NO. 35 • March 2013 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

ANATOMY OF A BOTNET

HIGH AVAILABILITY
PART 2

فلسفة الحماية
بـ WPA -WPA2

كيفية إعداد خدمة
DHCPv6
على لينكس سيرفر

9 من أهم تطبيقات
الـ Apple IOS
تستخدم الشبكات اللاسلكية

مدخل إلى تقنية
الـ WAN Optimization

DOS ATTACK

WHAT'S NEW IN WORD 2013

الترجمة

منذ عدة أشهر أعلنت عن قسم جديد في المدونة خاص بالمقالات المترجمة، والحقيقة القسم الجديد حسن وطور من المدونة بشكل كبير وخصوصاً أن المقالات المترجمة التي نقدمها من الصعب جداً أن نجد أحد لديه الخبرة لكي يكتب عنها وقد يوجد لدينا هذه الخبرات لكن علمهم ووقتهم لنفسهم فقط بعكس الغرب الذي تطور في مجال العطاء بشكل كبير جداً وبأضعاف مضاعفة عما نحن منه، نحن أمة الإسلام وأمة العطاء وللأسف لاحياة لمن تنادي.

سوف أتحدث في هذا المقال عن طريقة الترجمة المثالية التي تفيد القارئ وتفيد الكاتب في نفس الوقت، فعندما أرسل مقال لأحد الأصدقاء لكي يترجمه أطلب منه أمران فقط، الأول أن يحافظ على المصطلحات الإنجليزية الهامة ولا يترجمها. وعلى سبيل المثال كلمات مثل: أي أسم لبروتوكول , Subnetting, Broadcast, Loopback والخ . . . الفكرة ليست في مسألة اعتزاز باللغة العربية أو لا فالتأخر الذي نحن فيه أجبرنا على أن نسير على مصطلحاتهم وأن نتعلمها بلغتهم فهذا يسهل عملية الدراسة والتعليم وبالتالي التطوير.

عندما نبدأ الترجمة يجب أن نعتمد على أسلوب الفهم دائماً لانترجم حرفيا مهما كانت الظروف، أولاً حاول أن تقرأ كل فقرة على حدا افهمها جيداً وإن لم تفهمها ابحث في غوغل عن الكلمات والأفكار التي لم تصلك وبعدها ترجم الفقرة بطريقتك الخاصة فبهذه الطريقة أنت تستفيد وغيرك يفهم بشكل أكبر. فالمقالات يستفيد منها من يكتبها في المقام الأول وبعدها القارئ الذي يراها كمعلومة لكن المترجم يفهمها بشكل كامل ويتمكن من صياغتها بطريقته الخاصة.

في أيام مجد المسلمين وعصور الظلام في الغرب عمد علمائهم على ترجمة كل كتبنا إلى لغتهم ولولا تلك الترجمة لضاع الكثير من تعبهم في أبحاث ونتائج توصل إليها غيرهم وبذلك تمكنوا من التطوير ومتابعة العلوم التي وضع أساسها العلماء المسلمين ونحن لابد لنا من هذه الخطوة فالبداية من الصفر شيء سلبي جداً مثل أن تسمع عن نظام تشغيل عربي مبني من الصفر وهذا أعتبره هباءً منثوراً فهناك أنظمة يمكن الإعتماد عليها وتطويرها ونشرها كأنظمة عربية ونفس الشيء مع كل العلوم.

في النهاية سوف أنهي مع قصة عمرها عشرة سنوات تحديداً عام 2003 , عندما كنت أعيش في سوريا وكان الانترنت حينها محدود جداً وعن طريق التليفون وبسرعة 56 كيلو في الثانية كحد أقصى (56= سرعتها الفعلية 6 كيلو تقريباً في الثانية) في ذلك الوقت كنت أتعلم الـ Cracking وكيفية قرصنة البرامج والتعديل عليها وكنت أجهد كثيراً في البحث على الانترنت عن أي مصادر عربية حول هذا العلم ولم أجد أي شخص عربي مهتم بهذا الأمر وكان كل ما هو متوفر هو المقالات الإنجليزية والتي كانت للأسف سيئة جداً (إنجليزية المدارس العربية كالعادة) جلست ثماني أشهر في هذا العالم، تعلمت الكثير لكن وصلت في النهاية إلى أبواب مغلقة وكان لدي حينها خمسة أسئلة فقط أحتاج أجوبتها لكي أنطلق بشكل أوسع وأصل إلى أماكن أبعد من كثير من البرامج التي قرصنتها لكن لا حياة لمن تنادي، حاولت وحاولت و حاولت ولم أجد شخص عربي يشرح لي هذه الأمور وبعد فترة خمسة سنوات رجعت لتلك العادة وفكرت أن أبحث مرة أخرى والنتائج كانت سيئة جداً ولم تتغير كثيراً، من هنا وجدت فكرة دعم المحتوى العربي في مجالي بكل الطاقات الممكنة بحيث نصل يوماً ما إلى شيء لا يجعل أحد يتوقف عن العلم لأنها لم يجد جواب لسؤال كان دائماً يحيره فأنا وأنت والجميع مسؤول عن علمه أمام الله والمجتمع والأمة جمعاً فكن مبادراً. فالكثير يتعذر من قلة الأفكار التي يمكن الكتابة عنها وهذا عذر له اسباب كثيرة وأولها عدم البحث والقراءة الكافية في المجال الذي هو فيه والحل هو أن نترجم المقالات الإنجليزية الموجودة في أشهر المواقع العالمية مثل techrepublic الشهير. أدخل هذا الموقع وسوف ترى عشرة الآف مقال مفيد ومهم ويمكن ترجمته للعربية والأهم من كل هذا لاتجلس بلا زكاة للعلم فالدنيا قصيرة ووقتك يضيع في أشياء كثيرة تافهة وأنت تعلم ذلك جيداً. هذا العدد وجد تراجع كبير في المقالات ولا أعلم لماذا لازلنا نعاني من هذا الأمر فهل العيب فينا أم فيكم يا مستهلكين. أتخيلكم أمامي جميعاً وأنتم تقرؤون المقال بلا حول ولاقوة وكل واحد يقول اللهم نفسي ثم نفسي ودمتم بود.

أيمن النعيمي - سوريا

مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

أسـرة المجلـة

المؤسس

م.أيمن النعيمي

رئيس التحرير

م.أسامة كامل

المحـررون

م.نادر المنسي
م.شيماء الرازق
م.محمد عماد الجغصي
م.محمد تركي الرفاعي
م. غسان محمد أبو جسار
م.خالد الدسوقي
م.احمد فتح الله
م.حسام الدين حشيش

التصميـم و الاخـراج الـفني : محـمـد زرقـة

www.networkset.net

تقرؤون في هذا العدد

NetWork Set

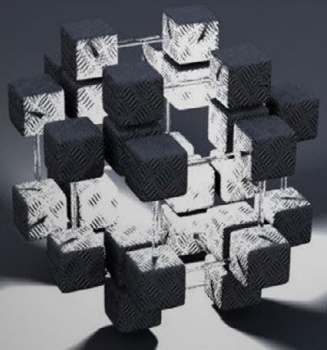
First Arabic Magazine For Networks

الكلمة الافتتاحية

مقال العدد المميز

مقالات العدد

قسم آراء القراء



NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية

Magazine NetworkSet

أول مجلة عربية متخصصة
في مجال الشبكات

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

أول مشروع عربي لترجمة
المواد العلمية و التقنية

YouTube

قناة المدونة على يو تيوب

قسم خاص بالأسئلة والاجوبة

NetWork Set
First Arabic Magazine For Networks

مقال العدد المميز

ANATOMY OF A BOTNET

واحدة من أهم متطلبات أمن المعلومات هي معرفة كيفية التعامل مع كارثة نتجت عن استخدام قوى الـ «بوت نت» حيث أن مصممي هذه الأنواع من البرمجيات وبالتعاون مع المؤسسات الإجرامية التابعة لهم يقوموا بتطوير طرق جديدة مبتكرة تستهدف تسخير ضحايا جدد والربح من خلالهم.

_ من هم وراء البوت نت والمتسببين فيه؟
_ ما السبب وراء انتشارهم وما هي حوافزهم؟
_ كيف يمكن للهاكرز أن يقوموا ببناء بنية تحتية متكاملة من البوت نت؟
_ كيف يمكن أن تقرر ما إذا كان السيستم جزءاً من شبكة بوت نت أم لا؟

هذا التقرير سوف يجيب على العديد من التساؤلات بالإضافة لسرد ما يمكن فعله لمكافحته.

ما هو البوت نت وكيف يستخدمه من يقومون بإرتكاب الجرائم الإلكترونية؟؟

بأبسط أشكاله يمثل البوت نت مجموعة من أجهزة الكمبيوتر والتي تم نقل العدوى لها باستخدام برامج الميل وير لفرض سيادتها على الجهاز المسيطر عليه وجعل الهاكر هو صاحب القرار. كل بوت نت « هناك العديد منهم ويقدر بالآلاف « يمكّن الهاكر من القيام ببعض الأمور البغيضة دون علم الضحية «صاحب الجهاز» وبمجرد السيطرة على الجهاز من خلال نقل البوت نت ميل وير اليه فإنه يصبح بمثابة جسد بلا عقل مستعد لتقديم العطاءات لسيده مهما كانت العواقب.

الهدف الأول من وراء استخدام البوت نت والذي يمثل الحافز لدى أي هاكر هو تحقيق العوائد المالية باستخدام العديد من الطرق منها:

Distributed Denial of Service (DDoS) attacks

يهدف لتوجيه كميات هائلة من الترافيك للسيرفرز وغالباً ما تكون ويب سيرفرز والنتيجة هي عدم قدرة السيرفر على الاستجابة لأي طلب بما فيها المستخدمين الشرعيين.

Spmming

تم اختراع البوت نت في الأساس من أجل إرسال الرسائل المزعجة أو ما تسمى بالسبام وحتى هذا اليوم فإن إرسال السبام يعد أحد أهم الأدوار التي يقوم بها البوت نت. بعد إرسال هذا النوع من البوت نت لجهاز ما سيصبح هذا الجهاز مسؤول عن إرسال أعداد مذهلة من الإيميلات اليومية والغير مرغوب فيها.

Financial fraud

مؤخراً ومع التوسع في ابتكار أنواع جديدة من البوت نت برامج بوت نت مسؤولة عن عمليات الاحتيال المالي للأشخاص أو حتى المؤسسات البنكية الكبيرة. فمن الممكن سرقة أرقام بطاقات الإئتمان أو الأسماء أو العناوين أو تواريخ الميلاد أو أي داتا هامة يمكن استخدامها في سرقة الأموال من بطاقات الإئتمان أو الحسابات البنكية.

Search Engine Optimization (SEO) poisoning

هي طريقة يحاول بها الهاكر التلاعب بتصنيف وترتيب ال على محركات البحث لكي يقود الباحث للوصول إلى ال التي تقوم بحقن البوت لجهاز الضحية أو أن تقوده إلى بعض ال التي تبيع منتجات مزورة أو وصفات طبية زائفة.

Pay-per-Click (PPC) fraud

هي حيلة يتم من خلالها تصميم ويب سايت يبدو خارجياً على أنه عادي جداً ومشروع ثم يتم تأجيره للإعلانات المشروعة والدفع بناءً على عدد الزيارات أو الأنشطة التي تتم على الإعلان. في الواقع من يقوم بفتح الإعلان وقرائته هو البوت الذي لا يتوقف عن العمل في خلفية السايت وليست أشخاص ترغب في الشراء. هذه الأنشطة تأتي من أجهزة بعدد كبير جداً ومن أماكن جغرافية متعددة.

Corporate and Industrial Espionage

على الرغم من وجود جدل شرس بين خبراء الجرائم الإلكترونية على نطاق ومدى استخدام البوت نت في إجراء التجسس، إلا أنه ثبت فعلياً استخدام بعض أنواع البوت نت لشن هجمات تستهدف بعض الإيميلات سواء كانت تابعة لمؤسسات أو حكومات ونجحت بالفعل من سرقة معلومات مثل ملكيات فكرية قيمة أو بيانات تخص أمن وأسرار بعض الدول.

كيف نقل البوت نت لجهاز الكمبيوتر

تتعدد الطرق التي يستخدمها الهاكرز لنقل العدوى للأجهزة بقدر تعدد الطرق التي يستخدم فيها مرتكبى الجرائم الالكترونية البوت نت والتي سبق ذكرها ومن هذه الطرق ما يلي:

Drive-by Download

عن طريق زيارة أحد ال والتي لم تصنف بعد لدى أي أنتي فايروس على أنها تسبب مخاطر أمنية وبها هذا النوع من البرمجيات الضارة وبتحميل وتشغيل السوفت وير يكون الجهاز قد دخل في شراك البوت نت.

Email

أحد الطرق التقليدية والتي مازالت تحمل شهرة على نطاق واسع يتم فيها إرسال ميل لجهاز ما ولكن هذا الميل يحتوي على لينك أو أي محتوى ضار. أحياناً يكون المرسل هو شخص معروف وموثوق فيه لدى المستلم وفي

هذه الحالة من المؤكد أنه جهاز المرسل هو أيضاً جزء من شبكة بوت نت.

Pirated software

مبرمجين ومصممين الميل وير يقومون بإدراج بعض البرمجيات الضارة مع السوفت وير داونلود ومع بدء تشغيل البرنامج يقوم البوت نت بالبدء وفرض الهيمنة على الجهاز بدون علم المستخدم تماماً.

ماذا يحدث بعدالعدوى

أثناء تحميل البوت نت يقوم الميل وير بتحميل سوفت وير آخر يعرف بـ:

Backdoor

وهو عبارة عن برنامج يساعد الهاكر من الاتصال والسيطرة وتحميل برمجيات أخرى لجهاز الضحية. بعد تنزيل الباك دور إلى جهاز الضحية يكون من الصعب جداً إغلاقه أو إزالته من الجهاز حتى لو استخدمنا أحدث الإصدارات لأي أنتي ميل وير. بمجرد التحميل وبدء التشغيل يكون البوت نت قادر على إرسال معلومات كثيرة للهاكر أو ما يمكن أن نطلق عليه مجازاً «سيد البوت نت » تشتمل هذه المعلومات على الآي بي الخاص بجهاز الضحية ليتمكن من تحديد الموقع الجغرافي لهذا المستخدم، كذلك تحديد اسم مستخدم الجهاز ونوع نظام التشغيل وأي باتشات مستخدمة وغيرها الكثير من المعلومات.

بعد التأكد من إمكانية الاتصال في أي وقت يمكن لسيد البوت نت أن يفعل ما يشاء في الجهاز مثلا بإمكانه أن يرسل إصدار أحدث من الميل وير لينصب نفسه بنفسه يكون مسؤوليته مثلاً

مراقبة نشاط بعينه للمستخدم كالدخول على حساب بنكي مثلاً .أو مراقبة أنشطة المستخدم على الانترنت أو إرسال رسائل سبام من خلاله أو إرغامه على المشاركة في هجمات حجب الخدمة أو تنصيب المزيد من الميل وير على جهاز الضحية. الطريف في الموضوع أنه بسبب المنافسة الشديدة بين أصحاب البوت نت فإن المبرمجين يمكنهم تصميم بعض برامج الميل وير والتي بإمكانها أن تعرف ما إذا كان هذا الجهاز عليه بوت نت لأحد المنافسين أم لا وإن كان هناك أحدهم فإن البرنامج يتولى مسؤولية إزالته أولاً وتنصيب نفسه بدلاً منه.

كيف يتمكن البوت نت من إخفاء نفسه جيداً وتجنب الكشف عنه؟

هناك مفهوم خاطئ شائع عند الكثير من المسؤولين عن تأمين الشبكات وهو اعتقادهم أن البوت نت حتى لو نجح في إنشاء كونيكشن بينه وبين الماستر فيما «سي آند سي سيرفر»Command and Control ((C&C فإن أدوات السكيورتي المستخدمة للتأمين مثل أنتي ميل وير أو آي بي إس بإمكانها منع الاتصال من الأساس لكن في الحقيقة يحدث غير ذلك .البوت نت دائماً يحتفظ بقائمة طويلة من الآي بي الخاصة بـ «سي أند سي سيرفر» على فرض أن الأولى لم تنجح فهو يظل دائماً يحاول أن يصل إلى آي بي يمكنه من عمل اتصال متكامل مع السيرفر المطلوب .برامج البوت نت المتطورة تستخدم ما يسمى بـ

Domain Generation Algorithms (DGA)and fast flux

والغرض من ذلك هو ضمان أن البوت قادر دائماً على الاتصال بالسيرفر، يقوم الميل وير فيها بتخمين عناوين للـ «سي آند سي سيرفر» باستخدام بعض DGA الخوارزميات بعدها يحدد الميل وير متى يمكنه أن يتصل بما يبدو أمامه عنوان عشوائي أو أونلاين دومين نيم .كل ما يجب أن يفعله صاحب البوت هو ضرورة التأكد من تسجيل الدومين نيم هذا بيوم أو يومين قبل موعد الاتصال وعمل ريكورد مناسب في DNS لتوجيه الاتصال للـ «سى آند سى سيرفر».

للموضوع بقية في العدد القادم....

NetWork Set

First Arabic Magazine For Networks

مقالات العدد

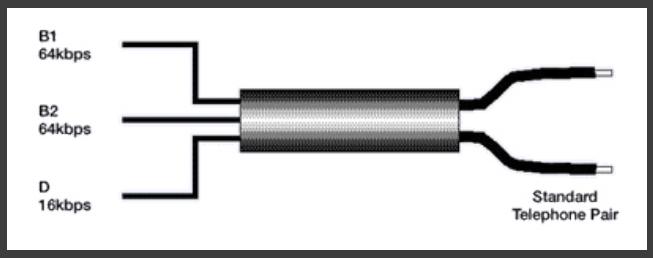
Bandwidth Management

الكثير منا يتسائل عن موضوع ضبط الحزمة وكيف تقوم مزودات خدمة الانترنت بتقسيم السرعات على عدد كبير من المستخدمين .
والسؤال الذي يدور في خلد كل مستخدم للانترنت هل من الممكن زيادة سرعة الاتصال دون الرجوع للمزود ؟ بعد قراءة هذا المقال ستكون قادر على الإجابة بنفسك.
سنتحدث اليوم عن الأساليب التي يتبعها مزود خدمة الانترنت لضبط سرعة الاتصال لكل مستخدم وهي عبر مرحلتين .
المرحلة الأولى : نوع الاتصال وتحديد السرعة الفيزيائي . (Physical speed assignment)
يعتبر نوع الاتصال العامل الأساسي لتحديد سرعة الانترنت إذ تقسم أنواع الاتصالات المنتشرة في معظم الدول إلى عدة أقسام أهمها:

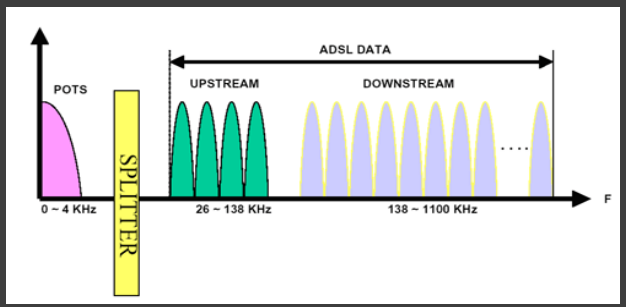
A. Dial-Up: شارفت هذه الخدمة على التقاعد في معظمة عواصم العالم العربي والغربي. من الناحية الفنية لايمكن لهذا النوع من الاتصال أن يتجاوز سرعة الـ 56 Kbps في أفضل حالته. يقوم جهاز يدعى (Remote access Server) بتحديد هذه السرعة وقد تتأثر سلباً بالكثير من العوامل منها طول الكبل النحاسي الواصل بين المشترك ومقسم الهاتف والحالة الفنية للكبل بالإضافة لسماكة النحاس بالكابل المستخدم ونوعه.

B. ISDN: تشبه هذه الخدمة الخدمة السابقة من حيث المبدأ ولكن بنية الاتصال الرقمية تسمح بتقسيم التردد المرسل عبر الكبل النحاسي إلى قناتي اتصال يمكن استخدام كل قناة للحصول على سرعة أقصاها 64kbps لكل قناة . كما يمكن استخدام كلتا القناتين للحصول على اتصال بسرعة 128 kbps كحد اقصى .

ملاحظة : القناة الثالثة ادناء (D Channel) غير مستخدمة للاتصال فقط للتحكم والإشارة .



C. ADSL: يعتبر هذا النوع من الاتصال الأكثر انتشاراً عبر العالم. كما أنه يختلف كلياً في بنية الاتصال. إذ يقوم باستثمار التردد الفارغ في الكبل النحاسي غير المستخدمة. مما يتيح استخدام هذا النوع من الاتصال مع خدمة الهاتف معاً دون انشغالية خط الهاتف . كما في الشكل التالي:



نلاحظ أن المساحة المتاحة لعملية التحميل (Download) أكبر من المساحة المستخدمة لعملية الرفع (Upload) لذلك يطلق على هذه الخدمة اسم (ADSL) خط المشترك الغير متناظر .
بمعنى آخر إذا كانت سرعة الاتصال لديك 512 kbps بالتالي وبعد التحويل من بت إلى بايت ستحصل على سرعة تحميل 64 kBps وسرعة رفع لا تتجاوز 16 kBps
أما سرعة هذا الاتصال العظمى هي 24Mbps (ADSL2+) يقوم جهاز يدعى (DSLAM) بتحديد سرعة المشترك بشكل فيزيائي على المنفذ المتصل به الكبل النحاسي . ولا يمكن للمشترك التلاعب بهذه السرعة . كما تتأثر سلباً السرعة بعوامل الكبل النحاسي التي تم ذكرها سابقاً .

D. T1 & E1 : يدعم الـ (E-carrier) سرعة أقصاها 2 Mbps و الـ (T-carrier) 1.5 Mbps في حال الاتصال المباشر . أما في حال الاتصال عبر كبل نحاسي فيقوم جهاز المودم المستخدم بتحويل اشارة الـ E1 إلى نحاسي بضبط السرعة بناءً على كفاءة الكبل النحاسي او حسب رغبة المستخدم. لكن مهما زادت سرعة اتصال النحاسي بالـ (E1) لن يحصل المستخدم إلا على سرعة الاتصال المضبوطه على (Multiplexer) والتي في اقصى الحالات 2Mbps . عادة ما يكون جهاز (Multiplexer) في مقسم الهاتف لذلك يقوم المستثمر بنقل الخدمة عبر كبل نحاسي لمقره مستخدماً مودمات (GHDSL Modems) .

ملاحظة هامة : يتم تحديد السرعة الفيزيائية للمستخدم عبر التجهيزات المتواجدة بمقسم الهاتف مثل (DSLAM , RAS , Multiplexer) .وذلك لتوافر البنى التحتية من كوابل نحاسية فقط لدى شركات الاتصالات الأرضية .

وتعود ملكية هذه التجهيزات حسب نظام الاتصالات المعتمد في الدولة إذ نادراً ما تكون ملك لمزودات خدمة الانترنت .

أما في الدول المتقدمة فيتم تجهيز كل حي بتجهيزات خاصة متصلة عبر كبل ضوئي بالمزود كما في الشكل ادناه .

المرحلة الثانية : تحديد السرعة البرمجية (Software Based Bandwidth management)
كما لاحظنا بالمراحل السابقة أن معظم عمليات ضبط الحزمة يقوم بها تجهيزات بشكل فيزيائي لكن ماذا إن أراد مدير الشبكة بمزود خدمة الانترنت ضبط الحزمة لكل مستخدم على حداً او ادارة الحزمة وتوزيعها على المشتركين بخوارزمية معينة ؟
وماذا عن إدارة سرعة باقي انوع الاتصالات في البلدان المتقدمة كـ (Fibre to home ,Cable and PPPOE)

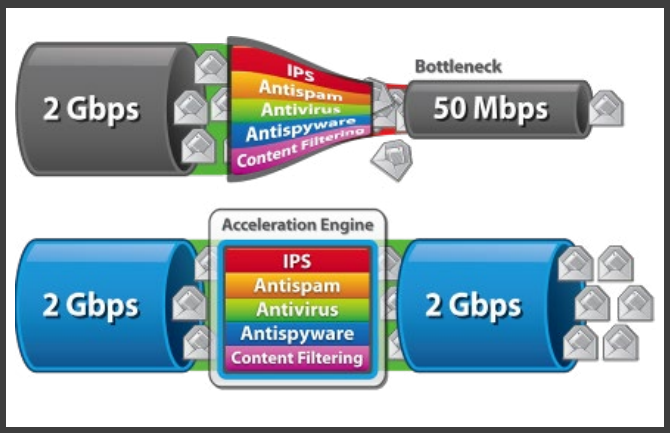
في هذه الحالة لا بد من استخدام تجهيزاة خاصة تعمل على ضبط الحزمة بناءً على عوامل يحددها مدير الشبكة كعنوان (IP) للمشترك او بروتوكول معين او معرف متغير في حال في حال وجود (Radius integration)

تقوم عدة شركات بتقديم هذه المخدمات أهمها (Blue-Coat packeteer) و (Ipoque) .

كمحصلة وإجابة لتساؤلات الكثيرين. لا يمكن زيادة سرعة الاتصال عن السرعة الفيزيائية. أما الاتصالات الأخرى التي لا تضبط فيزياءً يمكن اختراقها في في حال عدم استخدام المزود لاجراءات التحقق من المستخدم (AAA) او من خلال استخدامها دون تحديد سماحية تعداد الدخول لنفس المستخدم (Simultaneous login limits). مثال استخدام نفس اسم المستخدم وكلمة المرور في انشاء (PPPOE) لمضاعفة عدد الـ (Sessions) وبالتالي مضاعفة السرعة وأخيراً في حال عدم استخدامهم تجهيزات ضبط الحزمة المذكورة سابقاً .

المقصود بـ (PPPOE) ليس المستخدم بخاصية (DSL) انما في بعض الدول تقوم مزودات خدمة الانترنت بوصل كابل ضوئي لبناء معين وربطه بموزع شبكه عادي و توصيل كبلات (Ethernet) لكل مستخدم على حدا ويقوم المستخدم بربط الكبل أما على الحاسب بشكل مباشر وإنشاء اتصال (PPPOE) عبره أو من خلال ما يسمى بـ (Broadband Router)

ي معظم مزودات خدمة الانترنت يتم ضبط سرعة الاتصال بالمرحلتين السابقتين معاً وتحدد سرعة المشترك بالرقم الأصغر دائماً. في حال كانت السرعة الفيزيائية لمشترك خدمة (ADSL 512 kbps) وسرعته المضبوطة على جهاز (lpoque 256 kbps) او العكس لن يستطيع المستخدم الاستفادة الا من السرعة الأصغر وهي (256 kbps) .
تسمى العملية السابقة بعملية الخنق أو عنق الزجاجة (Bottleneck) كما في الشكل التوضيحي التالي .



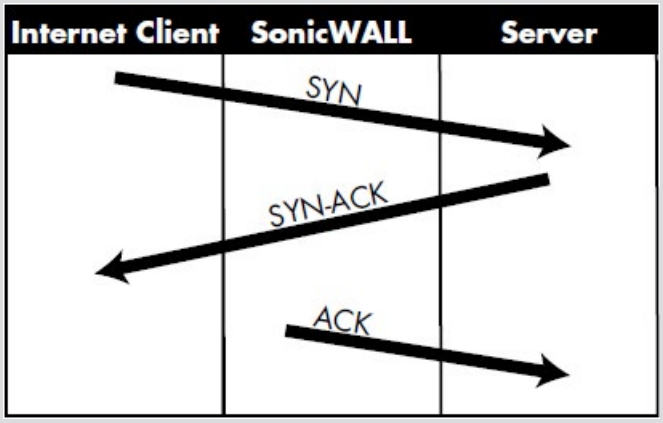
DOS ATTACK

تعتبر الإتاحة أو كما تسمى Availability من الخصائص الهامة للبيانات والخدمات المقدمة عبر الشبكة وتعني توفر الخدمة أو البيانات للمستثمرين في أي وقت يطلبونها خلال زمن استجابة محدد، وقد انتشرت في الآونة الأخيرة هجمات تسعى إلى إيقاف هذه الخاصية وسميت حينها هجمات الحرمان من الخدمة أو ما يعرف ب هجمات Denial of Service Attacks DOS.

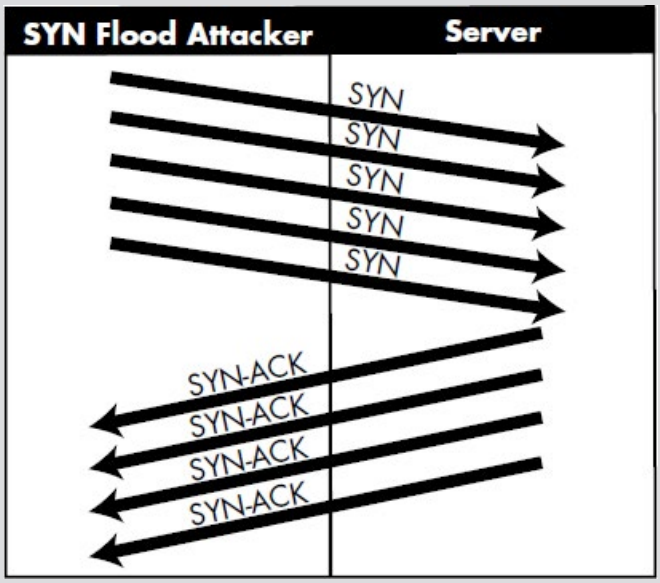
يسعى المخترقون من خلال هذا الهجوم إلى حجب خدمة ما أو موقع الكتروني على الشبكة وذلك من خلال إغراق المخدم بسيل من البيانات والطلبات ليست بذات أهمية، ويقوم بهذا الهجوم شخص أو أكثر بغية إيقاف الخدمة مؤقتاً أو إلى أجل غير مسمى. يعتبر هذا النوع من الهجمات سهل التطبيق فهو ليس بحاجة لكسر ملفات أو اختراق حسابات مستخدمين بل يتم ببساطة من خلال أدوات جاهزة يتم توظيفها للقيام بالهجوم.

ما هي آلية عمل هذا الهجوم؟؟

حتى نفهم هذا النوع من الهجمات سنتحدث عن مثال يمكن من خلاله إيصال فكرة هذا النوع من الهجوم: كما نعلم فإن ضمن جلسات الانترنت تتم عملية تدعى بالمصافحة Hand Check حيث يقوم من خلال هذه العملية أحد الأطراف بإرسال حزمة Syn للمخدم المضيف ومن ثم يقوم المضيف بدوره بإرسال Syn-Ack للمرسل يخبره باستجابته لطلبه ويقوم بالوقت ذاته بتسجيل الطلب ضمن جدول خاص ويربطه مع عنوان هذا الطرف الذي طلب المصافحة بالإضافة إلى ذلك يحدد المضيف مدة زمنية ينتظر خلالها رد هذا الطرف من خلال حزمة Ack بحيث يقطع الاتصال مالم تصل تلك الحزمة خلال هذا الزمن،



الآن يأتي دور المخترق حيث أنه يعمل ومن خلال أدوات خاصة بإغراق المضيف بطلبات Syn وكل منها مزود بعنوان منطقي وهمي مما يعني امتلاء الجدول الخاص بعملية المصافحة، وعندها لن يستطيع المضيف استقبال طلبات الزبائن الأصلية وبالتالي تم حجب الخدمات التي يقدمها من قبل المخترق



أنواع هجمات الحرمان من الخدمة:

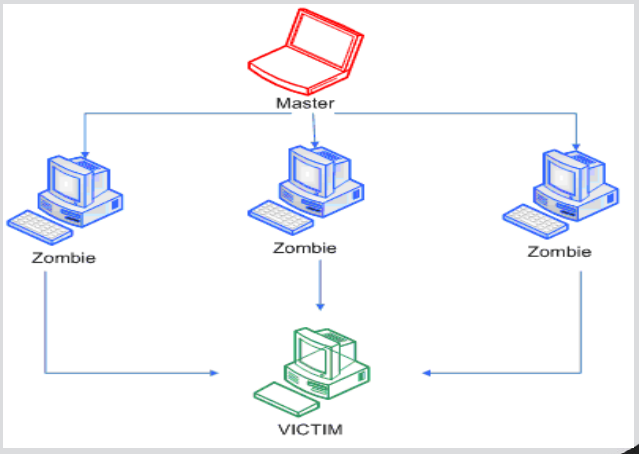
تصنف أنواع هجمات الحرمان من الخدمة إلى صنفين أساسين هما:

1 - Typical Denial of Service

ويدعى حجب الخدمة التقليدي، يحدث هذا النوع من الهجمات عندما يقوم المستخدم بإرسال كمية كبيرة من البيانات إلى الجهاز المستهدف من مصدر واحد، وفي أغلب الأحيان سيكون مصيرٍ هذا الهجوم هو الفشل لأن الجهاز المستهدف غالباً سيستطيع تحمل الطلبات القادمة من مصدر وحيد.

2 - Distributed Denial of Service

هنا تختلف آلية العمل، حيث تم تطوير آليات لشن الهجوم بحيث لن يستطيع الضحية تحمل الطلبات لأنها لم تعد من مصدر واحد، فالمهاجم لن يستخدم جهازه فقط لشن الهجوم، بلٍ سيعمد إلى أن يكون الهجوم بشكل موزع مستخدماً عدة حواسب في وقت واحد وتسمى تلك الحواسبٍ بـ zombies، ولكن هل سيكون المخترق مضطراً ليملك عدداً كبيراً من الحواسب حتى يقوم بهجوم حجب الخدمة الموزع؟؟ بالتأكيد لا، بل يكفي وجود حاسب رئيسي Master فقط يدير من خلاله العمليات، حيث يستطيع بواسطة الحاسب الرئيسي استغلال ثغرات أمنية معينة في الحواسب الأخرى الموجودة على الشبكة حتى يضعها تحت تصرفه ويقوم بزرع الأدوات الخاصة بالهجوم فيها واستخدامها متى أراد بدء الهجوم وحينها لن يستطيع الضحية استيعاب الكم الكبير من الطلبات التي انهالت عليه من عدة مصادر وبالتالي سيتوقف عن العمل وسيعجز عن تأمين الخدمات إلى المستثمرين الشرعيين.



الآليات المتّبعة في هجوم حجب الخدمة:

1 -استهلاك موارد الضحية « كمساحة الخزين مثلا»، أو استهلاك قدرة المعالج كاملة.

2 -تعطيل ضبط الإعدادات «مثلا معلومات التوجيه Routing Information».

3 -تعطيل معلومات الحالة.

4 -تعطيل المكونات المادية للشبكة.

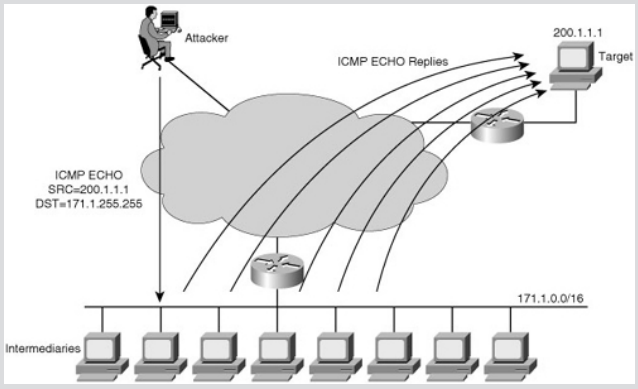
5 -تعطيل آليات الاتصال بين أجزاء الشبكة.

الطرق المستخدمة في هجوم حجب الخدمة:

ICMP Flood: Internet Control Message Protocol تعد من أكثر الطرق المستخدمة في شن هجمات حجب الخدمة، يستخدم هذا البروتوكول لإرسال الرسائل الخاصة ورسائل التحكم ويقع ضمن TCP/IP ومن أشهر الأمثلة عليه هي تعليمة الاختبار Ping، فعند إرسال حزم ICMP فإن الجهاز المستقبل سيرد بحزم مماثلة وبالتالي أصبح من السهل الآن إغراق الجهاز الضحية بكمية كبيرةٍ من حزم Icmp ولأنه لن يستطيع الرد عليها جميعاً سيصبح الهدف غير قادر على الاستجابة وسيتوقف عن العمل.

*SMURF يعتمد المخترق هنا على نوع خاص من حزم ICMP تدعى:

ICMP echo requestأي أنها حالة خاصة من ICMP



يعمد المخترق في هذه الطريقة إلى إرسال هذه الحزم إلى عنوان بث Broadcasts على الشبكة بحيث يتوجب على الحواسب عند استقبال الرسالة أن ترد عليها ولكن ما هي الوجهة التي سيتم الرد لها؟؟ في هذا الطريقة يقوم المخترق بتزوير عنوانه

المنطقي الذي أرسل منه بحيث يضع بدلا منه عنوان جهاز ضحيته وبالتالي استطاع إيهام حواسب الشبكة التي وصلتها رسائل ICMP بأن حاسب الضحية هو من أرسل هذه الطلبات وبالتالي سيكون الرد موجهاً إليه وبالتأكيد لن يصمد أمام سيل الردود التي ستتوافد عليه مما يؤدي إلى انهياره.

SYN flood هذا النوع الذي تم شرحه في البداية مسبقاً وكما ذكرنا فإن هذا النوع يعتمد على جلسة المصافحة في إقامة هجومه.

UDP Flood: User Datagram Protocol يتم هنا أيضاً إرسال كمية كبيرة من هذا النمط من الحزم إلى جهاز الضحية، يقع أيضاً ضمن بروتوكول TCP/IP ويقوم على إرسال البيانات بشكل غير مرتب ولا يحتاج إلى إنشاء قناة اتصال Connection less وبالتالي هذه الميزة ستزيد من فعالية الهجوم.

TCP Flood بعكس الآلية السابقة تماماً فهذا البروتوكول ينشئ قناة اتصال بين المرسل والمستقبل Connection oriented وبالتالي يمكن من خلال هذا النمط من الهجوم إنشاء عدداً كبيراً جداً من القنوات بين المرسل وجهاز الضحية بحيث لن يكون قادراً على استقبال طلبات الزبائن الشرعيين فيما بعد.

Fragmentation وتعني التجزيء، عندما يكون حجم الرسالة المرسلة كبير فإننا نضطر إلى تقسيمها إلى وحدات صغيرة ومن ثم إرسالها ومع كل وحدة يتم إرفاق رقم تسلسلي خاص بها ليدل المستقبل على كيفية ترتيب الأجزاء المستلمة عند محاولة التجميع إن فكرة هذا النوع من الهجوم مبنية على اعطاء أرقام عشوائية وهمية وكبيرة يستطيع المرسل من خلالها إيهام الضحية بأن هناك كمية بيانات كبيرة جداً سوف تصله فيضطر لحجز مكان لها في الذاكرة استعداداً لوصولها، ولكن توافد عدد كبير من الطرود الوهمية ذات الأرقام الزائفة سيثقل على المستقبل ويجعله غير قادر على استقبال المزيد والخروج عن الخدمة.

الحماية من هذا الهجوم:

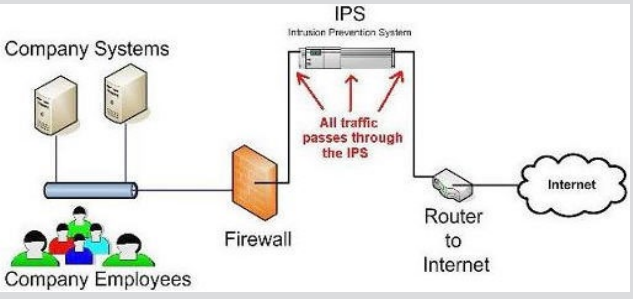
إن الوقاية من هجمات حجب الخدمة غالباً ما تكون مزيج من عدة أنظمة لكشف الهجوم ودراسة طبيعة Traffic الذي يمر عبر الشبكة بالإضافة إلى أدوات الاستجابة التي ستقوم بمنع حركة البيانات المريبة ضمن الشبكة، ومن الأدوات التي يتوجب استخدامها هي:

الجدار الناري:

من خلال الجدران النارية نستطيع تحديد عدة قواعد تنظم عمل تلك الجدران، بحيث تنظم عملية مرور البيانات أو تسمح وتمنع المرور حسب العناوين أو المنافذ، موضوع القواعد وتحديدها ليس بالسهل بل هو أمر في غاية التعقيد فمثلا إن كان المهاجم يعمد إلى إرسال كمية بينات كبيرة عبر المنفذ 80 فهذا لا يعني أننا سنغلق هذا المنفذ لإيقاف الهجوم بل يجب إيجاد آليات أفضل لإيقافه لأن إغلاق المنفذ سيحرم المستخدمين الشرعيين من استخدامه.

أنظمة منع الاختراق IPS

تكون هذه الأنظمة ذات فعالية عندما تكون الهجمات المطبقة ذات توقيع Signature معروف من قبل وقد تم توليد قاعدة خاصة لمنعه على أساس هذا التوقيع، وهذه الأنظمة قد تكون ضعيفة أمام هجمات حجب الخدمة لأن تلك الهجمات لا تملك أي توقيع يتم اكتشافها من خلاله بل يجب أن يتم اكتشافها عبر دراسة سلوكها فقط .



الموجهات Routers

من خلال الموجهات نستطيع وضع قواعد ACL للتحكم بطبيعة البينات التي تمر عبر هذه النقطة وستكون ذات فاعلية لأنها تطبق على مستوى الطبقة الثالثة أي القواعد ستطبق على العناوين المنطقية.

تطبيقات التجهيزات الأمامية

توضع هذه التطبيقات على تجهيزات خاصة تكون في الخطوط الأمامية للشبكة وقبل دخول الترافيك إلى حواسبها ومخدماتها، تقوم هذه التطبيقات بدراسة سلوك البيانات و Traffic المار وعلى أساسه تقرر فيما إن كانت ستسمح لهذه البيانات بالمرور باتجاه المخدمات والحواسب أم لا تماماً كبيئة Honey Pot.

9 من أهم تطبيقات الـ Apple IOS تستخدم الشبكات اللاسلكية

من آلاف التطبيقات التي يتم إنشاؤها لأجهزة آبل والتي تعمل على أنظمة التشغيلIOS لا يوجد إلا عدد قليل من هذه البرامج لوصفها الأكثر أهمية في مجال الشبكات اللاسلكية والتي قلصت استخدام عمل الحواسيب واستبدالتها بالـ IPhone و IPad و Touch ipod لاستخدامها في مجالات أوسع عن طريق استخدام الشبكة اللاسلكية.
ومن هذه البرامج:

DisplayLink

ttp://itunes.apple.com/us/app/displaylink/id411678720

DisplayLink

تم تطوير هذا البرنامج من قبل شركة لها نفس اسم البرنامج، وهذا التطبيق يتيح للـ IPad ليتم تكوينه وإعداده كجهاز عرض ثانوي من جهاز كمبيوتر يعمل على نظام ويندوز قم بتنزيل برنامج DisplayLink Windows device driver software على جهاز الحاسوب الخاص لديك ثم قم بإنشاء اتصال لاسلكي من ipad إلى الكمبيوتر من خلال التطبيق.
DisplayLink يرسل frame buffers من الكمبيوتر الى ipad عن طريق wifi في معدل إرسال مناسب بين الطرفين وهو يقوم بالإرسال بالوقت الحقيقي مع معدل تأخير قليل، قد تلاحظ هذا التأخير عند البث المرئي وهو يدعم ipad فقط وهو تطبيق مجاني.

Wi-Fi Finder by JiWire

http://itunes.apple.com/us/app/wi-fi-finder/id300708497

يقوم بتصفح قاعدة بيانات يمتلكها تحتوي على 500,000 WiFi wireless hotspots حول العالم لإيجاد أفضل المواقع للحصول على الانترنت أثناء السفر Wi-Fi Finder يقوم بترشيح أماكن مثل الفنادق أو المطاعم سواء كان مزود انترنت مجاني أو بأجر. فهو يخبرك بذلك وهو تطبيق لايقوم بمسح حقيقي للشبكات المحيطة للكشف عن hotspot

CoBrowser

http://itunes.apple.com/us/app/cobrowser/id392915628

مصطلح Tethering لمن لايعلمه هو طريقة لإعداد الكمبيوتر وبالعادة يكون لابتوب ليتصل بالانترنت عن طريق wireless access باستخدام هاتف خلوي كمودم اتصال CoBrowser يدعم هذه الطريقة بالاتصال والتشارك بتصفح الانترنت ولكن بصورة أخرى دون tethering suppor أو jailbreaking CoBrowser لايدعم تصفح مستقل للانترنت من الأجهزة. بل هو عبارة عن مرآة تعكس جلسة تصفح من جهاز واحد على الآخر في الوقت الحقيقي .

فعندما يقوم جهاز الحاسوب المتصل بالانترنت فعليًا هو الذي يقوم بالتصفح ويرسل نسخة إلى جهاز Iphone الذي طلب التّصفح بالأساس عبرالبلوتوث.

يترواح سعر التطبيق من 2 دولار الى 10 دولار.

Best Baby Monitor, by Martin Man

http://compnetworking.about.com/gi/o.htm?zi=1/XJ&zTi=1&sdn=compnetworking&cdn=compute&tm=7236&f=00&su=p284.13.342.ip_p504.6.342.ip_&tt=3&bt=0&bts=0&zu=http%3A//itunes.apple.com/us/app/best-baby-monitor/id432791399id392915628

المحيطة وإنما هو عبارة عن قاعدة بيانات محملة مسبقا تحتوي على wifi hotspot في أرجاء العالم كله وهو تطبيق مجاني.

Syncellence

http://itunes.apple.com/us/app/syncellence/id442974896

الطريقة التقليدية في مشاركة الملفات بين الأجهزة عن طريق الإيثرنت أو اليو اس بي ليست موجودة في الأجهزة التي تعمل على نظام IOS Syncellence يسمح بتشارك الملفات ونقلها بين الأجهزة عن طريق Wi-Fi أو عن طريق البلوتوث وهو تطبيق يأتي بنسختين مجانية وأخرى بـ5 دولارات.

النسخة المجانية تسمح بـ peer-to-peer file sharing بين جهاز يعمل على نظام IOS وجهاز آخر يعمل على أي نظام سواء كان IOS او mac أو ويندوز أو لينكس ويقوم بتشفير البيانات المرسلة على الشبكة اللاسلكية أما النسخة الغير مجانية فهي تدعم التزامن في نقل الملفات synchronization support ويدمج به تطبيق Facebook و Dropbox وله القدرة على الحفاظ متطابقة تلقائيًا من الملفات بين هذه الأجهزة.

NumPad Wireless Numeric Keypad

http://itunes.apple.com/us/app/numpad-wireless-numeric-keypad/id297623436

على عكس الآلات الحاسبة ولوحات المفاتيح الموسعة معظم الاجهزة المحمولة لاتحتوي لوحات مفاتيحها على الـ 10 مفاتيح الاساسية على اليمين مما يبطئ عمل المستخدمين الذين يقومون بادخال البيانات بشكل متكرر. NumPad يسمح لمستخدمي أجهزة iOS أن تكون بمثابة الـ10 مفاتيح التي على يمين الكيبورد الموسّع لاسلكيًا لكمبيوتر آخر والتطبيق يدعم:

OS X Screen Sharing and Remote Access to interface with Mac computers over Wi-Fi

ويمكن استخدامه مع أجهزة ويندوز للتحكم عن بعد بسطح المكتب remote desktop connection

سعره حوالي الـ 5 دولارات.

قم بوضع جهاز يعمل على نظام IOS في غرفة الأطفال واستخدم هذا التطبيق للمراقبة المرئية والصوتية عن بعد ولهذه العملية فأنت تحتاج جهاز ios يحتوي على كاميرا ومتصل بجهاز IOS آخر عبر WiFi ويمكن وضع الجهاز Alert mode، أي إعداده كنظام أمني وتحذيري فيقوم جهاز الهاتف بالاتصال برقم هاتف محدد قمت بإعداده أنت مسبقًا عند كشف أي حركة يلتقطها هذا الهاتف عبارة عن سنسور يحتوي على إضافات مثل ضوء ليلي وأغاني أطفال للنوم سعر التطبيق 4 دولار. `

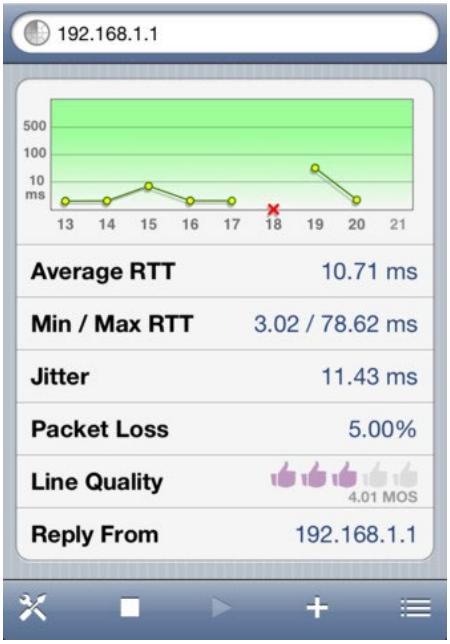
PrintCentral

http://itunes.apple.com/us/app/printcentral-for-iphone-ipod/id367455861

الطباعة من أجهزة الكمبيوتر تتعرض لأخطاء وأحيانا مملة تم تصميم PrintCentral لتبسيط عملية الطباعة إلى حد كبير من أجهزة IOS وتمكين الطباعة اللاسلكية مباشرة مع الطابعات التي تدعم خاصية WiFi ويدعم البرنامج خاصية Apple AirPrint and Google Cloud Print وهناك إصدارات مختلفة من هذا التطبيق متاحة للـ IPad و الـ iPhone /iTouch كل على حدة سعر التطبيق يتراوح من 8 الى 10 دولار.

Ping Analyzer – Graphical Network Ping

http://itunes.apple.com/us/app/ping-analyzer-graphical-network/id**406772587**



لمدمني الشبكات الحقيقيون ويريدون مراقبة جميع التفاصيل الفنية لشبكاتهم Ping Analyzer. يزود مستخدمي أجهزة IOS القياسات التقليدية مثل أدوات network ping بما في ذلك dropped packets و round-trip times و jitter ويحتوي على تمثيلات رسوميّة سعر البرنامج دولار واحد.

Net Master HD

http://itunes.apple.com/us/app/net-master-hd/id**473144915**?mt=**8**

يمكن لـ Network administrators استخدام Net Master HD لعمل مسح للشبكة المحلية لجمع معلومات عن الأجهزة المتصلة بالشّبكة. هذا التطبيق يقوم بالحصول على عناوين IP للعملاء والـ MAC address وأسماء البائعين كما أنها تدعم وظائف إدارية نموذجية مثل:

Ping و trace route, و port scanning ويحتوي على آلية حسابية بسيطة لحساب subnet تكلفة التطبيق حوالي 10 دولار

High Availability
Part two

تكلمنا في الجزء الأول من المقال عن التكنولوجيات التي تتيح لنا عمل داتا سنتر بدون Downtime ، أو بمعنى أصح بأقل مدة Down time طبقاً لاتفاقيتنا مع العميل على مدة الـ Down time المسموح فيها طبقاً لعقد الـ SLA الموقع بيننا لتقديم الخدمة.

تعرفنا أيضاً على تكنولوجيات ال Cluster – DRS – FT ، اليوم سوف نستكمل موضوعنا ونتكلم عن اخر هذة الأنواع وأضخمهم وأصعبهم وأقلهم مشاهدة في الواقع.
وهي الـ Site Recovery or Disaster site
لو فرضنا أننا قمنا بتأمين الداتا سنتر لدينا من نواحي الـ Cluster وبذلك نكون قمنا بحل مشكلة أن يحدث مشكلة أو عطل في الهاردوير أو السوفت وير الخاصة بأحد السيرفرات التي لدينا فيكون لدينا سيرفر بديل يقوم بنفس العمل.

لكن لو فكرنا بمنظور أوسع وهو في حالة حدوث مشكلة في الداتا سنتر ككل على سبيل المثال حريق أو زلزال فى مبنى الداتا سنتر، فبهذا الوضع نكون قد فقدنا كل شيء السيرفرات والداتا والكلاستر لم ينفعنا في شيء في هذا الوضع.

ما الحل إذن؟ البعض سوف يقول أننا نملك نسخ Backup في مكان آخر، هذا حل صحيح لكنه سوف يأخذ وقتاً طويلاً للغاية في عملية إعادة بناء السيرفرات بدءاً من الشراء إلى التجهيز واسترجاع الداتا وغيرها سوف تستغرق من عدة ساعات إلى أيام على حسب حجم الداتا سنتر التي لديك.
إذن هل يوجد حل آخر؟ بعض الشركات لا يمكنها بأي حال من الأحوال أن تتوقف عن العمل تحت أي ظرف من الظروف مثل البنوك وشركات المحمول وغيرها.

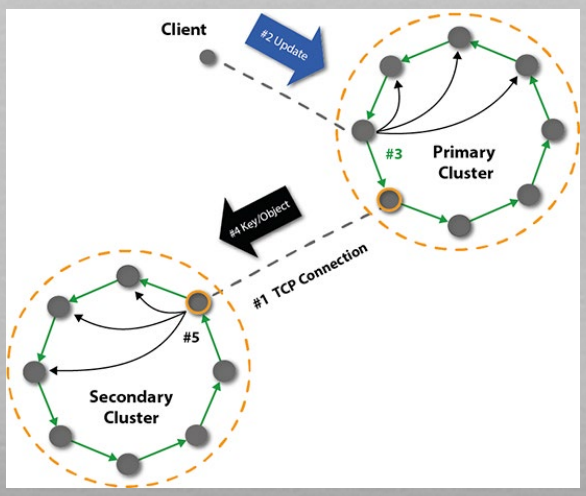
لذلك يوجد حل لهذه المشكلة وهو الـ Site Recovery

هو ليس بحل جديد وفكرته قديمة لكنه تطور بشكل رهيب في التكنولوجيا التخيلية وأضيف له العديد من المميزات التي يمكنك بواسطتها أن تستعيد عملك بعد فقد الـ Primary Site خلال 15 دقيقة فقط.

فكرة عمل الـ Site Recovery

الفكرة تعتمد على نقل نسخ من الداتا من الـ Primary site إلى secondary site، وتتم عملية نقل الداتا بين الفرعين بواسطة برامج تقوم بنقل الداتا باستمرار وتسمى هذه العملية بالـ Replication.

وهذة العملية تقوم بنقل الداتا الجديدة فقط كل فترة زمنية نقوم نحن بتحديدها بناءً على حجم الداتا وسرعة خط الربط بين الفرعين



صورة لعملية الـ Replication

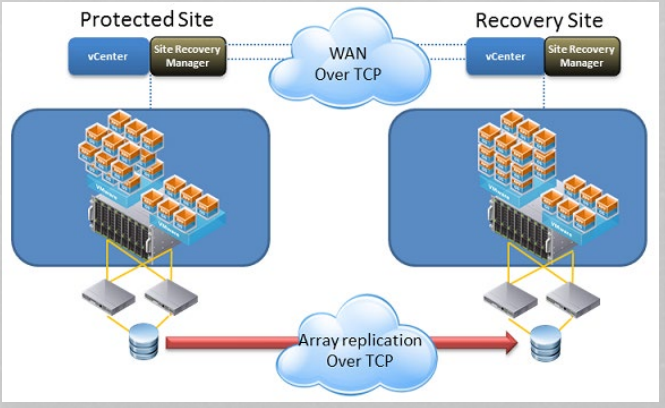
ولهذة العملية نوعان :

1 - Array Replication

وهذا النوع عبارة عن أن عملية الـ Replication للداتا بين الفرعين تتم على مستوى الـ Storage وتحديداً عن طريق برامج موجودة على الـ SAN Storage وبذلك نحتاج فى كل فرع SAN Storage وبرنامج يكون عادة داخل هذة ال SAN ويقوم بعمل نقل لهذه الداتا باستمرار إلى الـ SAN Storage الموجودة في ال Recovery site.

أغلب شركات الـ Storage تقوم بتقديم برامج تقوم بعمل هذا الـ Replication بين الـ SAN بين عدة فروع

لكن يوجد شركات منفصلة تقوم بنفس العمل وتعمل على نوع من الـ SAN بغض النظر عن منتجها.



صورة توضح الـ Array Replication

هذا النوع هو من أقدم الأنواع في عمل Site Recovery وأشهرهم وغالبية الشركات تستخدم هذا الأسلوب لقوته وبساطته – فنحن لن نحتاج لعمله سوى SAN storage في كل فرع وبرنامج يدير عملية النقل وخط ربط أو انترنت سريع للربط بين الفرعين.

لكن يعيب هذا النوع أنه في حالة انتقالنا للعمل على الـ secondary site سوف يكون لدينا الداتا داخل الـ SAN

ونحتاج إلى سيرفرات وإلى Application لكي يستطيع اليوزر التعامل مع هذه الداتا، على سبيل المثال لو قمنا بعمل Site recovery للداتا الخاصة بالـ Mail Server فقمنا بنقل الداتا من الفرع الرئيسي إلى الفرع الاحتياطي فسوف نحتاج إلى سيرفرات وعليها برامج الـ mail Server Application (Exchange – Lotus Notes -).

وتكون هذة السيرفرات بنفس الاسم والإعدادات هي نفس الإعدادات التي كانت موجودة في السيرفرات التي كانت في الفرع الرئيسي.

بالطبع هذه عملية صعبة في وضعنا هذا لأننا نقوم بنقل الـ Database for Email وليس التطبيقات والإعدادات

لذا يعب هذا النوع أننا نحتاج إلى ساعات طويلة لعمل بناء السيرفرات من جديد بنفس الإعدادات في الفرع الاحتياطي وعمل ربط لها بالداتا الموجودة في الـ SAN.

2 - النوع الثاني:
Virtual Machine Replication (vSphere Replication)

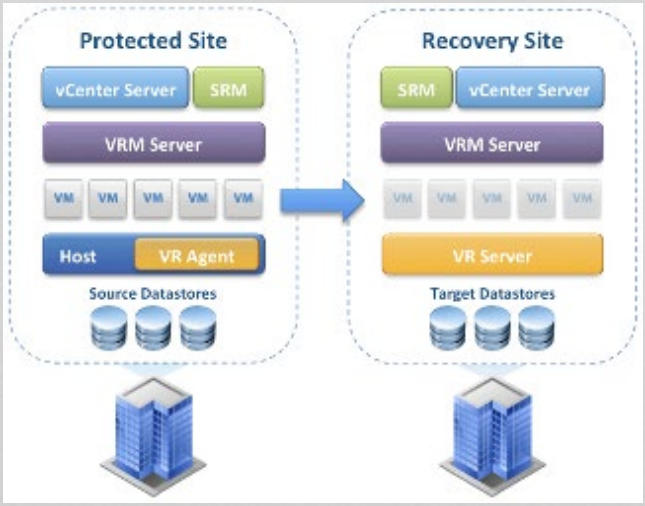
هذا الاسم أنا قمت بتسميته لأنه لا يوجد لدي اسم عامل لهذا النوع الجديد لذلك هذا الاسم ينبع من طريقة عمله الموحدة مع اختلاف الشركات التي تقدمة.

فكرة هذا النوع أنه يقوم بعمل Replication لأنظمة التشغيل والداتا الموجودة بداخلها وبكل الإعدادات وكل شيء

ويقوم بنقلها إلى الفرع الاحتياطي وعمل نقل لأي تحديث يحدث فيها باستمرار.

لاحظوا أنه قام بنقل الـ OS + Database فبذلك إذا حدث مشكلة في الفرع الرئيسي وانتقلنا للعمل من خلال الفرع الاحتياطي فلن تحتاج إلى بناء سيرفرات أو عمل إعدادات للسيرفرات وإنما سوف نقوم بعمل تشغيل للسيرفرات فقط لا غير.

البعض يفكر كيف نقوم بعمل نقل لأنظمة التشغيل بما تحتويها، هذا سهل للغاية لو عرفنا أن هذا النوع مصمّم خصيصاً للسيرفرات التي تعمل بواسطة التكنولوجيا التخيلية، وهذه السيرفرات هي عبارة عن Virtual machine داخل Storage سواءً داخلية في السيرفر أو خارجية على SAN or NFS.



صورة لـ VM Replication

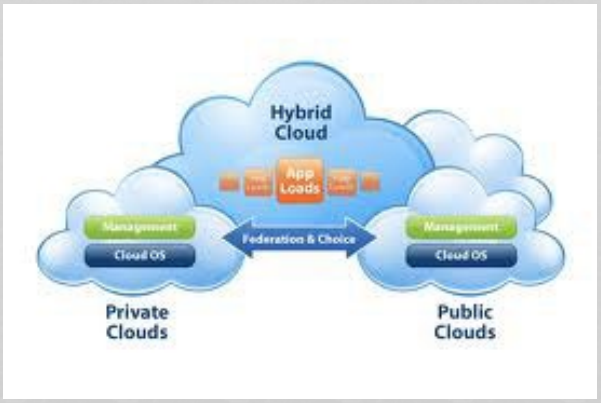
لكن تختلف معنا في هذه الحالة لأن هذا النوع يعمل بعمل نسخ من الـ VMs الموجودة في الفرع الرئيسي إلى الفرع الاحتياطي ويقوم بنقل أي تحديث أو تعديل يحدث على هذه الـ VMs. هذا يوفر لنا وقت ضخم للغاية لأننا لن تحتاج إلا لعمل تشغيل للسيرفرات الموجودة في الفرع الاحتياطي فقط وأيضاً هي أرخص في المكونات لأننا هنا لن نحتاج ال SAN Storage وإنما يمكننا أن نعمل على نوع من أنواع الـ Storage.

تقدم العديد من الشركات العاملة في التكنولوجيا التخيلية حلول تقوم بعمل هذا النوع مثل شركة VMware Site Recovery manager 5

في هذا التطبيق يمكنه عمل النوعين ويوجد العديد من الشركات الأخرى التي تقدم هذا النوع بشكل بسيط وسهل للغاية مثل شركةVeeam and Quest, vKernel وغيرها.

من الجدير بالذكر أنه مع انتشار تكنولوجيا الـ Cloud Computing أصبح حالياً بالإمكان أن نقوم بعمل بدل الفرع الاحتياطي أن يكون في مكان آخر بعيداً عن الفرع الرئيسي أو يكون في مدينة آخر

أصبح يمكننا أن نقوم بعمل نقل لهذه للسيرفرات إلى إحدى الداتا سنتر الموجودة على الإنترنت والتي تقوم بتقديم خدمة الـ Hybrid Cloud وهي عبارة عن اندماج الـ Private Computing .Cloud and Public Cloud



صورة للـ Hybrid Cloud

كيفية عمل Prot Forwarding على أجهزة سيسكو

سوف نتحدث في هذه التدوينة السرعة عن طريقة عمل Port Forwarding لأجهزة سيسكو بحيث نستطيع الوصول إلى أحد السيرفرات أو الاجهزة من خارج الشبكة (الأنترنت) .

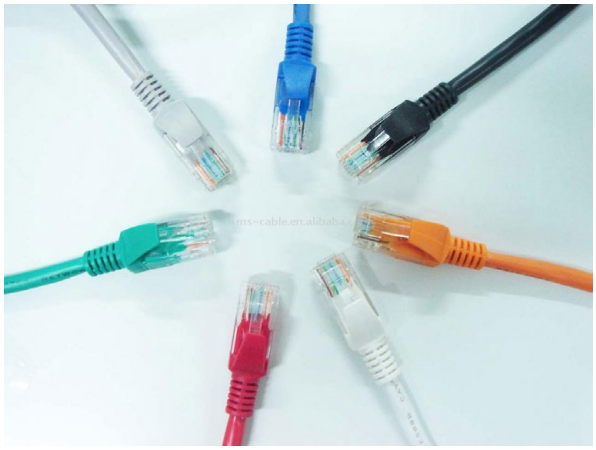
منذ فترة وجيزة قامت أحد الشركات بتركيب نظام كاميرات ICTV داخل أحد فروعها لمراقبة العمال داخل أحد مخازنها وكان من المفترض أن يتم مشاهدة ومتابعة هذه الكاميرات من خلال الفرع الرئيسي وكما هو معروف أن للوصول إلى هذه الكاميرات من خارج المبنى كان من الضروري وجود أي.بي حقيقي أو DDNS, بعد توفير أي.بي من خلال DDNS وربطه مع راوتر سيسكو من خلال بعض الأوامر التي تحدثت عنها مسبقا في تدوينة مسبقة على هذا الرابط:

http://www.networkset.net/201101/11//ip-ddns-cisco/

وصلنا إلى لحظة عمل Port Forwarding للبرنامج الذي سوف يدخل إلى الشبكة ويصل إلى الـ DVR ومن خلاله سوف نتمكن من مشاهدة ومتابعة الكاميرات الموجودة داخل الفرع.

طريقة عمل الـ Port Forwarding في راوترات سيسكو لا تحتاج منك أكثر من أمر واحد وهو يتم من خلال استخدام الـ Nat وصيغة الأمر على الشكل الآتي:

```
Cisco's
router#enable
router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# ip nat inside source static tcp 192.168.20.20 37777 interface Dialer0 37777
```



الأي .بي الأول 192.168.20.20 هو أي.بي الـ DVR والبورت 37777 هو المنفذ الخاص لـ DVR والذي يسمح للبرنامج بالدخول إلى إليه, Interface dialer0 هو المنفذ الخاص بالإنترنت وقد يختلف بحسب طريقة الربط الخاصة بالإنترنت فأحيانا يكون الربط مباشر وبدون وجود مودم.

طبعا هناك طريقة أخرى بأن نضيف Rules جديدة للأكسس ليست الخاصة بالنات نفسها لكن هذه الطريقة أبسط وأسرع.

كيفية إعداد خدمة DHCPV6 على لينكس سرفر

الجميع يعلم أن عناوين IPv4 انتهت منذ فترة وبالتحديد في شهر فبرايرعام 2011 تم حجز أخر رقم آي بي بنظام IPv4 وذلك أجبر الكثير من المواقع والمؤسسات على تجربة IPv6 لفترة مؤقتة للانتقال بعد ذلك لاستخدامه بشكل دائم وبالفعل كانت الفترة السابقة هي المرحلة التي تم فيها انتقال الغالبية العظمى لاستخدامه بشكل دائم ومن هذا المنطلق سنتحدث اليوم عن كيفية إعداد خدمة DHCPv6 على لينكس سيرفر (توزيعات ريدهات ودبيان).

أولاً: سنبدأ بالحديث عن كيفية إعداد سيرفرات التوزيعات المشتقة من توزيعة ريدهات لأنها الأكثر شيوعاً وأقصد بذلك توزيعة ريدهات - فيدورا - سنت أو إس وستكون البداية كالتالي :-

تفعيل الإعدادات الخاصة بخدمة DHCPv6 على سيرفر من نوع وستكون البداية مع تنصيب حزمة الـ DHCPv6 RPM :-.

```
#yum -y install dhcpv6g
```

وبعد الانتهاء من تنصيب حزمة RPM سنبدأ الان في تشغيل IPv6 حتى يستطيع السيرفر في أستقبال وأرسال الحزم التي من نفس النوع

```
#vi /etc/sysconfig/network
NETWORKING_IPV6=yes
IPV6FORWARDING=yes
```

ثم سنقوم بتشغيل IPv6 على جهاز ما ونضيف أيضاً بعض العناوين على نفس الجهاز

```
#vi /etc/sysconfig/network-
scripts/ifcfg-eth0
IPV6INIT=yes
IPV6ADDR=»2002:1851
:c622:1::164/»
```

الآن سنقوم بتحديد كارت الشبكة الذي سيعمل معه خدمة DHCPv6 سيرفر

```
#vi /etc/sysconfig/dhcp6s
DHCP6SIF=eth0
DHCP6SARGS=
```

بعد ذلك سنقوم بالتعديل في ملف الإعدادات الخاص بالخدمة من المسار التالي

```
#cp /usr/share/doc/dhcpv6-*/dhcp6s.conf /etc/
#vi /etc/dhcp6s.conf
interface eth0 {
      server-preference 255;
      renew-time 60;
      rebind-time 90;
      prefer-life-time 130;
      valid-life-time 200;
      allow rapid-commit;
      option dns_servers 2002:1851:c622:1::1 example.com;
      link AAA {
            pool{
                  range 2002:1851:c622:1::2 to 2002:1851:c622:1::964/;
                  prefix 2002:1851:c622:1::/64;
            };
      };
};
```

```
#service network restart && service dhcp6s start && chkconfig dhcp6s on
```

وبعد ذلك سنقوم بضبط الإعدادات على جهاز المستخدم وسنبدأ كالعادة بتنصيب حزمة DHCPv6 RPM

```
#yum –y install dhcpv6_client
```

ثم نقوم بتفعيل IPv6 على جهاز المستخدم كما حدث مع السيرفر سابقاً

```
#vi /etc/sysconfig/network
NETWORKING_IPV6=yes
```

بعد ذلك سنقوم بضبط الإعدادات على جهاز معين «سيرفر» عن طريق إضافة الأسطر التالية إلى ملف الإعدادات

```
#vi /etc/sysconfig/network-scripts/ifcfg-eth0
IPV6INIT=yes
DHCPV6C=yes
```

بعد ذلك سنقوم بالتعديل في ملف الإعدادات الخاص بالمستخدم على النحو التالي

```
#cp /usr/share/doc/dhcpv6_client-*/dhcp6c.conf /etc/
#vi /etc/dhcp6c.conf
nterface eth0 {
      send rapid-commit;
      request domain-name-servers;
};
```

وفي النهاية سنقوم بإعادة تشغيل الشبكة على جهاز المستخدم حتى يستطيع الجهاز أن يحصل على عنوان IPv6 من السيرفر

```
#service network restart
```

وبعد ذلك من الممكن للعميل أن يكتب الأمر التالي على جهازه وسيرى أن العنوان الجديد

```
# ifconfig eth0
```

ثانياً: سننتقل الآن للحديث عن كيفية إعداد خدمة DHCPv6 على توزيعة ديبان ولكني الآن سأستخدم توزيعة أوبونتو (المشتقة من ديبان) وسأستخدم في هذه الحالة خدمة ISC DHCPv6 (ولمن لا يعرف هذه الخدمة فهي سوفت وير شهير مفتوح المصدر يتوفر للتحميل مجاناً تحت شروط رخصة ISC ويستخدم في الشبكات الداخلية ويتميز في التطبيقات كبيرة الحجم عالية الموثوقية) المهم عند تحميل السوفت وير أن تقوم بتحميل الإصدار الذى يدعم عناوين IPv6 وهو الإصدار رقم 4 وما بعده وتستطيع أن تتعرف على معلومات أكثر عن الخدمة وتحميلها من هذا الرابط

http://www.isc.org/software/dhcp

وستكون الخطوة الأولى مع إعطاء كارت الشبكة عنوان IPv6 ثابت «Static» ولفعل ذلك علينا التعديل في ملف /etc/network/interfaces

```
auto eth1
iface eth1 inet static
address 192.1.1.189
netmask 255.255.255.0
gateway 192.1.1.190
iface eth1 inet6 static
pre-up modprobe ipv6
address 2001:620:40b:555::4
netmask 64
gateway 2001:620:40b:555::1
```

وبعد ذلك نقوم بإعادة تشغيل الخدمة الشبكية عن طريق كتابة هذا الأمر

```
# /etc/init.d/networking restart
```

بعد ذلك سنقوم بتنصيب خدمة DHCPv6 عن طريق كتابة الأمر التالي

```
#apt-get install isc-dhcp-server
```

وسنبدأ الآن في تفعيل خدمة الـDHCPv6 ولكن هناك نقطة لابد أن نذكرها وهي أن هذه الخدمة لا تستطيع أن تدعم DHCPv4 أو DHCPv6 ولذلك سنكون بحاجة إلى تفعيل كارت الشبكة الآخر (كارت لعناوين IPv6 وأخر لـ IPv4) ولذلك لابد أن نتأكد من أن نختار كارت الشبكة الصحيح ويمكنا التعديل من هذا الملف /etc/default/isc-dhcp-server

```
INTERFACES=»eth1»
```

بعد ذلك سنعدل في الملف التالي /etc/init.d/isc-dhcp6-server حتى نضمن أن يتم دعم عناوين IPv6.

ونضيف "6-" كخيار لخدمة dhcpd process
نغير بعد ذلك ملفات "dhcp.leases" إلى "dhcp6.leases".

نعدل بعد ذلك في ملف CONFIG_FILE بالقيمة التالية:
CONFIG_FILE=/etc/dhcp/dhcpd6.conf
نعدل بعد ذلك في ملف DHCPID بالقيمة التالية:
DHCPDPID=/var/run/dhcp-server/dhcpd6.pid

ثم نعدل في قائمة عناوين IPv4 بالتعديل في الملف التالي /etc/dhcp/dhcpd.conf

```
option domain-name «NetworkSet.net»;
option domain-name-servers ns.NetworkSet.net;
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.100 172.16.14.150;
```

ثم نعدل في قائمة عناوين IPv6 بالتعديل في الملف التالي /etc/dhcp/dhcpd6.conf

```
option domain-name « NetworkSet.net»;
option domain-name-servers ns. NetworkSet.net;
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
subnet6 2001:620:40b:555::/64 {
    range6 2001:620:40b:555::100 2001:620:40b:555::150;}
```

ونقوم بعد ذلك بإنشاء ملف أخر (كاحتياطي) لبدء تشغيل خدمة DHCPv6

```
#cp /etc/init.d/isc-dhcp-server /etc/init.d/isc-dhcp6-server
```

حسنا، نحن نعلم أن خدمة DHCP مربوطة بـ apparmor «وحدة أمان للنواة لينكس» ولذلك نحن بحاجة لعمل تفويض للـ DHCPv6 حتى تستطيع أن تعمل الخدمة بالشكل المطلوب ولذلك سنقوم بإضافة بعض التعديل في الملف الموجود في الرابط التالي /etc/apparmor.d/usr.sbin.dhcpd

```
...
network inet6 raw,
@{PROC}/[09-]*/net/if_inet6 r,
/var/lib/dhcp/dhcpd6.leases* lrw,
/var/run/dhcp-server/dhcpd6.pid w,
...
```

ولا تنسى أن تقوم بإعادة تشغيل عملية «apparmor»

```
#/etc/init.d/apparmor restart
```

الآن ستكون جاهز لتشغيل الخدمة عن طريق الأوامر التالية ونكون انتهينا بفضل الله من عمل الإعدادات اللازمة لتشغيل الخدمة

```
#/etc/init.d/isc-dhcp-server start
#/etc/init.d/isc-dhcp6-server start
```

WHAT S NEW IN WORD 2013 ?

نعيش الآن حالة فريدة من نوعها مع التطور المتسارع للتكنولوجيا وهي إنه لا نستطيع الانتهاء من معرفة منتج أو خدمة جديدة إلا ويظهر إصدار جديد. وهذا الشيء سلبي لحدّ ما لنا لذا يجب علينا متابعة كل ماهو جديد وما الشيء الذي يميز الاصدار الجديد عن غيره من الإصدارات؛ لأنني لاحظت البعض يتم تنصيب النسخ أو الاصدارات الجديدة من المنتجات ولكن يبقى وكأنه يعمل على النظام القديم بل والأقدم منه .

إن كان على صعيد السوفت وير أو على صعيد الهارد وير فلا بد من المتابعة جيداً، وبإذن الله سوف أكون متابع للتطورات والخدمات الجديدة لشركة مايكروسوفت وإفادة قرائنا بأحدث الخدمات لها.

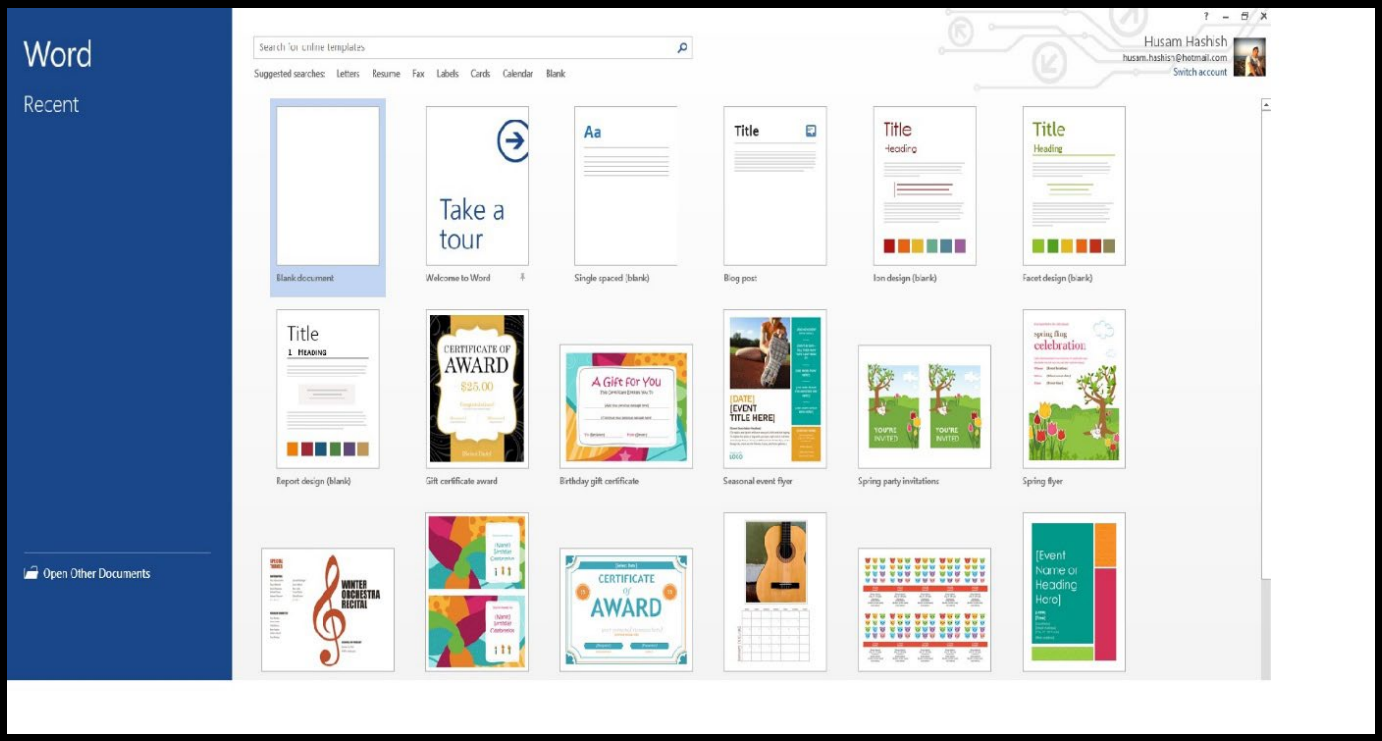
Word 2013 : الغني عن التعريف وهو البرنامج من حزم مايكروسوفت اوفيس.

ولكن ما هو جديد الإصدار 2013 وهل هو فقط تغيير للواجهة؟ بالتأكيد لا.

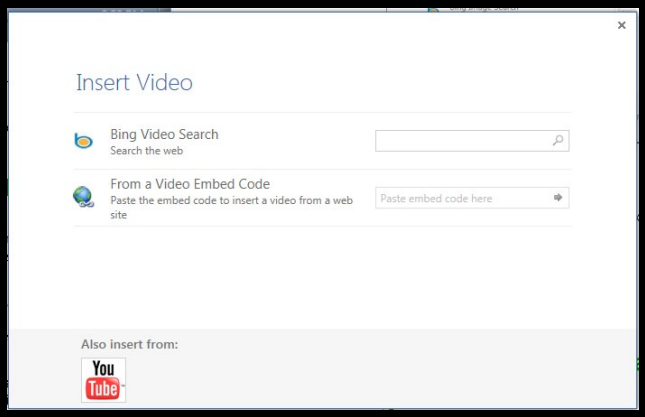
التحسينات الجديدة (New features) :

1 - بداية جميع منتجات ميكروسوفت تطلب منا الدخول بحسابنا على الهوتميل أو غيرها من حساباتها بغرض الاستفادة من ميزات الكلاود أو الـSky Drive وأيضاً من أجل أن يكون لنا ستايل معين وإعدادات معينة نحتفظ بها في أي مكان فقط عند تسجيل حسابنا من مكان أخر سوف تكون الإعدادات ونفسها وهذه من أكبر المزايا الجديدة في الويندوز 8 وإصدارات الـ 2013.

2 - الـ Template الجاهزة في جميع منتجات office 2013 التي نستطيع من خلالها إنشاء مستندات جميلة وجذابة وذات أغراض محددة فقط عند الضغط على إنشاء ملف جديد وأيضاً مع إمكانية البحث أونلاين عليها على غرض معين.

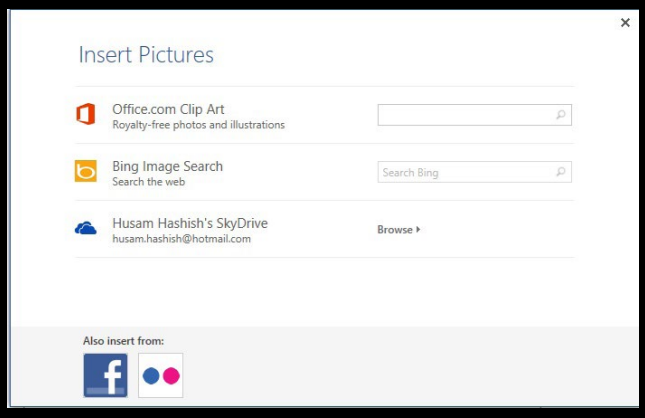


3 - الميزة الأجمل والتي يعاني منها جميع المستخدمين وهي قضية ملفات الـ PDf وكيفية تحريرها إن كان أونلاين أو عن طريق برامج أخرى ولكن الآن أصبح بإمكاننا فتح ملفات بصيغة PDF والعمل على تعديلها وحفظها بالصيغة التي تريدها والفائدة الأجمل وهي أنه أصبح بإمكاننا فتح وتعديل ملفات PDF وباللغة العربية مع الاحتفاظ بالتنسيق وهذه هي كانت مشكلة أكبر البرامج التي تعمل تحويل بين الصيغتين يعني يمكننا الآن أن نقول سوف يقل عدد مستخدمين برامج مثل Acrobat reader.



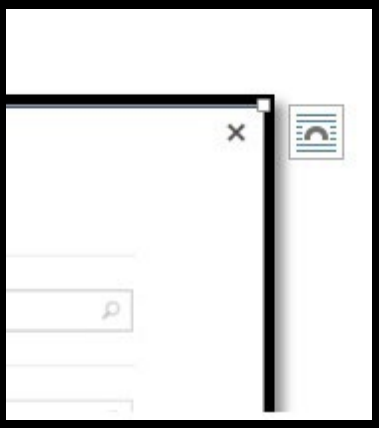
4 - إدراج فيديو أو صور ولكن عن طريق الإنترنت مباشرة دون وضعها على الملف وزيادة حجم الملف يمكننا الآن ربط الفيديو عن طريق اليوتيوب مثلا والصور عن طريق لينك أو موقع مثل Flickr

بالنسبة للفيديو :
الضغط على insert tab
ثم Online Video
ثم Insert Video

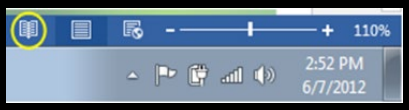


إضافة صور من :
الضغط على insert tab
ثم Online Pictures
ثم Insert Pictures

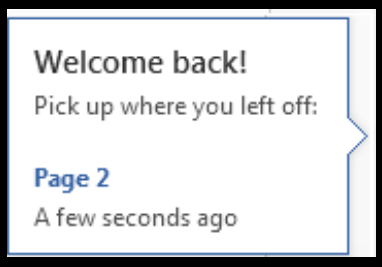
5 - استخدام محاذاة الصور أو الفيديو يمكنك الآن المحاذاة مباشرة فقط عند الضغط على الصورة أو الفيديو سوف يظهر لنا ايقونة جديدة لم نعتد على مشاهدتها من قبل وهي تعطينا إمكانية التنسيق بين الصور والنصوص المكتوبة في المستند.



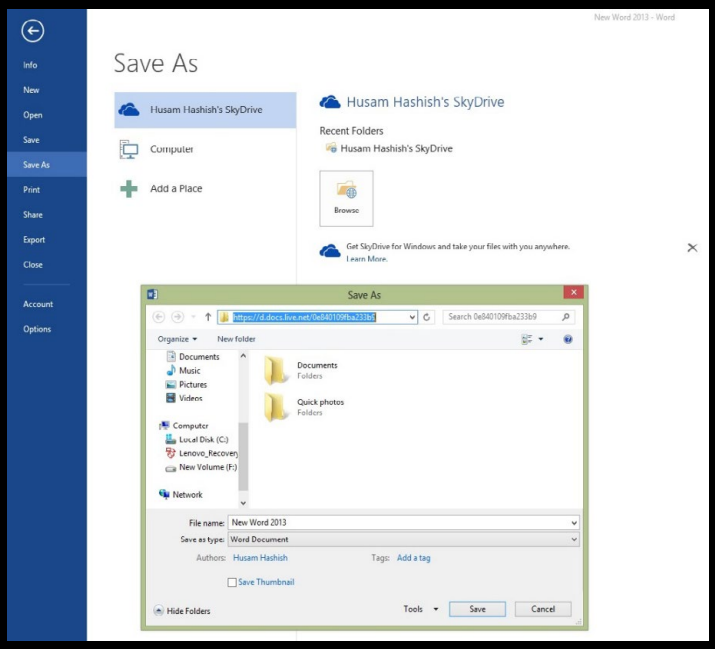
6 - عند الضغط على زر وضعية القراءة الموجود أسفل الشاشة يتم تغيير حجم الأعمدة تلقائياً لتناسب الشاشة ويتم عرض العناصر القائمة الأقل وللتنقل بين الصفحات أصبحت أسهل وأجمل وخصوصاً إن كنا نملك شاشات الـ Touch



وعندما تريد أخذ استراحة أو تم غلق الملف التي تقرأ منه تلقائياً يتم حفظ أين وصلت في القراءة بظهور عبارة :

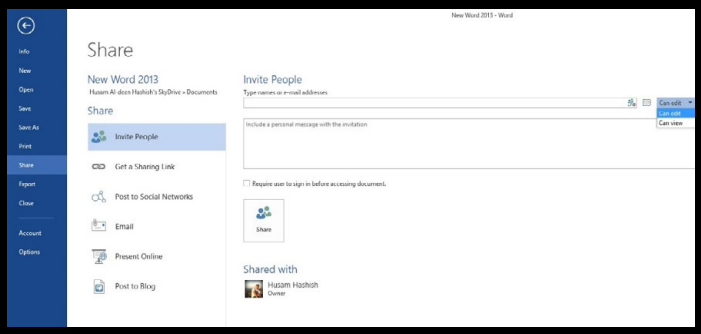


7 - حفظ الملفات على ميكروسوفت كلاود مباشرة Sky Drive ولكن بعد تسجيل دخولك ببريدك الخاص لنلاحظ بإمكانية الحفظ على الكلاود



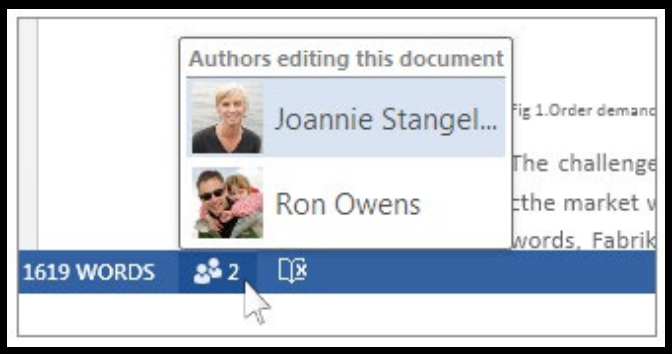
مع إمكانية استعراضهم أوف لاين بعد انقطاع النت وعند وصل النت يتم المزامنة بين الملفين ويأخذ الملف ذات التعديل الأخير بالوقت.

8 - نستطيع من مشاركة هذا الملف وإرسال الرابط للشخص ليتم استعراضه وتحميله من خلال office 2013
دون الذهاب إلى البريد الالكتروني وإعطاء الصلاحيات التي تريد من الشخص استخدامها عن طريق إيميل الشخص الآخر .



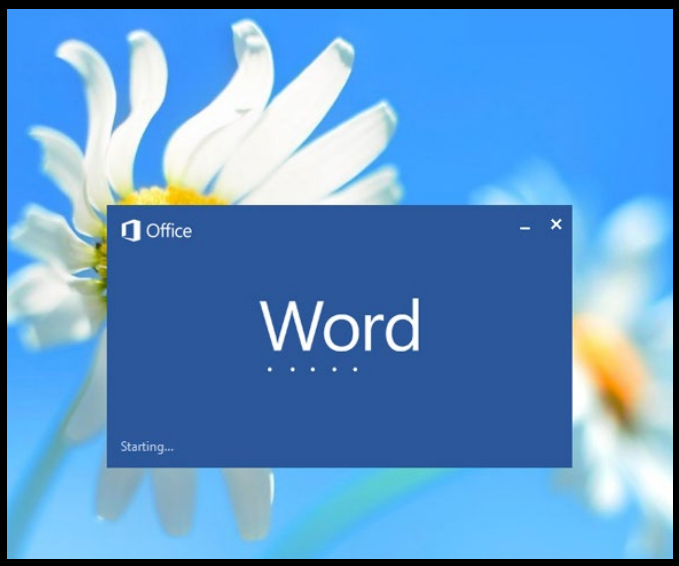
9 - استعراض الملف مباشرة ومتابعته ومناقشته مباشرة مع صديقك أو أستاذك عن طريق Presentation online
بعد إرسال رابط للشخص بقبول الدعوة والدخول عليها أون لاين يمكنك أن تتم المناقشة عليها وبفتح نافذة دردشة بسيطة موجودة أسفل الشاشة وهذا عن

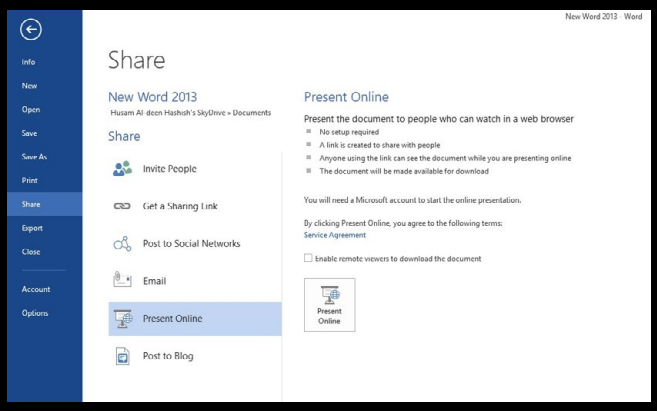
طريق حسابات ميكروسوفت هوتميل.
وإذا كنت تستخدم برنامج اللينك السيرفر الذي سبق وتكلمت عنه تصبح عملية المحاضرة بشكل أجمل بكثير وممكن إدخال المناقشات الصوتية والفيديوية أيضاً.
وأيضاً يمكننا العمل مع بعض في عملية إنشاء الملف مثال: لدينا وظيفة مشتركة بين شخصين نستطيع العمل بها أون لاين ولأكثر من شخص أفضل من أن يتم إنشاء الملف ثم إرساله ثم تعديله وإرساله الآن أصبح العمل أون لاين.

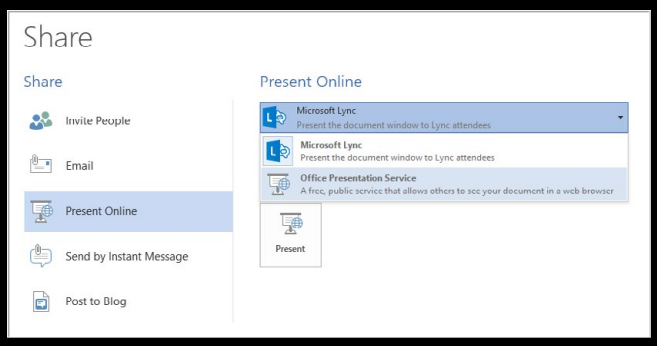


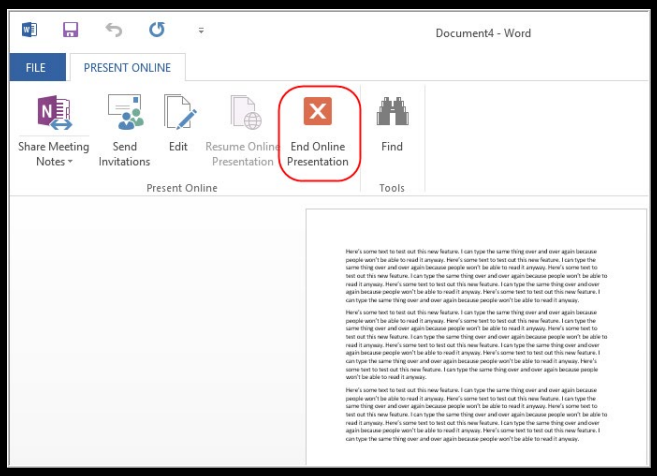
10 - التوافقية الكاملة مع الشاشات الـ touch وهو بشكل عام أي شيء جديد لدى ميكروسوفت مع الدعم الكامل تقريبا للشاشات اللمس.

جميع هذه الميزات والخدمات هي موجودة في أغلب باقي حزمة أوفيس ولكن الهدف من هذا المقال كما تحدثنا هو أن نتابع ميزات كل منتج أو اصدار جديد ونتعلمه وكأننا نتعلم شيئ جديد ليس له سابق.

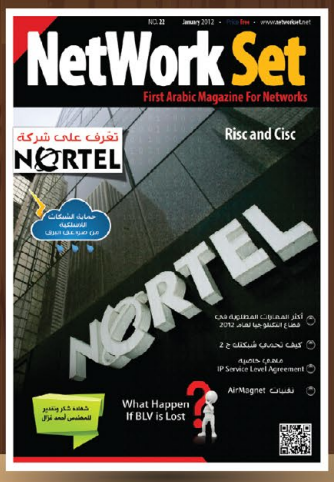


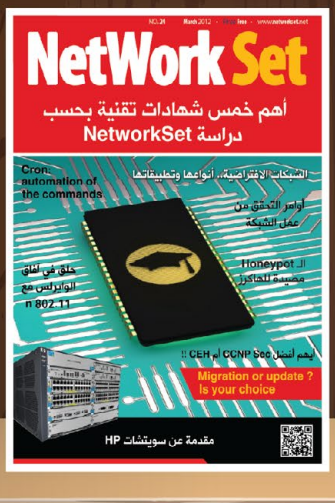






Network Set Magazine Gallery





مدخل إلى تقنية الـ WAN Optimization

منذ عدة سنوات أذكر أن لمحت على أحد صفحات الإنترنت مصطلح WAN Optimization فلم أفهم من هذا المصطلح إلا كلمة WAN بينما الكلمة الثانية لم أفهمها ابدا فقررت البحث عن ترجمتها باللغة العربية فوجدت أن معناها الحرفي هو "تحسين" أي تحسين الوان جلست وفكرت بهذا المصطلح العجيب فلم أفهم معناه ولم أصل إلى أي نتيجة تقودني إلى فائدته الحقيقة كون كنت مبتدأ فالمصطلح يفهم فقط عندما تدخل سوق العمل الحقيقي وترى متطلبات الزبائن، حينها فقط تصل إلى معناه واليوم قررت أن أضع لكم تفسير هذا المصطلح وخصوصاً أن لا أحد تحدث عن هذا الأمر مسبقاً على صفحات الإنترنت العربية.

تعتبر الـ WAN Optimization مجموعة من التقنيات تهدف إلى تسريع ورفع أداء الاتصال مع الأنترنت ولكن ليس بمفهومه العام، فالشركات الكبيرة والصغيرة الآن تملك فروع كثيرة وعادة ما تتطلب هذه الفروع وجود اتصال مع فرعه الرئيسي من أجل مشاركة الملفات أو وجود برامج محاسبة تتصل مع قواعد بيانات أو وجود Web server, Mail Server Voice or Video sharing والخ . . . كل هذه الخدمات تحتاج إلى انترنت سريع لكي تعمل بشكل جيد وبأداء عالي فلو كان أحد الفروع يعمل من خلال برنامج محاسبة ويتصل مع قاعدة البيانات الأساسية الموجودة في فرعها الرئيسي فلا بد من أن يكون الترابط بينهم جيد جداً بحيث يتم التعامل مع برنامج المحاسبة بشكل سريع من خلال فرعه وبدون وجود تأخير أو بطء في استخدام البرنامج. ونفس الفكرة مع باقي الخدمات، وكون الانترنت بدأ حديثاً بالتطور وأصبحت السرعة أفضل من السابق فلقد كان موضوع استحداث آليات وتقنيات تساعد على تسريع عملية الاتصال مع الانترنت وتسريع نقل البيانات والملفات بين هذه الفروع أمراً في غاية الأهمية وعدا عن ذلك محاولة التخفيف من معدلات التأخير والاختناقات وتوفير عملية إدارة الباند ويث كل هذه الأمور تتيحها لنا هذه التقنية، والجدير ذكره أن هذه الحلول وبحسب الشركات المصنعة تدعي أن معدلات السرعة تزيد أضعاف مضاعفة قد تصل أحيانا إلى ثلاث أو أربع أضعاف السرعة السابقة.

الآليات المستخدمة في ال WAN Optimization

تشير الدراسات إلى أن سوق المبيعات الخاص بالـ WAN Optimization عام 2008 تجاوز المليار دولار بينما نجد أن هذا الرقم تضاعف أربع مرات العام الماضي مما أعطى للشركات حافز كبير للتنافس على هذا النوع من الحلول. التنافس في هذا المجال كانت كبير ونوعي جداً ودخلت فيه أكبر الشركات في العالم في مجال التقنيات فهو سوق متطور وغير مكلف كثيراً بالنسبة للمصنع، وهذا التنافس ولد تقنيات وأفكار

كثيرة تستخدم في عملية التسريع أو التحسين كما تمت ترجمتها ومن بين هذه الآليات المستخدمة:

Compression أو الضغط أحد أهم الآليات المستخدمة في الـ WAN Optimization تختلف بين كل شركة وأخرى فلكل واحد منهم لديه خوارزمية خاصة للضغط وهناك شركات تقدم منتجات تتخصص في نوعية معينة من الداتا وتملك خوارزمية مخصصة أيضاً.

Caching الكاشينغ يعتبر من الأمور المعروفة في عملية أي تسريع موجودة في عالم الأنترنت وهي تستخدم بكثرة في عالم الشركات وتستخدم أيضا في هذا المجال.

DE duplication تقوم هذه التقنية بتوفير مراقبة ومتابعة للداتا التي يتكرر إرسالها عبر خطوط الـ WAN والتي ينعكس بدوره على معدل إرسال الداتا والنتيجة هي إنقاص معدل نقل الداتا التي يتكرر نقلها عبر تلك الخطوط باستخدام خوارزميات معدة مسبقاً.

Protocol optimization كلنا يعلم أن بروتوكول الـ TCP يحتاج في كل مرة إلى تأكيد عملية نقل البيانات بشكل صحيح بحيث ينتج عنها الكثير من التأخير في عملية الإرسال (المصطلح الخاص بهذه العملية يطلق عليه باللغة الإنكليزية Chatty أي ثرثارة وكثيرة الكلام) ومما يزيد الطين بلة، أن كل قطعة من البيانات المرسلة هي صغيرة نسبياً. هذه التقنية تقوم بتخفيض عدد الرسائل، وبالتالي تقليل معدلات الـ Delay، الأمر الذي ينعكس على سرعة الانتقال وعلى مدى استجابة خطوط الـ WAN. وهناك تقنيات أو لنقل حلول معينة لبعض الشركات تركز على بعض البروتوكولات الخاصة بالـ TCP مثل بروتوكولات الإيميل وقواعد البيانات والخ. ..

Latency optimization وهي تتحكم في بعض خواص الـ TCPمثل الـ Window Size.

Traffic Shaping وهي تقوم بالتحكم بنوعية البروتوكولات التي يسمح لها باستخدام خطوط الـ WAN, فقد يكون على الشبكة هناك أكثر من تطبيق أو Application تقوم بشكل دوري بإرسال داتا معينة مما يزيد الضغط على تلك الخطوط ويقلل من فعاليتها.

Forward error correction وهي تقوم بالتحكم بمعدلات تصحيح الأخطاء التي قد تحدث من خلال ضم مجموعة من الحزم المرسلة وإعطائه رقم معين عوضاً عن رقم لكل حزمة.

طبعا هذا كان جزء بسيط جداً من مبدأ عمل هذه التقنيات وهناك تقنيات أكثر بكثير من التقنيات المذكورة ولكل تقنية هناك أمور وتفاصيل كثيرة ومعقدة جداً وقد حاولت على مدى يومين أن أبسطها وأقدمها باللغة العربية فترجمتها وفهمها باللغة الإنكليزية أسهل بكثير من شرحها باللغة العربية لكن أصررت على تقديمها حتى أضع أمامك الطريق لفهم الأساسات لهذا العالم وبعدها الطريق سوف يكون مفتوح أمامك، وهذه النظرة تولدت لدي من تجاربي الشخصية فأنا دائما ما أحتاج مفاتيح بسيطة للدخول في أي شيء يخص عالم الشبكات ولا أجدها متاحة لدينا لذلك فأنا أعكس دائما الحالة التي تصيبني أثناء تعلمي ودراستي .

وهذه قائمة بأهم الشركات وأنظمة مفتوحة المصدر التي تعطينا حلول لهذه التقنية وهي مأخوذة من موسوعة الويكيبيديا.

Open-source based WAN optimization solutions

- OpenNOP
- WANProxy
- TrafficSqueezer

Products and companies implementing WAN optimization

- AppEx Networks
- ApplianSys
- Aryaka
- Black Box Corporation
- Bluecoat
- Cisco
- Citrix
- Expand Networks
- Exinda
- F5 Networks
- Fortinet
- Infineta Systems
- Internap
- Ipanema Technologies
- Juniper Networks
- Meraki
- Radware
- Riverbed Technology
- Silver Peak Systems
- SonicWALL
- Streamcore

فلسفة الحماية بـ WPA2 / WPA

نظراً لضعف تقنية التشفير Wired Equivalent Privacy (WEP) فقد قامت مؤسسة Wi-Fi و جمعية مهندسي الكهرباء و الإلكترونيات IEEE بالعمل سوياً لاستبداله بمعيار أكثر أمانا و خرج إلى النور جيلين الأول يخص Wi-Fi و هو Wi-Fi Protected Access (WPA) و الثاني يخص IEEE و يسمى 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 يسمى 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 يسمى أيضاً 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 أوتوماتيكي لكل Packet على عكس WEP الذي يستخدم مفاتيح تشفير بطول 40-bit أو 104-bit تدخلها في الأكسس بوينت و الجهاز الذي سيستخدم الشبكة و الذي يستخدم تقنية RC4 و تم بعدها تعديل بنيته ليعتمد على AES encryption.

يحتوي أيضاً WPA على تقنية تسمى 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 اختراقه بحجب عملية capturing التي تستخدم في أخذ نسخ من الرزم المرسلة و تحليلها لاختراق الشبكة و رغم قوة MIC إلا أنه استبدل أيضاً في WPA2 بوسيلة أكثر قوة.

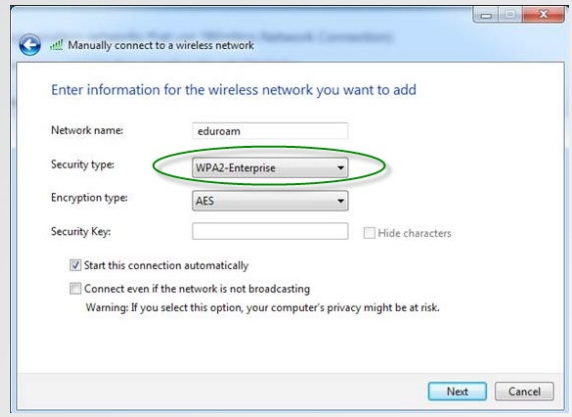
WPA Authentication Modes

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)

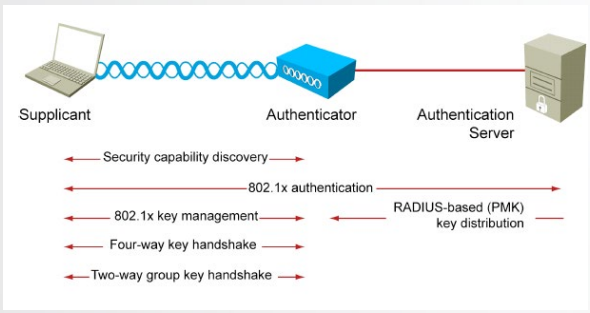
WPA Personal



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

WPA Personal

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

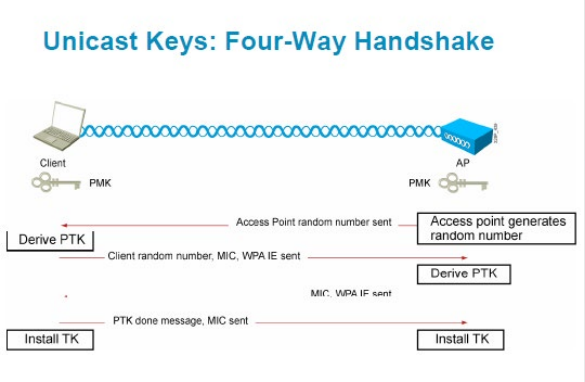


كما هو الحال مع بروتوكلات التوثيق يتم استخدام فريمات التراسل (probe request, probe response) بين الجهاز و الأكسس بوينت الا أن الاختلاف يكمن في أنه لابد أن يتوافق الأكسس بوينت و الجهاز على هذه العملية أمنياً ثم يستكمل خطوات توثيق 802.1X و عند استكمالها يقوم السيرفر بإرسال master key إلى الأكسس بوينت والتي أخذها مسبقاً من الجهاز الطالب للاتصال و لهذا يسمى المفتاح (Pairwise Master Key (PMK.

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

ثم يبدأ بعدها مرحلة جديدة من التراسل تسمى 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 تسمى four-way handshake ينتج بعدها مفتاح جديد Pairwise Transient Key (PTK)) يؤكد عملية الاتصال والتي 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 authentication server
ثم تتوالى الخطوات التالية:

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

ثانيا بهذا الرقم العشوائي و باستخدام أيضا PMK يقوم Client بتوليد مفتاح لتشفير البيانات التي سترسل إلى AP و يتم استخدام دالة تسمى (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 إلى Client بنفس السياسة الأمنية المستقبل بها و يقوم أيضا الأكسس بوينت بإرسال group key و بهذا يكون هناك توثيق بين الأكسس بيونت و الجهاز.

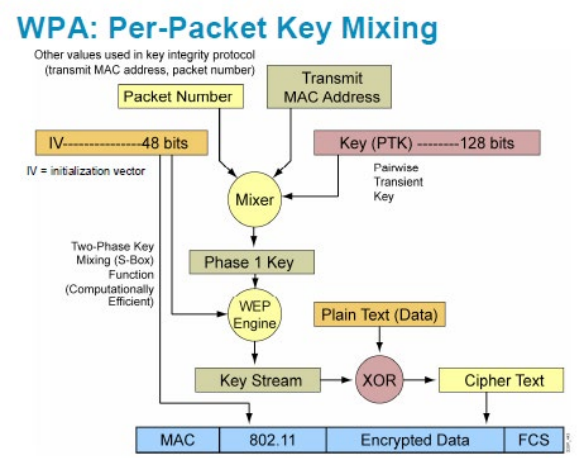
رابعا يتم تأكيد أن المفاتيح قد تم ارسالها و العملية جاهزة للتراسل .

بمجرد الحصول على المفتاح المؤقت PTK بطول 64 bit فإنه يتم تقسيمه إلى خمس مفاتيح.

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

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

WPA Encryption



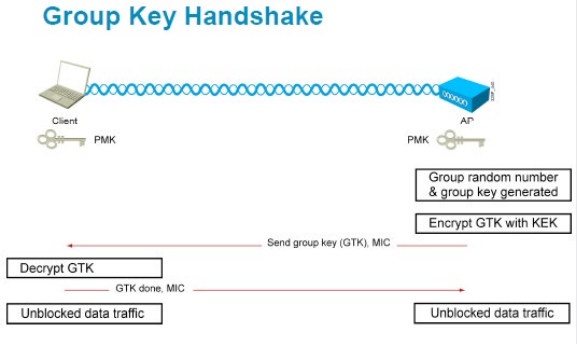
كما أن WPA قد دعم عملية التوثيق authentication بشكل كبير فإنه أيضاً قد قام بتحسين التشفير encryption أيضاً بشكل رائع حسن و ذلك عبر نظامين هما AES و TKIP أما AES فهو نظام جديد أقوى من نظام التشفير RC4 المستخدم مع WEP و لكنه يحتاج إلى الكثير من الطاقة بالإضافة إلى ضرورة دعم الجهاز لهذا النوع من التشفير.

و أما TKIP و هو اختصار Temporal Key Integrity Protocol فهو بروتوكول لا زال يستخدم تقنية RC4 و هي الخيار الإفتراضي للـ 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.

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

Unicast Keys: Four-Way Handshake



يستخدم GTK (Groupwise Transient Key) 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 باستخدام KEK و حمايتها باستخدام MIC.

ثانياً تقوم هذه الأجهزة بالاستجابة لـ GTK والرد على الأكسس بوينت.

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

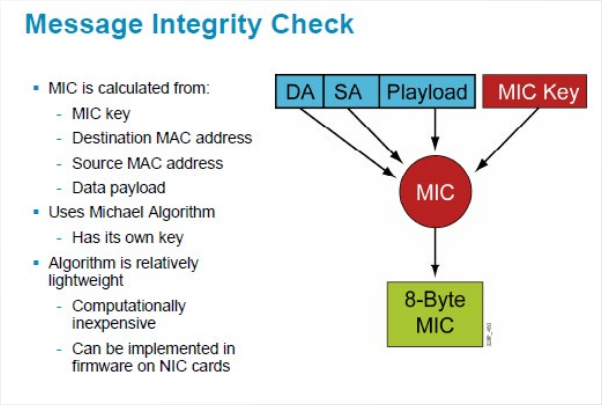
الأول بطول 16 byte و هو TK Temporal Key و يستخدم لتشفير و فك تشفير unicast data Packets

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

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 mixerلكل مفتاح PTK مع عنوان الجهاز MAC مع رقم كل باكت مخرجاً لنا مفتاح متغير لكل باكت ثم مزج ذلك مع IV ليتم تشفير البيانات المرسلة بها وبهذا فإنه بالإضافة لصعوبة كسر هذا التشفير فإنه الأكسس بوينت يستطيع اكتشاف عملية الاختراق بواسطة عنوان الجهاز المرسل مع مفتاح التشفير.

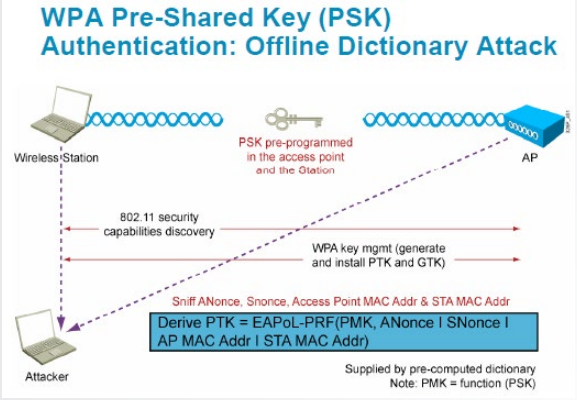
Message Integrity Check



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

WPA2 / 802.11i

الآن لدينا في WPA مفاتيح 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 افتراضياً في شبكات SOHO تغري بالاختراق و ذلك عبر عمل عملية فك الارتباط 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 إلى الانتقال إلى WPA2



WPA2 مبني على 802.11i و انتهى 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

(NIST Technology) والذي يستخدم عمليات مزج تسمى Rijndael algorithm و يعلو بالتأمين باستخدام IV لكل بلوك مرسل و يستخدم أيضا طلايقة التأكد من وصول الباكت MIC مثلما يفعل WPA.

و هذه مقارنة بين WPA, WPA2, 802.11i

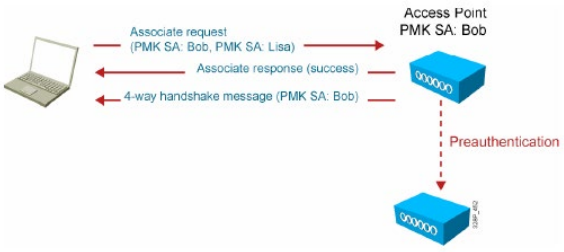
WPA/WPA2/802.11i Comparison

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 إلى حيز الشبكة يستطيع الدخول مرة أخرى بدون الحاجة إلى إعادة التوثيق

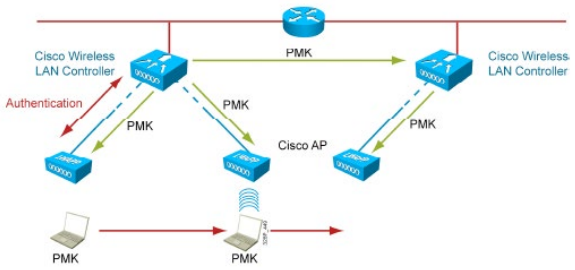
802.11i Key Caching and Preauthentication



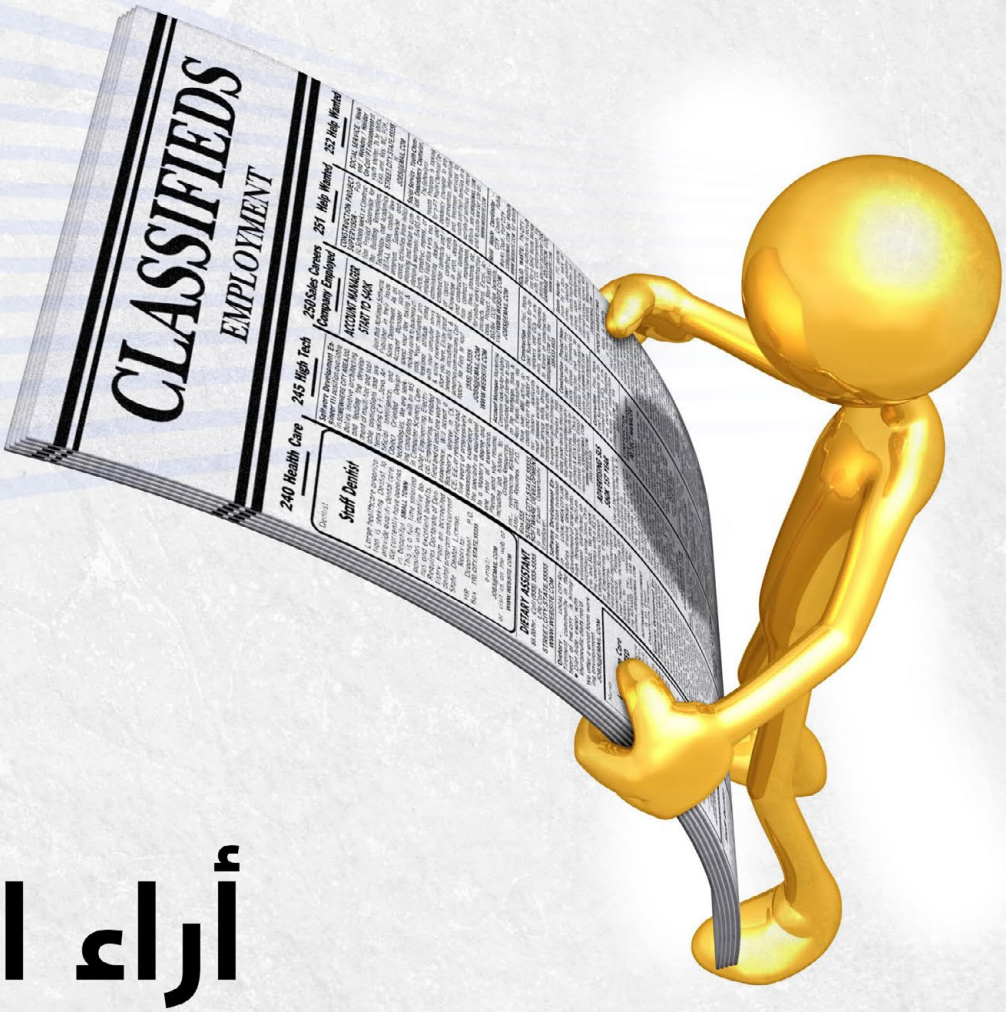
802.11i allows credentials to be cached on an AP, and a client to preauthenticate on several APs

كذلك قامت سيسكو بتطوير WPA بعمل مركزية لمفاتيح الولوج تسمى 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 أخرى في حال ابتعاده حيث يحدث تخزين caching لمفتاح PMK.

Cisco Centralized Key Management



NetWork Set
First Arabic Magazine For Networks



أراء القرّاء

أنس عيسى -فلسطين

انا من متابعي المجلة منذ صدور العدد الاول-واشكركم على مجهوداكم المستمرة في افادة القارئ العربي وانا شخصياً أعجبت بالمواضيع التي تتحدث عن إدارة الشبكات خصيصاً سيرفر الميكروتك واتمنى ان يكون هناك المزيد من المواضيع في هذا المجال خصوصاً ان شريحة كبيرة سوف تستفيد من هذه المقالات.

عماد جبران - ليبيا

عدد شهر يناير 2013 كان رائع واستفدت منه الكتير
أعجبني مقال عن الحلول الكاملة للشبكات اللاسلكية الخلوية
Cisco mobile exchange Architecture
فلم أكن اعلم بوجود هده الخدمة عند سيسكو

وليد الغربي - كندا

المهندس ايمن النعيمي والأخوة المشرفين على مجله نيتورك ست ،، بكل امانه عملك كلمه شكر قليله في حقه ، وانا جدا اتلهف لقراءة الجديد لمجلتكم الرائعة ، علما باني اقرأ الكثير من المصادر الإنجليزية لكن تغطيتكم للمواضيع تمثل لي طابع خاص واجد فيها اكثر اريحيه ،، شكرا من القلب ووفقكم الله جميعا واثابكم علي عملكم

ملاحظة: يرجى إرسال آرائكم على البريد الالكتروني التالي : magazine@networkset.net مع كتابة الاسم الثنائي وبلد الإقامة، تخضع الرسائل للمراجعة والتدقيق لغرض الاختصار والوضوح.

NetWork Set

First Arabic Magazine For Networks