NO. 27 June 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

بداية الطريق إلى عالم شبكات الـ SAN

Storage Area Network

How Computer Virus Work

الحماية في عالم التكنولوجيا التخيلية

بروتوكول الـ WCCP تحت مجهر NetworkSet

حلول تأمين البيانات في مايكروسوفت

عشرة أشياء يجب أن تتوفر لديك قبل دخول مجال تقنية المعلومات

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

أسـرة المجلـة

المؤسس و رئيس التحرير

م.أيمن النعيمي

المحـررون

م.نادر المنسي	م. سامي خالد الرجعي	---
م.خالد عوض	م. أحمد سلطان	---
م. أحمد خير الدين	م.خالد الدسوقي	---
م. تميم احميش	---	---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : عثمان اسماعيل

www.networkset.net

المقابلات الشخصية

تعتبر المقابلات الشخصية الخاصة بالعمل أحد الأمور التى تشغل بال نصف سكان الكرة الأرضية فكل من يبحث عن عمل أو وظيفة معرض لهذا النوع من الأمتحانات والتى قد تكون بالنسبة للبعض أصعب بكثير من دخول أمتحانات تخرج الجامعة وأحيانا أصعب من فكرة الذهاب إلى اب أحد البنات لطلب الزواج من ابنته, وسوف أحاول في هذا المقال توضيح بعض أسرار هذه المقابلات وبعض التجارب التى مررت بها من قبل وماهي أهم التحليلات التى وصلت إليها من خلال أجراء هذه المقابلات.

النصيحة الأولى التى سوف أقدمها لك هي أكثر من المقابلات الشخصية أكبر قدر ممكن حتى لو كان المنصب ليس لك أو حتى لو لم تكن جاهزا لمثل هذه الأعمال فكلما دخلت إلى مقابلات كلما سهل الأمر عليك وزادت فرص حصولك على وظائف في مقابلات شخصية آخرى فالمقابلة تمنحك خبرة المقابلات ونوعية الأسئلة التى تطرح عادة, لذلك ضع هذا الأمر في أعلى القائمة وابدأ البحث عن مقابلات وأطلب من أصدقائك القيام بعمل لجان وهمية لكي يختبروك وتختبرهم فيما بعد.أما النصيحة الثانية فهي تتعلق بطريقة إجراء المقابلة نفسها فلو أستثنينا الشركات الكبيرة جدا والمنظمة في مقابلات العمل لوجدنا أن الأشخاص الذين يقابلوك صنفان الأول جاهل لايعلم ماذا يسأل والثاني خبير ويعلم تماما عن ماذا يبحث وماهي الأسئلة التى يجب طرحها, لكن من حكم تجاربي وهي على فكرة ليست بالكثيرة, وجدت أن كلا الصنفان يرغبان بسماعك تتحدث عن نفسك أكثر مما يرغبان بسماع أجوبتك وبكلام آخر: المقابل يريد أن يحدد أمكانياتك ويريد أن يرى مدى فهمك لما درسته ويرى كيف تحلل الأمور العلمية بدون أجوبة أكاديمية لذلك تجد الكثير من الأسئلة حول فسر هذه العملية أو أشرحها والخ . . . وأنت يجب أن تعطيه هذه النقطة من خلال مناقشته أحيانا بالسؤال نفسه فلو وجدت سؤال غير منطقي أو سؤال طرحه غير صحيح فحاول إيصال هذا الأمر للشخص المسؤول بطريقة بسيطة وغير مباشرة وقد وضحت هذا الأمر على المدونة بمقال طرحت فيه أجوبة لبعض اسئلة المقابلات الشخصية. أما النصيحة الثالثة والتى أفضلها كثيرا هي الأمساك بالمقابلة نفسها, فكما ذكرت مسبقا أن المقابل يرغب عادة بسماعك تتحدث بنفسك وأنت ألتزم بهذا الأمر وكن على أستعداد لكي تتكلم عن كل مافعلته وتعلمته في عالم الشبكات لكن يتوجب عليك أن تتدرب على الأمر وتعلم كيف تنتقل من موضوع إلى آخر بحيث يبقى الشخص المقابل لك عبارة عن مستمع وأنت تتحدث بالأمور والنقاط التى تريد الحديث بها, وهذا ماكان يحدث معي كثيرا, بل أن لا أنتظر من المقابل أن يبدأ أسئلته الجاهزة وأجعل الأمر نقاش بيني وبينه.

أما التجارب التى مرت معي فكما ذكرت ليست كثيرة لكن سوف اذكر لكم بعضها, وسوف ابدا بأسوء مقابلة لي عندما أتصلت بي شركة كبيرة جدا في قطر وطلبت إجراء مقابلة معي في اليوم التالي لكن الصدمة الكبيرة أن المقابلة على الهاتف وهذا آثر علي وعلى أسلوبي في المقابلات فأنا أحيانا أفضل ان يكون لدي ورقة وقلم أحيانا لأشرح وخصوصا أن متأثر بعض الشيئ من عملي كمدرس في مجال الشبكات. أتصل بي في اليوم التالي شخص من أجل المقابلة والصدمة الثانية كانت أيضا مباشرة فالمقابلة باللغة الأنكليزية وأنا كنت حينها قد وصلت إلى قطر حديثا ومازالت لغتي الروسية هي اللغة الأم, وطبعا لم أكن سيئا جدا باللغة وبالكلام لكن الذي جعلني أنصدم هو لكنة المقابل فهو بريطاني الأصل ويتحدث لغة أنكليزية ثقيلة بعض الشيئ مما جعلني لا افهم أسئلته في بعض الأحيان وطبعا المقابلة لم تمر بالشكل الذي اردته على الرغم من بساطة الأسئلة المطروحة, وأذكر أيضا مقابلة أجريتها كانت الحقيقة مع شخص ضعيف جدا في أسئلته وفي فهمه لعالم الشبكات فلقد كان الـ IT Manager في الشركة وهو لايحمل CCNA ودار حينها بيننا حديث جميل وبدون أي أسئلة وأنصب الأمر عن الحديث عن التقنيات والشبكات ومفاهيمها العامة ونجحت في المقابلة لكن عرضه لم يعجبني. ومن فترة ليست بالبعيدة كنت أنوي بدأ العمل في شركة أمن وحماية وكنت حينها ذاهب لكي ننهي كل الأمور بيننا ونحدد موعد بدأ العمل لكن مدير الشركة فأجاني بمقابلة لم تكن على البال وعلى الخاطر فلقد جلب لي أثنان من الهنود وطلب منهم إجراء مقابلة لي لتحديد إمكانياتي لكن الذي جعلني أتجاهل هذا التصرف الغير متوقع من المدير هو ملاحظتي أن المهندسان الهنديان تفأجا مثلي من طلبه مما جعلني أسيطر على المقابلة من أولها حتى آخرها وكنت أحيانا أنا من يطرح عليهم الأسئلة لأحدد خبرتهم في مجال أمن الشبكات.

الحقيقة أنا أختصر كثيرا فالتجارب كثيرة ودروسها كثيرة ولن تتعلمها وتتقنها إلا لوجربت بنفسك, وقبل أن أنهي مقالي سوف أقول لكم ماهو أكثر شيئ جعلني أفشل في مقابلتي الأولى وهو عدم سؤالي عن ماهية الوظيفة وموقعها فالأسئلة دائما ما تتعلق بنوع الوظيفة وأنا حينها لم اكن خبيرا في هذا المجال وتعلمت درسا منها أتمنى أن تكونوا قد أستفدتوا من هذه النصائح وأن لاتنسونا من دعواتكم ودمتم بود

أيمن النعيمي - سوريا

حلول تأمين البيانات في مايكروسوفت
Data Security Solutions From Microsoft

في هذا العدد من المجلة سنتكلم عن حلول شركة مايكروسوفت في آمن البيانات سواء كانت على القرص ككل أو مجلدات وملفات موجودة على القرص الصلب او ثم أخدها إلى جهاز أخر وهنا أريد أن أقول ان هذا المقال لا يتكلم عن كيفية الأعداد وانما موضوع يتحدث عن عملية التخطيط لتنفيذ هذه التقنيات ..

في البداية نريد ان نقول ان أول خطوة في تصميم وتخزين وآمن البيانات هي اختيار طريقة الآمن التي ستستخدمها من أجل حماية البيانات في الشبكة . وهناك مجموعة من حلول آمن البيانات متواجدة وكل حل مصمم من أجل أن يلبي حلول آمن محددة . على سبيل المثال هناك ميزة في Windows 7 و W2K8 تسمى بالـ BitLocker وهو مصمم من أجل حماية البيانات داخل قرص صلب تم سرقته أو على جهاز كمبيوتر تم اقلاعه من قرص صلب مأخوذ من جهاز آخر .

أو هناك حل آخر يسمى EFS (Encrypting File System) وهو حل يقدم طريقة بسيطة لتشفير البيانات على القرص .

أن مميزات حماية البيانات تختلف من ناحية التكلفة و التعقيد ، عموما يجب ان تعمل مراجعة للمميزات التي تقدمها كل تقنية وبعد ذلك تقرر ماهي متطلبات الشركة من ناحية الحماية ، وعامتا المتطلبات الأعلى لحماية البيانات ستؤدي إلى زيادة في التكلفة والتعقيد ويجب عليك المراعاة في متطلبات الآمن .

حماية البيانات في القرص عن طريق الـ BitLocker :

أن تقنية الـ BitLocker عبارة عن ميزة لحماية البيانات متواجد في W2K8 وتقدم تشفير للبيانات للقرص ككل ، والفائدة من هذه الميزة هي حماية البيانات على القرص حتى وأن تم سرقته أو تم تركيبة على جهاز أخر . وتقنية الـ vvvker مصممة للعمل مع الـ TPM وهي عبارة عن قطعة موجودة في الـ Motherboard موجودة في الأجهزة الحديثة وإصدارة الـ TPM يجب أن تكون 1.2 من أن تعمل مع الـ BitLocker . واذا كانت الإصدارة 1.2 غير متواجدة ، جهاز الكمبيوتر يستطيع أن يستفيد من ميزة الـ BitLocker اذا كان الـ BIOS يدعم القراءة من أجهزة الـ USB قبل عملية الإقلاع (Booting) .

تشفير القرص باستخدام BitLocker :

في نظام التشغيل W2K8 الـ BitLocker يعمل تشفير لأقراص النظام وأيضا لأقراص البيانات (في Windows Vista الـ BitLocker يستطيع تشفير فقط أقراص النظام عكس Windows 7) . ومن أجل تشفير قسم كامل ، هناك مفتاح تشفير (Cryptographic Key) يسمى FVEK (Full Volume Encryption Key) يستخدم . وهذا المفتاح

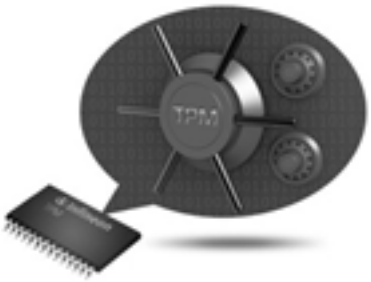
يخزن في البيانات التعريفة الخاصة بالقرص وهذا المفتاح يتم تشفير بمفتاح آخر يسمى (VMK (Volume Master Key . ومفتاح الـ VMK يتم أيضا تشفيره عن طريق الـ TPM اذا كانت موجودة أو عن طريق مفتاح إقلاع مخزن داخل USB تم إدخاله اثناء عملية الإقلاع .

مشاكل الأداء المتعلقة بالـ BitLocker :-

نظم تشغيل Win7 ، Vista ، W2K8 يقوموا بتشفير وفك تشفير قطاعات القرص على حسب حجم البيانات الموجودة ، وبهذا نستنتج أن الـ BitLocker يؤثر في أداء الجهاز لآن عملية التشفير تستهلك بعض من وقت المعالج . وهذا ايضا يتأثر بعدة عوامل منها الـ Hard Disk ، Caching Speed ، Processor Grade . لتعرف أكثر عن الـ BitLocker وكيفية تنفيذه يرجى التوجه لهذا الرابط http://technet.microsoft.com/en-us/library/97b4d762cf31-4957-b031-8ae6-c61f2a12

اختيار وضع المصداقة للـ BitLocker :-

تقنية الـ BitLocker تدعم أربع طريق مفصولة لعملية المصداقية Authentication .



والوضع الذي تختاره يعتمد على قابلية عتاد الكمبيوتر وأيضا ومستوى الآمن المطلوب للكمبيوتر .

• الـ BitLocker مع الـ TPM فقط :- في هذا الوضع الـ BitLocker يستخدم قطعة الـ TPM فقط من أجل عملية فك مفتاح الـ VMK وقرائه القرص . مميزات هذه الوضع انه لا يطلب من المستخدم أي تدخل وايضا يحمي البيانات حتى وأن تم سرقة القرص ويحمى القرص من أي برامج ضارة (Malware) . وعيوب هذا الوضع انه لا يحمى البيانات اذا تم سرقة الجهاز بأكمله لآن الـ TPM ملتصق باللوحة الأم للكمبيوتر

• الـ TPM مع جهاز الـ USB : في هذا الوضع

، كلتا القطعتين TPM and USB يجب ان يكونوا متوفرين . من أجل تشغيل الكمبيوتر ، المستخدم يجب علية أن يقوم بإدخال الـ USB الذي يحتوي على المفتاح وبهذه الطريقة يتم التأكد من مصداقية المستخدم . مميزات هذا الوضع انه يتم حماية البيانات حتى وأن تم سرقة الجهاز كاملا (لآن السارق يجب علية إدخال الـ USB لتتم عملية المصداقية) . العيوب انها تتطلب من المستخدم أن يتفاعل معها كل مرة يتم فيها تشغيل الكمبيوتر .

• الـ TPM مع مفتاح الـ PIN :- هذا الوضع يتطلب الـ TPM ومستخدم يقوم بإدخال رقم سري كل مرة يتم تشغيل الجهاز . مميزاته انه يقوم بحماية البيانات حتى وان تم سرقة الجهاز بالكامل وايضا انه من السهل إدخال رقم سري عوضا عن جهاز الـ USB اثناء عملية التشغيل . وعيوبه نفس عيوب الوضع الذي في الأعلى وايضا أقل آمنن .

• جهاز الـ USB فقط : وهذا الوضع الوحيد الذي من الممكن استخدامه مع الكمبيوترات التي لا تحتوى على قطعة الـ TPM .وفي هذا الوضع المستخدم اثناء عملية تشغيل الكمبيوتر يجب علية ان يقوم بإدخال جهاز الـ USB الذي يحتوى على المفتاح من أجل فتح الجهاز . ومميزاته هي انه من الممكن استخدامه على كل الكمبيوترات التي تحتوى على BitLocker-Compatible BIOS . لكن عيوبه انه لا يقدم فحصل لسلامة البيانات .

النظر في تصميم وآمن الـ BitLocker :

أستخدم القائمة التي في الأسفل من أجل ان تساعدك على تحديد أختيار الـ BitLocker مع وضع مصداقية محدد وايضا ما هو نظام التشغيل الذي ستستخدمه .

• فقط الـ BitLocker يستطيع عمل تشفير للبيانات كاملتن داخل القرص بالكامل ومن ضمنها الـ Page File , Hibernation file , Registry , and Temporary files . اذا كنت تحتاج من ان هذه الملفات

تمنع من القراءة حتى ولو تم سرقة الكمبيوتر أو سرقة القرص الصلب أستخدم الـ BitLocker ولا تستخدم اي تقنية آخرا مثل الـ EFS

- اذا كنت تريد حماية البيانات المخزنة على كل الأقسام وليس فقط على البيانات المخزنة داخل أقراص النظام على سبيل المثال (C) ، يجب عليك استخدام الـ BitLocker على Windows 7 , Windows 2008 R2 , 2008 Server وليس على Windows Vista .
- اذا كنت تريد من الـ BitLocker ان يكتشف التغيرات على بيانات النظام مثل التي تحدث بسبب اصابة الجهاز ببرنامج خبيث Malware ، يجب عليك استخدام جهاز يحتوي على قطعة الـ TPM . ولا تستطيع اختيار وضع الـ USB فقط .
- اذا كنت تريد حماية الـ BitLocker عن طريق عاملين من عوامل المصداقية يجب عليك استخدام جهاز يحتوي على قطعة الـ TPM وبعد ذلك ممكن ان تستخدم الـ USB أو الرقم السري (PIN) من أجل المصداقية بالأضافة إلى الـ TPM .

التخطيط لعمل الـ EFS :

الـ EFS عبارة عن تقنية لتشفير الملفات مصنوعة داخل نظام التشغيل والتي تستخدم لعملية تشفير الملفات المتواجد على قسم مهيئ بنظام الـ NTFS عندما المستخدم أو برنامج يحاول الدخول على ملف تم تشفير بالـ EFS ، نظام التشغيل تلقائيا يحاول ان يطلب مفتاح لفك التشفير واذا نجحت العملية بكل بساطة يعمل على تشفير وفك التشفير من دون تدخل من المستخدم .

لكن عندما المستخدمون ليس لديهم صلاحية الدخول للملف المشفر اذا ليس لديهم صلاحية فتح ملف مشفر حتى وأن كان لديهم صلاحيات الـ Read Permissions على الملف .

EFS يعتمد على مفاتيح الـ Symmetric and Public Keys . ومن أجل دعم الـ Public Key Cryptography الـ EFS يستخدم الشهادات Certificates وأيضا زوج من المفاتيح .
في شبكات الـ Workgroup هذه الشهادات وزوج المفاتيح يخزنوا محليا في كل جهاز . ولكن في بيئة الـ Domain هذه الشهادات من الممكن أن تمنح من قبل الـ CA (Certification Authority) وتدار عن طريق الـ GPO (Group Policy Object) وهنا يستطيع المستخدم ان يقرأ ملفاته المشفرة وهو داخل على أي جهاز موجود في الـ Domain .

عندما الـ EFS ينفذ داخل الشركة مع الـ CA المستخدمين المعنين بأنهم DRA (Data Recovery Agent) يستطيعون ان يعملوا استعاده للملفات المشفرة الموجودة داخل الـ Domain .

عامتا مميزات الـ EFS انه يقدم طريقة سهلة لحماية الملفات من القراءة داخل القرص حتى وان هذه الملفات تم الدخول عليها من جهاز أخر . ولكن العيب الكبير في الـ EFS انه لا يحمي البيانات وهي ترسل عبر الكابل أو بيانات تم نقلها إلى مكان أخر . EFS ممكن أن يحمي البيانات فقط عندما تبقى على قرص NTFS .

عندما تخطط سياسة الـ EFS لشركة معينة ، انه من المستحسن تحديد التهديدات التي ممكن أن تصيب النظام ، وايضا كيف الـ EFS يتعامل مع هذه التهديدات ، وايضا هل ممكن عمل CA أو لا .

ومن أجل أن تخطط لعملية تنفيذ الـ EFS ممكن الاستعانة بالخطوات التالية :-

- التحقيق في قدرات تقنية الـ EFS .
- تقييم الحاجة للـ EFS داخل الشركة .
- التحقيق من إعدادات الـ EFS باستخدام الـ GPO (Group Policy Object) .
- تعريف انظمة الكمبيوتر ومن هم المستخدمين المحتاجين للـ EFS .
- تعريف مستوى الحماية التي تحتاجها . على سبيل المثال هل شركتك تحتاج أن تستعمل بطاقة ذكية Smart Card مع الـ EFS .
- تطبيق الـ EFS بشكل مناسب لشركتك باستخدام الـ GPO (Group Policy Object) .

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

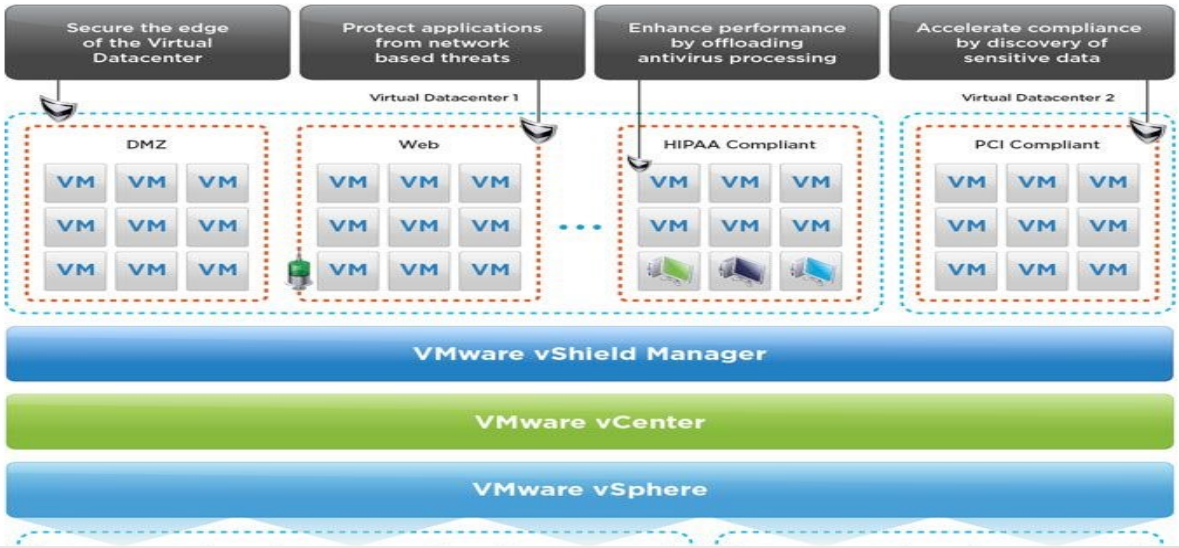
قناة المدونة على يو تيوب

قسم خاص بالأسئلة والاجوبة

الحماية فى عالم التكنولوجيا التخيلية
Security in virtualization Technology

تكلمنا فى مقالانا السابق عن تكنولوجيا الشبكات فى التكنولوجيا التخيلية . وتعرفنا من خلالها على اسلوب تعامل السيرفرات وانظمة التشغيل التى تعمل على سيرفرات تخيلية مع الشبكات من مكوناتها المختلفه (Cable – NIC – Switch – Router)وغيرها
وتعرفنا على انواع Switch's عند شركة VMware
وكنت انوى ان استكمل هذا الموضوع بالتعرف عن قرب على بعض الشركات التى تنتج Switch's تعمل على السيرفرات التخيلية مثل شركة سيسكو
لكنى وجدت انة لن يضيف شئ كبير للغالبية لانها تحتاج الى محترفى فى هذا المجال وذو خبرة فى مجال التكنولوجيا التخيلية
لذلك اجلت هذا الموضوع لمقاله قادمة ان شاء اللّه
وفكرت فى موضوع اخر اكثر اهمية واكثر طلبا واحتياجا للكل سواء كنت مبتدئ او خبير

وهو موضوع الحماية فى عالم التكنولوجيا التخيلية

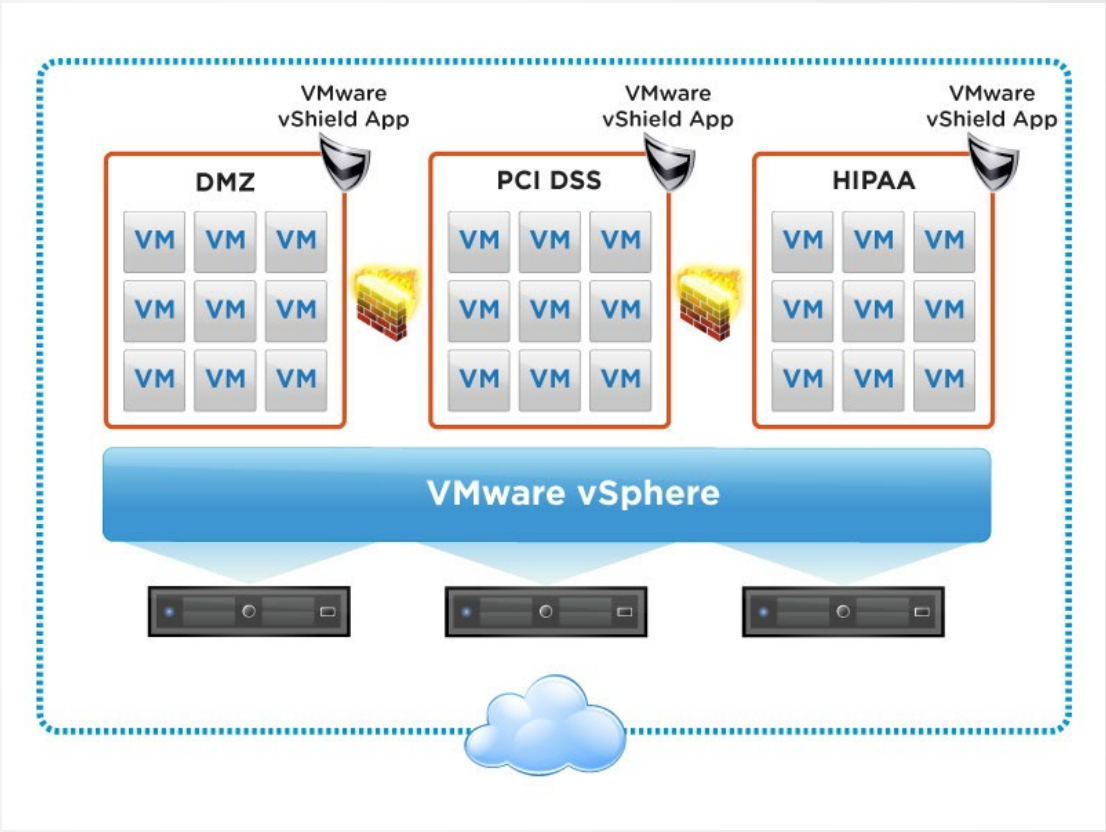


البعض سوف يتسال ما هذا العنوان الغريب وما معناه وهل يوجد شئ اسمة الحماية للتكنولوجيا التخيلية
اجيب علية بانة كما اتفقنا فى مقالنا السابق فى الشبكات التخيلية ان السيرفرات التخيلية ينطبق عليها كل شئ مثل اذا كانت هذة السيرفرات حقيقية

فعلى سبيل المثال اى شبكة تحتاج الى Firewall والى Antivirus. وهذا ما تحتاجة ايضا السيرفرات فى التكنولوجيا التخيلية نحتاج الى Firewall ونحتاج الى Antivirus لكنهم الاختلاف انها سوف تكون تخيلية مثل السيرفرات (انه عالم التكنولوجيا التخيلية)

على سبيل المثال Firewall لن يكون عبارة عن جهاز مثل السوتش يوجد فية مداخل للشبكة الداخلية والخارجية . وانما سوف يكون عبارة عن نظام تشتغيل يكون فى الاغلب لينكس وعلية تطبيق Firewall ويتم تحميلة على السيرفر الوهمى مثل VMware ESXi

ويسمى هذا الفيروول Appliance . وهوا يعمل مثل ال VM ومن داخلة نستطيع ان نربطة بالكروت الحقيقية الخاصة بالسيرفر الحقيقى ونربط بينة وبين ال VM ايضا ويقسمهم الى شبكات ويقوم بعمل Filters للاتصال بينهم والاتصال بالعالم الخارجى



صورة توضح الـ Firewall with VMware

اظن الموضوع اصبح شيق لكن يحتاج الى الكثير من التوضيح وفهم بعض المبادئ

اولا: لماذا نستخدم جدار نارى فى الشبكات ونحن نملك Firewall حقيقى؟

نجيب علية ان Firewall الخاص بالسيرفرات الوهمية يكمل Firewall الحقيقى الموجود وليس احداهما بديل عن الاخر Firewall تخيلى الذى يعمل على السيرفرات له وظيف اخر غير وظيفة Firewall الخارجى

كلنا نعرف ان Firewall الحقيقى دورة هوا حماية الشبكات الداخلية من عمليات الهاكرز لاقتحام الشبكة وايضا تنظيم الاتصال بالانترنت وتحديد اليوزر المسموح لهم فتح الانترنت وتحديد الصلاحيات لفتح مواقع معينة وغيرها وكل نعرف هذا الاشياء وغيرها عن ادوار Firewall العادى فى اى شبكة

اما Firewall فى التكنولوجيا التخيلية له دور اخر بمعنى لو فكرنا قليلا عندنا عدة سيرفرات تعمل VMware ESXi وبعمل على كل سيرفر عدة انظمة تشغيل وهمية VM هذه الانظمة تحتوى على تطبيقات وعلى داتا وغيرها مقدمة الى مستخدمين الشبكة

من خلال السطران السابقان نجد اننا عندنا مشكلتان فى الشبكات التخيلية:

1 - وجود اكتر من VM تعمل على سيرفر واحد
2 - اتصال المستخدمين الموجدين فى الشبكة الداخلية بالتطبيقات والداتا الموجودة داخل ال VM

ونوضح كل مشكلة وحلها:

1 - لو فكرنا قليلا فى العالم الحقيقى يكون كل سيرفر حقيقى يحتوى على احدى التطبيقات اذن كل تطبيق يكون على سيرفر منفصل لكن فى عالم التكنولوجيا التخيلية يوجد عدة سيرفرات فى صورة VM تعمل فى نفس الوقت على نفس السيرفر الحقيقى وهنا تظهر مشكلة فى ان كل هذا السيرفرات تتصل فيما بينهم بشكل داخل من خلال السوتش الوهمى الموجود على السيرفر ال ESX وهذا ممكن ان ياثر بالسلب على الاداء العام ونحن نريد ان نفصل بينهم ونحدد ال ports المفتوحة للاتصال بينهم فقط .

هنا بالطبع لن يفيدنا Firewall الحقيقى فى شئ لان VM فى النهاية على نفس السيرفر ولن يستطيع ان يكون فيما بينهم مثل السيرفرات الحقيقة

لذلك ياتى دور Firewall الوهمى فى الذى سوف يعمل فى صورة VM بجوار السيرفرات الوهمية الاخرى

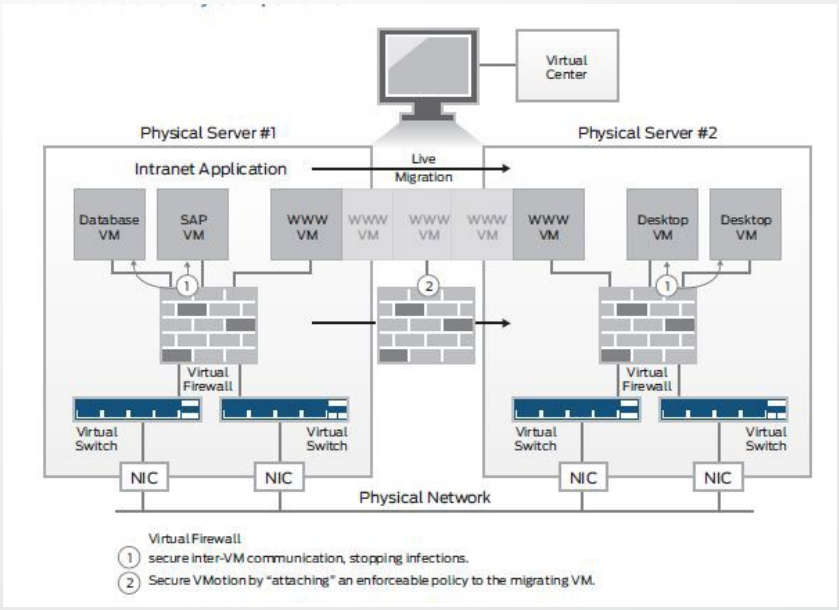
ويقوم بعملية Filter للداتا والاتصال بين هذة ال VM ويقوم بعمل تحديد لل Port وكل شئ مثل ما هوا موجود فى Firewall الحقيقى

2 - المشكلة الثانية التى يمكن ان تواجهنا هيا اتصال المستخدمين الموجودين بالشبكة الداخلية بهذة السيرفرات الوهمية بالطبع من اهم مبادئ الحماية فى اى شبكة هوا عمل Filter بين الداتا سنتر وبين اليوزر فى الشبكة الداخلية لعدم حدوث عمليات اختراق من الداخل (علميا عمليات الاختراق الداخلية اكثر من الهجمات من الخارج) ونريد ان نحدد ال Port التى تحتاجها التطبيقات التى تعمل الى السيرفرات الوهمية لكى تعمل عند المستخدمين لكى لا يحدث Traffic or broadcast بسبب ان كل ال ports مفتوحة بين الداتا سنتر والمستخدمين

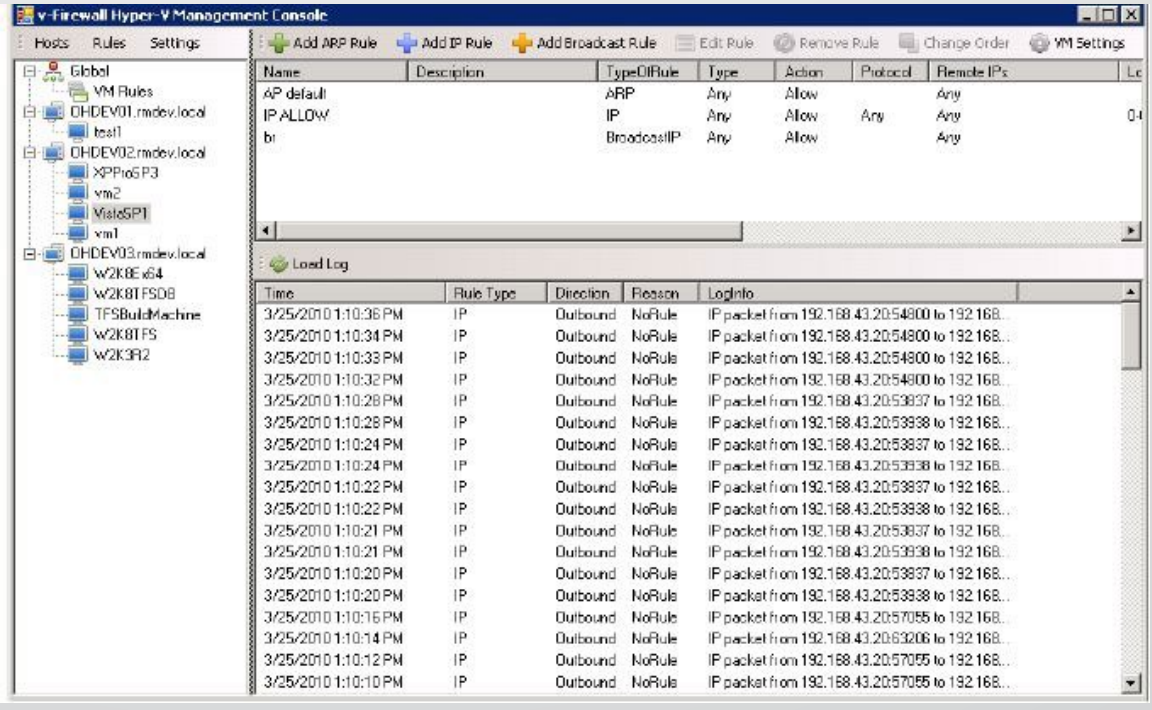
من خلال العمل لحل المشكلتان السابقتان يظهر لنا بوضوع اهمية Firewall فى التكنولوجيا التخيلية

فكرة عمل Firewall

فكرة عمل Firewall الوهمى بسيطة للغاية وهى عبارة عن ان Firewall يعمل على الطبقة الاعلى من الطبقة التى يعمل عليها السوتش الوهمى ويكون بين السيرفرات والسوتش ومن هنا يستطيع ان filter الداتا القادمة من السيرفر الحقيقى الى السيرفرات الوهمية او بين السيرفرات الوهمية بينها البعض .



مثال على ال Roles in Firewall with VM

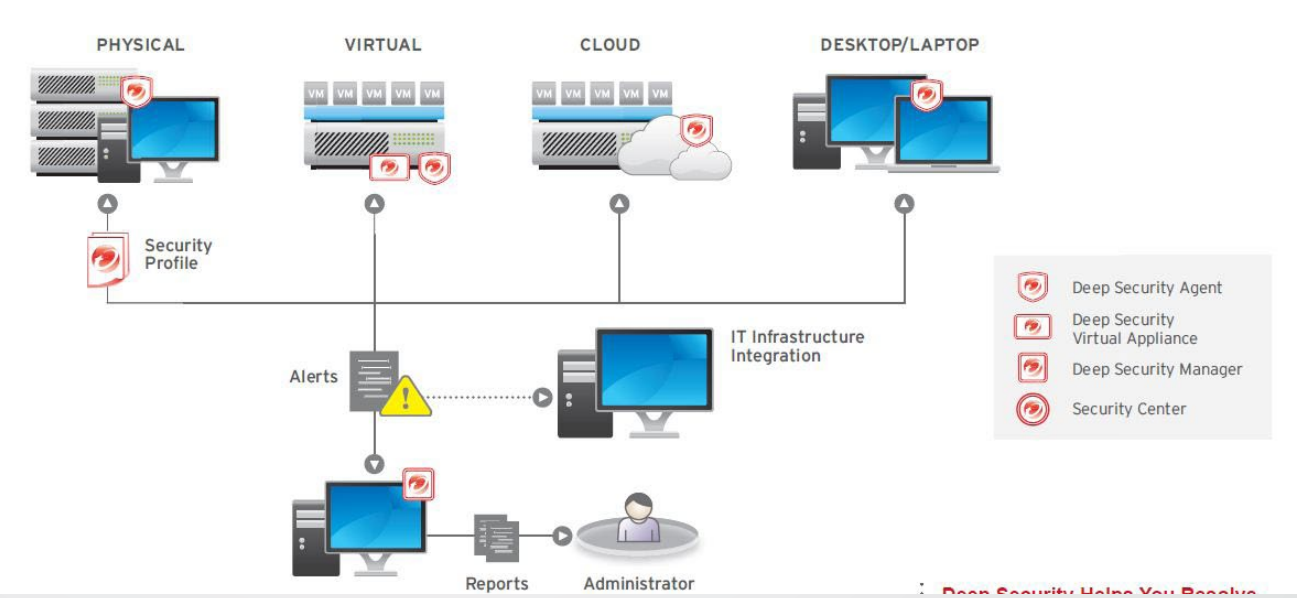


يوجد العديد من الشركات التى تقوم بعمل Firewall: سوف نتعرف عليها بايجاز

1 - VMware vShield يعتبر اقوى برنامج خاص بالحماية وعمل جدار نارى بين السيرفرات التخيلية وعمل فلترة للبرامج ايضا التى تعمل داخل السيرفرات
2 - Cisco ASA شركة سيسكو غنية عن التعريف وقامت بعمل فيروس تخيلى لحماية السيرفرات التخيلية
3 - Juniber VGW بالطبع نعرف وقامت فيروول ايضا
4 - Stone Gate تقوم بعمل جدا رنارى بالاضافة ال IPS and VPN
5 - 5nine الشركة الوحيدة التى تقوم بعمل جدار نارى خاص ب Microsoft HyperV

يوجد الكثير والكثير من الشركات التى قامت بعمل جدار نارى خاص بال VM

Antivirus فى التكنولوجيا التخيلية

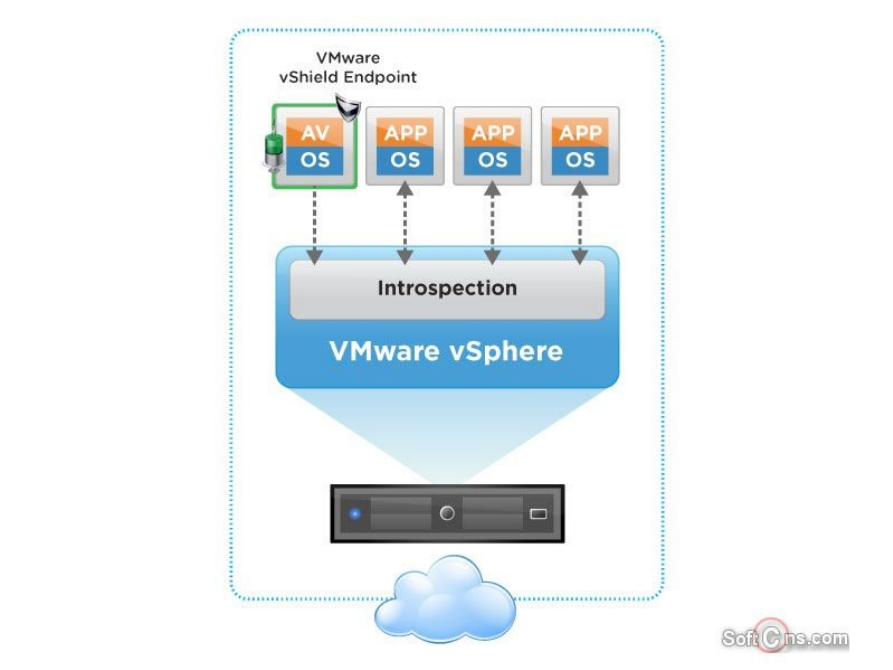


من منا لا يحتاج Antivirus على جهازة الشخص او السيرفرات . اذن سوف نحتاج Antivirus للسيرفرات الوهمية داخل ال VM
البعض يقول ما هى المشكلة اذن يمكننا ان نقوم بعمل اعداد Antivirus على اى سيرفر (كلام صحيح)
لكن يوجد مشكلة تواجهنا عندنا نقوم بتطبق موضوع ال VDI ونقوم بتحويل اجهزة اليوزر الى اجهزة VM داخل السيرفرات فى الداتا سنتر الخاصة بنا
المشكلة هنا اننا لو فرضنا اننا عندنا 100 مستخدم قمنا بعمل لهم100 VM لكى يعملوا عليها بواسطه تكنولوجيا ال VDI
(من لا يعرف ما هى VDI يمكن مراجعه موقع www.vmman.me سوف يجد مقاله تشرح هذة التكنولوجيا وكورس تعليمى لها)
اذن عندنا 100 VM تعمل على عدة سيرفرات ولو فرضنا اننا نريد ان نحمى هذة الاجهزة ونقوم بعمل Antivirus عليها لحمايتها من اى فيروسات تنتقل اليها سوف نقوم باعداد 100 نسخة Antivirus.
تصور عمل 100 Antivirus على سيرفر او اكثر ماذا سوف يحدث للاداء الخاص بالسيرفر وتصور ان البرنامج يقوم بعملية Scan عن فيروسات سوف يتاثر جدا اداء السيرفرات بهذة Antivirus لكثره عددها مما ياثر بالسلب على اداء ال VM التى تعمل عليها
والمشكلة هذه تسمى الى Antivirus Scan Storm
لذلك بحثوا عن حل لهذة المشكلة نحن نريد Antivirus لكن فى نفس الوقت لا نريد خسارة موارد السيرفرات فى عمليات الحمايةر
لذلك بداءت شركة VMware وشركات Antivirus فى عمل حل رائع لحل هذة المشكلة

وهوا عمل Antivirus رئيسى يعمل فى صورة VM ويعمل على السيرفر ويكون لهذا Antivirus الرئيسى Client داخل كل VM
لكن حجمها صغير للغاية ولا تستهلك اى شئ ولا تقوم بعمل اى Scan انما هيا تربط الاتنين ببعض فقط الانتى فيرس الرئيس يقوم بعمل اطار حول ال VM الموجود على السيرفرات ويراقب ويعمل Scan لكل داتا داخلة او خارجة من هذة الVM ويقوم بعمل Scan لها وبذلك نكون قد منعنا اى Virus من الدخول الى اى VM او الخروج منها لاصابة VM اخرى
وفى نفس الوقت لم يعمل سوى برنامج Antivirus واحد فى هذة العمليه على مستوى السيرفر ووفرنا موارد السيرفر

لتطبيق ذلك على ارض الواقع نحتاج الى برنامجين وهما :

1 - VMware vShield Endpoint
2 - Antivirus for VDI



يوجد عدة شركات تنتج Antivirus مخصص للتكنولجيا التخيلية اشهرهم:

1 - Trend micro deep security تعتبر او شركة انتجت Antivirus خصيصا لهذة التكنولوجيا وينصح باستخدامة
2 - MacAfee move من الشركات المعروفة ف عالم الحماية وانتجت برنامج مخصص لهذة التكنولوجيا
3 - Panda cloud تنتج هذة الشركة برنامج صغير جدا وخيف للغاية لكى يعمل على ال VM مباشرتا وهوا يختلف فى طريقة عملة عن الطريقة التى شرحناها

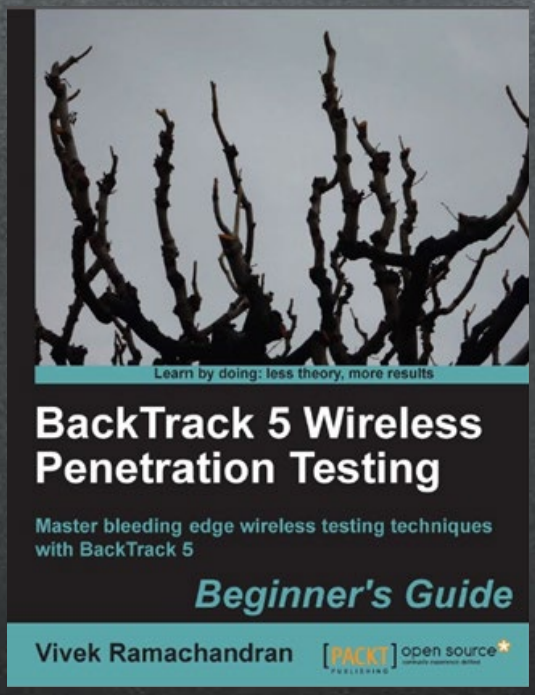
يوجد شركات اخرى بدات فى عمل Antivirus مناسب للتكنولوجيا التخلية وكل شركة حماية تتسابق لانتاج تطبيق مناسب لذلك لكى تاخذ قطعة من السوق المتنامى بقوة

بذلك نكون قد بدائنا خطواتنا الاول لعالم الحماية فى عالم التكنولوجيا التخلية . الموضوع بالطبع لم ينتهى هنا انما هو البداية فقط لان ببساطة هذة النكنولوجيا مازالت فى بدايتها وكل يوم سوف تتغير وتتطور فعلى كل مهتم بهذا العالم ان يتابعنا ويتابع هذا التكنولوجيا بشكل مستمر لان التطور كبير وسريع

كتاب أعجبني

إلى أعزائنا القراء ، إلى محبي أمن الشبكات .
أتنيا لكم اليوم لنعرفكم بأحد أجمل الكتب في مجال أمن وحماية الشبكات . وكتابنا اليوم يدور حول موضوع إختبار الإختراق او Penetration Testing.

إسم الكتاب :
Back Track 5 Wireless Penetration Testing
تأليف : Vivek Ramachandran
اللغة : الانكليزية
عدد الصفحات : 220 صفحة



ويسلط الضوء على إختبار حماية الشبكات اللاسلكية فقد أبدع فيه الكاتب ليكون أول مرجع لك للدخول في هذا المجال. والأجمل من ذلك أنه يتكلم عن إختبار الإختراق بإستخدام التوزيعة الشهيرة Backtrack .

ولاشك أن لكل مختص في الأمن الحماية يعلم بقوة الـ Backtrack وإذا كنت مبتدي وتريد التعرف على أختراق الشبكات اللاسلكية وأختبار الثغرات فإن هذا الكتاب هو مرجعك الأول .

قسم المؤلف هذا الكتاب إلى 9 فصول . في الفصل الأول يتحدث عن الأدوات اللازمة وتنصيب Backtrack وإعداده . كذلك تطرق لطريقة ربط الهاردوير مع الباك تراك مثل Wireless Adapter و Access point لبداية تجربة الهجوم .

أما في الفصل الثاني فيتكلم الكاتب عن تحليل الفريمات وعمل Packet Sniffing او تنصت لحزم البيانات . بعد ذلك تبدأ المعركة في الفصل الثالث وتبدأ عمليات الإختراق عندما يأخذك الكاتب معه ويتطرق لعملية تخطي بعض الحمايات وكشفت الشبكات المخفية وكسر حماية MAC Address وكذلك تخطي shared key .

الفصل الرابع !! تزداد الإثارة والحماس في هذا الفصل فستتعرف على طريقة كسر حمايات الشبكات اللاسلكية مثل WEP و WPA .

من ثم في الفصل الخامس يذكر الكاتب بعض التكتيات التي تحتاج لمعرفتها لتخطي حمايات الشبكات اللاسلكية فيعطيك نبذة عن Brute Force و Evil Twin والهجمة القاضية DoS Attack وهي أحد الهجمات الخطيرة والتي ما زالت ترعب الشركات. وبعد التعرف على الامور المهمة في الإختراق هنالك شي مهم سيتطرق له الكاتب في الفصل السادس وهو إستغلال الـ Client في عملية الإختراق ويعرفك كيف يتصل العملاء بالشبكة وكيفية خداعهم لإستغلالهم ومن هنا تفهم تكتيكات الإختراق أكثر . أما الفصل السابع فهو لا يقل أهمية عن الفصول السابقة فهو يركز على التكتيكات المتقدمة في الإختراق . والفصل الذي يليه ايضا متقدم لأن الكاتب يتحدث فيه عن ما يتعلق بكسر حماية WPA-Enterprise و Radius .

وبعد أن تعرفت مع الكاتب على طرق إختراق الشبكات اللاسلكية وأصبح لديك معلومات جيدة ، ينهي المؤلف كتابه بالفصل التاسع ويشرح لك أساسيات أختبار الشبكات اللاسلكية والمنهجية المستخدمة في الفحص .

تعرف على طريقة عمل فيروسات الحاسب

مقدمة

من منا لم يسمع عن الفيروسات من قبل وعن الأضرار التى تسببها يوميا سواء للأفراد العاديين أو الشركات المتوسطة وحتى الكبيرة ؟

اذا كنت مستخدم عادى للإنترنت فكل ما يهمك هو الإتصال بالإنترنت وتصفح جهازك للتنقل بين الملفات المتنوعة مثل الأفلام أو الألعاب ولكن فى بعض الأحيان يصبح جهازك أبطأ من المعتاد أو يغلق تلقائيا كل فترة أو يقف عن العمل فجأة (يتجمد) عندما تقوم بأمر معين .. بعض الأشخاص يظنون أن هذا شىء طبيعى وغالبا يلقوا باللوم على أن نسخة نظام التشغيل الموجودة على الجهاز قديمة ويعتقدون أن الحل فى تغيير نسخة نظام التشغيل ولكن ما ان تمر فترة من الزمن الا وتعاود نفس المشاكل فى الظهور مرة أخرى !

كل المشاكل السابقة توحى أو تشكك فى امكانية اصابة جهازك بـ فيروس فمثلما نستطيع أن نشخص الأمراض للانسان كالبرد والسعال ونأخذ الدواء المناسب لنعود الى حالتنا الطبيعية نستطيع أيضا تشخيص متى يصاب الجهاز بفيرس وما نوع الفيروس وكيفية علاجة .

قبل تشخيص نوع الفيرس وكيفية العلاج منه ينبغى علينا أن نتعرف على الفيرس بشىء من التفصيل ..

الفيروس كود خبيث صمم خصيصا للقيام بوظيفة تخريبية فى وقت محدد أو عند تفاعلك معه بطريقة مباشرة. من خصائص الفيروس أن بإمكانه التكاثر أو تكرار نفسه فى أكثر من مكان من نفس النوع كمثال: لنفرض أنك قمت بفتح ملف تنفيذى محمول بفيروس خبيث فسيتم تلقائيا تحميل الفيروس على باقى الملفات التنفيذية.أيضا من الشروط الرئيسية لوجود الفيروس وجود ما يسمى بالمضيف أو الهوست كـ فيروس الإنفلونزا كمثال عملى فلن يعيش الفيروس ويتنقل من شخص الى آخر الى فى حالة أصابة شخص ما بهذا الفيروس (شىء منطقى) .

بعد هذه المقدمة قد تشعر بالقلق بعض الشىء من أن فيروسات الحاسب شىء

ملموس وخطير حتى تشعر وكأنه كائن حى ! لن أخالفك الرأى فقد سبق وقال باحث فيزيائى يدعى «ستيفن هاوكينج: أن فيروسات الحاسب يجب أن تحسب على أنها كائنات حية لأنها تعكس الحياة الطبيعية لنا « ... دعنى أدعم كلام الباحث الفيزيائى بأن الفيروسات بالفعل لها دورة حياة تمر بها مثل الكائن الحى بداية من ظهورها وحتى تدميرها .

مراحل دورة حياة الفيروس

يمر فيروس الحاسب بسلسلة متتالية من المراحل بداية من ظهوره الى النور وحتى انتهاءه سواء تلقائيا أو عن طريق تدخل المستخدم . يمكن أن نسرد هذه المراحل فى 6 نقاط فقط :

1 - Design

أول مرحلة من حياة الفيروس مرحلة التصميم وهى المرحلة التى يتم فيها كتابة كود الفيروس بأى لغة من لغات البرمجة المعروفة مثل: (السى أو جافا أو بايثون أو روبى) أو الغير معروفة (لغة جديدة أو لغة غير مشهورة) وان كانت اللغات الغير معروفة هى الأنسب لكتابة الفيروسات لأنها تكون أصعب فى اكتشافها وتأخذ وقت أطول مثل فيروس (ستاكس نت الذى ضرب إيران عام 2010 وتسبب فى أعطال فى المفاعلات النووية لديهم) أو الفيروس الأشهر فى هذه الأيام (فيروس فليم أو «اللهب» الذى استغرقت شركات عملاقة فى محاربة الفيروسات وقت أطول من المعتاد فى الكشف عنه وتحليل طريقة عملة لايجاد العلاج له) .

2 - Replication

المرحلة الثانية وهى مرحلة التكرار , بمجرد إصابة جهازك بالفيروس فانه يقوم تلقائيا بتكرار نفسه على جهازك أو يتكاثر ان صح التعبير حتى يصيب أكبر عدد من الملفات ويكون له تأثير أقوى على الجهاز المضيف كمثال : إصابة كل ملفات الوورد بالفيروس وليس ملف واحد فقط , تعتبر هذه المرحلة هى الأهم بالنسبة للفيروس لأنه يتوغل أكثر فى ملفات الجهاز المضيف ويصيب أكبر عدد ممكن من الملفات وكلما تأخرت فى اكتشافه كلما زادت أضراره .

3 - Launch

مرحلة الإطلاق أو البدء وأسميها مرحلة الإشتعال , المرحلتين الأولى والثانية كانتا بمثابة عود ثقاب أشعلته وتسبب فى حريق كبير لاحقا .. أنت لا تعرف ان البرنامج الفلانى يحمل فيروس بداخلة يتربص لك فى انتظار الانطلاق وما ان ضغطت على البرنامج لتقوم بفتحه أو لعملية تنصيبه حتى يبدأ الفيروس فى الظهور الى العلن ويكشر لك عن أنيابه التى تكون على شكل رسائل خطأ متتالية من نظامك أو توقف الجهاز فجأه عن العمل ولا يستجيب لضغطاتك أو

فى أسوأ الأحوال يغلق جهازك تلقائيا وهذا يوحى بمؤشر خطير أن الفيروس قد انتشر كثيرا فى جهازك حتى وصل لملفات النظام نفسها وقام بتعطيلها !

Detection - 4

بعد المرحلة الثالثة سوف تجهز نفسك بالأسلحة اللازمة للقضاء على الفيروس من أهمها البحث عن برنامج مضاد للفيروسات قوى يقوم بعمل مسح كامل لجهازك واعلامك بالملفات المتضررة والموجود الفيروس بداخلها وهذه تسمى مرحلة الاكتشاف.

Incorporation - 5

مرحلة الإندماج أو الإلتحام وهى المرحلة التى يكون طرفاها الفيروس وبرنامج الفيروسات الخاص بك فبعد أن كشف برنامج مضاد الفيروسات لديك عن وجود فيروس غير مرحب به على جهازك حتى تبدأ المعركة ويستخدم مضاد الفيروسات كل الأسلحة المجهز بها لمحاولة تدمير الفيروس أو فى أضعف المواقف يقوم بإبطال مفعوله على الأقل حتى يوقف تأثيره الضار على جهازك وسوف أشرح لك فى نهاية الموضوع كيفية عمل برامج مضادات الفيروسات .

Elimination - 6

نهاية حياة الفيروس ... فى هذه المرحلة يتم القضاء نهائا على الفيروس وحذفه من على جهازك وغالبا يتم ذلك عند عمل تحديث لبرنامج مضاد الفيروسات لديك فعبد أن دخلوا فى عراك فى المرحلة الخامسة حتى ينهى برنامج مضاد الفيروسات المعركة لصالحة بتدمير الخصم وفى بعض الأحيان يكون الفيروس انتشر بشكل أعمق حتى تقل احتمالات نجاة الملف المتضرر لذلك يمكن أن يتم حذف الملف المتضرر كخسائر جانبية للمعركة.

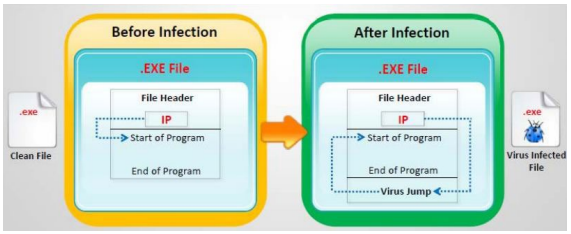
بعد أن تعرفت على مرحلة حياة هذا الشىء الدقيق المزعج تعالى لنتعرف أكثر على كيفية عمله أو كيف يصيب الملف من الداخل .

كيف يعمل الفيروس

فى المرحلة الثانية من دورة حياة الفيروس تحدثنا أن الفيروس ما ان يصيب جهازك حتى ويبدأ فى عملية التكاثر داخل الملفات ويستعد للانطلاق فىفالمرحلة الثالثة ولكنى لم أقل لك كيف يصيب الملف بشكل أعمق, يعمل أى فيروس على مرحلتين أساسيتين :

Infection Phase - 1

لنتعرف أكثر هذه المرحلة سوف نفرض أن الفيروس قام بإصابة ملف تنفيذى على جهازى والصورة التالية توضح شكل الملف قبل الإصابة بالفيروس وبعد الإصابة بالفيروس



عند تنفيذ جهازك لأى برنامج أو عند ضغط المستخدم على أيقونة البرنامج فعند التنفيذ يوجد فى داخل الملف ما يسمى بـ

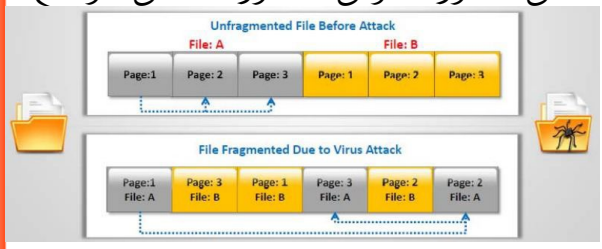
Instruction Pointer (IP)

أو مؤشر التعليمات وهو المسؤل عن ترتيب تنفيذ السطور البرمجية داخل البرنامج ... كمثال فى الصورة السابقة (اللون البرتقالى) قبل الإصابة بالفيروس فعند الضغط على البرنامج للتنفيذ يقوم مؤشر التعليمات بالقفر مباشرة الى كود بداية البرنامج وتنفيذ كاملا وفى النهاية يغلق البرنامج أم فى حالة بعد الإصابة بالفيروس (الصورة الخضراء) فعند تنفيذ البرنامج يقوم مؤشر التعليمات بالقفر مباشرة لتنفيذ كود الفيروس أولا ثم بعد ذلك يعود لتنفيذ الكود الأصلى للبرنامج لذلك أنت تقوم بإطلاق الفيروس فى كل مرة تنفذ فيها ملف مصاب.

Attack Phase - 2

رسائل الخطأ التى تظهر لك عند اطلاقك للفيروس بسبب أن الملف الذى قمت بتنفيذه أصبح متضرر وترتيب الأوامر بداخلة أصبحت متداخله وهذا ما يوضح أكثر فى الصورة التالية

فى الصورة الأولى (الصورة الأعلى) توضح



ترتيب الأوامر فى الملف قبل مرحلة الهجوم من الفيروس وتجد الترتيب صحيح ويتم تنفيذ الأوامر تباعا من الأولى للتانى وهكذا أما فى الصورة الثانية (الصورة السفلى) تجد أن ترتيب الأوامر اختلف بعد عملية الهجوم من قبل الفيروس ولذلك فى كل مرة تنفذ فيها الملف المتضرر يقوم بإظهار رسايل خطأ لك دليل على وجود خطأ داخل الملف فى ترتيب الأوامر .

قبل أن أنهى كلامى فى هذا الموضوع يهمنى أن تعرف كيف تعمل برامج مضادات الفيروس وكيف تقوم بإكتشاف الفيروسات وتدميرها .

طريقة عمل برامج الأنتى فيروس

كل فيرس جديد يتم اكتشافة يتم ادراجة فى مواقع خاصة بالكشف عن أخر الفيروسات واعطاءة رقم CVE يسمى الـ Common Vulnerabilities and Exposures أو الـ

وهو عبارة عن كود يصنف الفيرس على حسب الطريقة التى يعمل بها

فهناك فيروسات خاصة باصابة الملفات التنفيذية وأخرى خاصة بملفات النظام

يتم تجميع أرقام السى فى اى وتحديثها باستمرار فى ملفات تسمى ملفات الـ Signature

ومن ثم توزيعها على كل الشركات المصنعة للانتى فيرس

اذا كان عندك انتى فيرس فيجب تحديثة كل فترة زمنية قليلة أو ابقاءة متصل على الانترنت

ويستطيع أن يتعرف على الفيروسات عند عمل مسح للجهاز Signature حتى يجلب باستمرار أخر ملفات

اما اذا لم تحدث الانتى فيرس فعند عمل مسح للجهاز فيمكن أن يغفل بعض الفيروسات فى حالة وجودها لانه ببساطة لم يتعرف عليها أو اسمها ليس موجود عندة فى قائمة المطلوب القبض عليه .

الحديث عن فيروسات الحاسب كبير ويحتاج أكثر من موضوع ولذلك لى عودة بالجزء الثانى من الموضوع فى العدد القادم من المجلة بإذن اللّه .

تطبيق prefix-list في eigrp network وما هو الفرق باستخدام access-list

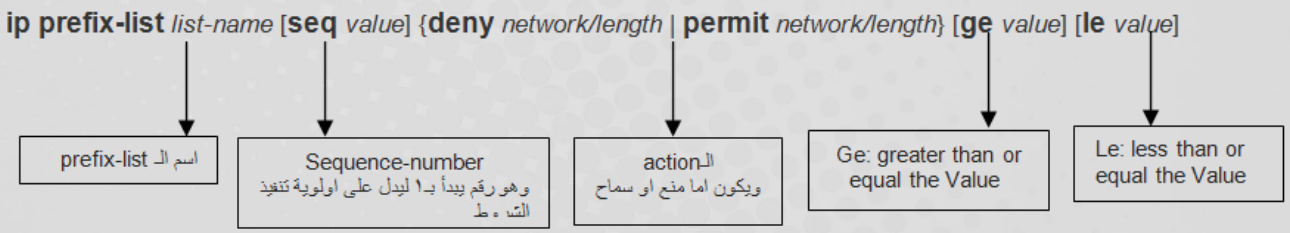
هناك الكثير من التساؤلات عن الفرق بين prefix-list وaccess-list مع ان كلاهما له نفس الغرض من حيث التعريف، حيث ان كلاهما يقوم بفلترة الـpacket و التأكد هل هي مرغوبة بالدخول الى الشبكة ام لا.

بالعودة الى الـaccess-list و كما هو معروف عند معظمنا ان هناك نوعان
Standard access-list
Extended access-list
و تعلمنا ان standard access-list تقوم بالنظر الى الـpacket اعتمادا على الـsource address فقط
اما مع extended access-list هنا تقوم بالنظر الى source and destination address كما انها تأخذ بعين الاعتبار ايضا عدد كبير من البروتوكلات، كما و تعمل على مستوى البورت ايضا.
لن اطيل الحديث عن الـ ACL لان معظمنا متمكن منها بشكل جيد كا فهم و تطبيق.

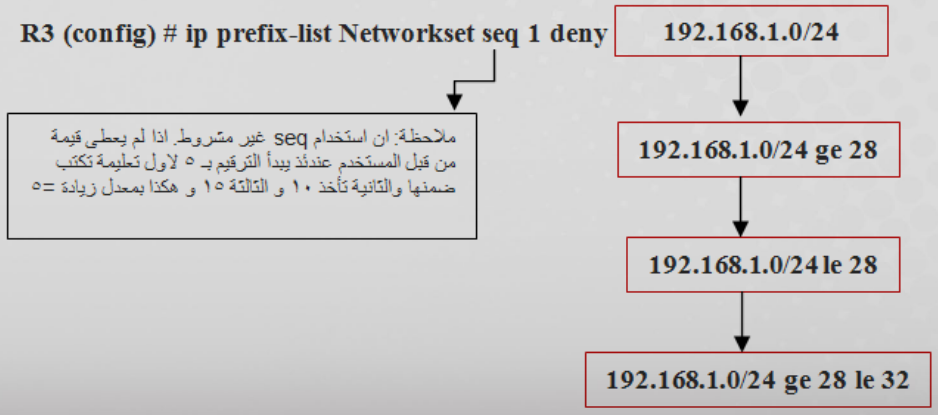
الان لنعرف المزيد عن prefix-list.
ابدأ بتعريف بسيط لهذه الاداة: وهي تقوم بعمل فلترة للـpacket بالنظر الى الشروط الواجب توافرها لتنفيذ الـ action بالمنع او السماح بالمرور، ونستطيع ان نستخدم شبكة واحدة او اكثرفي انٍ معا كما سوف نلاحظ.

ملاحظة: الشرح سوف يكون بالاعتماد على اجهزة سيسكو، إلا انني سوف اطرق باب اعدادها على اجهزة جونبر في المشاركات القادمة انشاء اللّه، لذا اقتضى التنويه.

الشكل العام للـprefix-list :
تكتب في الـ global configuration mode كالاتي



بعد ان تعرفنا على الشكل العام لنأخذ مثال يزيل بعض الغموض ان وجد:



الحالة الاولى: في هذه الحالة تبدأ prefix-list بمنع الشبكه من المرور بشرط ان يتحقق، التطابق في 24 بت و التطابق في الـsubnet mask وهو في حالتنا 255.255.255.0 . وهذا يقودنا الى القول انه في حال لم يوجد Ge or Le هذا يعني ان 24 في مثالنا تدل على عدد البتات الواجب النظر اليها و كذلك تمثل الـsubnet mask . الا ان هذا المعنى يختلف كليا في باقي الحالات.

الحالة الثانية: كما قلنا سابقا انه تبدأ prefix-list بمنع الشبكه من المرور بشرط ان يتحقق، التطابق في 24 بت و التطابق في الـsubnet mask وهو في حالتنا يجب ان يكون اكبر او مساوي 28 ، وهنا يمكننا القول انه و بمجرد استخدام Ge or Le يكون 24 يعبر عن عدد البتات الواجب النظر اليها فقط وقيمة الـ Ge and Le تعبر عن الـ subnet mask وفي حالتنا هنا يجب التطابق في 24 بت (X.192.168.1) و بالنسبة الى الـ mask تقبل جميع الـ subnet masks المحصورة بين 28-32 ضمنا اي (28-29-30-31-32).
نستطيع التلخيص بان prefix-list تقوم اولا بمقارنة عدد البتات المحدد و اذا تم التطابق سوف تنتقل لمقارنة الـsubnet mask واذا تم التطابق سوف تنتقل لتنفيذ المنع او السماح و هو في حالتنا هو منع الشبكة 192.168.1.0

الحالة الثالثة: تبدأ prefix-list بمنع الشبكه من المرور بشرط ان يتحقق، التطابق في 24 بت و التطابق في الـsubnet mask وهو في حالتنا يجب ان يكون اصغر او مساوي 28 وصولاً الى عدد البتات اي 24، لان القاعدة هنا تقول انه لا يمكن ان يكون الـsubnet mask اقل من عدد البتات التي نقوم بالنظر اليها للتحقق، في حالتنا تقبل جميع الـ subnet masks المحصورة بين 28-24 ضمناً اي (28-27-26-25-24).
بعد المقارنة تقرر prefix-list المنع او السماح اعتمادا على مقرنة عدد البتات و اللـsubnet mask

الحالة الرابعة: ايضا تقوم prefix-list بمنع الشبكه من المرور بشرط ان يتحقق، التطابق في 24 بت و التطابق في الـsubnet mask وهو في حالتنا يجب ان يكون اكبر او مساوي 28 واصغر او مساوي 32، في حالتنا تقبل جميع الـ subnet masks المحصورة بين 28-32 ضمناً اي (28-29-30-31-32).

كما ان هناك عدد من الحالات الاخرى مثل:

Permit/deny ANY

R3 (config) # ip prefix-list Networkset seq 1 permit 0.0.0.0/0 le 32

R3 (config) # access-list 1permit any

وهذا يعني ان جميع الـ ips و الـ subnet masks مقبولة و بالتالي السمح للـ all packets بالمرور.

Permit/deny default route

R3 (config) # ip prefix-list Networkset seq 1 deny 0.0.0.0/0

وهذا يعني ان منع الـ default route من المرور.

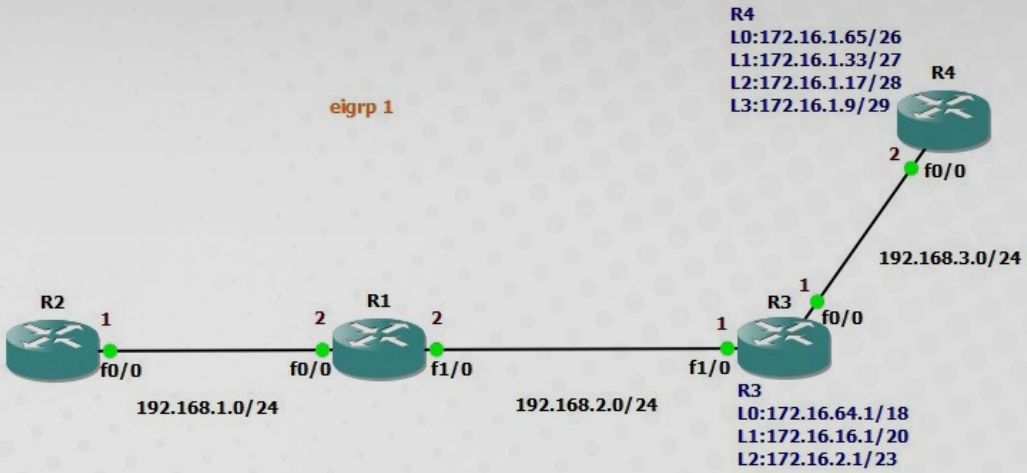
Permit/deny as per subnet mask

R3 (config) # ip prefix-list Networkset seq 1 permit 0.0.0.0/0 ge 25 le 28

وهذا يعني ان اسمح بالمرور لجميع الشبكات بغض النظر عن تطابق البتات و التي تحتوي على subnet mask بين ٢٥-٢٨ ضمناً.

القسم العملي (تطبيق prefix-list على eigrp network)

سوف اقوم هنا بتطبيق prefix-list على eigrp network من خلال Lab بسيط على الشكل التالي:



لنعتبر ان كل واحدة من الـloopback هي عبارة عن جزأ من شبكة متصلة بالراوتر ونريد تطبيق التالي
منع الشبكات 26/172.16.1.64 - 27/172.16.1.32 من الدخول الى الشبكة 24/192.168.1.0
نقوم بتطبيق الـprefix-list على الراوتر الذي يقوم بالاعلان عنها و هو في مثالنا R1

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip prefix-list Networkset seq 1 deny 172.16.1.0/24 ge 26 le 27
R1(config)#ip prefix-list Networkset seq 2 permit 0.0.0.0/0 le 32
R1(config)#
```

ومن ثم نعرف الـ prefix-list في الـeigrp

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#distribute-list prefix Networkset in
R1(config-router)#
```

الـ routing table للراوتر R2

```
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 5 masks
D       172.16.16.0/20 [90/158720] via 192.168.1.2, 00:33:38, FastEthernet0/0
D       172.16.1.16/28 [90/161280] via 192.168.1.2, 00:33:38, FastEthernet0/0
D       172.16.1.8/29 [90/161280] via 192.168.1.2, 00:33:38, FastEthernet0/0
D       172.16.2.0/23 [90/158720] via 192.168.1.2, 00:33:38, FastEthernet0/0
D       172.16.64.0/18 [90/158720] via 192.168.1.2, 00:33:38, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 192.168.1.2, 00:33:39, FastEthernet0/0
D    192.168.3.0/24 [90/33280] via 192.168.1.2, 00:33:39, FastEthernet0/0
R2#
```

و ايضا منع كل من الشبكات 18/172.16.64.0 - 20/172.16.16.0 - 23/172.16.2.0

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip prefix-list Networkset seq 1 deny 172.16.1.0/24 ge 26 le 27
R1(config)#ip prefix-list Networkset seq 2 deny 0.0.0.0/0 ge 18 le 23
R1(config)#ip prefix-list Networkset seq 3 permit 0.0.0.0/0 le 32
R1(config)#
```

الـ routing table للراوتر R2

```
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.1.16/28 [90/161280] via 192.168.1.2, 00:03:06, FastEthernet0/0
D       172.16.1.8/29 [90/161280] via 192.168.1.2, 00:03:06, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 192.168.1.2, 00:51:04, FastEthernet0/0
D    192.168.3.0/24 [90/33280] via 192.168.1.2, 00:03:06, FastEthernet0/0
R2#
```

الان بالعودة الى الوضع الافتراضي، حيث اني اريد منع الشبكات 26/172.16.1.64 في R4 و 23/172.16.2.0 من R3 ، يكون التالي:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip prefix-list Networkset seq 1 deny 172.16.0.0/16 ge 23 le 26
R1(config)#ip prefix-list Networkset seq 2 permit 0.0.0.0/0 le 32
R1(config)#
```

الـ routing table للراوتر R2

```
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 5 masks
D       172.16.1.32/27 [90/161280] via 192.168.1.2, 00:23:22, FastEthernet0/0
D       172.16.16.0/20 [90/158720] via 192.168.1.2, 00:23:22, FastEthernet0/0
D       172.16.1.16/28 [90/161280] via 192.168.1.2, 00:23:22, FastEthernet0/0
D       172.16.1.8/29 [90/161280] via 192.168.1.2, 00:23:22, FastEthernet0/0
D       172.16.64.0/18 [90/158720] via 192.168.1.2, 00:23:22, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 192.168.1.2, 01:28:31, FastEthernet0/0
D    192.168.3.0/24 [90/33280] via 192.168.1.2, 00:23:23, FastEthernet0/0
R2#
```

اخيرا كا جزء من المقارنة بين prefix-list و access-list ، اذا اردنا اعادة الاخير بستخدام access-list بكتابة امر واحد فقط، ولكي يشمل /26 و /23 يجب ان يكون بالصيغة التالية

R1 (config) #ip access-list 1 deny 172.16.2.0 255.255.0.0

ولكن هذا الامر تضمن جميع الشبكات على R4 و R3 و بالتالي تم تطبيق المنع على جميع الشبكات و ليس على المطلوب فقط، لذا سوف نكون مُجبرين على كتابة كل شبكة في سطر مستقل اذا اردنا استخدام access-list مما يزيد عدد السطور وبالتالي زيادة الحمل على الراوتر.

في العدد القادم سوف اتحدث عن Types of LSA based on OSPF انشاء اللّه.

في أقل من دقيقة حول جهازك إلى روتر وايرليس

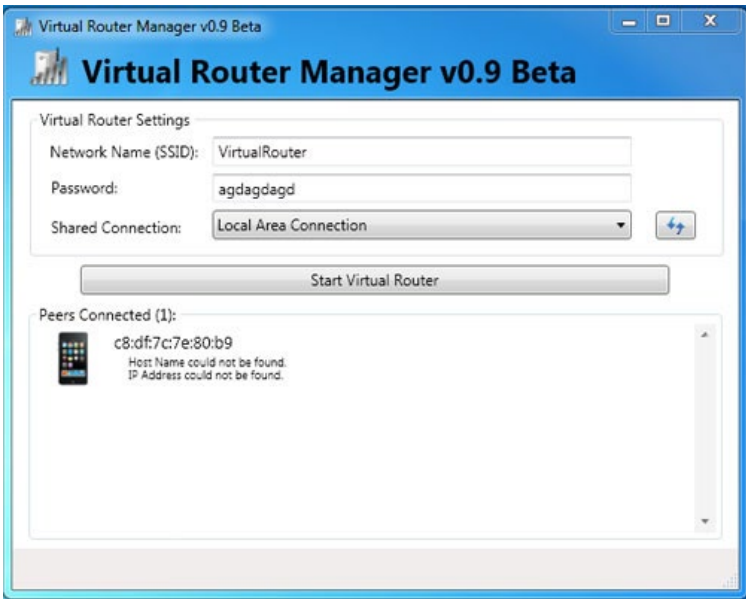
مقالي لهذا العدد سوف يكون عبارة عن طريقة لا أعلم كم بحثت عنها من الوقت لكن مر عام وأنا لا أجد طريقة مختصرة وبسيطة لتحويل جهاز المحمول إلى شبكة وايرليس تمكنني من مشاركة الأنترنت مع أجهزة آخرى والطريقة التى سوف أطرحها تعمل في أقل من دقيقة.

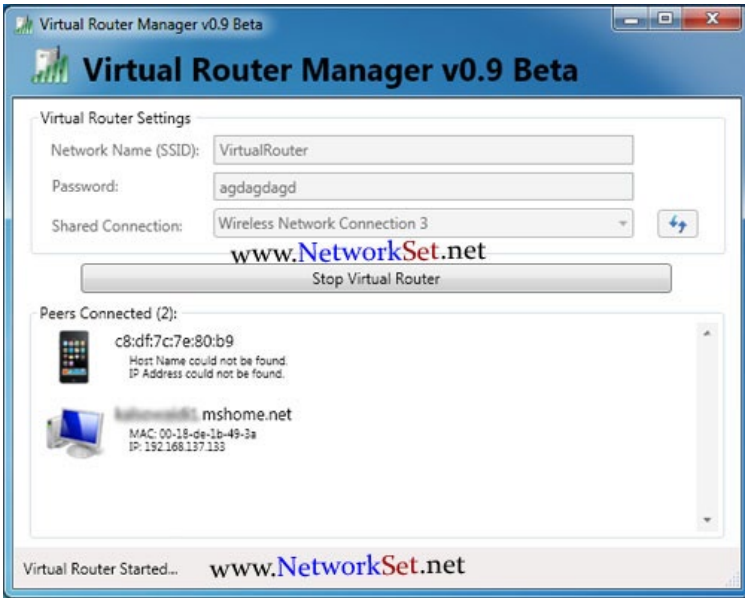
قد تكون هناك طرق موجودة ومدمجة مع أنظمة التشغيل التى تسمح لنا بتحويل الجهاز إلى شبكة وايرليس تشارك الأنترنت وهي طريقة تحتاج الكثير من الخطوات لكن مع البرنامج الذي سوف أطرحه في هذه التدوينة سوف تصبح قادر على تشغيل وتفعيل الشبكة في أقل من دقيقة من خلال برنامج يدعى Virtual Router.

يعتبر برنامج Virtual Router من البرامج المجانية وهو يعمل على أنظمة ويندوز 7 وويندوز سيرفر 2008 وهو يمكننا من تفعيل شبكة وايرليس بسرعة كبيرة لنقم أولا بتحميل البرنامج من الرابط التالي وبعدها نقوم بالتأكد من دعم البرنامج لكرت الشبكة الموجود لدينا من خلال هذه القائمة والتى وجدت فيها أغلب كروت الشبكة المعروفة لكن تأكد من تثبيت التعريف الآخير أو التعريف الموصى به من خلال القائمة السابقة.

بعد تحميل البرنامج قم بتثبيته وهو من النوع Next-Next-Finish وقم بتشغيل البرنامج لتشاهد معي نافذة البرنامج التالية

في المكان الأول قم بكتابة أسم الشبكة SSID وفي المكان الثاني ضع كلمة السر الخاصة بالوصول إليها وبعدها أختر كرت الشبكة المتصل مع الأنترنت وهو حتما سوف يكون كرت الأيثرنت لديك وبعدها Start virtual Router وأنتهي الأمر وبدأت الشبكة بالعمل,





نتجه إلى أحد الاجهزة الموجودة لدينا ونقوم بعمل بحث عن الشبكة ونكتب كلمة السر التى أخترناها ومبروك عليك الأنترنت.

إلى هنا أكون قد أنتهت وقد أعددتها لتكون مرجع لبعض المشاكل التى قد تواجه بعض المهندسين الباحثين عن حلول سريعة لمثل هذا النوع من المشاكل وبالمناسبة البرنامج يعمل تحت تشفير WPA2 وهو جيد نوعا ما لكن ليس آمن بشكل كبير كما يمكنك أستخدام هذه الشبكة مع أجهزة المحمول أو أجهزة التلفون الذكية والبلاك بيري

تقنيات سيسكو المكملة للمعايير اللاسلكية

CISCO Compatible Extensions Programs - CCX

الشبكات اللاسلكية تتغير وتتطور بشكل سريع جدا مقارنة بالمعايير التي تدعمها و كثير من البروتوكولات اللاسلكية تتعثر في ايجاد حلول لمشاكل مما تضطر الشركات المصنعة للأجهزة الي اللجوء الي حلول خاصة بها مكملة للنقص في هذه المعايير

و شركة سيسكو في مجال الشبكات اللاسلكية سباقة في هذا الأمر حيث تستطيع سيسكو ان تقوم بترقيع بروتوكول أو الإضافة اليه أو تطويره بدون انتظار تطوير المؤسسة التي تطلق المعايير و تسمي هذه التقنيات أو المعايير المكملة CCX CISCO Compatible Extensions Programs

و ليس هذا فقط بل إن سيسكو تجعل هذا المعيار مفتوحا مجانا لمن يريد أن يصنع أجهزته للتوافق معه حتي أصبحت تسعون بالمئة من الأجهزة اللاسلكية من خارج سيسكو تدعم هذه التقنيات المكملة و تقوم سيسكو بإطلاق مصطلح «جهاز متوافق مع سيسكو» علي الأجهزة التي تدعم هذه المعايير المكملة و تستطيع الإستفادة منها

فعلي سبيل المثال لو أن هاكر قم بإنتحال صفة عنوان فيزيائي MAC لأكسس بوينت ثم قام بنشر فريمات مزورة تجبر الأجهزة علي ترك الإتصال بالأكسس بوينت الأصلي disassociation

فمن المعروف أن عائلة بروتوكولات IEEE 802.11 ليس من ضمنها أي توصيف لتشفير أو حماية رسائل disassociation و لذلك و مؤقتا قامت سيسكو بتطوير نوع جديد من الفريمات لحماية تزوير رسائل disassociation

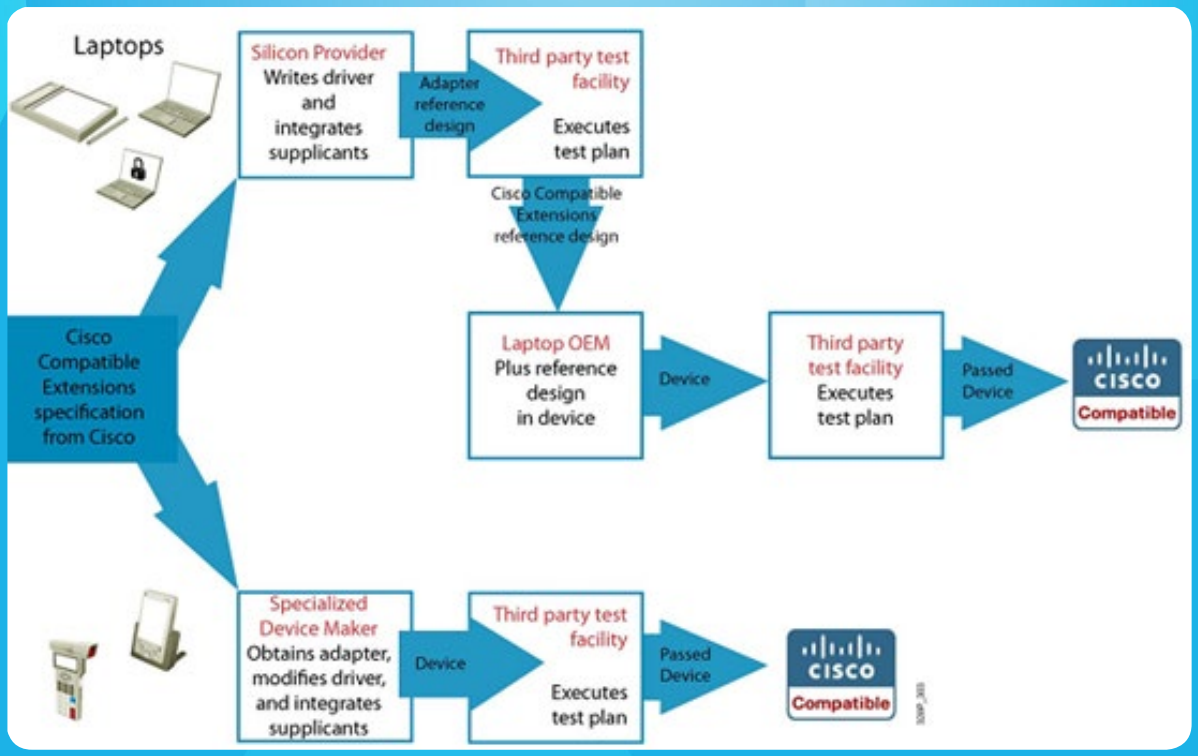
WIFI Tags

و ليس هذا فقط بل قامت سيسكو بجعل أجهزتها تتوافق مع أجهزة WIFI Tags أو ما تسمي بـ RFID Radio Frequency Identifier و هي أجهزة لاسلكية تعمل بمعايير 802.11 و لكل منها عنوان فيزيائي محدد MAC و لكن لها وظائف مختلفة عن أجهزة الشبكة اللاسلكية فهي تستخدم لإرسال معلومات عن البيئة التي صممت فيها فمنها ما يستخدم لإرسال بيانات عن حالات الطقس و منها ما يستخدم في السيارات أو المحطات لبيان مستوي الوقود أي أنها في كل الأحوال مجرد indicator
و بالطبع فإن هذه الأجهزة لا تستطيع العمل الا من خلال استخدامها للبنية التحتية للشبكة اللاسلكية و لقد قامت سيسكو بتسمية توافقها مع هذه الأجهزة بـ CCX for RFIDs

CISCO COMPATIBLE

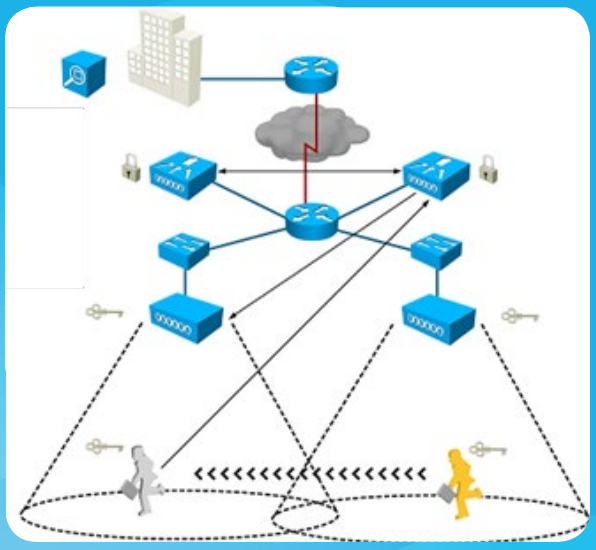
و بالنسبة لسيسكو فإن الأجهزة الموجودة في الشبكات من غير سيسكو يطلق عليها مصطلح third party و هو مصطلح عائم و نسبي تطلقه شركات تكنولوجيا المعلومات و الإتصالات علي تلك الأجهزة الموجودة في شبكتها و التي لا تنتمي اليها

كذلك تطلقه شركات تصنيع البرامج علي تلك البرامج المكملة لأداء برامجها و قد بدأت بالتعرف علي ذلك المصطلح أيام دراستي للغة البرمجة MS Visual Basic 6 حيث كانت تطلق علي أدوات OCX المصنعة من خارج ميكروسوفت
و عموما تلعب سيسكو دور رئيسي في هذا الأمر حيث ذكرنا أنها تقوم بمشاركة هذه الشركات بالمعايير التي كملتها سيسكو و بدون أي تكلفة و في حال تأكد سيسكو من أن أجهزة هذه الشركات استطاعت أن تستخدم هذه المعايير المكملة بشكل كامل فإن سيسكو تطلق عليها أجهزة متوافقة مع سيسكو CISCO Compatible و ذلك بعد اختبارات معتبرة لهذه الأجهزة يبينها الشكل التالي



و سنبدأ ببيان بعض التقنيات التي أكملتها سيسكو و رقعت بها معايير و بروتوكولات الشبكات اللاسلكية و تبعتها كثير من الشركات التي توافقت تقنياتها و أجهزتها مع هذه الترقيعات

CISCO CENTRALIZED KEY MANAGEMENT

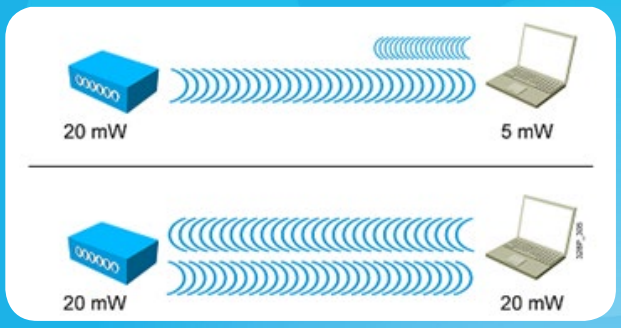


من أحد ميزات CISCO Compatible Extensions Programs هو استخدام خاصية في أجهزتها تسمي مفتاح التحكم المركزي CISCO Centralized Key Management

فعلي سبيل المثال عند استخدام سيرفر لتوثيق دخول الأجهزة الي الشبكة اللاسلكية يعمل ببروتوكول IEEE 802.1X فإنه تحدث مشكلة عند انتقال الجهاز من حيز أكسس بوينت الي أكسس بوينت آخر في نفس الشبكة بما يسمي عملية Roaming , فالجهاز متصل و موثق من قبل الأكسس بوينت الأولي و عند خروجه من نطاق اشارتها فإنه يفقد اتصاله بها و يبدأ في اعادة الإتصال بالأكسس بوينت الأخري و لن يسمح له الأكسس بوينت بالإتصال به حتي يقوم بمراجعة السيرفر و الذي سيقوم بالتأكد من صلاحية طلبه ثم يعطيه عنوان IP جديد و من ثم يتصل بالشبكة

و هنا تكمن المشكلة فرغم أن الجهاز قد عاود الإتصال الا أنه قد انقطع الإتصال أثناء انتقاله و هنا تكمن ميزة CCX من سيسكو فإنها تقوم بإستخدام مفتاح التحكم المركزي CISCO Centralized Key Management و الذي يسمح بعمل Roaming للأجهزة المتنقلة بدون فقدان الإتصال و اعادة الإتصال مرة أخري و ذلك بإستخدام كنترولر مركزي يقوم بالتحكم بأجهزة الأكسس بوينت و عدم الحاجة الي اعادة طلب الإتصال بسيرفر التوثيق

ضبط إعدادات القدرة للأجهزة
AP – Specified Maximum Power



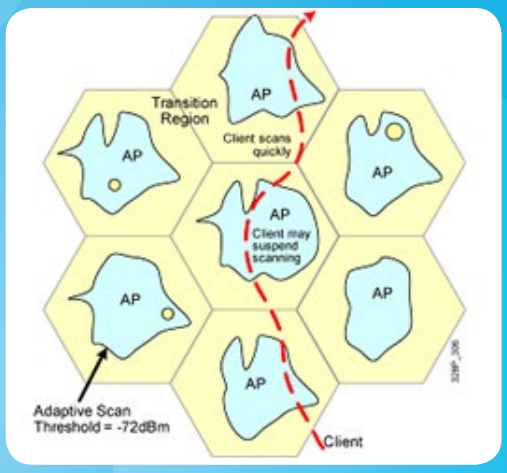
في الشبكات الغير متجانسة و التي يتم استخدام أجهزة كمبيوتر و IP phone و غيرها فإن تصميم الشبكات اللاسلكية يقابله مشكلة تنوع متطلبات الأجهزة و عدم امكانية توزان طلبات الإتصال علي الأكسس بوينت و هذا ينشأ عنه تنوع و اختلاف في القدرة المرسلة بين الأكسس بوينت و الأجهزة

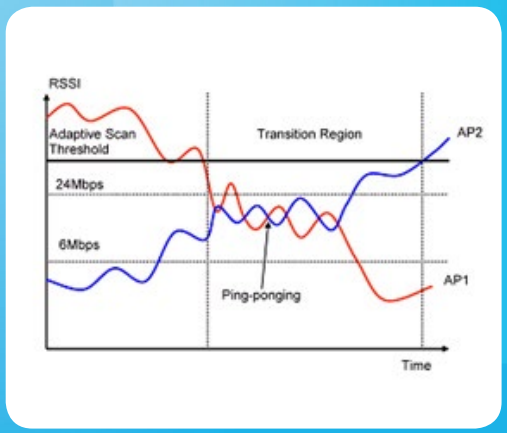
و هنا تحدث عدة مشاكل فبعض الأجهزة سترسل اشاراتها بقدرة كبيرة مما يجعل الأكسس بوينت يسمعها جيدا في حين تكون أجهزة أخري لها قدرة ارسال أقل من القدرة التي تصلها من الأكسس بوينت مما يجعل الإتصال يحدث من طرف واحد و في اتجاه واحد فقط و هو من الأكسس بوينت الي الجهاز
هناك سيناريوهات كارثية أخري فقد تكون قدرة بعض الأجهزة كبيرة جدا في الإرسال و هذا يجعل ارسالها يصل الي أكثر من أكسس بوينت مما يعطي أحقية تواصلها مع كل الأكسس بوينت مما يجعل الجهاز في حالة اتصال و انقطاع اتصال دائم أو roaming دائمة بين أكثر من جهاز

أو ربما يجعل تفاوت القدرة هذا في اتصال الجهاز بأكسس بوينت ليس في نطاقه المصمم له في حين ينقطع اتصاله من الأكسس بوينت

المفبروض أن يكون في حيز اتصاله
و هنا تخرج لنا سيسكو بتقنيتها المكملة – AP Specified Maximum Power و المنتمية الي CISCO Compatible Extensions Programs النسخة الثانية و الذي يقوم فيها الأكسس بوينت بضبط قدرة كل جهاز اوتوماتيكيا طبقا لموقعه و ايضا تحديد سعة خلايا الأكسس بوينت طبقا لقدرة الأكسس بوينت المرسلة و بهذا نتلافي كل هذه المشكلات

التخلص من ظاهرة Ping Pong
Removing Ping Pong Effect





أحد القضايا التي عالجتها سيسكو بتقنياتها المكملة خصوصا النسخة الرابعة و الخامسة من CISCO Compatible Extensions Programs هي ظاهرة Ping-Pong و هي ظاهرة تحدث عندما يكون الجهاز علي حافة خليتين لجهازي أكسس بوينت و تتساوي عنده اشارتي الأكسس بوينت مما يجعله يتأرجح في الإتصال و انقطاع الإتصال بين الخليتين

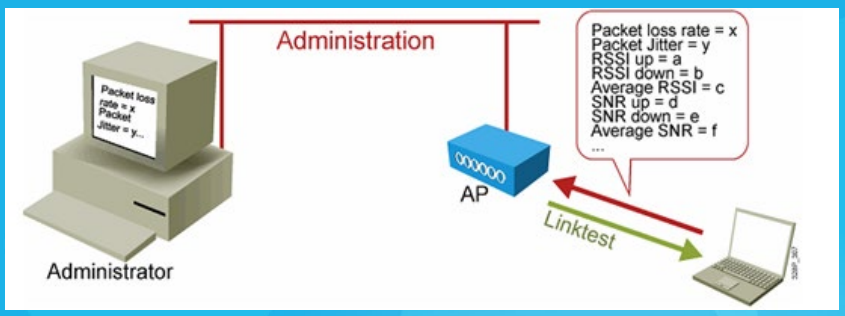
و لحل هذه المشكلة فإن سيسكو منعت الجهاز من الإتصال مباشرة بأي أكسس بوينت بمجرد وجوده في حيزه اللاسلكي و لكنه سيقوم بالتصنت الي كافة أجهزة الأكسس بوينت أولا ثانيا سيقوم كل أكسس بوينت بالتعرف علي الأكسس بوينت المجاور له و يقوما «بترسيم الحدود» طبقا لقدرة كل منهما و يكون لكل أكسس بوينت دولة تسمي inner region و سيعتبر أي منطقة خارج دولته علي أنها outer region

و تكون inner region هي المنطقة التي تصبح قيمة الإشارة RSSI تتعدي مستوي الإشارة العتبية و التي تصلح لإلتقاطها من قبل أي جهاز , و في هذه المنطقة لن يسمح الأكسس بوينت بعمليات roaming لأي أكسس بوينت خارجي من قبل اي جهاز موجود به و يكون هو فقط المسؤال عن تحقيق الإتصال به و خدمته مادام في حيزه مما يجبر الأجهزة علي الإمتناع من مراسلة أكسس بوينت أخري

و أما Outer Region فهي المنطقة خارج الحدود الخاصة بالأكسس بوينت حيث تكون قيمة إشارة RSSI تقل عن القيمة العتبية المسموح للأجهزة بالإتصال بها و عند اقتراب الجهاز من حدود هذه المنطقة فإن الأكسس بوينت يخبر الجهاز بالسماح له ببدء عملية المسح scanning كي لا يضيع اتصاله

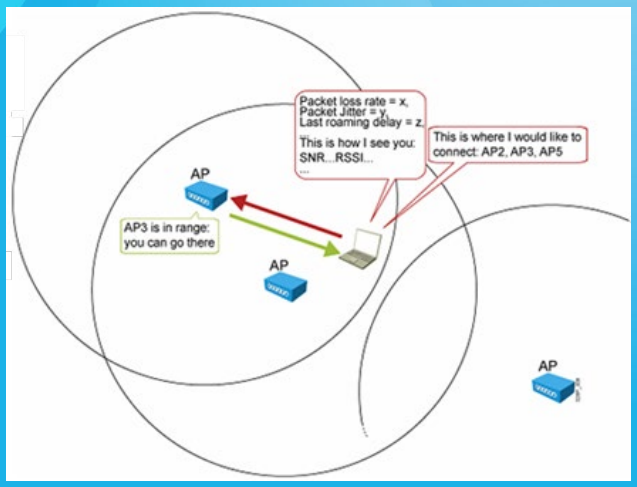
أما في حالتنا و التي سيظل الجهاز قريبا من حدود الخلية فإن الجهاز سيظل متصلا بالأكسس بوينت حتي و ان كانت اشارة الأكسس بوينت الأخري أكبر و ذلك لتخطي ظاهرة ping pong و عند التأكد من خروج الأكسس بوينت من منطقة الحدود و وصوله الي حيز الأكسس بوينت الأخري فإنه يتم اخباره بإمكانية الإتصال بها بشكل آمن و بدون أن نقلق من احتمالية عودة ظاهرة ping pong

فحص اتصال الأجهزة
Client Link Test



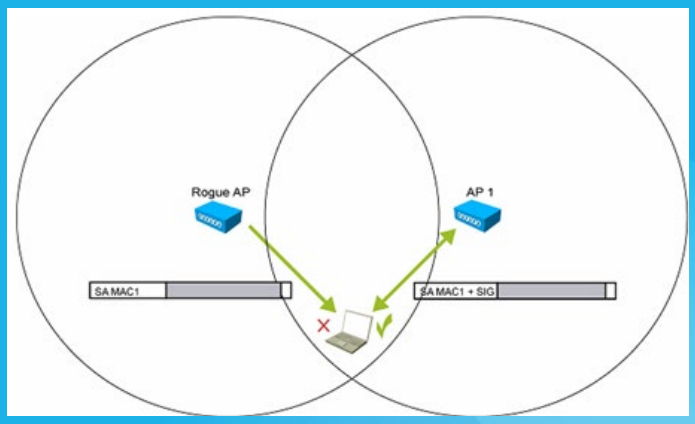
عندما تريد أن تختبر إتصال جهاز بأكسس بوينت فإنك تقوم بعمل ping و هذه الطريقة تخبرك بحالة الإتصال عن طريق اعطائك بيانات طبقة layer 3 أي طبقة Network في طبقات OSI و لكن المعلومات التي ستصلك قد تصلح لإختبار الإتصال السلكي و لكنها ليست كافية لإختبار الربط اللاسلكي لأن هناك معاملات لابد من معرفتها للحكم علي سلامة الإتصال و هي غالبها معاملات تقع في الطبقة الثانية التي تنتمي لها اصلا الشبكات اللاسلكية و هي Datalink Layer 2
و من هذه المعاملات مستوي الإشارة بالنسبة لمستوي الشوشرة Signal to Noise Ratio SNR و قوة الإشارة الواصلة Received Signal Strength Indicator RSSI و غيرها من الأشياء التي لابد معرفتها للتعبير عن مدي سلامة الإشارة اللاسلكية
و هذا ما تفعله النسخة الثانية من CISCO Compatible Extensions Programs و تقنيتها المكملة Client Link Test و التي تختبر الإتصال اللاسلكي عبر بيان لمعاملات الإتصال التي ذكرنا بعضا منها

تقارير دائمة عن الأجهزة
Client Reporting



في النسخة الثانية من CISCO Compatible Extensions Programs و تقنيتها المكملة Client Reporting فإن الجهاز مجبر علي إعطاء بيانات دوزرية عن حالة اتصاله و معاملاتها مثل حالة الباكت و تأخيرها Packet Loss و مدي التأخر في عمليات roaming كذلك يسمح له بالتعبير عن أجهزة الأكسس بوينت التي يفضل الإرتباط بها و التي في حيز اشارته
كا هذه المعاملات تمكن الشبكة اللاسلكية من عزل المشكلات التي تقابل الأجهزة و تبقي الأهمية القصوي لتلك المعلومات في حالة عمل اتصالات VOIP عبر الشبكة اللاسلكية

Management Frame Protection MFP
تشفير فريمات التحكم



في شبكات الوايرلس المعتمدة علي 802.11 تكون هناك فريمات البيانات data frames مشفرة encrypted و تكون فريمات الإدارة management frames غير مشفرة و هي مثل فريمات التوثيق و الربط و غيرها و هذا يجعل من الممكن اختراق الشبكة اللاسلكية
و لكن مع النسخة الخامسة من CISCO Compatible Extensions Programs و تقنيتها المكملة Management Frame Protection MFP فلقد تم تشفير بيانات و فريمات الإدارة بحيث يكون هذا النوع من لإختراق يعتبر شبه مستحيل
بل ان اكتشاف الأجهزة التي تحاول اختراق الشبكة اللاسلكية أصبح جزءا من بنية سيسكو اللاسلكية و أصبح وصم جهاز ما بكلمة جهاز دخيل rogue كافيا لمنعه من دخول الشبكة أو الإرتباط بها و هذا كله علي عاتق اجهزة الكنترولر و WCS في الشبكة

أجيال CCX

و في النهاية هذا هو ملخص لأجيال CISCO Compatible Extensions Programs مع بيان للتقنيات المكملة التي يدعمها كل جيل

	v1	v2	v3	v4	v5
Security	WEP IEEE 802.1X LEAP Cisco TKIP	PEAP-GTC WPA	WPA2 EAP-FAST	NAC (wireless) EAT-TLS PEAP-MSCHAP	Management Frame Protection for clients
VLANs and QoS	Multiple SSIDs/VLANs on AP	eDCF	Wi-Fi Multimedia (WMM)		
Voice over IP				U-APSD TSPEC CAC Voice metrics	Expedited bandwidth request
Mobility And Management		AP-assisted roaming Cisco Centralized Key Management with LEAP Proxy ARP information element	AP-assisted roaming Cisco Centralized Key Management with EAP-FAST Single sign on: LEAP, EAP-FAST	AP-assisted roaming Cisco Centralized Key Management with other EAP types AP-directed roaming Location Keep alive Link test	AP-assisted roaming Cisco Centralized Key Management enhancement Gratuitous probe Response Diagnostic channel Association Location service

بداية الطريق إلى عالم شبكات الـ SAN

حان الوقت للإبتعاد عن الزحمة . حان الوقت لنشق طريقاً جديداً .

وحان الوقت لنقدم شيئا جديداً للمهندس والدارس العربي . لقد سلطت ساحتنا العربية الضوء للحديث عن Routing & Switching والتعامل مع أنظمة مايكروسوفت وتمديد الشبكات اللاسلكية .

إننا دائما ما نهتم بأبسط الأشياء ونهتم ببناء شبكة تلبي إستخداماتنا البسيطة مثل مشاركة الملفات وإدارة المستخدمين .

إلا أن هنالك مواضيع كثيرة تفتقرها ساحتنا العربية وأنت بحاجة لمعرفتها لعمل تكامل بين معلومتنا في مختلف المجالات. فإرتأيت أنه من الضروري أن نتحرك لنثري محتوانا العربي لنخرج جيل عربي متعمق في عالم الشبكات وقادر على بناء شبكات ضخمة تلبي مختلف الإستخدامات .

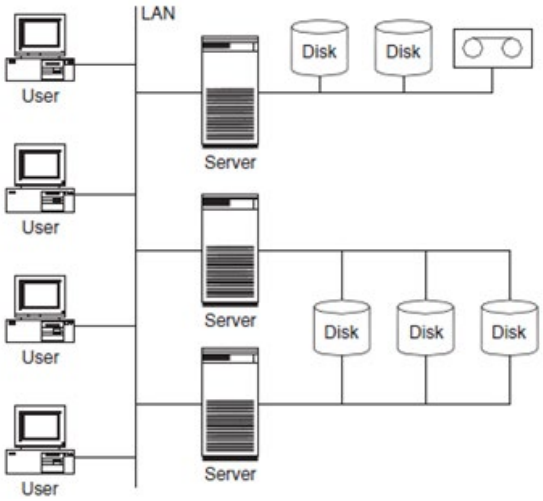
ومن هنا لقد جئتكم اليوم لأقدم لكم شيئا أغلبكم قد يكون سمع عنه إلا أنه لم يصادفه في حياته ولم يتطرق لأساسياته .

وموضوعنا اليوم يتحدث عن شبكات الـ SAN والذي سنتكلم فيه عن أساسيات بناء هذا النوع من الشبكات ليكن لديك فكرة جيدة عن طريقة عمل وتصميم هذا النوع من الشبكات فالموضوع طويل ومعقد فسأكتفي بذكر المفيد والمهم لك .

ما المقصود بشبكات الـ SAN ؟؟

SAN هي إختصار لـ Storage Area Network وهي نوع من الشبكات عبارة عن مجموعة من أجهزة الحاسب الآلي سواء كانت سيرفرات أو أجهزة العملاء موصلة مع وحدات تخزين تسمى Disk Array وتكون موصلة عن طريق كابلات عالية السرعة في نقل البيانات .

وإن عملية التوصيل هذه بهدف تخزين وحماية البيانات في وحدات منفصلة عن أجهزة الحاسب الآلي أو السيرفرات . والصورة التالية توضح بنية شبكات الـ SAN بشكل مبسط :



ما هي فوائد شبكات الـ SAN ؟؟

أن هذا النوع من الشبكات له عدة فوائد وهي كالتالي :

1 – توفر سرعة نقل بيانات عالية وذلك بإستخدام Fiber Channel والتي سنتلكم عنها .

2 – وحدات تخزين مركزية تسمح لعدة سيرفرات الوصول إليها في نفس الوقت .

3 – توفر حماية للبيانات وتمكننا من إستعاداتها وذلك بعزلها عن الأضرار التي قد تصيب السيرفرات.

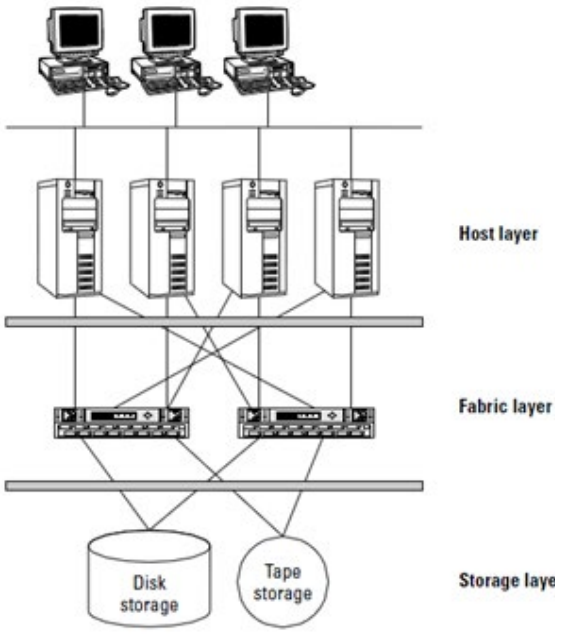
4 – تقلل من عدد السيرفرات فبدلا من وضع File Server لكل شبكة ، نضع وحدة تحزين مركزية.

5 – تسهل الوصول للبيانات والتطبيقات وتوفر لنا الوقت . على سبيل المثال يستطيع كل الموظفيين المتواجدين في مختلف فروع الشبكة تجربة التطبيقات والتعامل مع قواعد البيانات وذلك بالوصول إلى وحدات التخزين بدلا من التنقل بين الفروع .

6 – تمكنك من عمل إتصال في بين مختلف أنواع السيرفرات في الشبكة مثل ريدهات ، ويندوز ،...الخ.

معمارية شبكات الـ SAN ؟؟

تتكون معمارية شبكات الـ SAN من ثلاث طبقات وهي Host Layer والتي تمثل أجهزة العملاء والسيرفرات في الشبكة و الطبقة الوسطى Fabric Layer والتي توصل لحواسب والسيرفرات مع وحدات التخزين عن طريق Hubs, Switches, Routers, Cables والطبقة الأخيرة وهي Storage Layer والي تمثل وحدات النخزين . والصورة التالية توضح شكل المعمارية :



تقنيات شبكات الـ SAN ؟؟

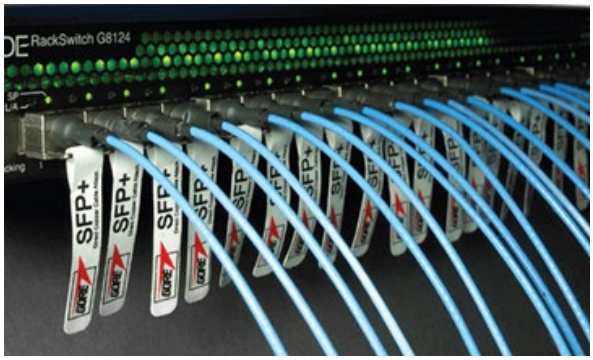
هنالك الكثير والكثير من التقنيات المعقدة في شبكات الـ SAN إلا أننا سنذكر الأساسي منها حتى لا نطيل في الموضوع وندخل في تفاصيلَ تبعدنا عن الأساسيات :

SCSi

SCSi هي إختصار لـ Small Computer System Interface وهي تقنية نقل بيانات من نوع Parallel .

وتستطيع نقل البيانات بسرعة أقصاها 160Mbps وبمسافة أقصاها 25 متر . وتعتبر هذه التقنية قديمة ولا تستخدم الان كونها تسمح بتوصيل عدد محدود من السيرفرات .

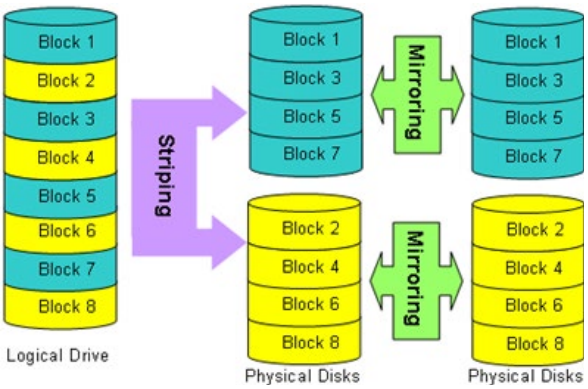
Fiber Channel



هو التقنية التي تمكننا من ربط وحدات التخزين مع السيرفرات بإستخدام كابلات الفايبر او الكابلات الضوئية والتي تسمح لنا بنقل البيانات بسرعة عالية جداً تصل إلى 10 Gbps وهذا ما يفيدنا لو كنا على سبيل المثال نقوم بتصوير مؤتمر بالفيديو ونريد نقله مباشرتا إلى وحدات التخزين فسنحتاج إلى سرعة عالية جدا كون الفيديو كبير الحجم .

كما أنها تمكنت من نقل البيانات للمسافات الطويلة . وهي الأكثر شيوعاً وإستخداماً.

RAID



وهي إختصار لـ redundant array of independent disks وتعد هذه التقنية من أحد أهم التقنيات المستخدمة في السيرفرات وأجهزة حفظ البيانات فهي تقوم بعملية دمج عدة وحدات تخزين مع بعضها البعض ليس بشكل فيزيائي أو عن طريق الكابلات ولكن بطريقة منطقية مقسمة إلى عددة مستويات مثل RAID 0 و RAID 1 و RAID 5 ولكل واحد منها خصائصه فمثلا RAID 0 يقوم بزيادة سرعة النقل والأداء وذلك بتقسيم حزمة البيانات بين عدة وحدات تخزين حيث أن كل وحدة تأخذ جزء من البيانات لتحفظها وهذا يقلص من وقت الحفظ كون وجود عدة أقراص تشتغل في عملية الحفظ بدلا من واحد .

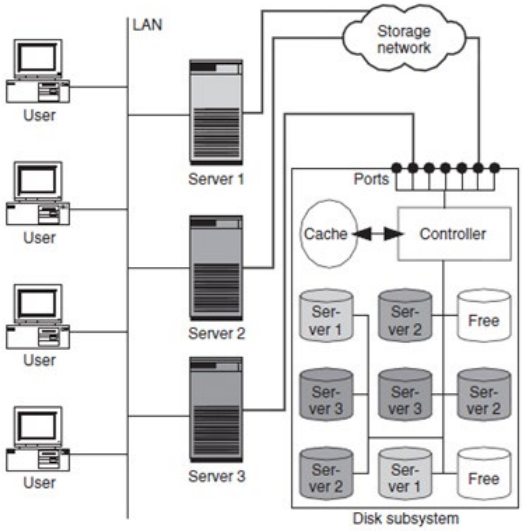
أما RAID 1 فهي تعمل عند تواجد وحدتيين تخزين أو أكثر فهي تقوم بأخذ نسخة إحتياطية من وحدة التخزين ونسخها للأقراص الأخرى بشكل كامل بهدف الحفاظ على البيانات من الضياع .

وهنالك خصائص أخرى أكثر تعقيدا في المستويات الأخرى حيث يمكننا دمج عدة مستويات مع بعض للحفاظ على البيانات من الضياع بشكل أفضل ولتسريع أداء النقل أيضا.

Disk Array

وهذه الأقراص تتوزع على السيرفرات فكل سيرفر يخزن بياناته في وحدة معينة . والجدير بالذكر أن هنالك وحدات تخزين تترك فارغة وذلك إذا إمتلئت أحد الأقراص فإن السيرفر يكون قادر على الإتصال مباشرتا بوحدات التخزين الفارغة وحجز مساحة حتى لا تضيع البيانات المتدفقة بعد أن إمتلئت وحدة التخزين الأساسية الخاصة به .

والصورة التالية توضح ذلك :



وكما ترى في الصورة السابقة يوجد هنالك Controller والذي وظيفته التحكم بتدفق البيانات . وكذلك يوجد Cache والذي كما تعلمون وظيفته تسريع عملية الطلبات التي نطلبها بشكل متكرر .
ففي المرة الأولى تستغرق وقت أطول لتنفيذ الطلب من المرات التي بعدها.

نصائح لبناء شبكات الـ SAN :

قبل الشروع في بناء الشبكة يجب عليك أن تركز على عدة أمور :

1 – السرعة التي تحتاجها تطبيقات شبكتك .

2 – إختيار الكابلات المناسبة مع التركيز أن كل الكابلات تحمل نفس السرعة .

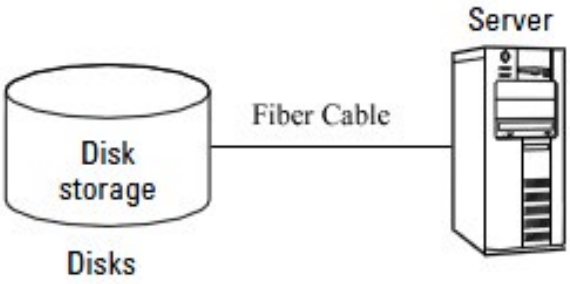
3 – إختيار الأجهزة المناسبة والعالية الجودة وخصوصا السوتشات فإنك ستحتاج Core Switches لتحقيق سرعة عالية ومثال على ذلك Cisco Catalyst 4500E.

طوبولوجيات شبكات الـ SAN :

هنالك أنواع متعدة من الطبولجيا لكل منها خصائصه . سنتعرف لكل واحد منها وفوائدة .

- Point-to-Point Topology

هذا النوع هو أبسط أنواع التصميم فهو بإختصار . توصيل السيرفر بشكل مباشر مع وحدة التخزين دون الحاجة للـ Fiber Layer التي تكلمنا عنها :

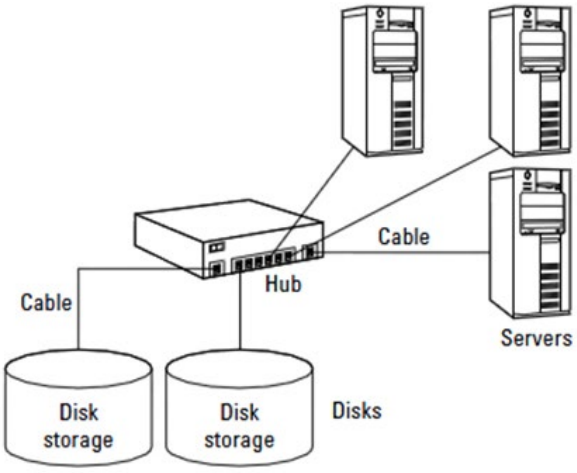


ويمكنك توصيل عدة سيرفرات بهذه الطريقة مع وحدة تخزين واحدة لمشاركة البيانات وهذا يعتمد على عد المنافذ الموجدة في Fiber Channel الخاصة بـ Storage Unit .

وأعلم أن تحب النقاش وتريد أن تسألني قائلا « لماذا لا أستخدم File Server بدلا من هذه الطريقة وأقلل التكلفة » ولكن يا أستاذي أقول لك «ماذا لو كان ذلك السيرفر يحتوي على بيانات كل موظفي الشركة وقررت عمل ترقية للهاردوير وقمت بتركيب power supply أقوى من سابقه مما أدى إلى إحتراق الهاردسك وفقدت كل بيانات الموظفيين وتم طردك من العمل » اليس من المهم عزل البيانات بشكل منفصل عن السيرفر في الشبكات الضخمة بحيث تستطيع حماية البيانات بعيداً عن المخاطر التي غالبا ما تحدث للسيرفرات كونها تعمل ليل نهار دون توقف .

- **Arbitrated Loop Topology**

في هذا النوع من التصميم سنتعامل مع Fabric Layer والتي ستحتوي على Fiber Channel Hub لربط بين السيرفرات ووحدات التخزين . وكما تعلم أن Hub جهاز غبي لم يعد له وجود فقد إستبدل بالـ Switch .



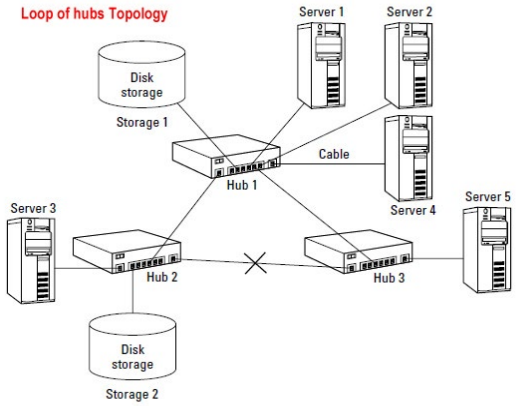
لكن عادة تقوم الشركات المصنعة بالحد من ربط Hubs مع بعضها إلى عدد أقصاها 3 أجهزة ، وذلك كما تعلم أن الـ Hub عندما يقوم بإرسال البيانات فأن جميع الأجهزة يجب أن تتوقف عن الإرسال حتى ينتهي الـ Hub من توصيل البيانات.

وهذا يعني إن نقوم بزيادة ربط الـ Hubs مع بعضها البعض عندما نحتاج لإضافة سيرفرات أضافية للشبكة .

وكلما زاد عدد السيرفرات زادت مدة التأخير في توصيل البيانات.

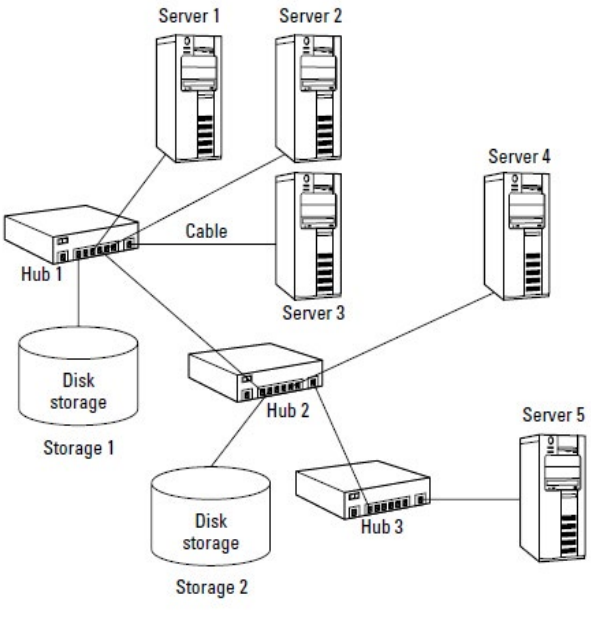
- **Loop of hubs Topology**

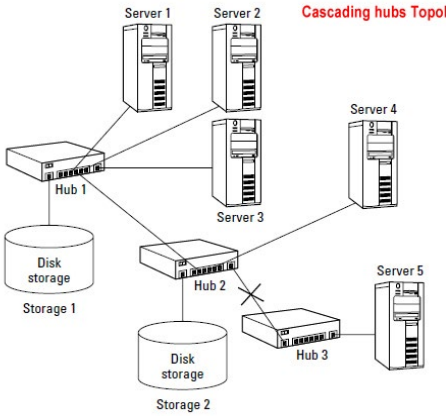
هذا أحد أنواع التصميم الممتازة في بناء شبكات الـ SAN . حيث يتم ربط الـ Hubs على بشكل مع بعضها البعض بشكل مغلق. وإن الربط بهذه الطريقة يزيد من مرونة عمل الشبكة عن حدوث إنقطاع لأحد الأسلاك فإن هنالك سلكاً أخر يمكن إستخدامة كبديل للوصول إلى وحدة التخزين . وهذا ما يميز هذا النوع من التوبولجي عن سابقه . والصورة التالية توضح ذلك :



- **Cascading hubs Topology**

يتم ربط الشبكات في هذا الطبولوجيا عن طريق ربط عدة Hubs مع بعضها البعض. ويكون كل Hub مربوط مع الأخر عن طريق كيبل واحد . وأن أقصى عدد من الـ Hubs يمكن ربطها مع بعضها 127 جهاز Hub وهو العدد الذي يستطيع تحمله Fiber Channel.



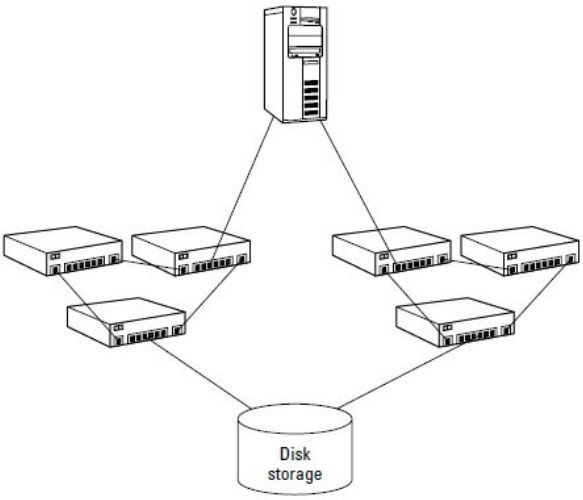


كما تلاحظ أن Server 5 في التوبولجي السابق لو إنقطع الكيبل الموصل بين Hub 2 و Hub 3 فإنه سيفقد الوصول إلى وحدة التخزين Storage 2 . والعكس في Loop of Hubs topology فإنه السيرفر سيجد مسار أخر وهو الكيبل الموصل بين Hub 3 و Hub 1 .

Fault-tolerant loops Topology

أما هذا النوع فهو لأصحاب الدراهم ففكرته الزيادة من إستخدام حلقات التوصيل بين الـ Hubs وهذا ما يستلزم زيادة مضاعفة في التكلفة وهو تصميم فعال لأصحاب الشركات الضخمة وخدمات التخزين السحابي مثل Dropbox و Google Drive .

وطبعا لمثل هذه الخدمات أقول لك أن هذا التصميم لا يكفي بل لديهم تصميم معقدا أكثر بمراحل لكن هذا هو أساس تصميمهم كما يظهر في الصورة :



فلاحظ أن إنقطاع كيبل واحد أو حتى 3 كابلات لن يؤثر على فقط الإتصال بوحدة التخزين إلا في حال إنقطاع الكيبل الموصل بالكرت الخاص بالسيرفر. ولحل هذه المشكلة يمكنك اضافة حتى 10 كروت شبكة لسيرفر واحد .

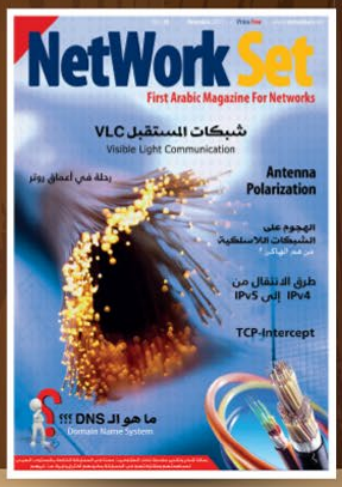
الخـتـام :

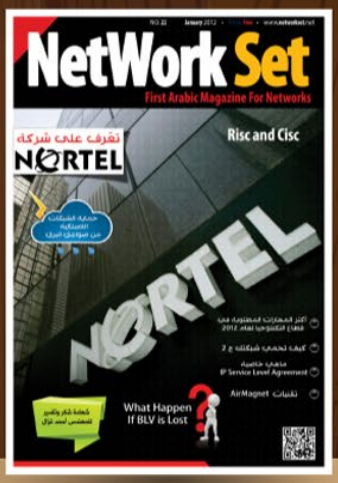
أتمنى أن أكون قد وفقت في توصيل المعلومات لكم بإسلوب بسيط .

فلم أتحدث سواء عن أبسط الأشياء فهنالك الكثير والكثير من بورتوكولات الـ SAN وطريقة عنونة شبكات الـ SAN ....الخ .

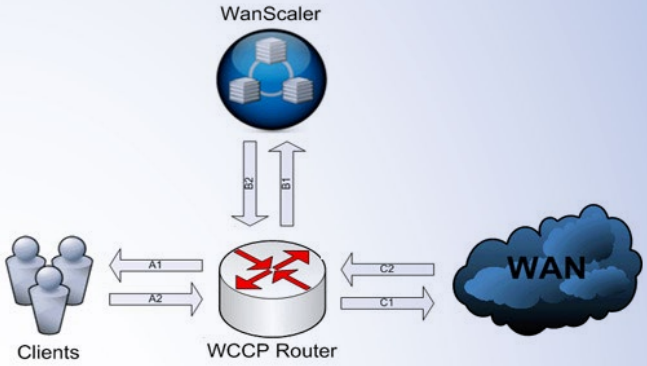
ولربما نكمل معكم الحديث عندما يكون قد حل الشيب في رأسي وحصلت على CCIE Storage ولربما في عدد لاحق من هذه المجلة المميزة .

Network Set Magazine Gallery





بروتوكول الـ WCCP تحت مجهر NetworkSet



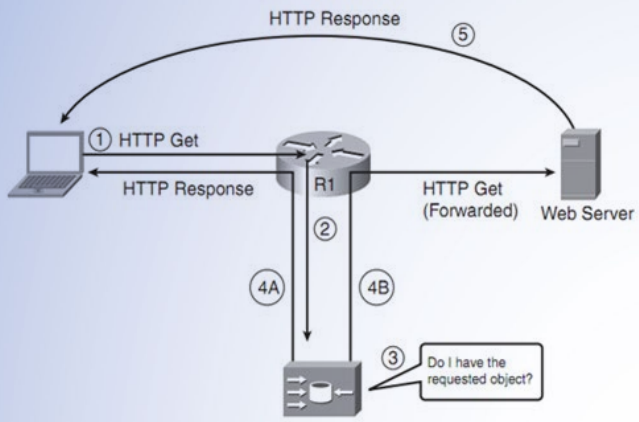
يعتبر الـWCCP أحد البروتوكولات التى قامت سيسكو بتطويرها عام 1997 وهو أختصار لي Web Cache Communication Protocol وهو بروتوكول يقوم بتوجيه طلبات الـ HTTP إلى سيرفرات وظيفتها عمل Cache لكل الترافيك الذي يمر من الأنترنت

ماهو WCCP ؟

قد تكون فكرة وجود سيرفرات للكاش شيئ معروف عند الجميع وأفضل مثال هو سيرفر الـ ISA لكن لنفكر قليلا ونطرح سؤال صغير لماذا سيسكو قررت تطوير بروتوكول لهذا الأمر ؟ إدعاءات سيسكو تقول أن هذا البروتوكول لايحتاج إلى أجبار العملاء والمستخدمين الموجودين على الشبكة لتغيير أعدادات المتصفح وربطه مع سيرفرات كاش مخصصة وبالتالي المستخدم لن يشعر بوجود أي عملية كاش للترافيك على الشبكة, وسوف أقدم مداخلتي حول هذا البروتوكول في آخر الموضوع, وكما ذكرت في البداية بأنه بروتوكول وظيفته الرئيسية توجيه طلبات الـ HTTP إلى سيرفرات وظيفتها عمل Cache وليس الكاش نفسه.

كيف يعمل البروتوكول ؟

لتوضيح فكرة عمل البروتوكول سوف أستعين هذه الصورة المأخوذة من كتاب CCIE R&S



الخطوة الأولى: تبدأ من جهاز العميل الذي يرسل طلب معين HTTP Get request إلى الـ Default Gateway وهو عادة الروتر.

الخطوة الثانية: يستلم الروتر الطلب ويقوم بأعادة توجيهها الـ HTTP Get request إلى سيرفر الكاش أو الـ Cache engine (سوف أعود لأتحدث عن بعض أنواعها)

الخطوة الثالثة: يستلم الطلب سيرفر الكاش ويبدأ البحث في ملفاته وقاعدة بياناته عن الطلب.

الخطوة الرابعة A: لو وجد الطلب المقصود يتم أرسال المطلوب HTTP response إلى الروتر ليقوم بعدها بتمريره إلى العميل بدون أن يشعر بشيئ.

الخطوة الرابعة B: لو لم يتم إيجاد الطلب على السيرفر يتم إعادة توجيه الطلب HTTP Get request إلى الروتر ليتم بعدها أيصاله إلى العالم الخارجي وإلى وجهته الأصلية.

الخطوة الخامسة: هي الرد على طلب العميل من السيرفر الخارجي المخصص.

وقد تم بناء هذا البروتوكول على فكرة ذهبية تساعد في تسريع تحرك البيانات وضمان عدم المساس بمحتويات الباكيت لو في حال لم يجد الطلب مايريده على السيرفر وذلك من خلال ممر مخصص من تطوير سيسكو أيضا يطلق عليه Generic Routing Encapsulation أو GRE يعمل هذا الممر على حفظ الباكيت كما هيا وهي فكرة سيسكو عندما وصفت هذا البروتوكول بالشفافية Transparent, فلو في حال لم يتم إيجاد المطلوب يتم إعادة أرسال الطلب إلى الروتر ليمرره إلى العالم الخارجي وكأن شيئ لم يحدث وبذلك تتحرك البيانات بشكل أسرع بين الروتر والسيرفر بدون الحاجة إلى تغيير معلومات الأيبي أو الماك أدريس.

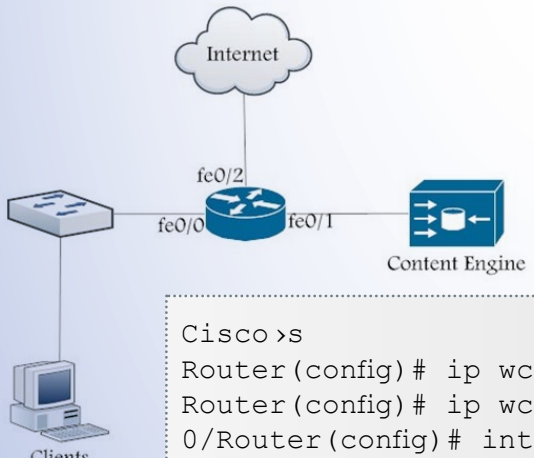
ملاحظة: البروتوكول يرتبط مع السيرفر من خلال بروتوكول الـ UDP مستخدما المنفذ 2048.

إصدارات البروتوكول.

لهذا البروتوكول إصداران ويختلف الاول عن الثاني بعدة أمور حساسة وهذا جدول بسيط للتوضيح

WCCP v2	WCCP v1
يدعم الـ TCP, UDP	فقط TCP يدعم الـ
يعمل مع أي IP Protocol وهذا يشمل HTTP, FTP	HTTP يعمل مع المنفذ 80 فقط أي بروتوكول الـ
يقوم بتشفير كلمة السر من خلال MD5	لايوجد كلمة سر
يدعم عناوين الملتي كاست لتبسيط الأعدادت لو في حال كان لدينا أكثر من كاش سيرفر	لايدعم الملتي كاست
يدعم عمل منظومة تضم اكثر من روتر مع أكثر من كاش سيرفر	فقط روتر واحد
كلا البروتوكولان يدعمان ربط الروتر حتى 32 سيرفر	

طريقة الأعداد :




```
Cisco>s
Router(config)# ip wccp version 2
Router(config)# ip wccp web-cache password NetworkSet
0/Router(config)# interface Fa0
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)#exit
1/Router(config)# interface Fa0
Router(config-if)# ip wccp web-cache redirect out
seconds
```

الأوامر واضحة ولاتحتاج إلى شرح وهي الأعدادت الأساسية اللازمة لتشغيل البروتوكول وهناك أوامر وأعدادت آخرى مثل لو كان لدينا أكثر من سيرفر ونريد ربطهم من خلال ملتي كاست أيبي, يمكن ربط الطلبات الداخلة بي Access-List لعزلها عن بروتوكول الكاش وارسالها مباشرة إلى الأنترنت والخ

أجهزة سيسكو التى تدعم البروتوكول

- Cisco 1000 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2500 series access servers
- Cisco 3600 series
- Cisco 3800 series
- MC3810
- Cisco 4000 series
- Cisco 4500 series
- Router Switch Module (RSM) for Catalyst 5000 Series
- Cisco AS5100 access server
- Cisco AS5200 universal access server
- Cisco AS5300 access server
- Cisco AS5800 series
- Cisco 7000 series
- Cisco 7200 series
- Cisco 7500 series

الأجهزة والبرامج التى تدعم هذه البروتوكول

كثيرة هي الشركات التى تدعم هذه الخاصية على أجهزتها وهذه لائحة ببعض الشركات وأجهزتها المخصصة للعمل مع هذا البروتوكول بالأضافة إلى بعض البرامج.

Aladdin/SafeNet eSafe Web
ApplianSys CACHEbox
Barracuda Networks Barracuda Web Filter
Blue Coat ProxySG
Citrix Systems, Inc. WANScaler
CensorNet Ltd CensorNet Professional web filter
CYAN Network Security CYAN Secure Web
Cymphonix Corp. Network Composer/Conductor
F5 Networks Wan Optimization Module
Fortinet FortiOS4.0
M86 Security Secure Web Gateway
McAfee McAfee Web Gateway Formerly Webwasher
Microdasys SCIP SSL Content Proxy
PerfTech, Inc. Bulletin System
Replify Accelerator
Riverbed Technology Steelhead
SmoothWall Ltd Guardian Web Content Filters
Sophos Web Appliance
Squid
Stampede Technologies Stampede Application Acceleration Series
Trend Micro IWSVA 3.x and 5.x
Websense Web Security Gateway
Wedge Networks BeSecure
XipLink XA Optimizers

من هذه القائمة وجدت برنامج Squid أحد البرامج المجانية المفتوحة المصدر وهو برنامج معروف وتستخدمه شركات كثيرة في العالم.(وأكيد لن أدخل في طريقة إعداده)
إلى هنا أكون قد وصلت وفصلت البروتوكول والحمد لله أن نفدت للمرة الثانية فالبروتوكول أعرفه وقرأت عنه قبل ستة شهور تقريبا لكن لم أدخل في كل تفاصيله لكن اليوم قرأت عنه كل شيئ, أما مداخلتي على هذا البروتوكول فأنا اقول أن عمر هذا البروتوكول قد أنتهى فإستخدامه كان مفيد في ايام السرعات البطيئة والـ Dial UP والآن لا أجد داعي للتكلف وأحضار سيرفرات للقيام بعملية الكاش وخصوصا أن هناك أجهزة أسعارها تصل إلى آلاف الدولارات والنقطة الثانية التى أود أطرحها هي عن ماهية الشركة التى تطر إلى إستخدام الكاش في عملها فأنا أتصورها شركة كبيرة جدا ولديها عدد كبير جدا من الموظفين وتحتاج إلى الأنترنت بشكل كبير حينها يمكن الأستفادة من هذا البروتوكول أما على صعيد الشركات المتوسطة والصغيرة فأنا لا أعتقد أن الأمر هام إلى هذه الدرجة

عشرة أشياء يجب أن تتوفر لديك قبل دخول مجال تقنية المعلومات

يبدو أن الجميع متفقون أن مجال It هو حقل صعب.لكن يجب أن نسأل أنفسنا مالذي نحتاجه لكي نتغلب على هذه الصعوبات دعونا نرى بعض الصفات قد تكون المفتاح الامثل لكي تحترف عالم الـ it

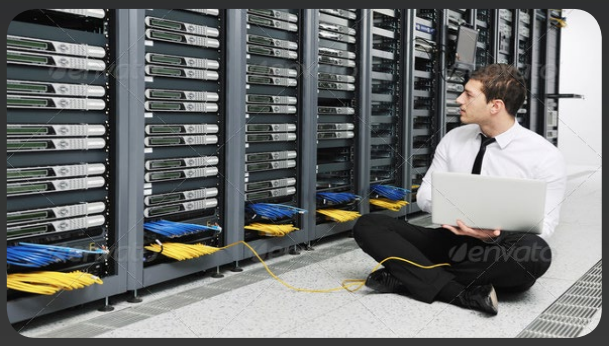
1 – التحمل

في الحقيقة يوجد نسبة كبيرة من الفنيين الذين يعملون في مجال ال It يتعرضون لمشاكل كثيرة أن كانت مجادلات مع الزبائن أو مع المدير لذا يجب على المهني تخطي جميع هذه المشكل لكي يستطيع النجاح والتميز في هذا المجال الرائع.

2 – الإصرار

من أكثر المهن التي يوجد فيها تغيير كثير هي تكنولوجيا المعلومات فكل يوم هناك مشكلة نصادفها لأول مرة لذا يجب على جميع العاملين في هذا المجال القدرة على التعامل مع هذه المشاكل وهكذا نرى إن من يريد الخوض في هذا المجال يجب أن تكون عنده روح التحدي والأصرار أو أن يبتعد عن هذا المجال بأقل الخسائر الممكنة.

3 – الشباب



لا أفضل بأن يكون مجال it محصور في عمر الشباب ولكن السن الأفضل للمهنيين المختصين في تكنولوجيا المعلومات هو هذا الجيل لأن هناك أسباب عديدة لهذا.أولا في مجال تكنولوجيا المعلومات تحتاج كثير من الأحيان الى ساعات عمل طويلة أو أوقات أضافية لذا سوف يكون هناك بعض الصعاب على الفئة الكبيرة بالعمر.

4 – الصبر

في هذا المجال من العمل يجب أن يتوفر عندك الصبر الكافي لأن سوف يمر عليك نسبة كبيرة من العملاء الذين يجعلون صبرك ينفذ مما يؤدي الى التوتر وعدم التركيز وليس فقط من العملاء ممكن ايضا من بعض المشاكل التي سوف يمر بها جهازك من مشاكل تكنيكية ولقد شاهدنا عدد كبير من مقاطع الفيديو التي تضهر لنا بعض الذين يقومون بتحطيم أجهزتهم لذا الصبر مطلوب.

5 – المهارات

من أهم الأشياء التي ممكن ذكرها عن تخصص تكنولوجية المعلومات هي المهارات. والاحترافية في هذا المجال تأتي من خلال الحصول على بعض الشهادات العلمية التي تأهلك لكسب المزيد من المهارات لذلك أحرص على أن تحصل على بعضها.

6 – القدرة على الأرتجال

هذه من النقاط الهامة التي يجب أن نتكلم عنها وهي قدرة الشخص على التكلم والأقناع مع اي شخص موجود معك في مجال ال IT اي اثبات قدرتك والثقة بنفسك واثبات انك قادر على حل جميع المشاكل التي سوف تواجهك .

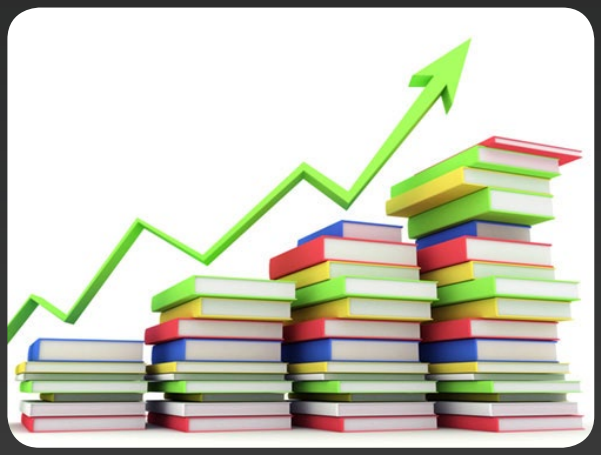
7 –العلاقات الخارجية

من أهم الأشياء في الشركات الكبيرة أو الصغيرة هي العلاقة مع المحيط الخارجي اي بمعنى اخر التسويق مع الشركات الأخرى عبر وسائل عديدة إن كانت عن طريق شبكة الانترنت وتقديم الإعلانات في جميع وسائل التعارف لذا كل ماكان التسويق أوسع كان مردود المادي للشركة أكبر وهذه من النقاط المهمة التي يجب نعطيها أهتمام كبير جدا.

8 – الأتصالات

قد يبدو هذا غريبا بعض الشيئ ولكن انت كعضو في مجال تكنولوجية المعلومات يجب أن يكون لك الاتصال الكافي مع جميع المهن التي ممكن أن يحتاجها الزبون الذي يتعامل مع شركتك واذا لم تكن تتقن بعض المهن على سبيل المثال الكهربائية او الاكترونية يجب ان يكون عندك الاتصال مع الذين يتقنون هذه المهن لكي توفر لزبائنك هذه الخدمة

9 _ الرغبة في التعلم



كما ذكرت سابقا ان صناعة ال IT هي عبارة عن مهنة متطورة بشكل سريع ولا يجب علينا التوقف بعد قراءة كتاب او الحصول على شهادة. لذا لكل من يريد التصدي لتكنولوجية المعلومات يجب أن يكون لديه الرغبة القوية في التعلم وبهذا سوف يكون تحدي كبير لكي تقوم بتعلم كل شيئ جديد إذا كنت لا تحب التعلم (سواء كان ذلك لوحدك، مع شخص آخر، أو في أحد الفصول)، يجب عليك نسيان هذا المجال

10 - الشغف

الشغف حاجة جوهرية لمن يعمل في مجال IT وأذا كنت لا تحب التكنولوجيا وحل المشاكل فهذا ليس هو المجال الموفق لأختيارك.

Magazine

NetworkSet