

ITRAINONLINE MMTK

إعدادات نقاط الولوج – كراسة المتدرب

إعداد: IT +46

إعتماداً على العمل الأصلي لأونو بوربو وسيباستيان بويتريخ
النسخة العربية: أنس طويلة، www.tawileh.net/anas

1	ITRAINONLINE MMTK
2	1. عن هذا المستند
2	1.1. معلومات حفظ الملكية الفكرية
2	2.1. درجة الصعوبة
2	2. مقدمة
2	3. قبل أن تبدأ
3	4. تركيب التجهيزات وبرمجيات تشغيلها
3	1.4. التركيب الفيزيائي
4	2.4. تطوير برمجيات تشغيل نقطة الولوج Firmware
4	3.4. توصيل الحاسب بنقطة الولوج
5	5. إعداد التجهيزات وفقاً لنموذج ISO المعياري
6	1.5. الطبقة الفيزيائية Physical Layer
6	1.5.1. رقم القناة
6	1.5.2. قدرة الإرسال Transmitting Power
7	1.5.3. السرعة أو الإستطاعة
7	2.5. طبقة الوصلة Link Layer
7	2.5.1. نمط التشغيل
8	2.5.2. معرف مجموعة الخدمات SSID
8	2.5.3. التحكم بالوصول إلى الناقل Media Access Control
10	2.5.4. التحكم بالوصول إلى الشبكة باستخدام فلترة العناوين الفيزيائية MAC
10	2.5.5. التشفير ((WEP, WPA
10	2.5.6. التحكم بالوصول إلى الشبكة عبر التحقق من الهوية
11	2.5.7. التشفير من النهاية إلى النهاية End-to-End Encryption
11	3.5. طبقة بروتوكول الإنترنت IP Layer
11	4.5. طبقة التطبيقات Application Layer
12	7. الخلاصة

1. عن هذا المستند

تشكل هذه المواد التدريبية جزءاً من حزمة تدريب الوسائط المتعددة (Multimedia Training Kit (MMTK). توفر هذه الحزمة مجموعة متكاملة من المواد التدريبية والموارد الداعمة للإعلام الإجتماعي، مراكز الوسائط المتعددة للمجتمعات، مراكز الولوج البعيد وغيرها من المبادرات باستخدام تقنيات المعلومات والاتصالات لتدعيم المجتمعات ودعم نشاطات التنمية.

1.1 معلومات حفظ الملكية الفكرية

لقد تم إصدار هذه الوحدة ضمن إتفاقية الترخيص Creative Commons Attribution-ShareAlike 2.5 السويد. للحصول على المزيد من المعلومات عن كيفية استخدام هذه المواد يرجى الإطلاع على نص حماية الملكية الفكرية المضمن مع هذه الوحدة أو راجع <http://creativecommons.org/licenses/by-sa/2.5>

2.1 درجة الصعوبة

درجة صعوبة هذه الوحدة: مبتدئ مع بعض الأجزاء المتقدمة. لقد تم التنويه إلى الأجزاء المتقدمة بوضعها ضمن إطار أحمر لتنبيه القارئ إلى درجة الصعوبة الأعلى لهذه المواد.

2. مقدمة

تقدّم هذه الوحدة منهجيةً عامةً لتكوين وإعداد نقاط الولوج وموجهات الشبكات اللاسلكية. هدفنا أن يتمكن القارئ من استيعاب نتائج كل الإعدادات ومتى ولماذا نحتاج إلى كل من هذه الإعدادات وذلك عوضاً عن التركيز على "أي مفتاح يجب أن تضغط". تتبع هذه المنهجية نموذج ISO المعياري مع التركيز بشكل خاص على الطبقة الفيزيائية وطبقة الوصلة،

توفّر هذه الوحدة بالإضافة إلى ذلك دليلاً لإعداد نقاط الولوج باستخدام الواجهات الرسومية بالإعتماد على الوب يشرح طريقة الإعداد خطوةً خطوةً (الملحق 1).

3. قبل أن تبدأ

بغض النظر عن التجهيزات التي ستستخدمها أو بنية الشبكة التي تريد إعدادها، عليك الإنتباه إلى مجموعة من التوجيهات العامة:

1. اقرأ دليل استخدام نقطة الولوج وتعرّف على هذا الجهاز وإعداداته الافتراضية.
2. فكّر في التوضع الفيزيائي لنقطة الولوج (إمكانية توصيل التيار الكهربائي، الهوائيات، درجة الحرارة، الرطوبة إلخ). لمزيد من المعلومات، راجع "دراسة الموقع".
3. صمّم الشبكة (TCP/IP) قبل البدء وارسم بنية الشبكة المطلوبة. يتضمن تصميم الشبكة معرفة إعدادات مزود خدمة الإنترنت أو الشبكة المحلية بما فيها مخدّم أسماء النطاق DNS، إلخ.

4. تأكد من أنك تملك جميع المواد والمعلومات (فيزيائياً لا على شبكة الإنترنت وحسب) بحيث يمكنك العمل حتى لو لم تستطع الوصول إلى الإنترنت أثناء التركيب.

5. دون كل خطوة تقوم بها أثناء الإعداد، خاصة عند تغيير عناوين الإنترنت IP، إعدادات الشبكة وكلمات السر.

6. تأكد من أنك تملك جميع التجهيزات المطلوبة (حاسب شخصي أو حاسب محمول يحتوي على بطاقة شبكة لاسلكية وبطاقة شبكة إيثرنت).

7. تأكد من أنك تملك جميع البرمجيات المطلوبة مثل:

• أدوات إعداد بروتوكولات (TCP/IP (ping, route

• برمجيات خاصة بمصنع التجهيزات (تطبيقات نظام تشغيل التجهيزات، برمجيات التعريف، إلخ)

• برمجيات قياس وكشف الإشارات اللاسلكية (Kismet, Netstumbler)

4 تركيب التجهيزات وبرمجيات تشغيلها

تتمثل الخطوة الأولى في إعداد نقاط الولوج بتركيب التجهيزات، توصيل نقطة الولوج إلى الحاسب و(اختيارياً) تطوير برمجيات تشغيلها. تقدم هذه الفقرة تعريفاً بالمخطط الفيزيائي العام لنقاط الولوج وكيفية تركيب هذه التجهيزات فيزيائياً.

1.4 التركيب الفيزيائي

عليك الإنتباه إلى جزئين مختلفين من نقاط الولوج:

1. أضواء الحالة Status LEDs¹

2. منافذ مرسل الراديو والإيثرنت

تتضمن نقاط الولوج عادةً من الأعلى مجموعة من الأضواء التي تشير إلى حالة الجهاز. تشير هذه الأضواء عادةً عبر إشارات ضوئية ثابتة أو منقطعة (برتقالية أو حمراء) إلى المتغيرات التالية:

1. وصول القدرة الكهربائية إلى نقطة الولوج

2. المنافذ النشطة

3. الأخطاء الداخلية

4. وصلة الإيثرنت Uplink

قد توفر لك هذه الأضواء معلومات قيمة لدى تتبع المشاكل في الشبكة. ننصحك بشدة لدراسة معاني هذه الإشارات الضوئية بعناية في دليل استخدام نقطة الولوج الخاصة بك قبل البدء بإعداد الشبكة.

تتضمن نقاط الولوج المنافذ الأساسية التالية:

1. منفذ إيثرنت: يدعى غالباً (منفذ الشبكة الواسعة WAN – للوصل مع الإنترنت) أو (منفذ

الشبكة المحلية LAN للوصل مع الشبكة المحلية). تتضمن نقاط الولوج المخصصة (الجسر

¹ LED = دايمود مشع للضوء Light Emitting Diode

اللاسلكي (Wireless Bridge) منفذ إيثرنت واحد. تعتبر نقاط الولوج التي تحتوي على أكثر من منفذ إيثرنت واحد بالموجّهات / البوابات اللاسلكية.
2. مرسل الراديو / الهوائي: الوصلة اللاسلكية مع الزبائن.

قد تتضمن التجهيزات اللاسلكية المتطورة منفذين لاسلكيين أو أكثر (مرسلين راديويين أو أكثر).

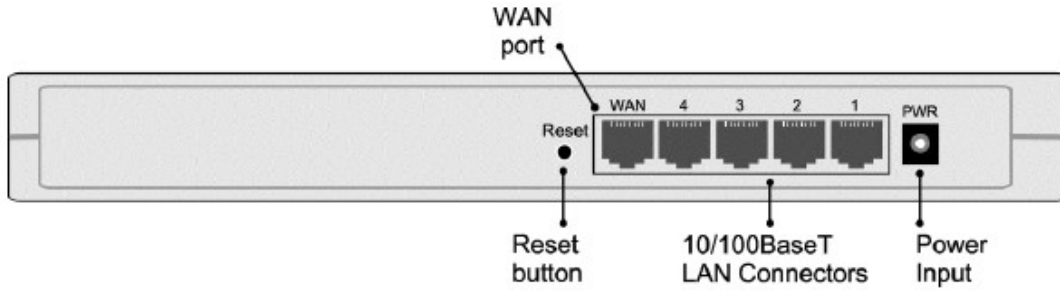
غالباً ما ستجد منافذ الإيثرنت في إحدى الجهات الخلفية بالإضافة إلى مجموعة أخرى من الميزات التشغيلية:

1. مدخل القدرة الكهربائية (12، 5 أو 3.5 فولت تيار مستمر DC): يتصل بمصدر القدرة الكهربائية.

2. مفتاح إعادة التشغيل Reset: يستخدم لاستعادة الإعدادات الافتراضية.

3. منافذ الشبكة المحلية (RJ45): LAN: تتصل بالشبكة المحلية.

4. منفذ الشبكة الواسعة (RJ45): WAN: يتصل بموجّه Cable Modem، DSL أو أية تجهيزات لتوفير الإتصال بالشبكة الواسعة أو الإنترنت.



شكل 1: الترتيب النموذجي للوصلات والمنافذ ضمن خلفية نقطة و لوج لاسلكية (موجّه لاسلكي)

كما تتضمن نقطة الولوج عادة زوجاً من الهوائيات التي قد تكون مضمّنة في نقطة الولوج أو موصولة بغطائها. يمكن على الأغلب تعديل الهوائيات الخارجية لتلائم متطلبات التركيب الخاصة.

2.4 تطوير برمجيات تشغيل نقطة الولوج Firmware

تتم كتابة برمجيات تشغيل نقطة الولوج Firmware ضمن ذاكرة للقراءة فقط Read Only Memory (ROM) بحيث تصبح جزءاً دائماً من نقطة الولوج. يمكن تسمية برمجيات التشغيل هذه بالبرمجيات الثابتة. تبقى هذه البرمجيات ضمن ذاكرة القراءة فقط ROM حتى بعد إيقاف تشغيل الجهاز. تعتبر برمجيات الدخل والخرج الأساسية BIOS التي تتحكم في الحواسيب أثناء بدء تشغيلها إحدى أشكال البرمجيات الثابتة.

يقوم منتجو التجهيزات بتطوير برمجيات تشغيل تجهيزاتهم على الدوام لتقديم أحدث الإعدادات وحل المشاكل التي تم اكتشافها. حاول دائماً أن تقوم بتطوير نقطة الولوج الخاصة بك لآخر نسخة مستقرة من برنامج تشغيلها قبل البدء بإعداد الشبكة وتحقيق من توفر أية تعديلات بشكل دوري.

3.4. توصيل الحاسب بنقطة الولوج

ينبغي عليك قبل إعداد نقطة الولوج أن تقوم بتوصيلها إلى حاسبك الشخصي أو المحمول. يمكنك القيام بذلك سلكياً أو لاسلكياً. ننصحك بشدة أن تبدأ عملية الإعداد باستخدام وصلة سلكية ومن ثم الانتقال إلى الوصلة اللاسلكية بعد الإنتهاء من الإعدادات الأساسية وعندما تملك ثقة أكبر بمعرفتك بعملية الإعداد.

يمكن إجراء الوصلة السلكية عبر:

1. سلك إيثرنت باستخدام بروتوكول النقل التشعبي HTTP
2. سلك إيثرنت باستخدام برنامج خاص بمنتج نقطة الولوج يعتمد على بروتوكول إدارة الشبكة البسيط SNMP
3. سلك تسلسلي (Null Modem) باستخدام برنامج HyperTerminal أو أي برنامج آخر للاتصال التسلسلي (إذا احتوت نقطة الولوج على منفذ تسلسلي)

يعتبر أسلوب الوصل عبر سلك إيثرنت باستخدام بروتوكول HTTP أكثر هذه الخيارات شيوعاً. لا يرتبط هذا الأسلوب في الإعداد بأي نظام تشغيل محدد ويحتاج فقط إلى متصفح للإنترنت. عليك الإنتباه بأن واجهة الاستخدام ستختلف من منتج إلى منتج ومن طراز إلى آخر، هذه الواجهات تتغير باستخدام وسيصعب عليك أن تجد جهازين يملكان نفس واجهة الاستخدام. لكن جميع هذه الواجهات تحتوي على نفس العناصر الأساسية. لاحظ أيضاً بأن المنتجين قد يستخدمون كلمات مختلفة للإشارة إلى نفس المفهوم.

إليك فيما يلي هذه المفاهيم الأساسية:

يتوجب عليك لكي تتمكن من التواصل مع نقطة الولوج أن تنتمي إلى نفس الشبكة. راجع دليل استخدام نقطة الولوج لمعرفة عنوان الإنترنت IP الافتراضي لنقطة الولوج وقم بتغيير عنوان الإنترنت الخاص بك لتصبح قادراً على التواصل معها. يمكنك بعد ذلك تشغيل متصفح الإنترنت على حاسبك لمتابعة إعداد نقطة الولوج باستخدام الواجهة التي تعتمد على الوب.

هناك أيضاً بعض الأدوات "الخاصة" والتي يمكنك تثبيتها ضمن حاسبك لإعداد نقطة الولوج. تعتمد غالبية هذه الأدوات على بروتوكول يدعى (بروتوكول إدارة الشبكة البسيط SNMP). (راجع وحدة كشف الأخطاء).

يمكنك استخدام الخيار الثالث (السلك التسلسلي) باعتباره الحل الأخير عندما تعجز الأساليب الأخرى عن تحقيق غايتها. يتطلب هذا الأسلوب الوصول فيزيائياً إلى نقطة الولوج لذا فمن الصعب أن يتم من قبل أي شخص كان. يستخدم السلك التسلسلي لإعادة إعداد نقطة الولوج فيما إذا نسيت كلمة السر دون الحاجة لإعادة الإعدادات الافتراضية. يمكنك عادة الوصول إلى نقطة الولوج عبر المنفذ التسلسلي دون معرفة كلمة السر (بإمكانك أيضاً إعداد الوصول عبر المنفذ التسلسلي لكي لا يتطلب كلمة سر).

5. إعدادات التجهيزات وفق النموذج ISO المعياري

قد يبدو لك إعداد نقطة الولوج للوهلة الأولى أمراً فائق التعقيد، خصوصاً بعد الإطلاع على سماكة دليل الاستخدام المرفق. تتضمن إعدادات نقاط الولوج عادةً كمّاً هائلاً من المتغيرات مما يجعل من الصعب التمييز بين الإعدادات الأساسية وتلك المتقدمة.

تحتاج نقاط الولوج "الصرفة"¹ إعداد متغيرين فقط:

1. معرف مجموعة الخدمات SSID

¹ نعني بنقطة الولوج "الصرفة" أنها تعمل كجسر لاسلكي Wireless Bridge دون أية قدرات للتوجيه. لا توفر نقطة الولوج هذه خدمات NAT، DHCP، إلخ.

2. رقم القناة

لكنه من الأفضل القيام ببعض الإعدادات الإضافية أيضاً. تشير غالبية المتغيرات الاختيارية إلى أمن الشبكة من حيث التشفير وتحديد الوصول، إلا أنّها فائقة الأهمية في حال رغبت في تأمين شبكتك اللاسلكية.

إليك فيما يلي أسلوباً نظرياً لإعداد تجهيزات الشبكة اللاسلكية وفقاً لنموذج OSI المعياري مع التركيز على وظيفة كل إعداد وأسباب الحاجة إليه. نحن نعتقد بشدة أنّ استيعاب "لماذا" نحتاج للقيام بإعداد ما، و"ماذا" يعني إعداد متغير ما، يشكل شرطاً أساسياً لبناء شبكات لاسلكية ذات نوعية عالية.

تعرفنا فيما سبق بأنّ الشبكات اللاسلكية محصورةً بالطبقتين الأولى والثانية فقط من نموذج ISO المعياري: الطبقة الفيزيائية وطبقة الوصلة. بما أن نقطة الولوج (والتي هي في الأساس جهازاً للتشبيك اللاسلكي) لا تعدو كونها مجرد "مجمّع لاسلكي" فإن جميع إعداداتها اللاسلكية الصرفة تتعلق بالطبقتين الأولى والثانية لنموذج OSI المعياري.

إذا ما احتوت نقطة الولوج على ميزات التوجيه وترجمة عناوين الشبكة NAT فإنّ إعداداتها ستتضمن متغيرات متعلّقة بطبقة OSI الثالثة: طبقة بروتوكول الإنترنت IP.

1.5. الطبقة الفيزيائية Physical Layer

فيما يلي متغيرات إعداد نقطة الولوج التي تؤثر في الطبقة الفيزيائية:

1.51.. رقم القناة

إنّ إعداد القناة لنقطة لوج يحدد نطاق الترددات (غيغاهرتز GHz) التي ستعمل ضمنها هذه النقطة. ينبغي عليك قبل إعداد القناة أن تقوم بمسح شامل لنطاق الترددات الموافق باستخدام برنامج مثل "Netstumbler" أو برنامج شبيه وذلك لتجنّب إعداد نفس القناة المستخدمة في شبكات أخرى (في حال وجود شبكات أخرى مجاورة). إن قيامك بذلك سيبيح لك التأكد من استخدام نطاق ترددات أفضل من ناحية التشويش.

ننصحك باستخدام الأقنية 1، 6 أو 11 للشبكات العاملة وفق معيار 802.11b وذلك لضمان توفّر فواصل كافية بين الترددات لتجنّب التعارض. لا ينطوي استخدام الشبكات اللاسلكية العاملة وفق معيار 802.11a على أية مخاطر لتداخل الأقنية، لذلك عليك فقط التأكد من أنّ نقاط الولوج المجاورة والتي تعمل وفق نفس المعيار تستخدم قنوات مختلفة عن تلك التي ستستخدمها في إعداد نقطة الولوج التي ستركبها.

تمتلك بعض نقاط الولوج الحديثة ميزةً تمكّنها من اختيار القناة التي ستعمل وفقها تلقائياً بناءً على الترددات الهادئة المتوفرة التي تجدها بعد مسح طيف الترددات وإيجاد الترددات المستخدمة في نقاط لوج أخرى. لمزيد من المعلومات راجع وحدة "دراسة الموقع".

1.52.. قدرة الإرسال Transmitting Power

يزداد نطاق تغطية نقطة الولوج كلما ازدادت قدرة الإرسال المستخدمة. إذا ما أردت الحصول على أوسع تغطية ممكنة ينبغي عليك إعداد قيمة قدرة الإرسال بقيمتها الأعظمية. تحدد قدرة الإرسال الأعظمية القانونية

في غالبية البلدان بـ 100 ميللي وات (20 ديسيبل)، إلا أنّها قد تصل في دولٍ أخرى (كغالبية الدول الأفريقية) إلى 1-3 وات.

لا تتيح جميع نقاط الولوج إمكانية تحديد قدرة الإرسال. عليك الإنتباه إلى أنّه ينبغي حساب القيمة الأعظمية القانونية لقدرة الإرسال مع اعتبار ربح الهوائيات المستخدمة (راجع وحدة "حساب الوصلة الراديوية").

في المقابل إذا ما أردت زيادة استطاعة الشبكة اللاسلكية عبر إضافة المزيد من نقاط الولوج القريبة من بعضها البعض عليك تخفيض قيمة قدرة الإرسال للتقليل من التداخل واحتمالات التشويش. يمكنك أيضاً تركيب الهوائيات بشكل ملائم لتخفيض آثار التشويش بين نقاط الولوج.

1.53.. السرعة أو الإستطاعة

تتيح بعض نقاط الولوج إمكانية اختيار السرعات المفضّلة (11، 5.5، 2 أو 1 ميغابت في الثانية للشبكات العاملة وفق معيار 802.11b). إن تحديد السرعة المفضّلة سيغيّر تقنية الترميز المستخدمة لنقل البيانات.

ننصحك بإعداد السرعة على أعلى قيمة ممكنة. إذا ما أردت تركيب وصلة لاسلكية بعيدة المدى ولاحظت بعض مشاكل فقدان البيانات يمكنك عندها تجربة تخفيض السرعة للحصول على إشارة أكثر ثباتاً.

2.5. طبقة الوصلة Link Layer

فيما يلي متغيرات إعداد نقطة الولوج التي تؤثر في طبقة الوصلة:

2.51.. نمط التشغيل

ينبغي عدم الخلط بين نمط تشغيل نقطة الولوج ونمطي تشغيل مرسل الراديو الأساسيين لبطاقات الشبكة اللاسلكية (وهما النمط الخاص Ad hoc ونمط البنية التحتية Infrastructure).

يشير نمط التشغيل في نقطة وولوج إلى أنواع المهام التي تقوم بها هذه النقطة. قد يتسبب استخدام مصطلح "نمط Mode" بالإلتباس في كثير من الأحيان نتيجة اختلاف الأسماء المستخدمة من قبل منتجي التجهيزات للإشارة إلى نمط تشغيل منتج ما.

تذكر دائماً بأنّ نقطة الولوج الصرفة تقوم فقط بالمهام المتعلقة بإرسال الإشارات الراديوية "كالتجسير Bridging". إذا كان الجهاز المسمى (نقطة وولوج) قادراً على إنجاز المهام المتعلقة ببروتوكول الإنترنت IP كالتوجيه وترجمة عناوين الشبكة NAT فإننا نتحدث هنا عن موجّه لاسلكي. تختلف أنماط تشغيل نقطة الولوج بشكل أساسي فيما إذا كانت نقطة الولوج تقوم بمهام التجسير أو التوجيه وترجمة عناوين الشبكة NAT.

تشرح الفقرة التالية مجموعة من الأنماط النموذجية التي قد تصادفها في نقاط الولوج (أو الموجّهات اللاسلكية). لاحظ بأن اسم النمط قد يختلف من منتج لآخر.

تجسير نقطة الولوج Access Point Bridging (أو نمط نقطة الولوج)

تعمل نقطة الولوج كجسر صرف بين موجّه و عددٍ من زبائن الشبكة اللاسلكية. لا تقوم نقطة الولوج بأي من مهام التوجيه أو ترجمة عناوين الشبكة NAT. يعتبر هذا النمط أبسط إعداد لنقطة وولوج لاسلكية.

البوابة Gateway

تقوم نقطة الولوج بدور الموجّه اللاسلكي بين شبكة محلية LAN ومجموعة من زبائن الشبكة اللاسلكية عبر القيام بمهام التوجيه أو ترجمة عناوين الشبكة NAT لزبائنها. قد تحصل نقطة الولوج على عنوان إنترنت IP من مخدّم ضمن الشبكة عبر بروتوكول الإعداد التلقائي للمضيف DHCP. يمكن لنقطة الولوج أن تزود زبائنها بعناوين إنترنت IP عبر بروتوكول DCHP أيضاً.

جسر بين نقطتين Point-to-Point Bridge (أو نمط التكرار)
يتم استخدام نقطتي وولوج لبناء جسر بين شبكتين سلكيتين. لا تقوم أي من هاتين النقطتين بمهام ترجمة عناوين الشبكة NAT لأن دورها لا يتجاوز تمرير حزم البيانات.

التوجيه بين نقطتين Point-to-Point Routing (أو وصلة الجسر اللاسلكي)
تستخدم نقطة الولوج كموجه لاسلكي بين شبكتين محليتين LAN منفصلتين.

بطاقة شبكة الإيثرنت اللاسلكية (أو نمط زبون الشبكة اللاسلكية)
يستخدم هذه النمط لتشبيك الحواسيب التي لا تدعم بطاقات الشبكة اللاسلكية. يمكن استخدام نقطة الولوج كبطاقة شبكة لاسلكية يربطها مع الحاسب عبر منفذ الإيثرنت أو USB.

2.52 معرف مجموعة الخدمات SSID

معرف مجموعة الخدمات SSID هو اسم الشبكة اللاسلكية، ويستخدم أيضاً ضمن جميع حزم "الإرشاد" Beacon التي ترسلها نقاط الولوج. يتألف معرف مجموعة الخدمات SSID من كلمة نصية قد يصل طولها حتى 32 حرفاً أو رقماً (وهي حساسة لحالة الأحرف الكبيرة والصغيرة). يستخدم هذا المعرف أثناء عملية الربط مع الشبكة اللاسلكية. تكافئ عملية الربط في الشبكات اللاسلكية توصيل سلك الشبكة بالمنفذ الجداري في الشبكات السلكية.

ينبغي على زبائن الشبكة اللاسلكية الراغبين بالتواصل مع نقطة وولوج معينة استخدام معرف مجموعة الخدمات SSID أثناء عملية الربط. (لمزيد من المعلومات راجع وحدة "إعداد زبون الشبكة اللاسلكية").

تقوم نقاط الولوج بشكلٍ إفتراضي بإرسال معرف مجموعة الخدمات SSID (عبر حزم الإرشاد) وذلك للتنويه بوجود هذه النقاط، مما يعني أن أي شخص يملك بطاقة شبكة لاسلكية سيتمكن من "رؤية" شبكتك من خلال هذا المعرف. في حال عدم إعداد أية آلية أخرى لأمن الشبكة ضمن نقطة الولوج أو الشبكة (كالتشفير باستخدام بروتوكول WPA أو التحقق من الهوية باستخدام فلترة العناوين الفيزيائية MAC أو البوابات المقيدة Captive Portals) فإن أي شخص سيتمكن من الربط مع نقطة الولوج الخاصة بك وبالتالي الوصول إلى الشبكة التي تليها.

تتيح غالبية نقاط الولوج إمكانية إيقاف إرسال معرف مجموعة الخدمات SSID وبالتالي "إخفاء" شبكتك عن أعين العامة. يمكن استخدام هذه الحيلة لتعزيز أمن الشبكة اللاسلكية في وجه المستخدمين العاديين، لكنها تعتبر إجراءً أمنياً ضعيفاً في وجه المستخدمين المحترفين لأنه يمكن باستخدام الأدوات الصحيحة مراقبة سير البيانات عبر الشبكة اللاسلكية والحصول على حزم بيانات معينة تتيح إيجاد معرف مجموعة الخدمات SSID.

2.53 التحكم بالوصول إلى الناقل Media Access Control

تحتوي نقاط الولوج على بعض الإعدادات المتقدمة والتي تبرز أهميتها على وجه الخصوص في حالات الشبكات المزدحمة. من هذه المتغيرات على سبيل المثال تواتر إرسال حزم الإرشاد، RTS/CTS والتجزئة.

¹ لمزيد من المعلومات حول معرف مجموعة الخدمات SSID راجع: http://www.issa-uk.org/downloads/presentations/issa-uk/wp_ssid_hiding.pdf

تواتر إرسال حزم الإرشاد Beacon Interval

تواتر إرسال حزم الإرشاد هو الفترة الزمنية بين إرسال حزم الإرشاد في نقطة الولوج. تكون القيمة الافتراضية لهذا التواتر عادةً 10 ميلي ثانية، ما يعني أنه سيتم إرسال 10 حزم إرشاد كل ثانية.

تقدّم هذه القيمة دعماً كافياً للتحرك ضمن بيئة مكتبية. إذا ما رغبت في الحصول على دعم للتحرك بشكل أكبر يتوجب عليك زيادة تواتر الإرسال. إن تخفيض قيمة تواتر إرسال حزم الإرشاد سيؤدي إلى تخفيف الحمل الزائد على الشبكة لكنه قد يعيق عمل التجوال بين المحطات المركزية.

ننصحك بعدم تغيير هذه القيمة ما لم تملك مبررات مقنعة للقيام بذلك.

طلب الإرسال / جاهزية الإرسال (Request-to-Send (RTS) / Clear-to-Send (CTS)

وهو الأسلوب المعتمد في الشبكات اللاسلكية العاملة وفق معايير IEEE 802.11 لتخفيض التصادمات الناتجة عن "النقاط الخفية" (راجع وحدة "الشبكات اللاسلكية المتقدمة"). وهو باختصار أسلوبٌ لمنح حق استخدام الناقل يتضمن آلية للمصافحة Handshaking بين نقطة الولوج وزبون الشبكة اللاسلكية.

يحتوي أسلوب RTS/CTS على آلية تجنب التصادم Collision Avoidance في بروتوكول الوصول إلى الناقل بتحمس الناقل مع تجنب التصادم CSMA/CA مما يزيد من وثوقية أسلوب الوصول إلى الناقل. لكنه وفي الوقت نفسه يضيف المزيد من الحمل على الشبكة.

يعمل أسلوب RTS/CTS كما يلي: تبدأ إحدى نقاط الشبكة اللاسلكية والتي ترغب بإرسال البيانات بعملية المصافحة مع نقطة الولوج عبر إرسال إطار طلب الإرسال RTS. تستقبل نقطة الولوج هذا الطلب وتردّ بإرسال إطار جاهزية الإرسال CTS إذا ما كان الناقل متاحاً. عندما تستقبل النقطة المرسله هذا الإطار تبدأ بدورها بإرسال البيانات. بما أنّ جميع نقاط الشبكة اللاسلكية قادرة على الإستماع لنقطة الولوج فإنّ إطار جاهزية الإرسال CTS سيصل إلى جميع هذه النقاط. يتضمن هذا الإطار قيمةً زمنيةً يتوجب على جميع نقاط الشبكة انتظارها قبل إرسال أي إطار لطلب الإرسال RTS. تضمن آلية المصافحة عبر RTS/CTS بأنّ النقطة اللاسلكية ستتمكن من إرسال بياناتها دون أن تصطدم بإطاراتٍ مرسله من نقاطٍ أخرى.

إذا احتوت شبكتك اللاسلكية على عددٍ محدودٍ من الزبائن بحيث أنّ جميعها قادرة على رؤية بعضها البعض فإن من الأفضل إيقاف عمل ميزة RTS/CTS. إنّ استخدام ميزة RTS/CTS في هذه الحالة سيزيد من الحمل الزائد على الشبكة بسبب إرسال إطارات RTS/CTS ويقلص من إستطاعة الشبكة الكلية.

يتوجب عليك التفكير في استخدام ميزة RTS/CTS في حال وجود نقاطٍ خفية ضمن الشبكة. في هذه الحالة، وعلى الرغم من أنّ إطارات RTS/CTS ستشكل حملاً إضافياً على الشبكة إلا أنّها قد تخفّض من الحمل الزائد الكلي عبر تقليص إعادة إرسال إطارات البيانات. السؤال الأساسي هنا أيّ من هذين العاملين يملك الأثر الأكبر؟ هل يعتبر الحمل الإضافي الناتج عن استخدام ميزة RTS/CTS أكبر أم أصغر من الحمل الذي سيتم التخلص منه؟ للإجابة على هذه التساؤلات عليك قياس نسبة خسارة الحزم (على مستوى TCP) في كلا الحالتين.

التجزئة Fragmentation

يتضمن معيار IEEE 802.11 ميزة إضافية تتيح لبطاقات الشبكة ونقاط الولوج اللاسلكية إمكانية تقسيم إطارات البيانات إلى أجزاء أصغر لتحسين أداء الشبكة عند وجود تشويش أو مناطق ذات تغطية رديئة.

يؤدي إرسال إطارات أصغر حجماً إلى التقليل من مخاطر التصادم مع الإطارات الأخرى، مما يؤدي بدوره إلى زيادة إعتدالية إرسال الإطارات (إلا أنّ الحمل الإضافي سيزداد).

يمكن للمستخدم أن يتحكم بقيمة التجزئة والتي تتراوح عادةً بين 256-2048 بايت. تعمل ميزة التجزئة عندما تحاول نقطة الولوج أو بطاقة الشبكة اللاسلكية إرسال إطار يتجاوز حجمه قيمة التجزئة المحددة.

يتوجب عليك بدايةً (تماماً كما في حالة ميزة RTS/CTS) أن تقوم بمرآبة شبكتك وتوقع حجم إعادة الإرسال الناتج عن التصادم. إذا كانت نسبة التصادمات عالية عليك التفكير في تغيير قيمة التجزئة المستخدمة.

إذا لم تتجاوز نسبة التصادمات 5% فإننا ننصحك بعدم استخدام ميزة التجزئة لأنّ الحمل الإضافي الناتج عن تقسيم الإطارات سيتجاوز الحمل الناتج عن وجود هذه التصادمات (لأنّها بالأساس قليلة جداً).

2.54.. التحكم بالوصول إلى الشبكة باستخدام فترة العناوين الفيزيائية MAC

تعني فترة العناوين الفيزيائية MAC السماح لمجموعة محدودة فقط من العناوين الفيزيائية MAC المعروفة بالوصول إلى نقطة الولوج. يعتبر هذا الأسلوب إجراءً أمنياً ضعيفاً جداً إلا أنه من الممكن أن يستخدم على التوازي مع حلول أخرى أكثر تطوراً.

بإمكان المستخدم الخبير التلصص على الحزم المنقولة عبر الشبكة اللاسلكية والحصول على العناوين الفيزيائية MAC والتي يسمح لها بالوصول إلى الشبكة. بعدها يمكن للمستخدم تغيير عنوانه الفيزيائي MAC إلى إحدى هذه العناوين المقبولة لخداع نقطة الولوج بانتحال شخصية أخرى يتاح لها الوصول إلى الشبكة.

2.55.. التشفير (WEP, WPA)

تحتوي غالبية نقاط الولوج حالياً بروتوكول WEP (Wired Equivalent Privacy) للتشفير والذي يعتبر قديماً للغاية. على الرغم من أنّ هذا البروتوكول قد أثبت ضعفه الشديد ومع أنّه الآن لا يعتبر خياراً آمناً للتشفير إلا أنه ما زال مستخدماً بكثرة من قبل المستخدمين العاديين.

يستخدم بروتوكول WEP خوارزمية تشفير ذات 40 بتاً لتشفير جميع البيانات قبل إرسالها بين نقطة الولوج وزبون الشبكة اللاسلكية. يضيف معظم المنتجون ميزات تشفير خاصةً إلى منتجاتهم لرفع مستوى التشفير حتى 128 بت.

ينبغي أن ينعكس إعداد بروتوكول WEP ضمن نقطة الولوج على جهة زبائن الشبكة أيضاً. تأكد بأنّ بطاقات الشبكة اللاسلكية تدعم بروتوكول التشفير، أسلوب التحقق من الهوية وطول مفتاح التشفير المستخدمة في إعداد نقطة الولوج.

إذا ما اخترت تشغيل بروتوكول WEP ننصحك بإزالة مفاتيح التشفير الافتراضية المعدة مسبقاً من قبل المنتج وإعداد المفاتيح الخاصة بك. في حال استخدام مفتاح بطول 64 بت (40 بت للطول الفعلي للمفتاح) عليك إدخال مفتاح مكون من 10 خانة ست عشرية (0-9، a-f، A-F). أما المفتاح ذو الطول 128 بت (والذي يوفر مستوى أعلى من الأمن) فيتألف من 26 خانة ست عشرية.

تذكر:

البديل الحالي لبروتوكول WEP هو WPA (Wi-Fi Protected Access) وهو بروتوكول التشفير المصمّم لتجاوز المشاكل الموجودة ضمن WEP. بروتوكول WPA2 هو الجيل الثاني من بروتوكول WPA والذي يعتمد على تعديلات معيار IEEE 802.11i.

مع ذلك فإنّ غالبية نقاط الولوج المتوفرة في السوق حالياً (2006) تدعم بروتوكول WEP فقط بشكلٍ إفتراضي. ستجد عادةً تحديثاً لبرمجيات تشغيل نقطة الولوج وبطاقات الشبكة اللاسلكية لتدعم بروتوكول WPA. راجع موقع منتج التجهيزات الخاصة بك على الإنترنت للحصول على هذه البرمجيات المحدثة. لتحسين مستوى الأمان في شبكتك اللاسلكية عبر تشغيل بروتوكول WPA ينبغي تطوير برمجيات تشغيل كلٍ من:

1. نقاط الولوج اللاسلكية.
2. بطاقات الشبكة اللاسلكية.
3. برمجيات زبون الشبكة اللاسلكية (برامج التعريف، أدوات الإدارة إلخ).

للمزيد من المعلومات عن التشفير في الشبكات اللاسلكية راجع وحدة "أمن الشبكات اللاسلكية".

2.56.. التحكم بالوصول إلى الشبكة عبر التحقق من الهوية

يتم التحكم بالوصول إلى الشبكة عبر التحقق من الهوية باستخدام مخدّم Radius. تعمل نقطة الولوج في حال إعداد مخدّم Radius كزبون لهذا المخدّم ويجب أن تتعرّف على إعدادات قاعدة البيانات في المخدّم.

تتضمن نقاط الولوج كجزءٍ من ميزات العناوين الفيزيائية MAC القياسية في معايير IEEE 802.11 إمكانية التحقق المفتوح من الهوية وفي بعض الأحيان التحقق من الهوية باستخدام المفتاح المشترك. بما أنّ أيّاً من هذين الأسلوبين للتحقق من الهوية لم ينجح في إثبات أمانه فإنّ غالبية نقاط الولوج المتوفرة حالياً تتضمن آليات IEEE 802.1x لإتاحة التحقق من هوية المستخدم عبر مخدّم خارجي مخصص لهذا الغرض.

لا يدخل موضوع التشفير ضمن مجال هذه الوحدة لذلك نكتفي بهذا القدر من التوضيح.

2.57.. التشفير من النهاية إلى النهاية End-to-End Encryption

يعتبر التشفير من النهاية إلى النهاية أكثر الأساليب أماناً لحماية البيانات القيّمة أثناء نقلها عبر الشبكة. توفر ميزات الشبكة الخاصة الإفتراضية خدمة التشفير من النهاية إلى النهاية وهي مضمنة في معظم نقاط الولوج المتوفرة حالياً. في حال تشغيل ميزة الشبكة الخاصة الإفتراضية فإن نقطة الولوج ستتيح هذه الميزة عبر بروتوكول PPTP/IPSec.

لا يدخل موضوع الشبكة الخاصة الإفتراضية ضمن نطاق هذه الوحدة لذلك نكتفي بهذا القدر من التوضيح.

3.5. طبقة بروتوكول الإنترنت IP Layer

لا تشكل طبقة بروتوكول الإنترنت IP جزءاً من الاتصالات اللاسلكية. لكنّ غالبية نقاط الولوج ليست مجرد نقاط لولوج صرف بل تحتوي على ميزات إضافية كالتوجيه وترجمة عناوين الشبكة NAT.

يقدم الجدول التالي لمحة عن المتغيرات المتعلقة بطبقة بروتوكول الإنترنت IP.

الإعداد	التوصيف
عنوان الإنترنت IP Address	لا يستخدم عنوان الإنترنت IP لنقطة الولوج بالضرورة للقيام بمهامها الأساسية (كمجمّع للشبكة اللاسلكية). يستخدم هذا العنوان للوصول إلى نقطة الولوج من متصفح للوب ولتسهيل عملية الإعداد. في حال استخدام نقطة الولوج كموجه لاسلكي فإنّ عنوان الإنترنت IP الخاص بها ينبغي أن ينتمي لنفس الشبكة التي تحتوي الموجه كما ينبغي إعداد قواعد التوجيه.
قناع الشبكة Netmask	راجع "الشبكات اللاسلكية المتقدمة".
البوابة Gateway	عنوان الإنترنت IP للوصلة المرتبطة مع الشبكة الخارجية.
مخدّم أسماء النطاق DNS	عنوان الإنترنت IP لمخدّم أسماء النطاق DNS والذي ستقوم بإعلانه لزبائن الشبكة اللاسلكية عبر بروتوكول الإعداد التلقائي للمضيف DHCP.

4.5 طبقة التطبيقات Application Layer

يتواجد أكثر الإعدادات أهميةً ضمن طبقة التطبيقات: إعداد "كلمة سر" إدارة نقطة الولوج. تأتي نقاط الولوج غالباً مع كلمة سر افتراضية (اسم المستخدم: admin وكلمة السر: admin) والتي ننصح بشدة بتغييرها فوراً بكلمة سر أقوى.

تجذب استخدام كلمات سر يمكن ربطها بك أو بمؤسستك بسهولة لأن تخمينها سهل. إذا ما تمكن شخص "غير مرغوب به" من الحصول على كلمة سر إدارة نقطة الولوج فإنه يستطيع إختراق نقاط الولوج الخاصة بك وتغيير كلمة السر مما يجعلك عاجزاً عن الوصول إليها. الحل الوحيد في هذه الحال يتطلب إعادة الإعدادات الافتراضية لنقطة الولوج يدوياً أو توصيلها عبر المنفذ التسلسلي وتغيير كلمة السر.

7. الخلاصة

يمكن تلخيص إعدادات نقطة وولوج أو موجّه لاسلكي بالخطوات الأربع التالية:

- استيعاب التجهيزات والحل الذي تريد تنفيذه.
- إعداد المتغيرات المتعلقة بالشبكة اللاسلكية (الطبقة الفيزيائية) كالقناة، معرف مجموعة الخدمات SSID، قدرة الإرسال والسرعة.
- إعداد المتغيرات المتعلقة بالشبكة اللاسلكية (طبقة الوصلة) كالشفير أو التحكم بالوصول عبر العناوين الفيزيائية MAC.
- إعداد متغيرات بروتوكول الإنترنت IP إذا ما رغبت في تشغيل ميزات بروتوكول الإنترنت في نقطة الولوج الخاصة بك (كالتوجيه أو ترجمة عناوين الشبكة NAT أو مخدّم الإعداد التلقائي للمضيف DHCP).

يمكن التحدي في فهم ماهية ووظيفة كلٍّ من هذه المتغيرات وليس مجرد التعرف على واجهة استخدام أداة الإعداد. يملك كل منتج واجهة استخدام مختلفة لإعداد تجهيزاته لكن "المبادئ" الأساسية ستبقى نفسها على الدوام.