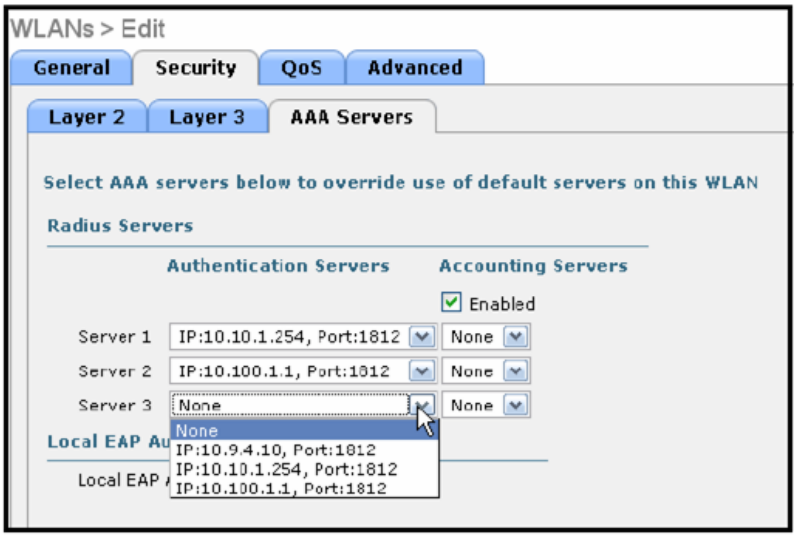
Server Timeout : قيمة من 2 الي 30 ثانية تبين

Network User : تفعسل عمل مستخدمين للشبكة

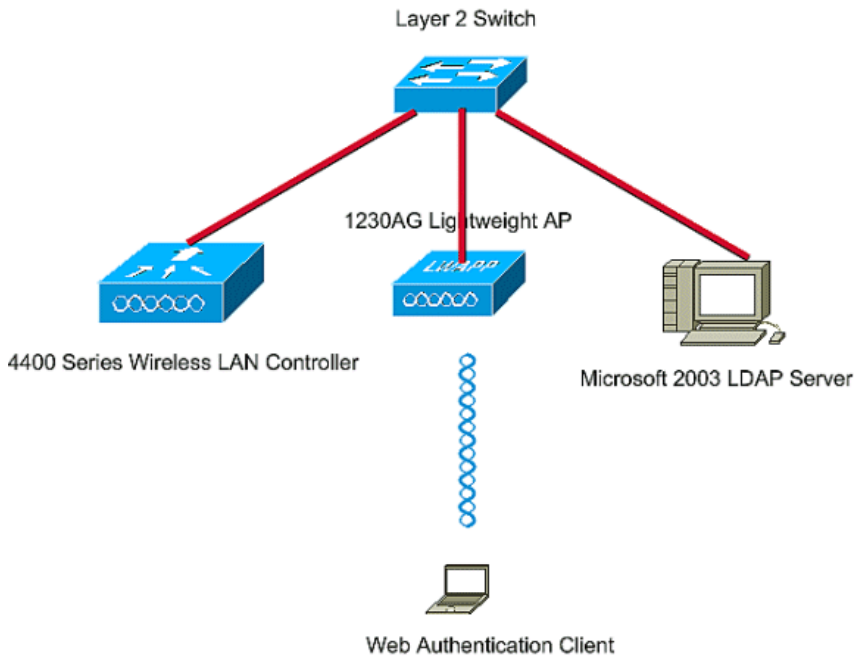
بعد إضافة السيرفرات الموجود عليها قاعدة بيانات المستخدمين تخرج لنا هذه الصفحة Security > AAA > RADIUS3 > Authentication



يتم بعدها ربط الشبكة بهذا السيرفر بالدخول الي WLANs > Edit ثم اختيار السيرفر من التبويب AAA Server



السيرفر اللاسلكي LDAP بإستخدام Win 2003 AD



سنقوم هنا بعمل سيرفر توثيق لاسلكي Lightweight Directory Access Protocol (LDAP) بواجهة صفحة ويب web authentication و ذلك باستخدام Microsoft Windows 2003 server

و يعتبر Web authentication من أحد طرق التأمين في الطبقة الثالثة Layer 3 security حيث يتطلب و لوج المستخدم للنظام الي اسم و كلمة مرور تظهر علي صفحة ويب

سنحتاج هنا أن يكون لديك إلمام بإعداد و ضبط اعدادت أجهزة Lightweight Access Points (LAPs) و Cisco WLCs و معرفة بالبروتوكول اللاسلكي Lightweight Access Point Protocol (LWAPP) و معرفة بطريقة التعامل مع ويندوز سيرفر و Active Directory و domain controllers

و سنقوم بعمل الطبولوجي السابقة و كما رأيت فإننا سنستخدم المعدات و البرمجيات التالية

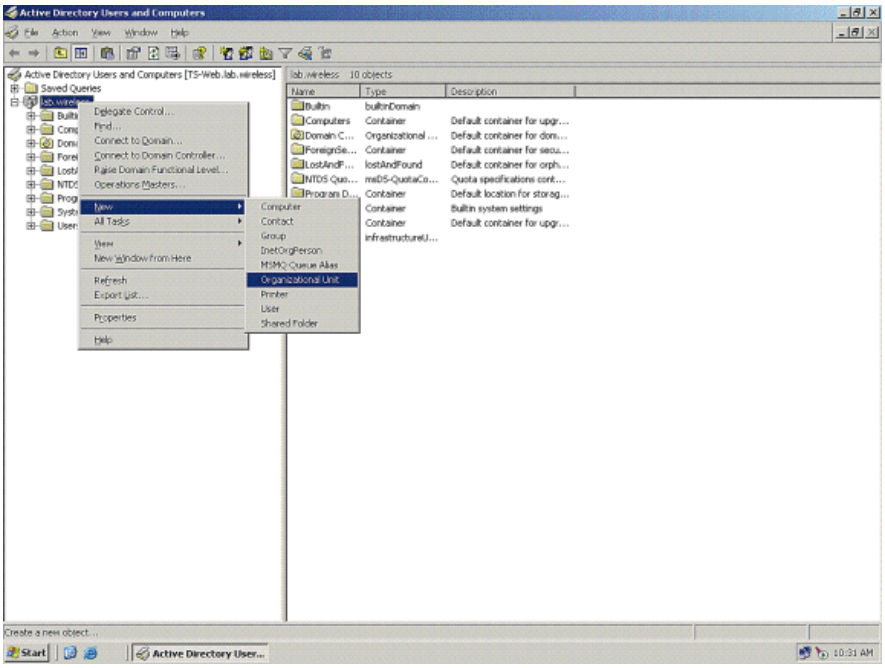
- Cisco 4400 WLC that runs firmware release 5.1
- Cisco 1232 Series LAP
- Cisco 802.11a/b/g Wireless Client Adapter that runs firmware release 4.2

- Microsoft Windows 2003 server that performs the role of the LDAP server

Configure LDAP Server

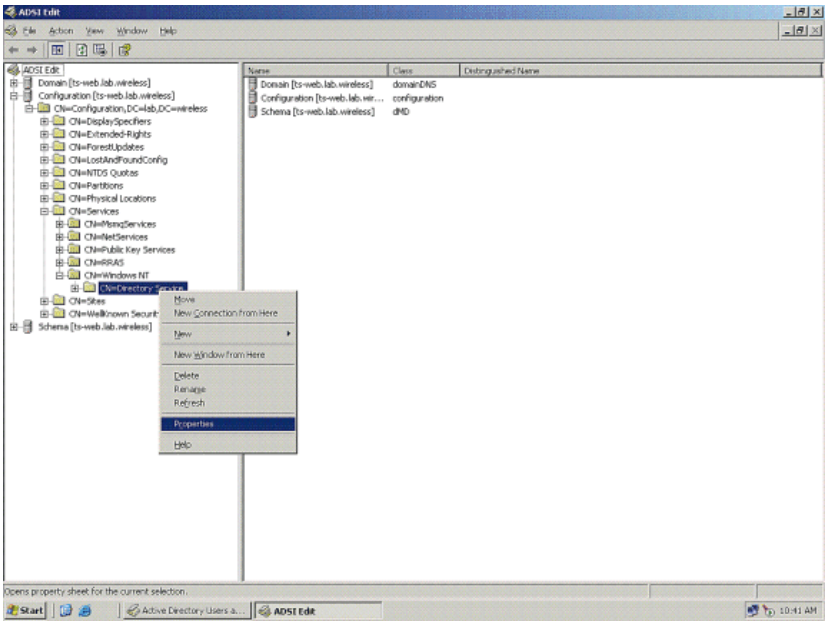
يعتبر سيرفر Lightweight Directory Access Protocol (LDAP) هو سيرفر لقاعدة بيانات لمستخدمي الأنظمة و نستطيع أن هنا سنستخدم Microsoft Windows 2003 server كسيرفر يؤدي هذه المهمة و ذلك بإستخدام Active Directory

سنقوم بعمل Organizational Unit (OU) و نضع بها مستخدمي الشبكة اللاسلكية



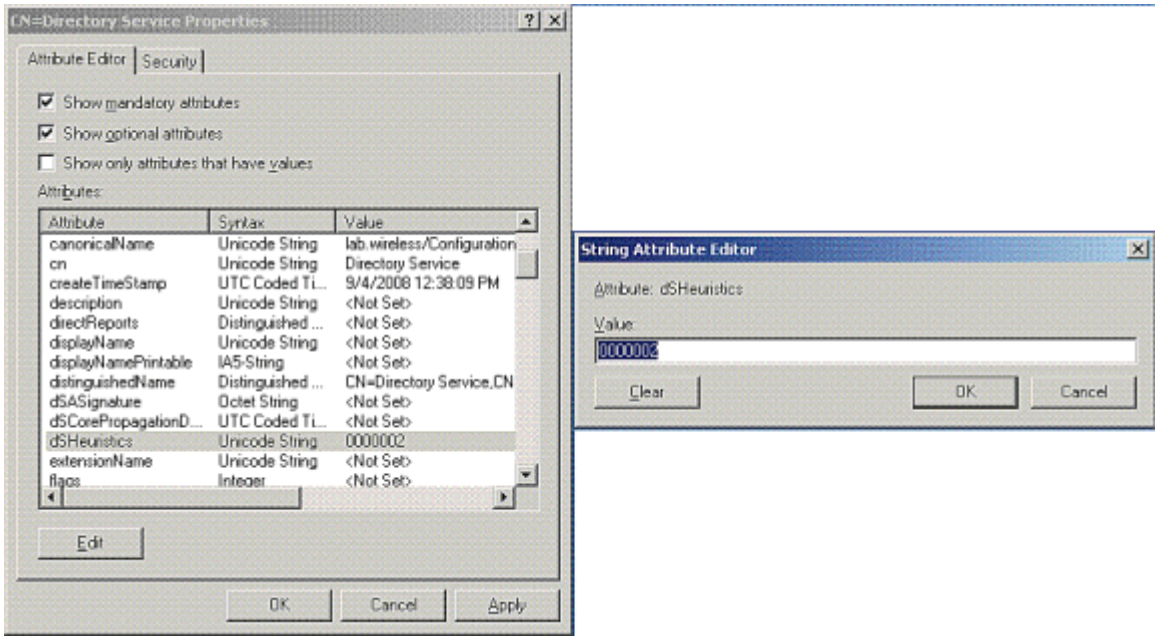
ثم نقوم بعمل حسابات لمستخدمي الشبكة داخل OU نسميها wireless-users

أهم خطوة بعد ذلك هي تفعيل الولوج المخفي و الذي ستستخدمه الشبكة اللاسلكية للولوج للسيرفر و ذلك بإستخدام ADSI Edit tool فإن لم تجد الأداه فقم بتحميل أدوات ويندوز 2003 من الرابط هذا و ذلك بالدخول الي **Start > Run > Type: ADSI Edit.msc** ثم الإنتقال الي **CN=Services > CN=Windows NT > CN=Directory Service** و اختيار خصائص الفرع **CN=Directory Service**

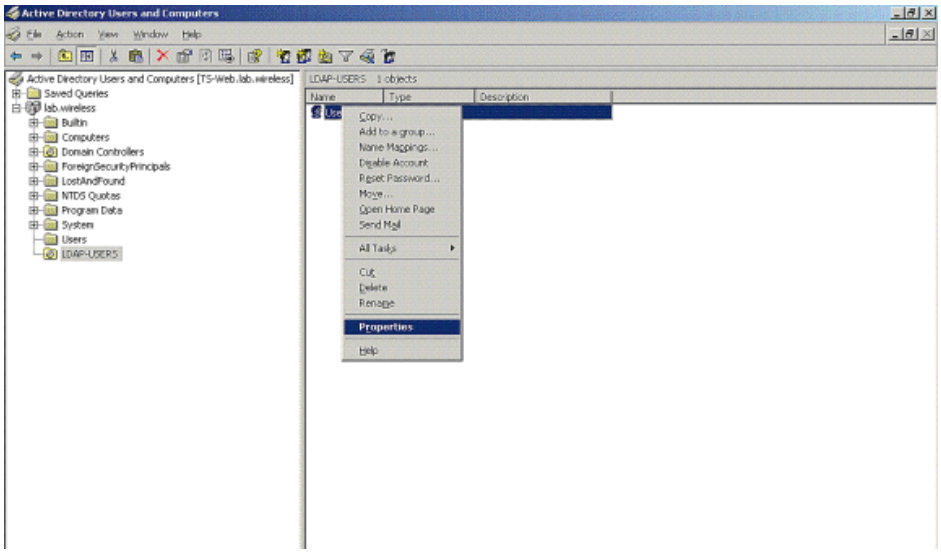


ثم تحت التبويب **Attributes** اضغط علي **dsHeuristics** و غير القيمة التي ستظهر الي **0000002**

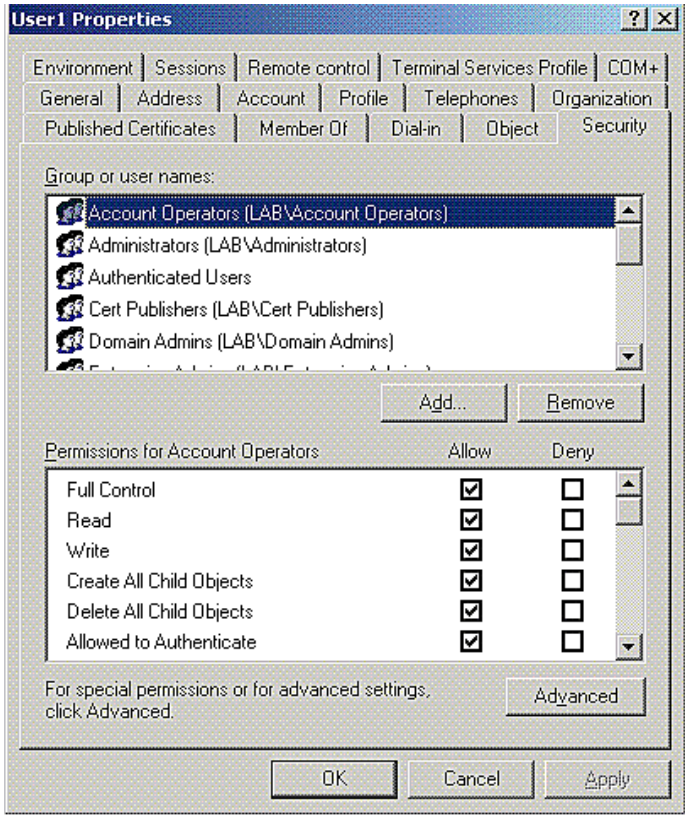
و بهذا نكون قد فعلنا الولوج الخفي للشبكة اللسالكية



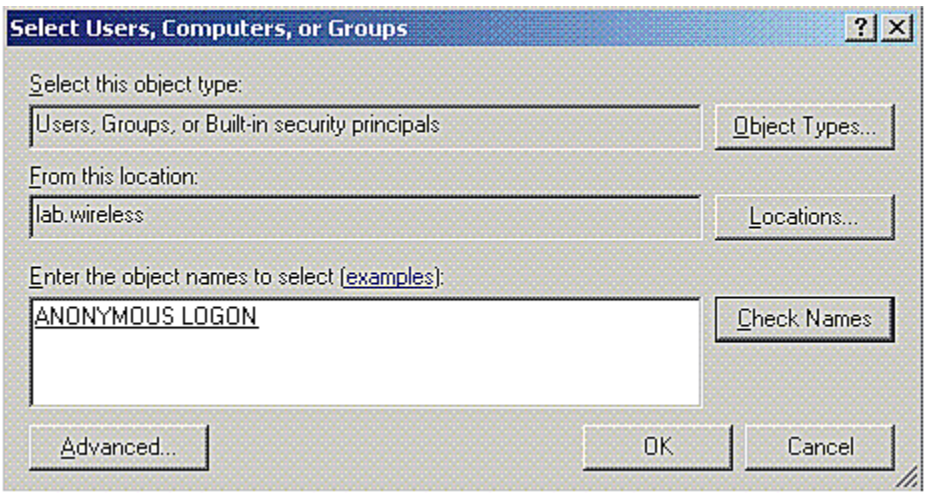
بعد ذلك نقوم بإعطاء مستحدمي الشبكة في AD صلاحية هذا الولوج ، سنقوم بالدخول علي خصائص المستخدم الذي قمنا بوضعه في OU الخاصة بالشبكة اللاسلكية



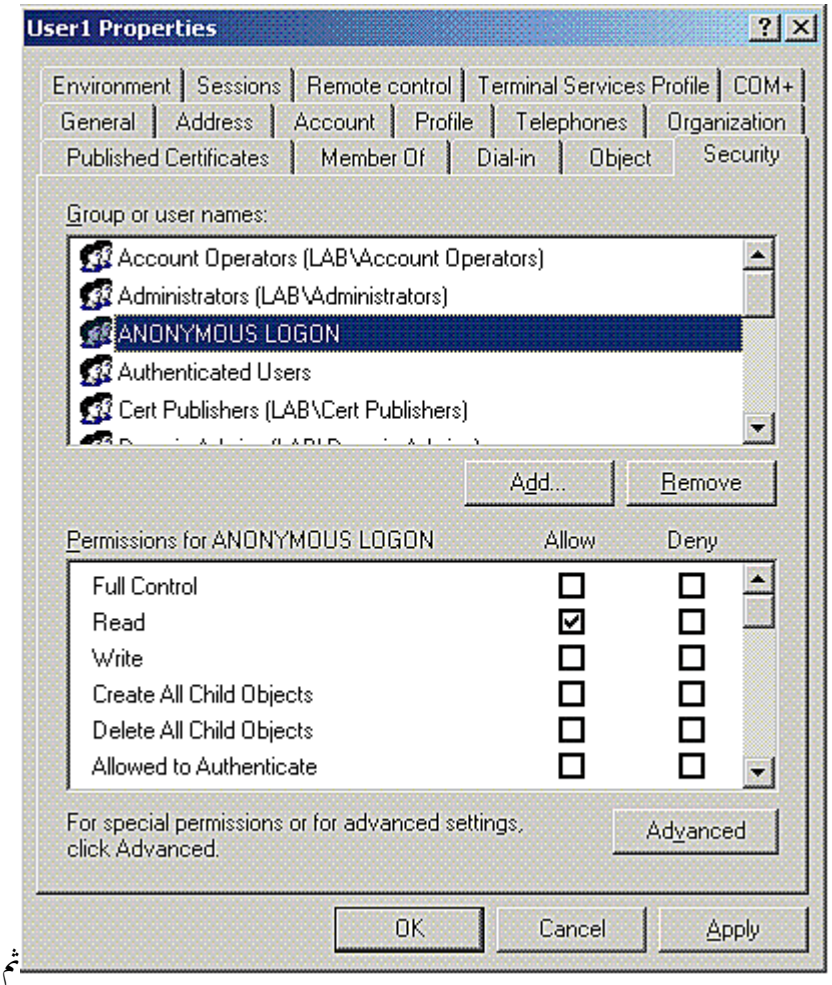
ندخل بعدها الي التبويب Security فإن لم يظهر قم بالتأكد من أن الخاصية **View Advanced Features** مفعلة



من الزر Add أضف **ANONYMOUS LOGON**



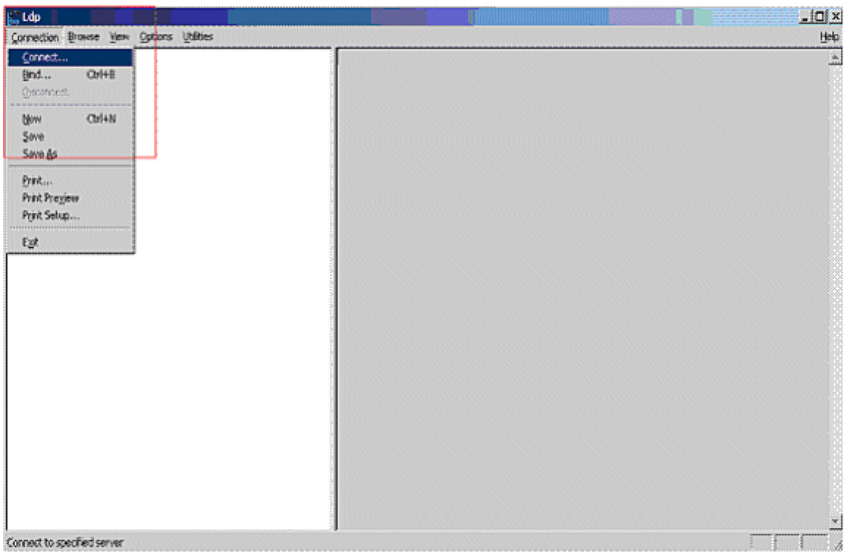
ثم اعطه الصلاحية Read فقط



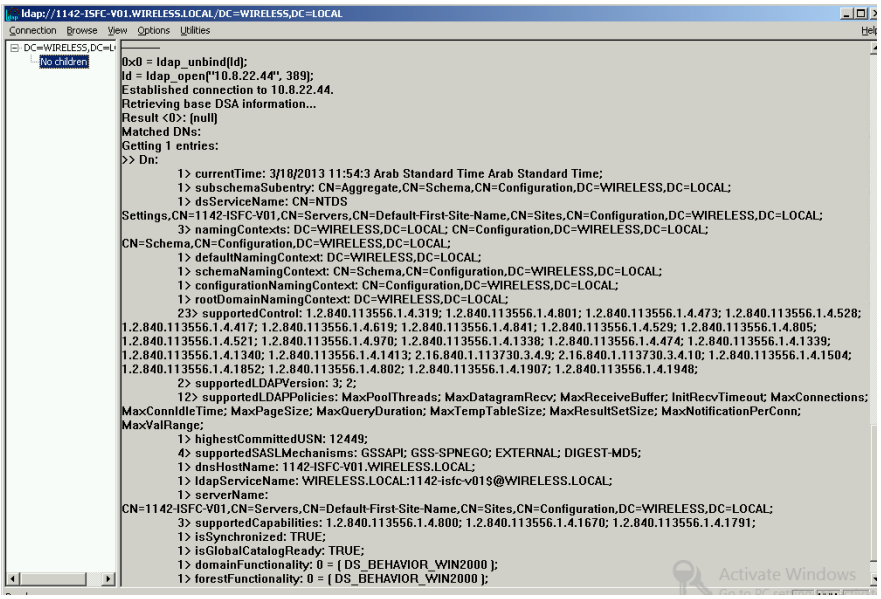
ثم

Use LDP to Identify the User Attributes

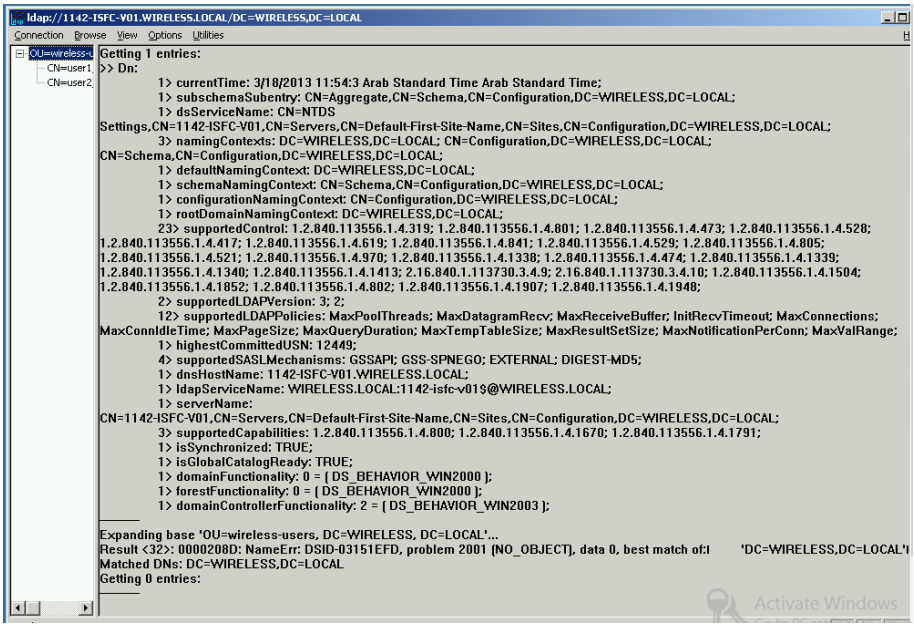
سنقوم الآن باستخدام أداة من ميكروسوفت تسمي LDAP Client ستساعدنا مستقبلا في اعداد الكنترولر لأننا ستحتاج الخصائص التي ستعرضها الأداة لربطه بسيرفر LDAP و هي نسخة خفيفة و مصغرة لواجهة AD و تقوم بتحديد خصائص و صلاحيات المستخدمين و تستطيع تحميلها من نفس الرابط السابق من صفحة ميكروسوفت التالية ، افتح البرنامج ثم اتصل بالسيرفر



ستظهر الصفحة هكذا



قم بالدخول علي القائمة view ثم اضغط tree و اكتب اسم مسار BaseDN للمستخدم فمثلا **user1** **مساره هو** OU=wireless-users, DC=WIRELESS, DC=LOCAL لتظهر الصورة التالية



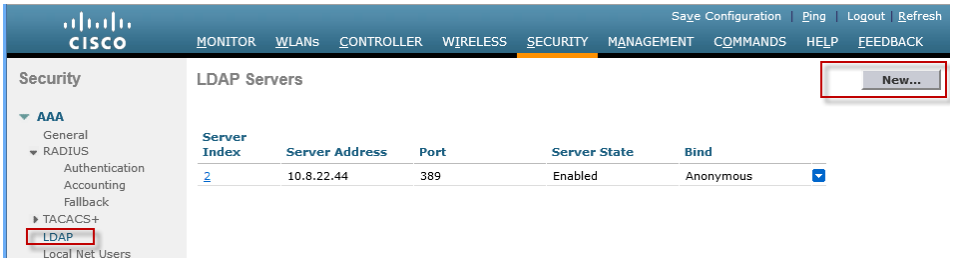
سيظهر علي يسار الصفحة users و بالضغط علي أي منهم سيظهر بياناته و خصائصه علي اليمين وهذا مثال علي user1

عند اعداد الكنترولر ستحتاج هذه الخصائص لربطه بسيرفر LDAP و ما يهمنا هنا هو User Base DN و الذي يساوي OU=wireless-users, DC=WIRELESS, DC=LOCAL و User Attribute و الذي يساوي sAMAccountName و User Object Type و الذي يساوي Person

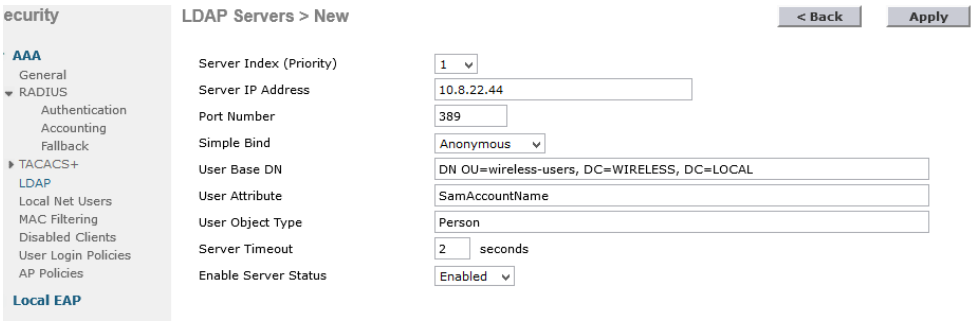
Configure WLC for LDAP Server

سننتقل الآن الي جهاز الكنترولر لنربطه بقاعدة بيانات المستخدمين التي هي AD 2003 و سندخل علي الصفحة

AAA > LDAP

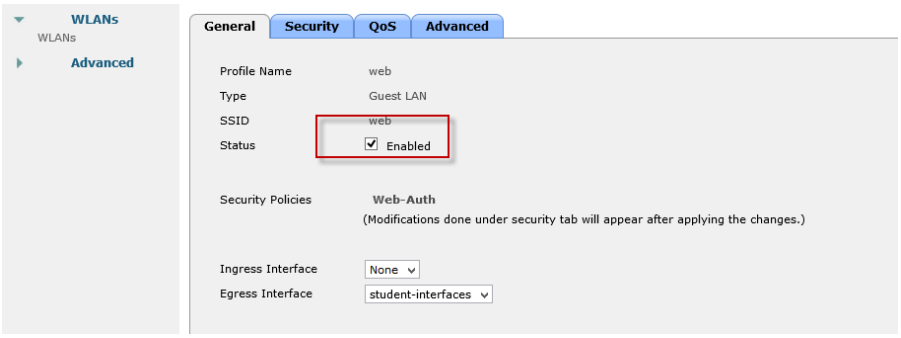


ثم New فتخرج لنا الصفحة التالية فنملأها بما استخرجناه مسبقا من الأداة LDP

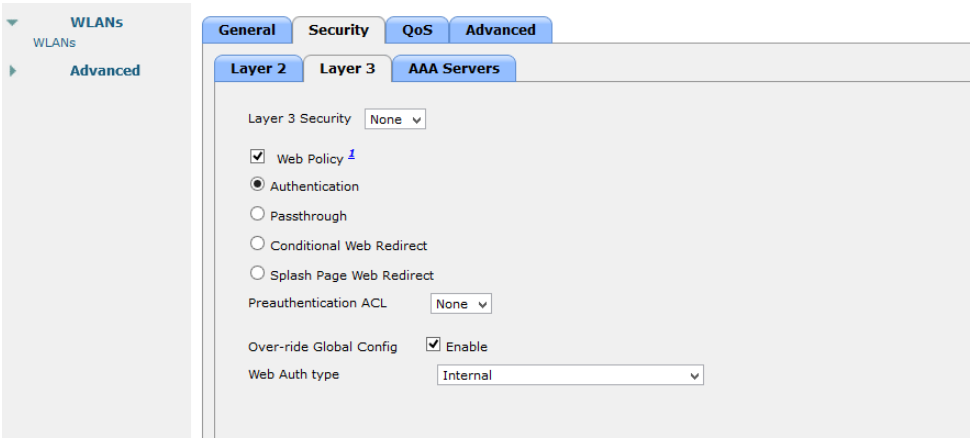


ثم apply ثم قم بالدخول الي شبكاتك اللاسلكية

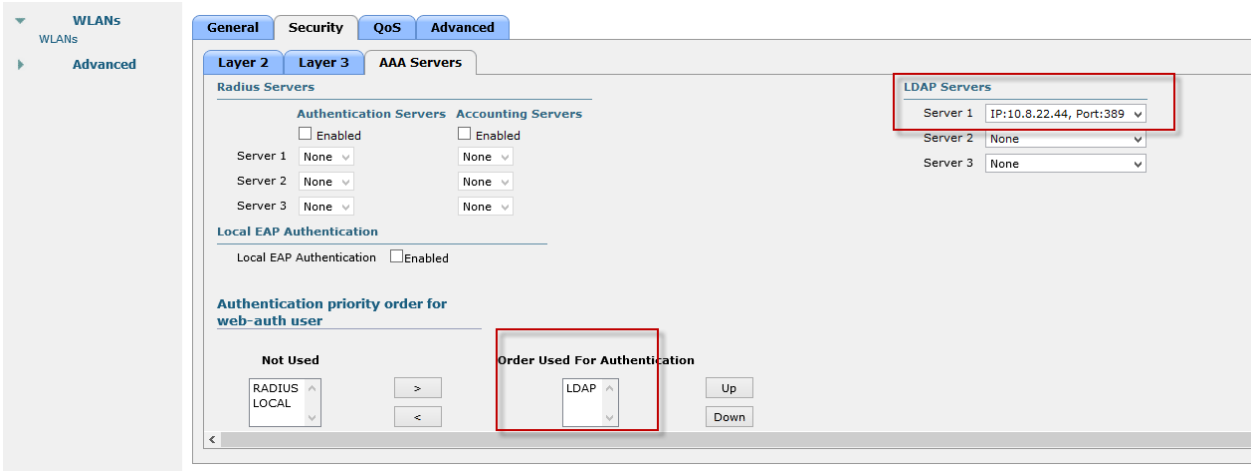
أو قم بعمل واحدة جديدة



ثم ادخل علي التبويب security ثم اختر layer 3 ثم اختر الخيارات الموجودة في الصفحة بالضبط



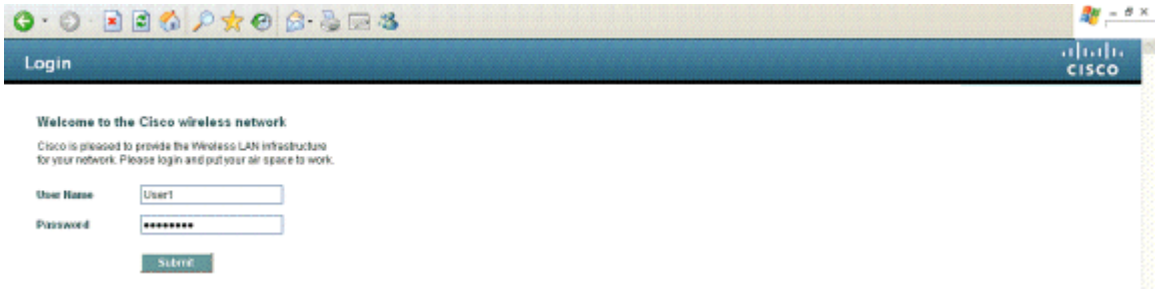
ادخل علي التبويب المجاور AAA Servers ثم اختر بيانات المطابقة لما فعلناه مسبقا



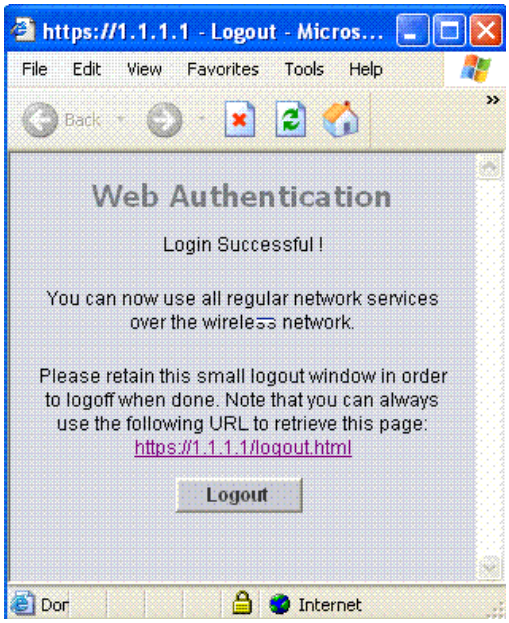
انهي عملك بالضغط علي apply و دعنا نتأكد مما صنعناه بالدخول علي الشبكة من خلال أي جهاز به اتصال لاسلكي و بمجرد الدخول علي أي صفحة انترنت ستأخذنا الي العنوان http://1.1.1.1/login.html و هو

Virtual Interface Address الذي وضعناه زمااان عند بداية اعداد الكنترولر و ستظهر هذه الصفحة و التي سيختلف شكلها تبعا للمتصفح

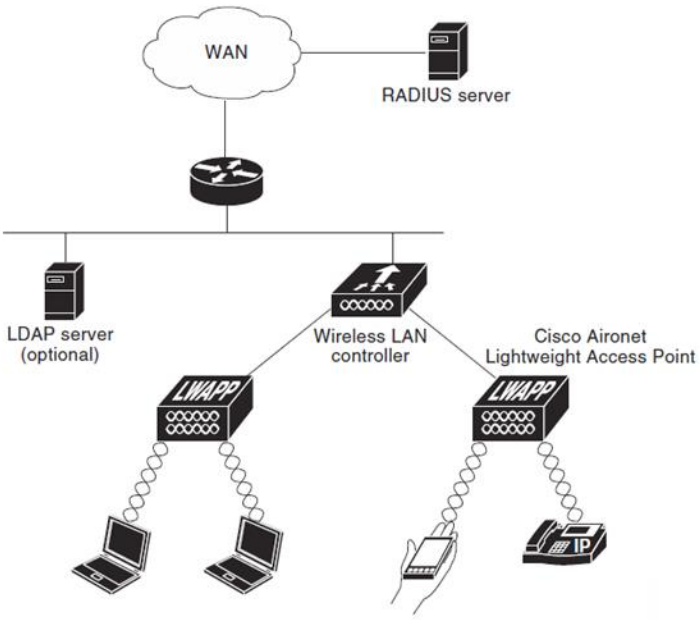
ستضطر بعدها لإدخال الإسم و الباسورد الذي أدخلناه في ad 2003



و مرحبا بك في عالم Web Authentication



تحويل الكنترولر لسيرفر لاسلكيRADIUS



ماذا يحدث ان لم تستطيع أن تعمل سيرفر خاص للتوثيق مثلRADIUS

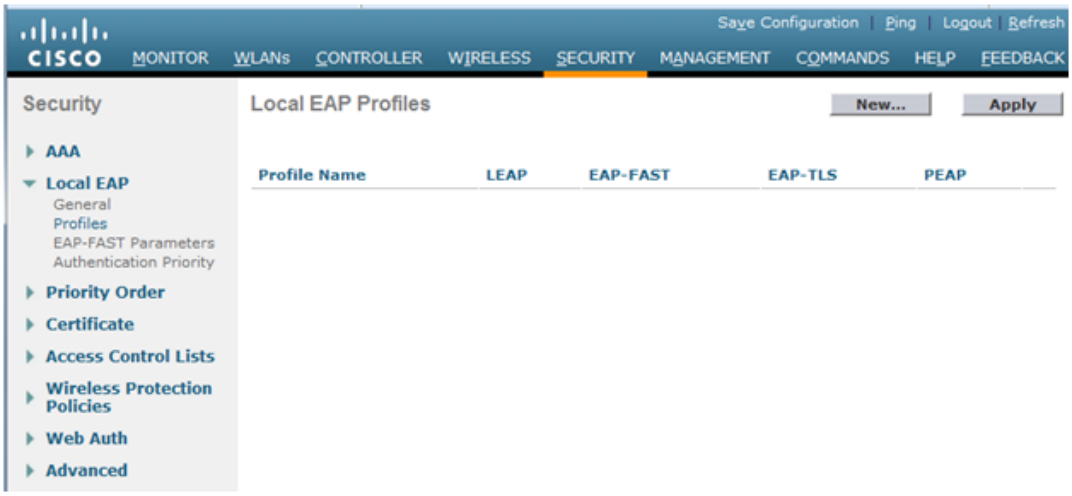
هنا تقدم لك سيسكو خدمة جليلة بجعل جهاز الكنترولر يقدم خدمة التوثيق أيضا و تسميها سيسكو Local EAP سيرفر التوثيق المحلي للشبكة اللاسلكية و تستطيع هذه الخدمة أن تكون كخدمة احتياطية عند فشل سيرفر RADIUS أيضا و لهذا فإن Local EAP لن يعمل اذا كان سيرفر RADIUS مفعلا في الشبكة

بالإضافة لذلك فإن الكنترولر الموجود عليه Local EAP لن يستطيع توثيق ولوج أجهزة لا توجد ضمن حيز هذا الكنترولر أي أنه خاص بأجهزته فقط و لا يستطيع تمرير هذه التوثيقات لأجهزة كنترولر أخري

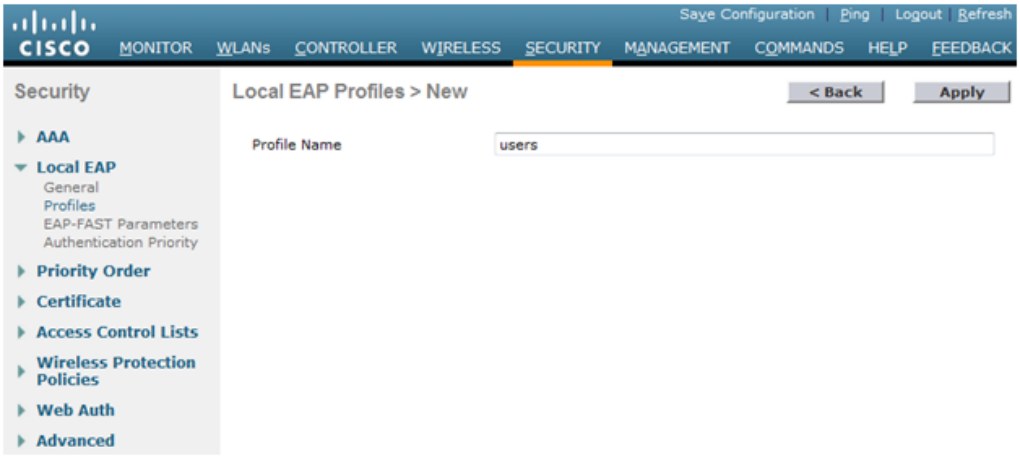
للعلم فإن هذه الخاصية وجدت في أجهزة الكنترولر بدءا من النسخة 4.1 و ما بعدها و تم تحديث هذه الخدمة و اضافة تحسينات لها في كل نسخة فمثلا النسخة 4.2 تم اضافة PEAP MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol)و PEAP GTC و في النسخة 5 تم اضافة معاملات مثل timeout

إعدادLocal EAP

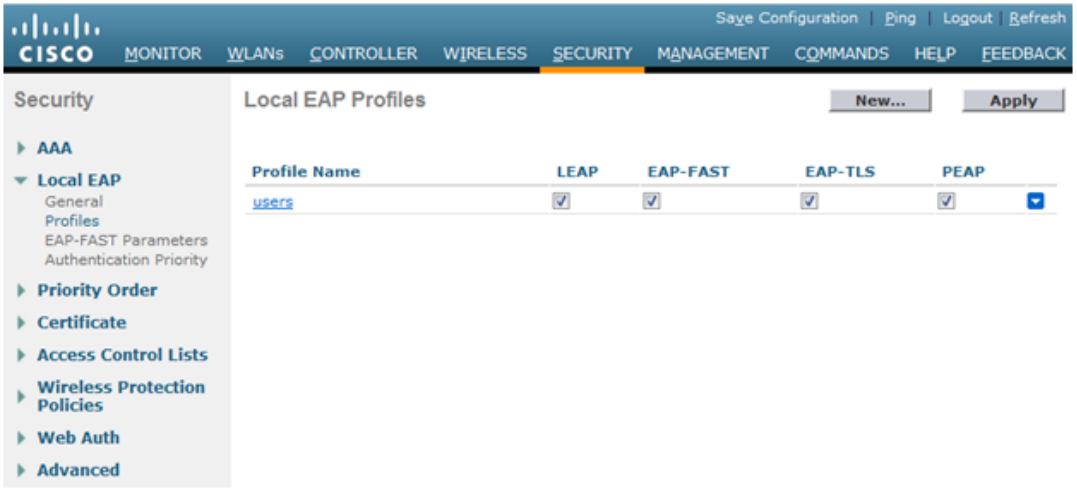
أدخل علي الصفحة Security>Local EAP>Profiles لعمل بروفايل جديد



اكتب اسم البروفايل ثم اضغطApply

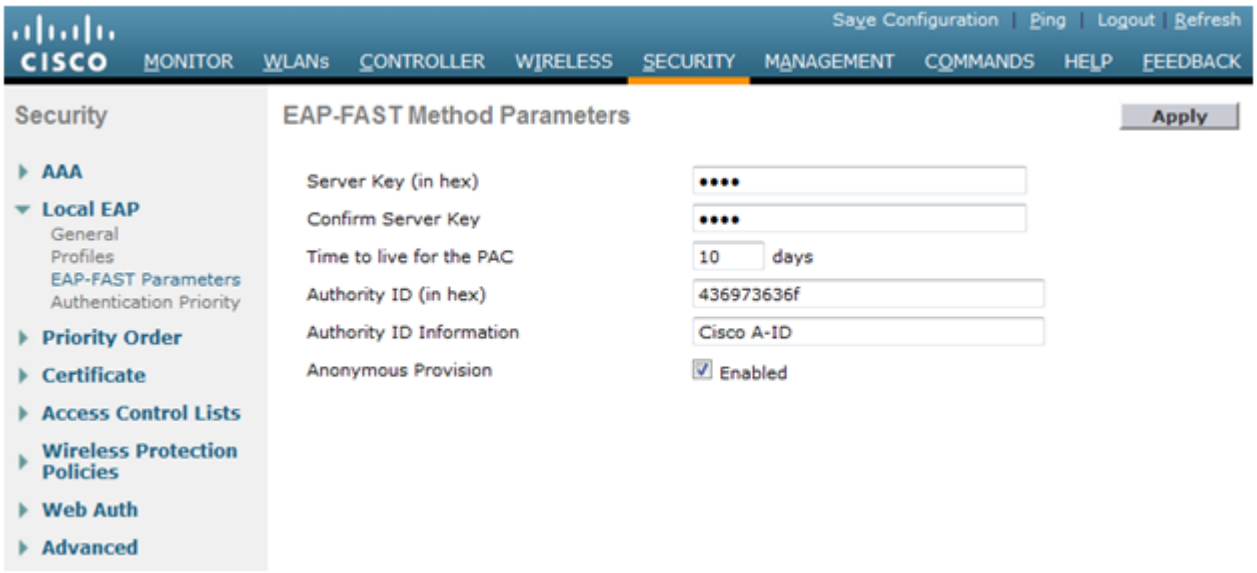


ثم اختر نوع التوثيق المعتمد مثل LEAP و PEAP ثم اضغطApply



اضغط علي Users لتخرج لك هذه الصفحة قم بالتأشير علي البروتوكولات التي سيدعمها هذا السيرفر و هي بروتوكولات سنتعرف عليها بالتفصيل في كورس السيسكيوريتي من CCNP Wireless بإذن الله تعالي

بعد ذلك قم بالدخول علي صفحة Security > Local EAP > EAP-FAST Parameters لعمل إعدادات EAP-FAST و ستظهر هذه الصفحة



Server Key (in hexadecimal) : هو المفتاح الذي سيستخدم في التشفير و فك التشفير و لابد أن يكون بالصيغة السداسية عشر 0-9 و A-F

Time to Live for the PAC : المدة المسموح بتفعيل هذا النظام و يسمح بوضع قيم من 1 الي 1000 يوم

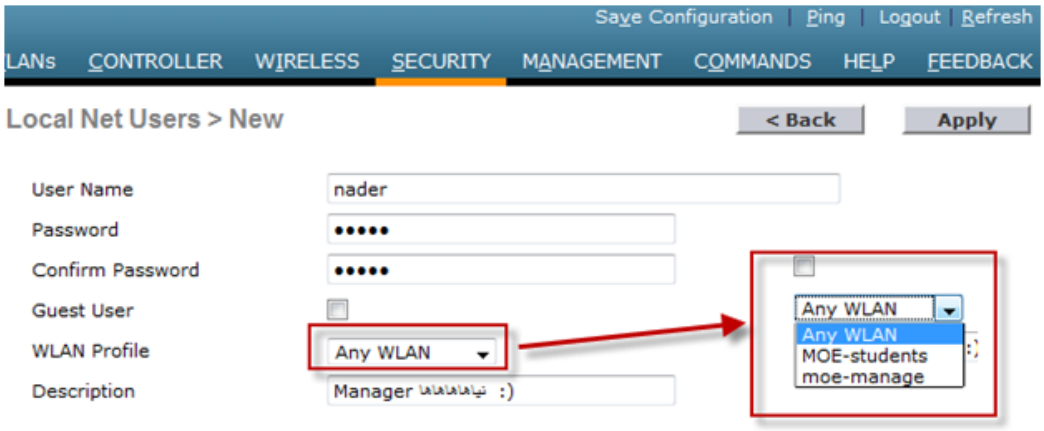
Authority ID (in hexadecimal) : يسمح بوضع 32 حرف و رقم سداسي عشر كحد أقصي

Authority ID Information : تعريف بالنظام

عمل مستخدمين للشبكة

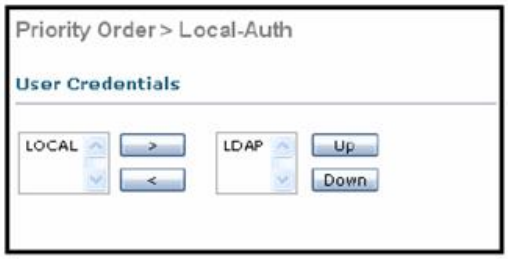
قم بالدخول علي Security > AAA > Local Net User لنبدأ في عمل مستخدمي الشبكة الذين سيطبق عليهم هذا السيرفر

اضغط New لعمل مستخدم جديد



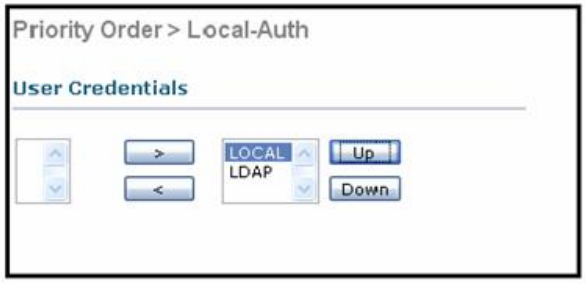
بعد أن قمنا بإضافة مدير و مستخدم للشبكة ستخرج لنا الصفحة

سنقوم بعد ذلك بتحديد أولوية Local EAP من الصفحة Security > Local EAP > Authentication Priority علما بأن LDAP هو أيضا سيرفر توثيق الا أنه خارجي يشبه Microsoft Active Directory

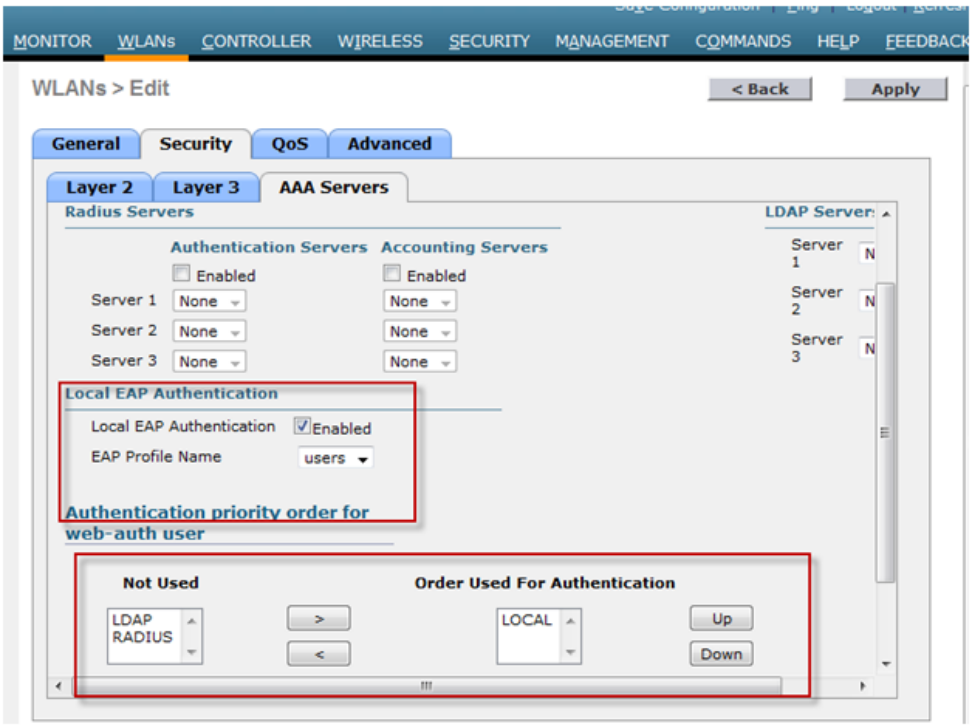


Only LDAP is used

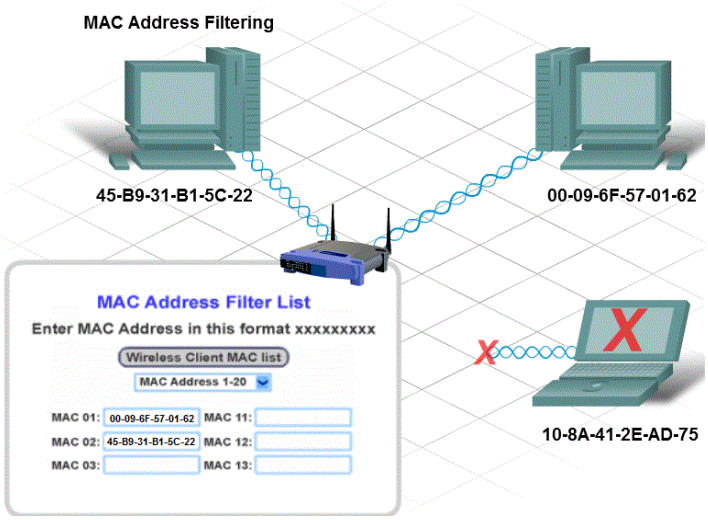
LDAP is used only if the local list does not contain the user



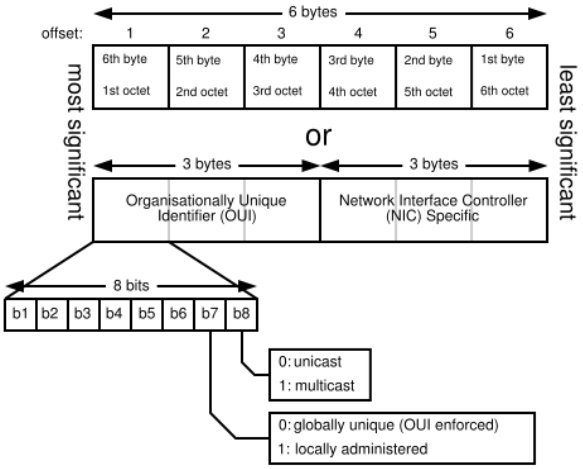
بعد ذلك سنقوم بتفعيل هذا التوثيق من الصفحة WLANs>Edit ثم من التبويب Security تختار Advanced و تختار نوع التوثيق و أولويته هكذا



MAC Address Filtering



يعتبر تأمين الشبكة في الطبقة الثانية من أشد الطرق و أسهلها ، فالطبقة الثانية Data Link تختص بعناوين الأجهزة MAC addressأو Media Access Control address و هي عناوين لا تتكرر إطلاقا و تتكون من 12 حرف تتخيرها من ستة عشر رمزا هي أرقام من 0 الي 9 و حروف من A الي F و تسمي بـ السداسية عشر Hexadecimalو يكتب هكذا من ست مجموعات يفصل بينها : أو – مثل-01-23-45-67-89 ab, 01:23:45:67:89:ab و هناك نظام نخر حيث يتكون العنوان من ثلاث مجموعات مثل ab 0123.4567.89 و في كل الأحوال يتكون العنوان من أثني عشر حرفا و رقما



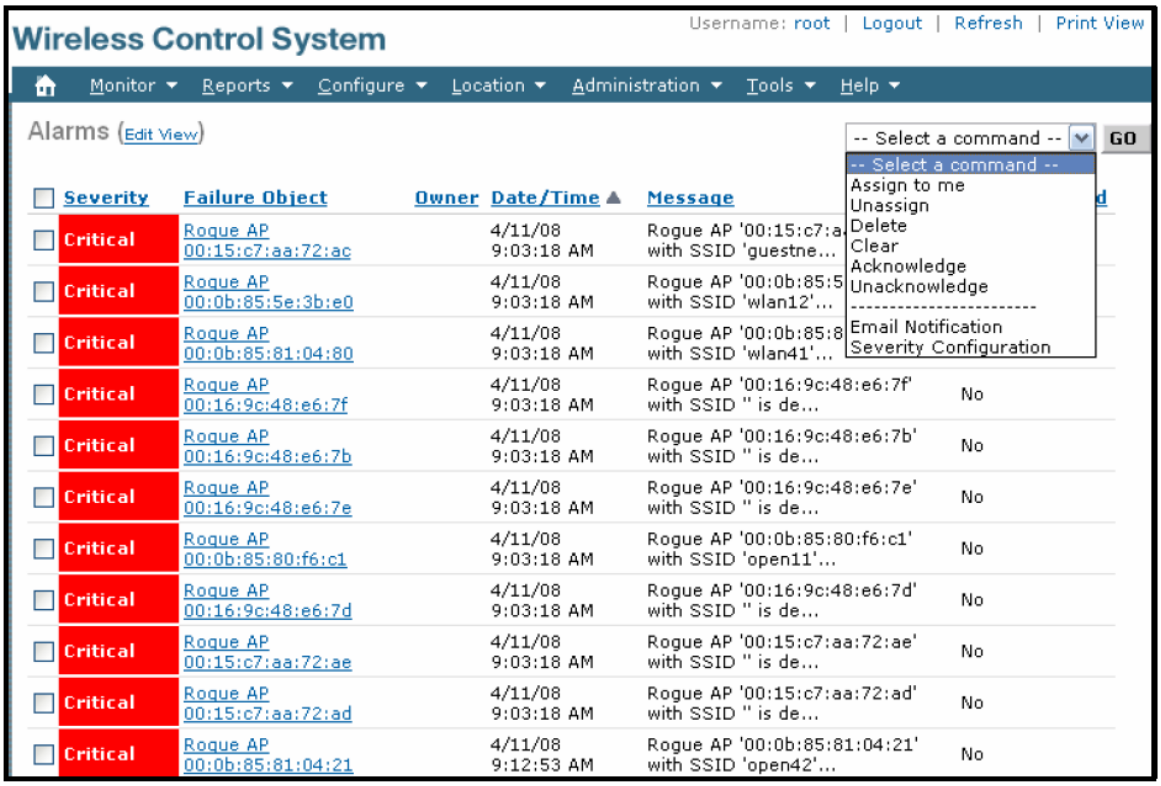
و هذه العناوين توجد في الشبكة لكروت الإيثرنت المستخدمة في الإتصال الشبكي و كذلك الراوترات و السويتشات و كافة أجهزة الشبكة و لا تتكر اطلاقا علي مستوي العالم و ليس الشبكة فقط

و لكل جهاز عنوان MAC يعرف به نوعه و الجهة التي صنعته فمثلا الرقم الذي يبدأ بـ 00-06-25 خاص بمعدات شركة لينكسيس من سيسكو حيث يتم تخصيص دوما

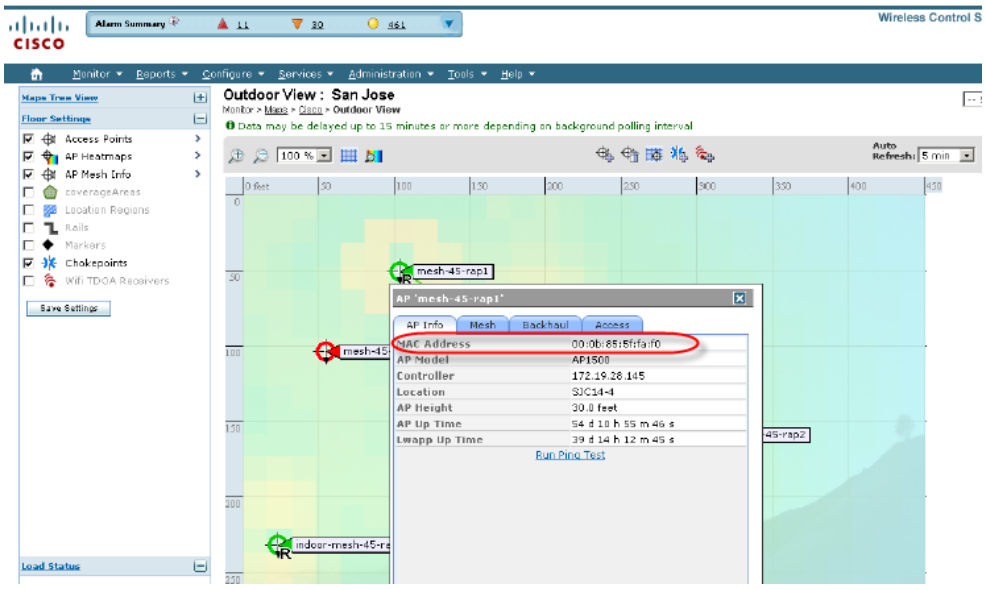
و لأن هذه العناوين فريدة فنستطيع في الشبكات اللاسلكية استخدامها في فلترة الأجهزة التي نسمح أو لا نسمح بدخولها للشبكة و هو ما يطلق عليه MAC Address Filtering و لكن لابد أولا من معرفة هذا العنوان

و لكن كيف تستطيع معرفة هذه العناوين

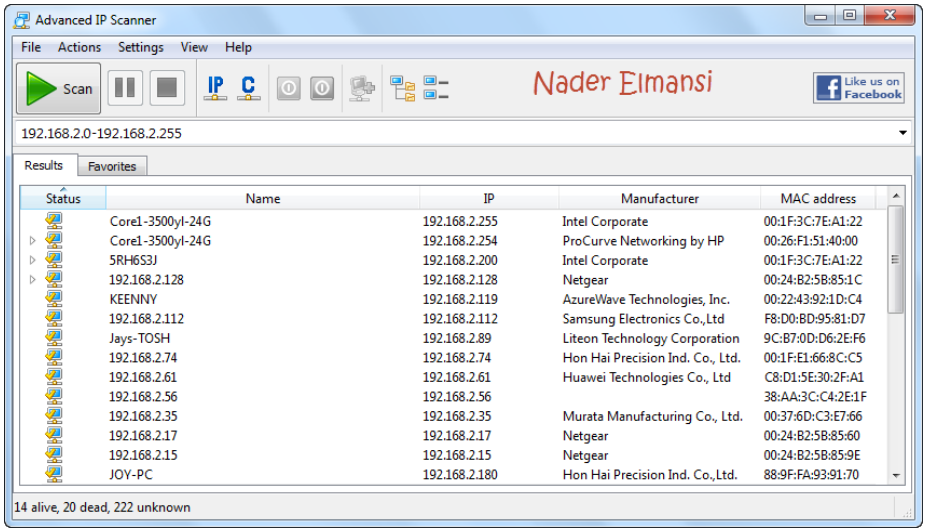
لدينا عدة طرق أولها في حال استخدام شبكات سيسكو اللاسلكية فإن سيرفر WCS يظهر لك الأجهزة الدخيلة Rogue بعناوينها الفيزيائية سواء كانت أكسس بوينت أخري أو كمبيوتر في شاشة الأحداث هكذا



أو في شاشة الخرائط هكذا



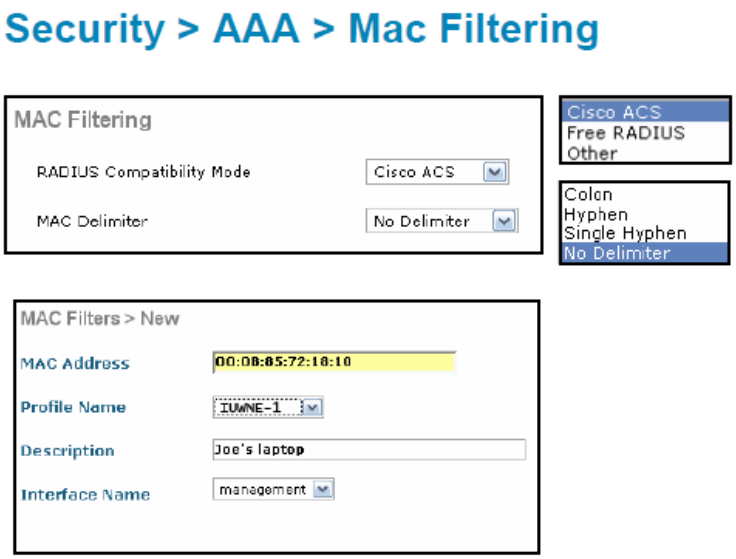
و هناك طريقة أخري لمعرفة هذه الأجهزة و ذلك باستخدام برمجيات البحث عن عناوين IP في الشبكة مثل Advanced IP Scanner و الذي تظهر الصورة التالية الأجهزة التي تشاركني الإتصال اللاسلكي مع بيان اسمها و عناوين MAC الخاصة بها و شركات تصنيعها



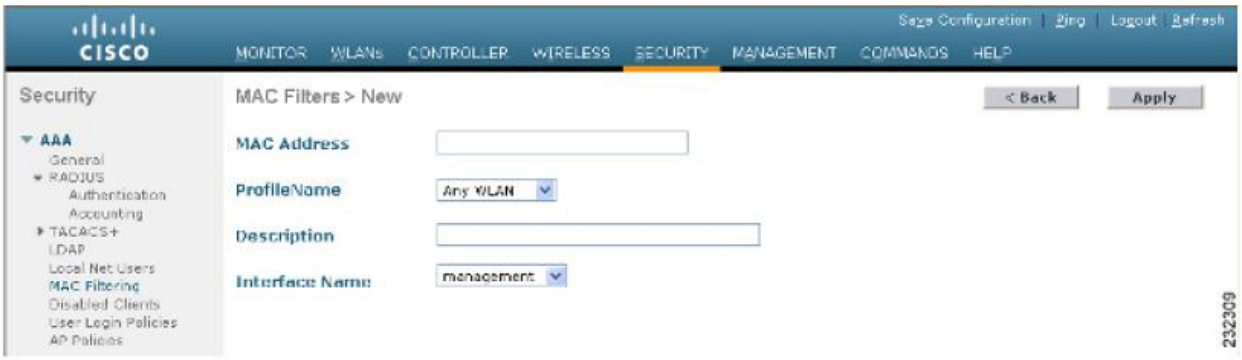
بعد جلبك لرقم الكارت الذي تريد منعه ادخل علي صفحة إدارة الأكسس بوينت الخاص بك ثم قم بإضافة العناوين التي تريد حجبها و هذه طريق عملها علي D-Link Access point

و كما تري فإن الأكسس بوينت منفردا لا يستطيع الا أن يحجب عشرين جهازا و هنا تأتي شبكات سيسكو اللاسلكية بجهاز الكنترولر الذي يستطيع أن يقوم بمركزية حجب 2500 عنوان سواء كان العنوان لجهاز كمبيوتر أو لأكسس بوينت أو أي جهاز لاسلكي يستطيع ولوج الشبكة و له عنوان فيزيائي

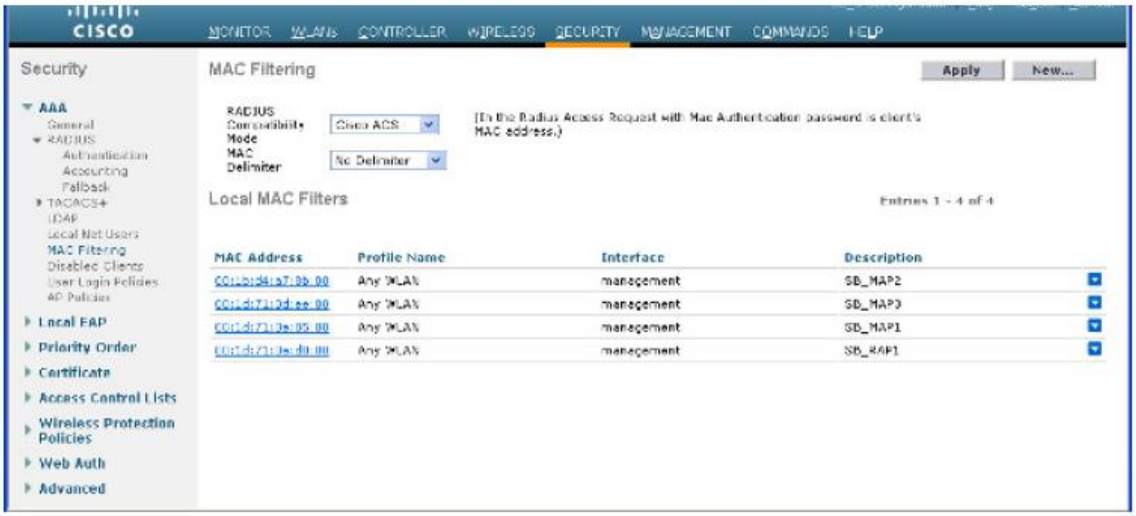
و يعيطك الكنترولر امكانية استخدام سيرفر مركزي لفلترة هذه العناوين باستخدام Raduis فقط ستدخل علي الكنترولر ثم ستتبع الصفحة **Security > AAA > MAC Filtering** الموجوده في الصورة و ستختار اماكن تواجد هذه العناوين و بالطبع سنجعلها local



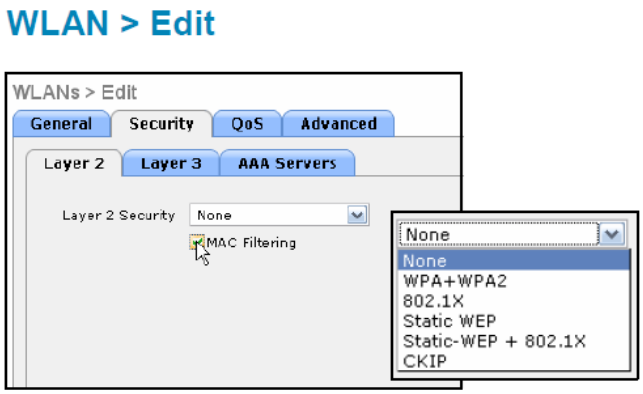
ثم تضغط علي New لإدخال العناوين التي تريدها مع امكانية وضع وصف لكل عنوان كما تري



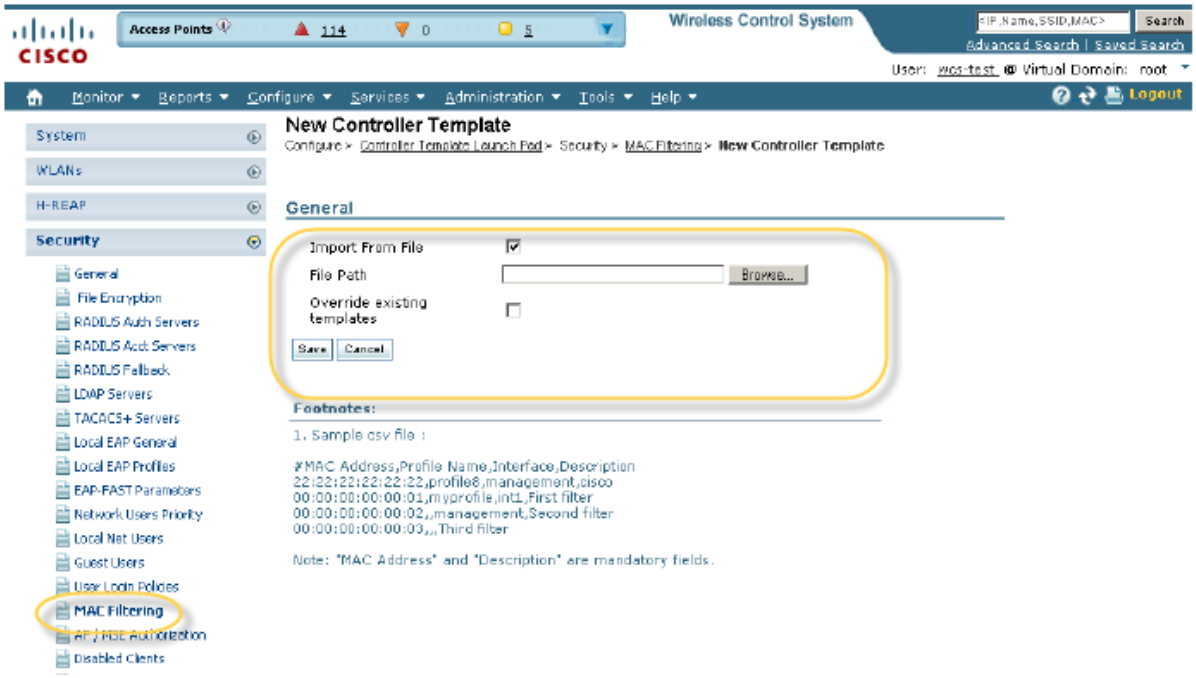
الآن لدينا قاعدة بيانات للعناوين كما تري



بعدها نقوم بتفعيل هذا الأمر بالضغط علي الخيار MAC Filtering و ستضمن منع هذه الأجهزة حتي لو لم يكن لديك أي نوع من التوثيق أو التشفير



تستطيع ايضا استخدام سيرفر WCS و تستطيع أن تقوم بتحميل ملف تعريف كامل بهذه العناوين



يذكر أن هذه الطريقة ليست ناجحة 100 % فهناك برمجيات تستطيع محاكاة عناوين MAC في الشبكة و هو ما يسمي بالتمثيل الكاذب الا أن هذه المحاكاة لا تصلح غالبا مع شبكات سيسكو اللاسلكية و التي يقوم الكنترولر بفلترة قوية لهذه العناوين

نادر المنسي