NO. 26 May 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

تقرير مفصل عن شركة:

FORTINET™
REAL TIME NETWORK PROTECTION
Complete Security Solution

Active Directory
Administrative Center

Sudo Command
Super user do

Network Scanning

الاتصال عبر الاقمار الصناعية

التحكم بسرعة الأنترنت
حسب وقتٍ معين

Upgrading and Downgrading CISCO Access Points

خمس خطوات لتجهيز
شبكتك من أجل ال VOI

مقارنة بين بروتوكول
IPoE و PPPoE

زكاة العلم

عادة ما أتعرف من خلال المدونة والمجلة على أناس كثيرة ومن شتى البقاع العربية وأغلبهم مهتمين بعالم نطلق عليه عالم الشبكات وأحيانا أرى مايحمله هؤلاء الأشخاص من شهادات وخبرات عالمية فمنهم من يملك ثلاث شهادات CCIE ومنهم من يملك شهادات عالية في الأمن والحماية ومنهم من يملك طن من الشهادات وأول مايخطر على بالي هو لماذا لايشاركنا معلوماته وخبراته, والله سوف نستفيد منه كثيرا فالمعلومة التى لديه قد توازي أضعاف مالدينا من معلومات. وطبعا السؤال يبقى في قلبي وعقلي فقط فهو يطلبني في شيئ ويريد أن يحصل عليه وبعدها يختفي بدون رجعة, ما أكثرهم وما أبخلهم فهم أعتبروا الدنيا أن اخذ ولا اعطي ونسوا أن للعلم حقوق وزكاة وهم سوف يسألوا عنها يوما ما, ما اصعب يوم الحساب عندما نسأل عن « عُمُرِكَ فِيمَا أَفْنَيْتَهُ ، وَعَنْ شَبَابِكَ فِيمَا أَبْلَيْتَهُ ، وَعَنْ مَالِكَ مِنْ أَيْنَ اكْتَسَبْتَهُ وَفِيمَا أَنْفَقْتَهُ ، وَمَا عَمِلْتَ فِيمَا عَلِمْتَ « ماعملت فيما علمت هل جلست قليلا وتفكرت في هذه الجملة ؟!!!...

أنا مازلت مبتدأ وكل الذي أملكه هو شهادة CCNA ومازلت غير قادر على مساعدة الناس, أنا لدي ضغط كبير في عملي ولا ارجع إلى البيت وإلا رأسي يكاد ينفجر, أما أنا فلا أجيد مساعدة الآخرين ولا أملك أسلوب أستطيع فيه مساعدة الآخرين, هذه هي أغلب اعذارنا وسوف أناقشه معكم في هذا المقال من خلال إسقاطها على بعض الأشخاص.

حجة المبتدأ: في القضية الأولى اسمحوا لي بتقديم نفسي فيها وخصوصا أن أحاول تقديم خبراتي وتجاربي في كل المقالات التى أطرحها, من يذكر عرب هاردوير ويذكر الأيام التى أشرفت فيها على المنتدى يتذكر معي كيف كنت اسابق الأعضاء في الاجابة على الأسئلة والأستفسارات وبل اصبحت مشرف عام على المنتدى وكل الذي لدي كان هو شهادة CCNA, وحتى لو لم يكن لدي هذه الشهادة فأنا كنت قادر على مساعدة الآخرين وأساعدهم لكن حينها لم يكن لدي خاطر في المنتديات لذلك حجتك الاولى واهية جدا فهناك كل يوم شخص يقرر دراسة CCNA ويحتاج المساعدة فهل يمكنك تزكية علمك بمساعدته؟

حجة الوقت والعمل: في القضية الثانية لن أجد أفضل من المهندس عادل الحميدي الذي صور لنا حتى الآن ثلاث وسبعين ساعة من الشروحات المصورة وبما أن والمهندس عادل على تواصل دائم فأنا على علم بالضغط الذي لديه في عمله فهو أحيانا يرجع إلى المنزل وهو لايريد إلا أن يأخذ قسط من الراحة والنوم فوظيفته ومشاريع شركته على درجة عالية من الصعوبة عدا عن حقوقه نحو أسرته ولكن هل هذا منعه من تزكية علمه ؟ الله عليك يامهندسنا والله يبارك لك في وقتك وعلمك وعملك .

حجة الأسلوب: في القضية الثالثة سوف أتحدث عن المهندس أنس المبروكي واتحدث عن كيفية بدايته معنا في تحرير المجلة, المهندس أنس كان لديه الأرادة وكان مصمم على المساهمة وأول مشكلة واجهته هي الكتابة باللغة العربية وخصوصا أن المهندس أنس من المغرب وهم يستخدموا الفرنسية أكثر من العربية وبعد أول مقال وفي التنسيق بيني وبينه بدأ يكتشف بعض الطرق الجديدة في الكتابة وفي الطرح, الآن أنس بعد كل مقال يرسله لي يتلقى مني رسالة أنبهار بالأسلوب والتطور الكبير الذي وصل إليه وأنا لا ازكيه أبدا فعمله لوجه الله تعالى ومبدأه هو تزكية العلم الذي منحه الله له.

أخواني أقولها لكم قولا صادقا وأنا هنا أتحدث عن الأسلام ومبادئه, فالله منحنا الكثير من أسراره وأخبرنا أن هناك طريق قصير وهنالك باب وأخبرنا ايضا ما وراء هذا الباب ومع هذا نحن مقصرين جدا فنحن أمة لاتقرا وإن قرأت لاتفهم وإن فهمت لاتطبق, أنظروا إلى المنتديات والمدونات الأجنبية كيف تكون الاجوبة احيانا, والله أن أغضب أحيانا عندما أجد أحدهم قد كتب أكثر من ألف كلمة لكي يرد على تسائل أحدهم ونحن مصريين على مقولة أعطني فقط, فكروا بهذا الكلام وما أنا إلا بناصح هنا فهل من يقبل النصيحة ويتخلى عن كنز جحى (علمه) لعامة الناس ؟ ودمتم بود.

أيمن النعيمي - سوريا

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.عبد الرقيب عبده صالح الفقيه
م.خالد عوض	م.أحمد هيكل	م.فادي الطه
م.أنس المبروكي	م. أحمد سلطان	---
م. شيماء الرازق	م.خالد الدسوقي	---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : عثمان اسماعيل

www.networkset.net

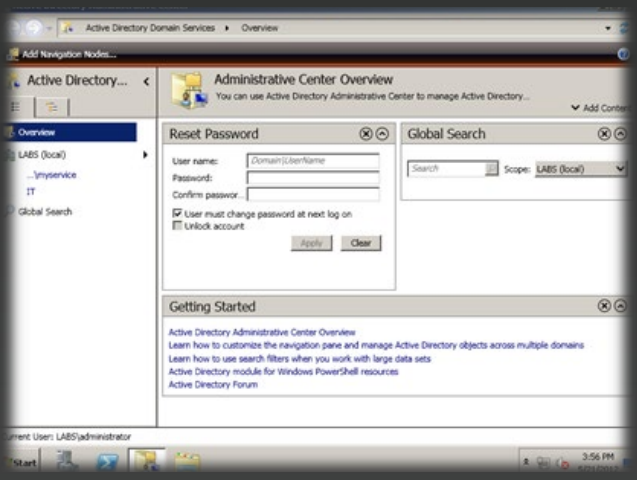
نظرة حول (ADAC)
Active Directory Administrative Center

طبعا اذا رجعنا وتكلمنا على الأنظمة السابقة مثل Server 2003 و Server 2008 سنلاحظ ان مدراء الشبكات كانوا يستطيعوا عمل إدارة لبيئة الدليل النشط (Active Directory) عن طريق كونسول الـ Active Directory Users And Computers . لكن مع ظهور Windows Server 2008 R2

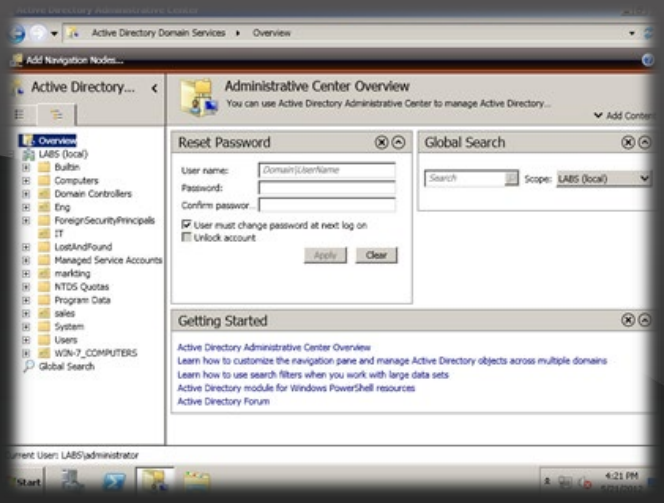
سهل على مدراء الشبكة الإدارة والعمل اليومي الذين يقومون به عن طريق الـ Active Directory Administrative Center او كما هو اختصارا (ADAC) . (طبعا بالإضافة إلى الـ Active Directory Users And Computers) . ومن الممكن ان نلاحظ هنا ان الـ ADAC عبارة عن واجهة رسومية GUI تعتمد أساسا على تقنية الـ PowerShell بمعنى اي تغيرات نقوم بها على الـ ADAC هي اساسا تترجم في الخلفية إلى أوامر نصية أو كما تعرف بالـ (Cmdlets) للقيام بالمهمة المطلوبة .

وبما اننا نتكلم عن Windows Server 2008 R2 فهنا سنقول ان الـ ADAC متواجدة فقط في W2K8 R2 وايضا متواجد في Windows 7 بعد إضافة ادوات الـ RSAT . ولا تستطيع ان تضيف الـ ADAC إلى أجهزة تعمل بأنظمة تشغيل سابقة مثل Windows® 2000, Windows Server 2003, Windows Server 2008, or Windows Vista ، وايضا ممكن تحميل الـ ADAC على إصدارات معينة من W2K8 R2 وهي ، Standard Datacenter ، Enterprise فقط .

وهنا ميزة الـ ADAC تضاف تلقائيا عندما نعمل للـ Server ترقية إلى متحكم بالمجال (Domain Controller) . ولكن من الممكن ان تضيفه كميزة Feature من الـ Server Manager ، وايضا من الممكن اضافة الـ ADAC إلى أجهزة محملة Windows 7 ولكن بالإصدارات التالية Enterprise , Ultimate , Professional وهذا طبعا بعد اضافة الـ RSAT .

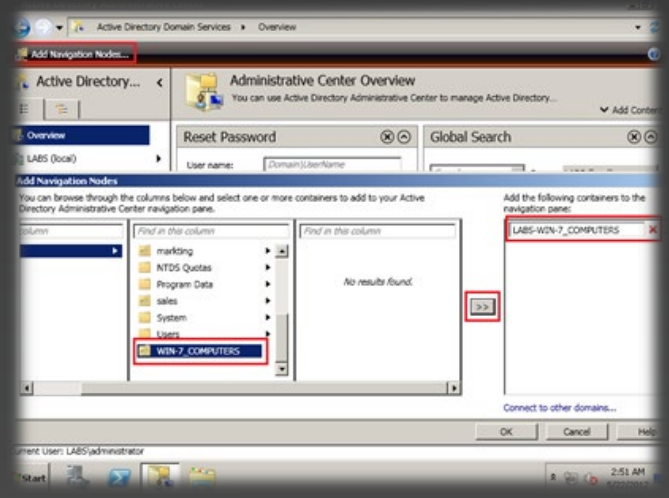


وللوصول إلى الـ ADAC فهوا موجود في الـ Administrative Tools . وعند فتحه كما هو ظاهر في الصورة ستلاحظ ان الـ ADAC عبارة عن واجهة رسومية تركز على الهدف بمعنى تستطيع عند فتحه ان تعمل على سبيل المثال إعادة كلمة السر لمستخدم معين ، او عمل بحث لكائن معين ، وهذا ما نفضله به عن نظيرة الـ Active Directory Users And Computers الذي يتطلب منا عده نقرات للوصول للشيء المطلوب تنفيذه .

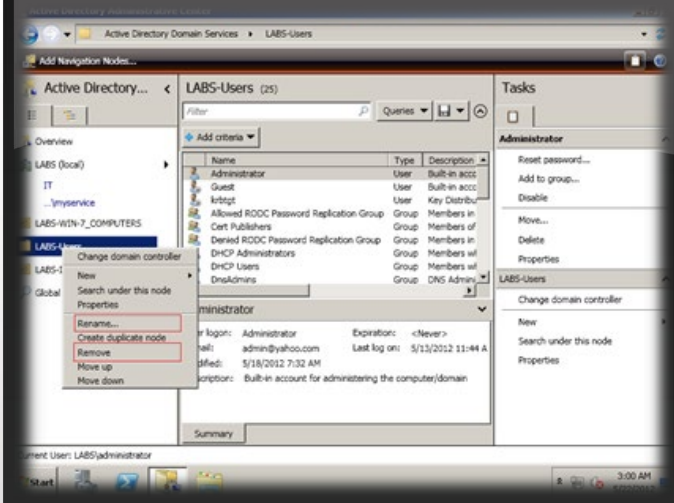


وعند النظر إلى الصورة نستنتج انه من الممكن مسح قائمة محتوى معين عن طريق الضغط على زر الـ X الموجود في اليمين الأعلى للصورة . على سبيل المثال ممكن مسح قائمة الـ Getting Started بضغط على زر الـ X الموجود في الركن الأعلى ، ومن أجل اضافته مرة أخرى من الممكن الضغط على زر Add Content وعمل علامة صح على المحتوى المطلوب .

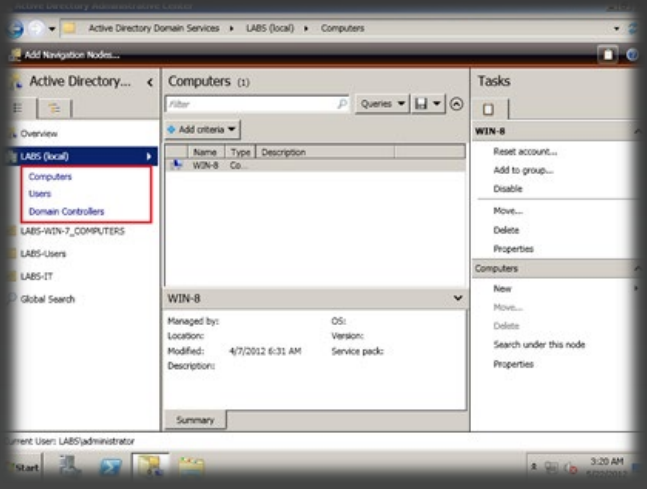
وهنا الـ ADAC يقدم لنا نظرة عامة عن هرمية الـ Domain والتي هي تساوي المنظر الموجود في الـ Active Directory Users And Computers . وبالنقر على الـ Tap الأخر الموجود على اليسار سيكون عندنا المنظر يساوي المنظر الموجود في الـ Active Directory Users And Computers كما في الصورة التالية .



عند عملنا كمسؤولين شبكة دائما ما نركز في أعمالنا اليومية على كائنات Objects موجودة ومتفرعة من وحدات تنظيمية OUs في الـ Domain ، على سبيل المثال الوحدات التنظيمية



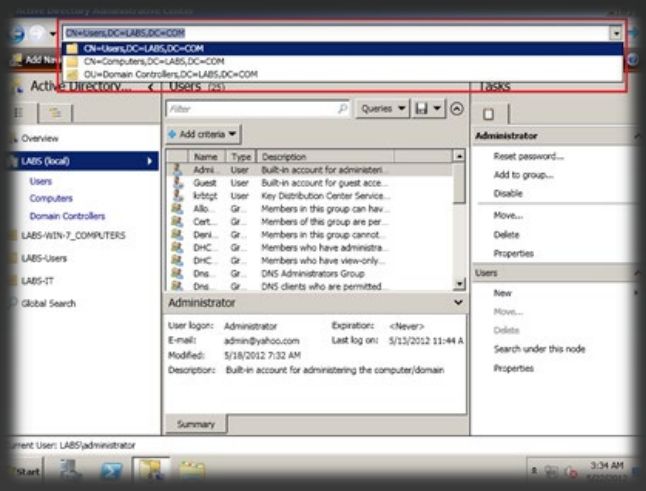
مثل الـ User OU وايضا Computer OU . ومن الممكن اضافة اختصار لوحدة تنظيمية تقوم انت بالتعامل معها بشكل مستمر إلى جهة اليسار وذلك عن طريق النقر على Add Navigation Node كما في الصورة وتحديد الوحدة التنظيمية ومن ثم النقر على الزر المرسوم علية >> وستلاحظ انها قد انضافت إلى جهة اليمين ولحذفها يجب النقر على زر علامة الـ X بالقرب منها ، وعند اضافتها في تظهر في كلا الـ Tabs بمعنى في الـ List View وايضا في الـ Tree View . ومن الممكن عمل إعادة تسمية او إعادة ترتيب او حتى مسح الـ OUs المضافة في الـ ADAC كما في الصورة



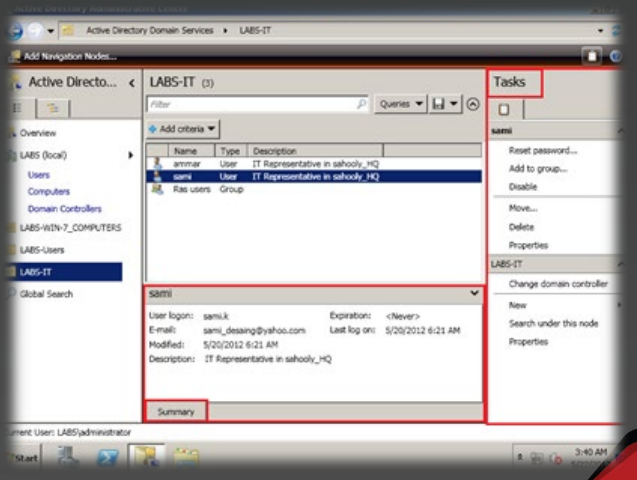
لكن الـ SubOU لا يمكن ان نغيرها . وعند اختيارنا لطريقة العرض من النوع List View نستطيع النقر مرة واحد على أسم الـ Domain أو حتى OU معين و الـ ADAC سيعرض لنا هرمية الـ OU وكل شيء تحتها والـ SubOU يتم توسعتها وفتحها بطريقة مشابه للـ Windows Start Menu . وفي عرض الـ List View ، عند اختيار الـ OU والدخول والعمل

عليها القائمة تعرض اخر ثلاث اشياء قمت بالدخول عليها أخر مرة مثل التي في الصورة ويطلق عليها قائمة الـ (Most-Recently Used (MRU

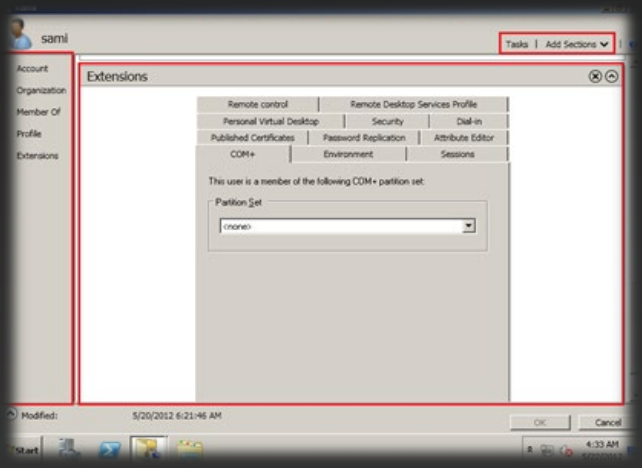
وفي عندنا ايضا بالـ ADAC في الأعلى هناك حاجة اسمها breadcrumb bar بمعنى الشريط التفصيلي الذي يعمل نفس عمل الشريط التفصيلي للـ Windows Explorer وهو يعطي لنا المسار كاملا للـ Object المحدد ومن الممكن ان نتصفح هرمية الـ Domain عن طريق الضغط على عناصر الشريط التفصيلي أو كما يسمى بالـ breadcrumb bar ، أو ممكن ان نحدد مسار OU معين عن طريق كتابة مسار الـ LDAP أو عن طريق الأسم المميز distinguished Name كما في الصورة .



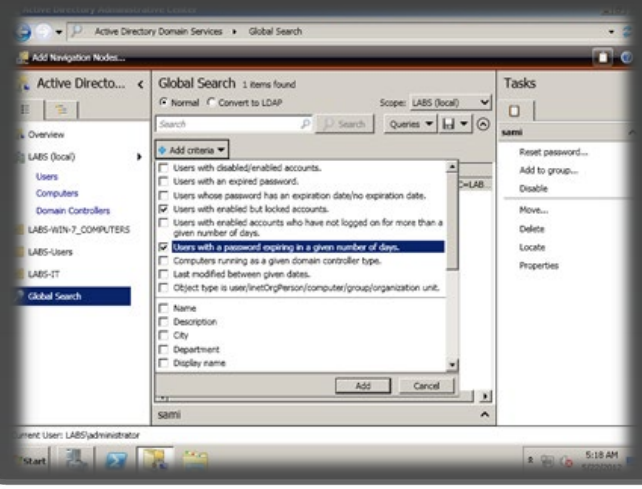
وعند اختيارنا لعنصر معين نستطيع ان نلاحظ ان هناك قائمة تلخيصيه بخواص ذلك العنصر تظهر في قائمة التلخيص Summary Panel ، والمهام الشائعة تظهر في قائمة الـ Task Panel كما في الصورة التالية وهي تظهر لنا ملخص عن المستخدم



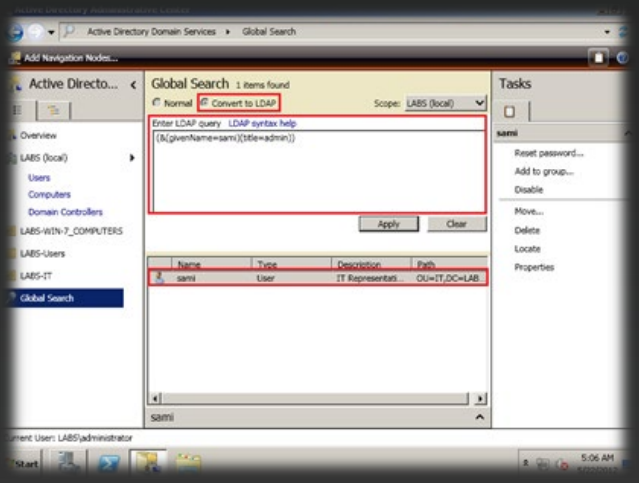
sami والمهام التي ممكن ان اطبقها على العنصر في قائمة الـ Tasks مثل Reset Password , Add to group , Disable , Move , Delete , Properties , وهي لفتح كافة خصائص المستخدم او النقر علية نقرتان او الضغط بالزر الأيمن واختيار Properties كلها تعمل نفس الأمر وبعد ذلك ستفتح امامنا نافذة خصائص العنصر وهي مختلفة تمام عن خصائص العنصر الموجودة في الـ Active Directory Users And Computers ، وكمثال الصورة التالية .



للقيام بالمهام المذكورة في الأعلى أضغط على زر Tasks في أعلى اليمين . وخصائص العنصر تظهر كاملة على طول الصفحة عكس الـ Active Directory Users And Computers حيث تظهر على شكل Tabs ، وهناك اختصارات متعلقة بخصائص معينة تظهر في الجهة اليسرى من الصفحة ولأضافه قائمة إلى اليسار أو حذفها ممكن الضغط على Add Section في الجهة اليمنى فوق . ويظهر لنا اخر مقطع في الصفحة وهو Extensions وهو يساوي بشكلة جميع واجهة الـ Tabs الموجودة في الـ Active Directory Users And Computers ومن خلاله ممكن الدخول على الخصائص الغير موجوده ضمن مقاطع الـ ADAC . عندما تريد تعمل بحث عن عنصر او عدة عناصر ، من

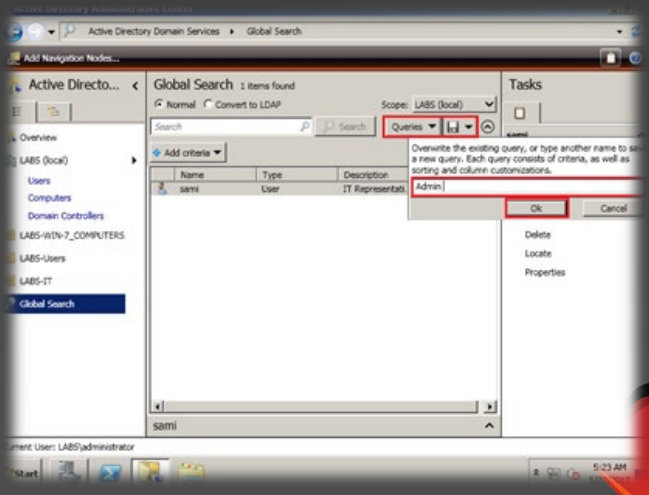


الممكن النقر على Global Search الموجودة في اليسار . وانت تستطيع عمل بحث لعنصر اعتمادا على معاير محددة مسبقا وهي تشمل على سبيل المثال مستخدمين مفعلين Enabled لكن حساباتهم مغلقة Locked وممكن ايضا كمان البحث عن مستخدمين كلمات السر حقهم ستنتهي في يوم محدد ، وممكن الضغط على Convert To LDAP لاستعمال البحث باستخدام تراكيب جمل الـ LDAP (LADP Syntax) على سبيل المثال كما في الصورة



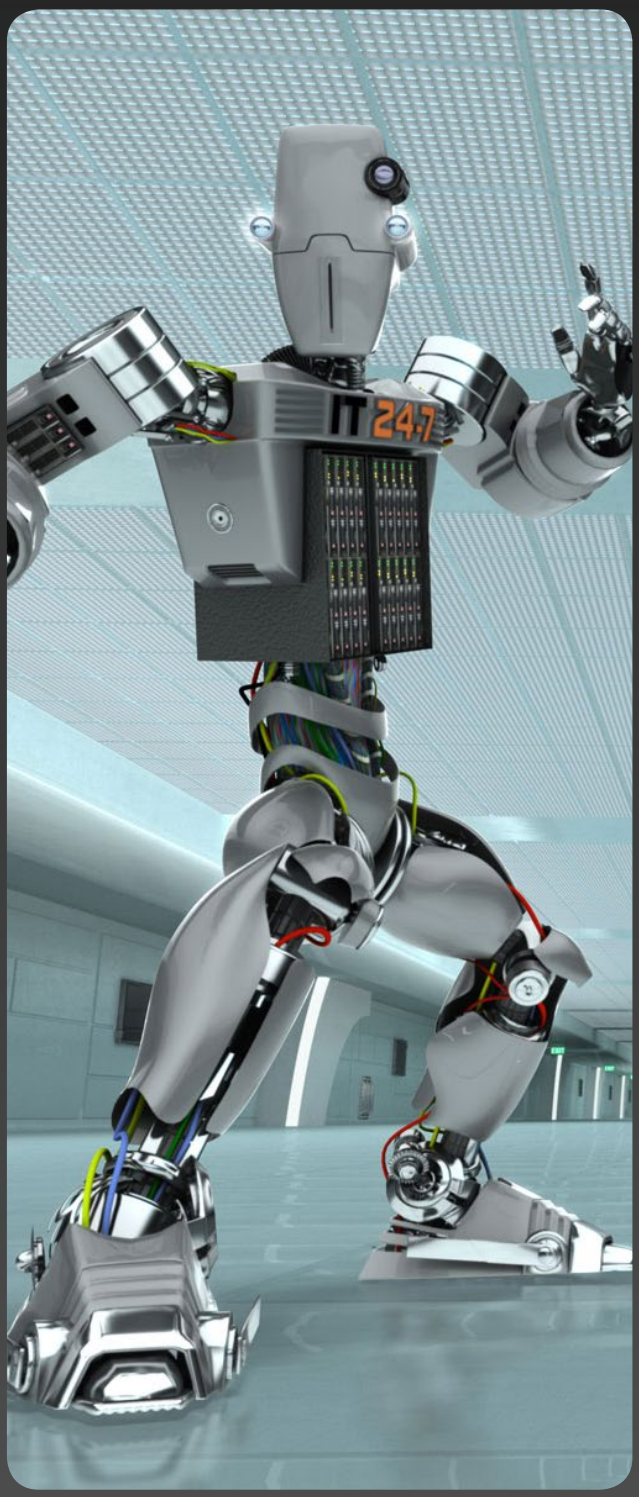
وهي البحث في الـ Domain ككل عن المستخدمين الذين اسمائهم sami ولديهم Job Title يساوي Admin . ولمزيد من المعلومات حول كيفية كتابة استعلامات LDAP يرجى الذهاب إلى الرابط التالي http://technet.microsoft.com/en-us/library/aa996205.aspx .

وفي الـ Normal View من الممكن عمل حفظ للاستعلام عن طريق الضغط على زر حفظ لاستعمال الاستعلام مرة أخرى مستقبلا كما في الصورة .



والضغط على استعلام Queries من أجل ان تفتح استعلامات تم حفظها من قبل .

وأخير الـ ADAC يقدم لنا خصائص جميلة ويسهل علينا الأعمال اليومية التي نقوم بها . انصح وبشدة ان تقضوا بعض الوقت في العمل علية واستكشافه بأنفسكم .. تحياتي لكم ودعواتكم لي وأن شاء الله نلتقى في العدد القادم مع موضوع جديد ..



ماهي أنظمة الـ IDS & IPS وماهي أهم الأختلافات بينها

في هذا المقال سوف أتناول موضوع لم يتناوله الوسط العربي بأي شكل من الأشكال وأحببت أن أقدمها لكم كون الموضوع هام وفي صلب الشبكات وهو يدور عن أنظمة الـ IPS وأنظمة الـ IDS ماهي ؟ وماوظيفتها ؟ وماهي أهم الأختلافات بينها وهي تدوينة خاصة بأمن وحماية الشبكات

ماهو الـ IDS ؟

الـ IDS أو intrusion detection system هو عبارة عن نظام حماية تستطيع تشبيه بي مضاد الفيروسات الموجود على جهازك يقوم بتحليل كل الترافيك المار عبر الشبكة من خلال أرسال نسخة من هذا الترافيك إليه وتتركز وظيفته الأساسية على التحليل العملي فقط وذلك أعتمادا على Rules يمكن تحميلها من الأنترنت أو أعداداها يدويا كما سوف نشاهد لاحقا بالأضافة إلى قواعد بيانات تحوي معلومات عن الفيروسات والديدان أستطاعت النفاذ من خلال جدار الحماية الموجود على الشبكة وتعمد إليه عمل النظام على مقارنة الـ Signature الخاص بكل فايروس والتى تكون مخذنة في قاعدة البيانات ولكن مايعيب هذا النظام أنه لايقوم بأي ردة فعل اتجاه هذا الفيروسات فكل مايقوم به هو أرسال تحذير إلى مدير الشبكة بوجود شيء غير طبيعي في الترافيك المار ومن هنا نستطيع ان نستنتج ان كلمة detection لاتعني إلا الكشف وقد يخطر على بالك سؤال صغير ماذا أستفيد من هذه العملية ؟

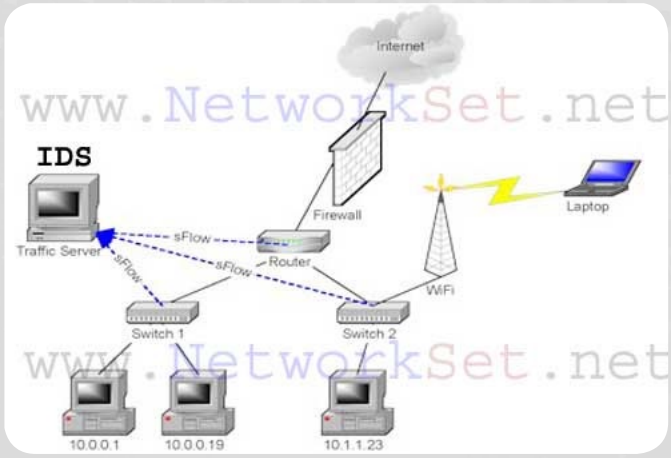
وبكلام آخر ماذا سوف أستفيد أذا دخل الفيروس إلى الشبكة ؟ الأجابة على هذا السؤال يجب أن نعلم أولا أن هذا النوع من الأنظمة مفيد في عدة حالات

الحالة الأولى كشف الثغرات الموجودة في أنظمة الحماية

الحالة الثانية أرشفة كل أنواع التهديدات التى تحدث للشبكة

الحالة الثالثة تحديد الأخطاء التى وقع فيها مسؤولوا الحماية وتصحيحها

ومايميز هذا النوع أيضا هو أمكانية وضعه بعيدا عن السار الحقيقي للترافيك بحيث لايؤثر على سرعة نقل الداتا وهذه صورة توضيحية

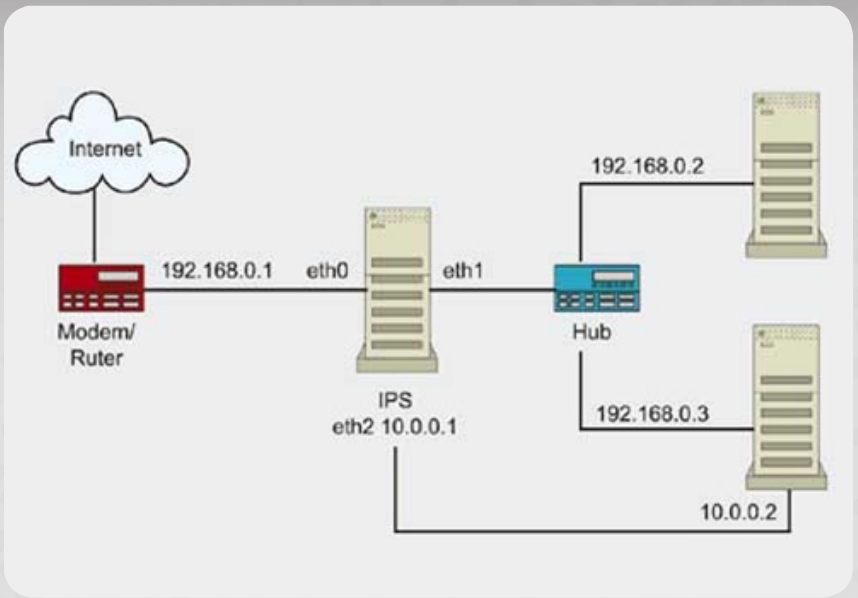


كما تشاهدون السيرفر موجود على منفذ آخر وكل مانقوم به هو أرسال نسخة من هذا الترافيك إليه وبذلك نكون قد ضمنا أن سرعة النقل أو عبور الداتا لن يتأثر أبدا بعمل النظام .

وآخيرا هذا النظام يعد نظاما قديما جدا بدأ مشروع تطويره أول مرة عام 1984 وأعلن عن اول نظام IDS عام 1986 وهو موجود كهاردوير أو سوفت وير وسوف أعود لأتحدث عنها

ماهوالـ IPS ؟

الـ IPS أو Intrusion Prevention Systems وهو نسخة مطورة من النظام السابق فهو يقوم بعملية الكشف Detection أولا وبعدها يقوم بتنفيذ ردة فعل معينة Prevention مثل عمل Drop للباكيت الضارة لذا يتوجب وضعه على ممر الترافيك مباشرة وهذه صورة توضيحية



وكما تلاحظ معي أن النظام هنا هو سوفت وير تم تنصيبه على نظام تشغيل لكي يعمل IPS للترافيك ومايميزه ايضا هو طريقة الأستجابة للترافيك الخطر فهو يستطيع أن يمنعه ويستطيع أيضا أن يقوم بأرسال أعدادات لأجهزة الأمن الموجودة على الشبكة مثل الجدران النارية أو الروترات لكي تقوم هي بأيقافه

وآخيرا لهذه السيرفرات كما ذكرت سابقا برامج سوفت وير واجهزة هاردوير وقد قمت بعملية بحص صغيرة على الأنترنت فوجدت الكثير من البرامج التى تقوم بهذه الوظيفة وأستخلصت لكم برنامج يدعى Snort وهو برنامج مفتوح المصدر يمكن تنصيبه على انظمة مايكروسوفت ولينوكس وطبعا أنا أنصح دائما لمثل هذه الأشياء أنظمة لينوكس فهي مستقرا وتعمل لفترات طويلة ولاتستهلك كثيرا من أمكانيات الجهاز بالأضافة إلى كونها أأمن وطبعا البرنامج مجاني وتستطيع أيضا تحميل Rules جاهزة وهذا رابط البرنامج

أما الهاردوير فهي أيضا كثيرة جدا فهناك أجهزة من سيسكو وأجهزة من 3com وأجهزة من جونيبر والخ..
أتمنى مشاركتكم العملية حول أفضل أنواع هذه الأجهزة ؟

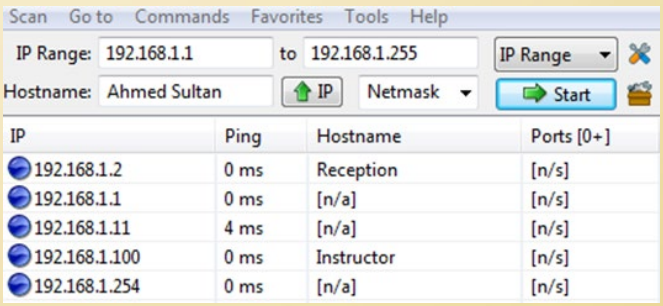
كما يمكنك شراء Module خاص بهذا النظام ووضعه على روترات أو جدران نارية خاصة بسيسكو مثل هذا الـ Module الخاص بي أجهزة 1841 3800 2800 and

مراحل عمل مسح للشبكة

من منا لا يمتلك شبكة محلية فى منزله أو يقوم بتوصيل خطوط لغيره ليكونوا على نفس الشبكة فى بعض الأحيان يتطلب الأمر أن تعرف عدد الأفراد معك عالشبكة لتقدير سرعة خط الانترنت المشبوك عليه وفى بعض الأحيان تريد أن تعرف الأجهزه المفتوحة حاليا هذا الأمر يفيد أيضا مختبرى الاختراق أو الـ Penetration Testers قبل عمل اختبار للشبكة المخترقة يهمه أولا أن يعرف عدد الأجهزة الموجودة فى الشبكة وأنظمة التشغيل حتى يصل فى النهاية الى الخدمات الموجودة على كل جهاز ليبدأ على أساسة معرفة مكان الثغرات فى الجهاز .
كل هذا يتطلب منك عمل مسح للشبكة , عندما نتحدث عن عمل مسح للشبكة فالموضوع ليس عشوائى ولكن ينقسم الى مراحل متسلسله على حسب الغرض المطلوب منها يوجد ثلاث مراحل رئيسيه لعملية المسح Network Scanning, Port Scanning and Vulnerability Scanning دعنا نتحدث عن كل واحدة على حده

Network Scanning - 1

المقصود به عمل مسح شامل للشبكة بغرض معرفة الأجهزه المفتوحة حاليا ويتم عمل ذلك بأحد أدوات المسح وأشهرها البرنامج المجانى
Angry IP Scanner
PING Sweep يعتبر الأسرع فى برامج المسح لانه يعمل معناها معناها بالعربية «مسح أو جرف» أى أنك قمت بعمل مسح كامل للشبكة Sweep وكلمة لمعرفة اذا كانت الأجهزه مفتوحة أو مغلقة عن طريق ارسال رسالة بينج والجهاز المفتوح فقط هو من يقوم بارسال الرد والمغلق لا يقوم بالرد على هذه الرسالة
مثال عند عمل مسح للشبكة 192.168.1.0/ 24
لمعرفة الأجهزة المفتوحة



فى بعض الأحيان لا تنفع هذه الخطوة فى البحث عن الأجهزة وأبسط مثال أن يكون الجهاز الذى أبحث عنه يستخدم جدار نارى يصد طلبات البينج ولا يقوم بالرد عليك حتى تعتقد انه مغلق ! لذلك يوجد أكثر من طريقة أخرى بخلاف طلب البينج أستطيع من خلالها معرفة اذا كان الجهاز مفتوح أم لا لمعرفة هذه الطرق أنصحك فى TCP البداية بمعرفتك التامة لكيفية عمل الإتصال بين جهازين يستخدمون بروتوكول الـ Three-Way Handshake أو ما يعرف بعملية الستة الموجودين فى هيدر البروتوكول لانهم محور الحديث Flags وأيضا معرفة الـ:

SYN لبدأ الإتصال
ACK للرد على إتصال
PSH يقوم بعمل ارسال للبيانات فى الحال دون انتظار فى الذاكرة
URG يبعث طلب لـ ذاكرة الـ Stack الموجودة فى نظام التشغيل يخبرة بترك كل ما يفعله ويفعل هذا الطلب الأن أقرب مثال اليها هو عند عمل الأمر بينج ثم الضغط على أزرار Ctrl+C لعمل انهاء للأمر .
FIN يستخدم عند طلب إنهاء الإتصال ويجب أن يتم التصديق على الطلب بـ الفلاج ACK أى يجب أن يجب الطرف الأخر بالموافقة على طلب الإنهاء
RST تستخدم لإنهاء الإتصال من طرف واحد دون انتظار الموافقة من الطرف الأخر

طرق المسح الأخرى تتم عن طريق ارسال بعض هذه الفلاجز أو كلها وانتظار الرد من خلالها وعلى أساسة يمكننى معرفة هل الجهاز مفتوح أم مغلق

Other Scanning Techniques

1 - TCP Connect (Full Open Scan) :

مثلما قلت سابقا يمكن أن يكون بروتوكول الـ ICMP المسؤل عن الأمر بينج مغلق فى جدار الحماية لذلك نقوم بالاحتيال عليه عن طريق ارسال باكت محملة بـ طلب اتصال

SYN Flag

فى هذه الحالة اذا جاء الرد على هيئة فلاج SYN /ACK

معناه ان البورت مفتوح ويكمل الجهاز باقى خطوات الإتصال أو ينهيه اذا أراد ويكفى أنه عرف أن الجهاز مفتوح بالفعل

2 - Stealth Scan (Half-open Scan)

فى هذا النوع يتم نصف الإتصال فقط بمعنى ارسال الطلب فقط وينتظر الرد عليه ولا يكمل الإتصال

الحالة الأولى

اذا رد الجهاز المستقبل بـ فلاج SYN/ACK هذا معناه أن هذا البورت مفتوح والجهاز بدوره مفتوح وفى انتظار اتمام الاتصال حينها يقوم الجهاز المرسل بإرسال RST لإنهاء الإتصال قبل أن يكتشف الجهاز المستقبل من هو الجهاز المرسل

الحالة الثانية:

اذا رد الجهاز المستقبل بـ RST هذا معناه ان هذا البورت مغلق وحينها يقوم بتجربة ارسال الإتصال على بورت أخر أو أن الجهاز مغلق بالفعل

3 - Xmas Scan

هذا النوع من الفحص يسمى بـ شجرة الكريسماس دليل على ارسال كل الفلاجز فى الباكت وانتظار الرد من الجهاز المستقبل

الحالة الأولى

اذا لم يصل رد هذا معناه ان البورت مفتوح وبالتالى الجهاز مفتوح

الحالة الثانية

اذا تم الرد بـ فلاج RST هذا معناه ان هذا البورت مغلق وحينها يقوم بتجربة ارسال الإتصال على بورت أخر أو أن الجهاز مغلق بالفعل

4 - FIN Scan :

فى هذا النوع من الفحص يتم ارسال الفلاج FIN وانتظار الرد من الجهاز المستقبل

الحالة الأولى:

اذا لم يصل رد هذا معناه ان البورت مفتوح وبالتالى الجهاز مفتوح

الحالة الثانية :

اذا تم الرد بـ فلاج RST هذا معناه ان هذا البورت مغلق وحينها يقوم بتجربة ارسال الإتصال على بورت أخر أو أن الجهاز مغلق بالفعل

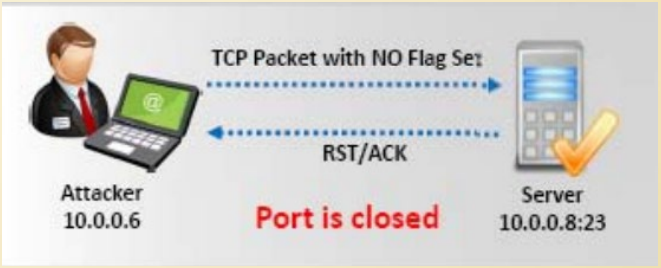
5 - NULL Scan

فى هذا النوع يتم ارسال الباكت خالية من أى فلاجز وانتظار الرد من الجهاز المستقبل

الحالة الأولى

اذا لم يصل رد هذا معناه ان البورت مفتوح وبالتالى الجهاز مفتوح

الحالة الثانية



اذا تم الرد بـ فلاج RST هذا معناه ان هذا البورت مغلق وحينها يقوم بتجربة ارسال الإتصال على بورت أخر أو أن الجهاز مغلق بالفعل

Port Scanning - 2

بعد أن قمت بعمل مسح شامل للشبكة ومعرفة الأجهزه المفتوحه حان الوقت لاختيار جهاز والتعمق أكثر فى تفاصيلة مثل سرعة المعالج وحجم الذاكرة ونظام التشغيل المستخدم و ... غيره من التفاصيل التى لا نلقى لها اهتمام ولكن هناك من يهتم مثل الهاكرز ويهمه أن يعرف كل صغيره عن الجهاز المستهدف لتحديد كيف سيقوم بالدخول اليه لعمل ذلك يتطلب أن يعرف المنافذ المفتوحة فى هذا الجهاز وبما أن كل منفذ مفتوح يقدم خدمات مثل خدمة التصفح , الشات أو الايميل فانه سيحاول الدخول الى جهازك من واحد من هذه المنافذ ولذلك كان لابد من عمل Port Scan الذى تكون نتائجه هى رقم المنفذ والخدمة الموجوده عليه حاليا ويتم عمل هذا النوع من المسح عن طريق أدوات مسح النوافذ وأشهرهم أداة Nmap أداة مفتوحة المصدر موجودة بشكل افتراضى فى بعض توزيعات نظام تشغيل لينكس وهى عبارة عن سطر أوامر وله أيضا واجهة رسومية لمستخدمى نظام تشغيل ويندوز تقوم بفحص المنافذ على جهاز معين أو مجموعة أجهزة وتنتظر نتيجة الفحص التى تكون على هيئة رقم المنفذ المفتوح واسم الخدمة التى تعمل عليه

مثال لشكل النتيجة الظاهرة عند عمل مسح المنافذ على العنوان 192.168.1.2

```
Starting Nmap 5.61TEST5 ( http://nmap.org ) at
2012-04-04 12:20 Egypt Standard Time
NSE: Loaded 92 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 12:20
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 12:20, 0.26s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:20
Completed Parallel DNS resolution of 1 host. at 12:20,
0.11s elapsed
Initiating SYN Stealth Scan at 12:20
Scanning 192.168.1.2 [1000 ports]
Discovered open port 445/tcp on 192.168.1.2
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 3389/tcp on 192.168.1.2
Discovered open port 554/tcp on 192.168.1.2
Discovered open port 135/tcp on 192.168.1.2
Discovered open port 2869/tcp on 192.168.1.2
Discovered open port 10243/tcp on 192.168.1.2
```

Vulnerability Scanning - 3

المرحلة الأخيره وهل مرحلة اكتشاف نقاط الضعف الموجوده فى الشبكة , لكل خدمة على منفذ بعض نقاط الضعف حسب اصدارها منها القديم والمعروف نقط ضعفه ومنها الحديث الذى تأخذ وقت فى اكتشافه أشهر برامج كشف هذه النقط هو Nessus

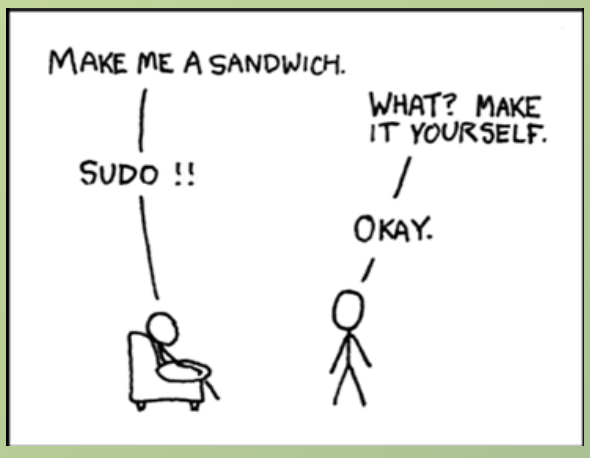
لعمل مسح للشبكة يجب أن تكمل الثلاث مراحل بنفس الترتيب لان كل مرحلة تنقلك للتى تليها

Sudo command

Super user do

فى اى موسسه يكون كل team عباره عن عدد من الافراد المسئولين عن شىء معين, فيكون هناك مثلا Oracle database team, and Unix Administrators team وهكذا. بالطبع كل فريق يكون مسئول عن شىء معين مثل نظام التشغيل او قواعد البيانات و يكون لديه صلاحيه privilege على هذا النظام او التطبيق الذى يعمل عليه. فى حاله اليونكس او اللينكس المستخدم الذى يمتلك كل الصلاحيات على نظام التشغيل هو root لذلك تخيل معى هذا الموقف, لديك مثلا عشره اشخاص يديرون نظام التشغيل سواء كان لينكس او يونكس وكلهم مسئولين عن النظام, اذا لنتخيل انه مشكله ما حدثت فهل تستطيع تحديد اى من العشره هو المتسبب ومن منهم الذى يجب عليه تصليح هذا الخطا, لذلك فمثل هذا الموقف معضله ضخمه ان تترك النظام هكذا بجانب احتمال ضياع كلمه السر من احدهم وغيرها وغيرها من المخاطر الى يمكن حدوثها.

من هنا اتت فكره بما ان root يمتلك كل الصلاحيات فلما لا نوزع هذه الصلاحيات على المستخدمين, بمعنى انه نوزع صلاحيات root على printers لمجموعه من المستخدمين العادين وصلاحياته على hard disks لمجموعه من المستخدمين العادين وبالتالى انت قمت بتخصيص المهمام حيث انه فى مثل هذه الحاله اذا حدث مشكله فى الطابعه مثلا تعرف من المتسبب ومن عليه اصلاح هذا وايضا فى hard disks وغيرها من الامور .



فكره sudo قائمه على هذا توزيع المسئوليات لمنع التضارب بين المستخدمين .ولكن كيف ؟

1 - مقدمه عن sudo

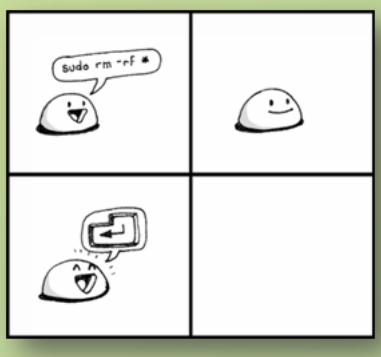
هى عباره عن اداه من خلالها تستطيع ان تجعل مستخدم عادى على نظام التشغيل ان يقوم باشياء تحتاج الى root لكى يتم تنفيذها على النظام وبدون ان يقوم النظام حتى بطلب root password منك .

2 - هل هناك ادوات اخرى مثل sudo ؟

طبعا هناك مثلا الامر su وهو يعنى switch user وهنا انت تقوم بالدخول كمستخدم عادى على النظام ثم تحول نفسك الى root عن طريق الامر التالى su – root وبالتالى انت تستطيع ان تمتلك كل صلاحيات root وان تفعل ما تشاء على النظام هناك ايضا ما يعرف باسم roles, and authorization وهى باختصار توزيع الادوار على المستخدمين وصلاحيتهم على السيرفر وما يستطيعوا ان يقوموا به وما لا يستطيعوا ان يقوموا به .

3 - هل sudo افضل ام su ؟

لكل منهما مميزاته وعيوبه وايضا من خلال sudo تستطيع ان تنفذ امر su و تمنعه ولكن الافضل من وجهه نظرالاغلبيه هو sudo لانها وباختصار تمتلك configuration file يسمى etc/sudoers/ الذى تستطيع ان تقوم بتعديله من خلال الامر visudo وبالتالى فهذا افضل لانه يعطيك امكانيه التحكم فى ما تريد فعله اكثر.



4 -كيف يتم تنصيب sudo package ؟

فى انظمه مثل اللينكس تاتى مع النظام لكنك ايضا يمكن تنزليها على السيرفر اذا احببت .

5 -كيفيه التعديل فى sudo configuration file ؟

ذلك يكون من خلال visudo فهو امر يفتح الملف الخاص بالاداه لكى تقوم بكتابه التعديلات فيه ولكن كيف يتم كتابه هذه التعديلات ؟
يكون شكل entry فى هذا الملف كالتالى :

Username/groups servername = (users commands can be run as) commands

Username/group

فهو عباره عن اسم اليوسر الذى سياخذ الحق فى تنفيذ هذه الاوامر او group والتى هى عباره عن مجموعه من المستخدمين ولاحظ انه عند كتابه group نقوم باضافه ٪ قبلها لتميزها عن اسم السمتخدم مثل ٪wheel ايضا يمكنك كتابه اسماء عدد من المستخدمين او من المجموعات وبينهم فصله لكى يميز النظام بينهم مثل الاتى :
Smith, Mohamed, Ahmed, ٪samba, ٪apache

Servername

اسماء السيرفرات التى سيتم تطبيق عليها هذا entry وهى هنا فى اغلب الاحوال نكتب بجانبها (ALL) والتى تعنى الكل اى ان هذا entry سيطبق على الكل

```
File  Edit  View  Search  Terminal  Help
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem


## Command Aliases
"/etc/sudoers.tmp" 107L, 3531C
```

الملف الخاص sudo والذى يتم فيه كتابه التعديلات التى نريدها

Commands

الاوامر التى ستعطى الحق للمستخدم فى القيام بها ولكن عليك ان تلاحظ انك اذا قمت مثلا باعطاء المستخدم Mohamed فى استخدام الامر التالى mount لكى يقوم Mohamed باستخدام هذا الامر ان يكتب التالى : sudo mount فيقوم النظام بسواله عن كلمه السر الخاصه به واذا اردت ان ينفذ الامر بدون السوال عن كلمه السر الخاصه بك فهناك entry وهو NOPASSWD يفعل ذلك كما سنرى فى الامثله الاتيه .

والان مع بعض الامثله لتوضح الاداه :

1 - Mohamed ALL=(ALL) ALL

وهذا معناها ان المستخدم محمد يستطيع القيام ياى امر يكتبه بعد sudo اى انه اصبح مثل root على نظام التشغيل .

2 - Mohamed ALL= /usr/sbin/visudo, /usr/sbin/mount

وهذا معناها ان محمد يستطيع فقط ان يقوم بتشغيل هذين الامرين فقط لا غير .

3 - Mohamed ALL= NOPASSWD: /usr/sbin/visudo, /usr/sbin/mount

هذا يعنى ايضا ان للمستخدم محمد الحق فى استخدام هذين الامرين ولكن من غير ان يقوم بداخل كلمه السر الخاصه به للنظام .

```
File  Edit  View  Search  Terminal  Help
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCE
SSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now
hikal ALL=(ALL)     ALL
ahmed  ALL=/usr/sbin/visudo, /usr/sbin/mount
mohamed ALL= NOPASSWD: /usr/sbin/visudo

-- INSERT --
```

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

Upgrading and Downgrading CISCO Access Points

عند شرائك أو تعاملك مع أجهزة الأكسس بوينت من سيسكو أو غيرها لابد أن تعرف اي وضع أو نمط يعمل فيه الجهاز و يتم معرفة نوع نمط الجهاز في سيسكو من اسم موديله فتعتبر الكلمة "LAP" معبرة عن نمط lightweight كما في موديل AIR-LAP1252AG-E-K9 و تعتبر الكلمة "AP" أو "BR" معبرة عن النمط IOS أو Standalone أو autonomous كما في الموديلين AIR-AP1242AG-x-K9 و AIR-BR1310G-x-K9

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

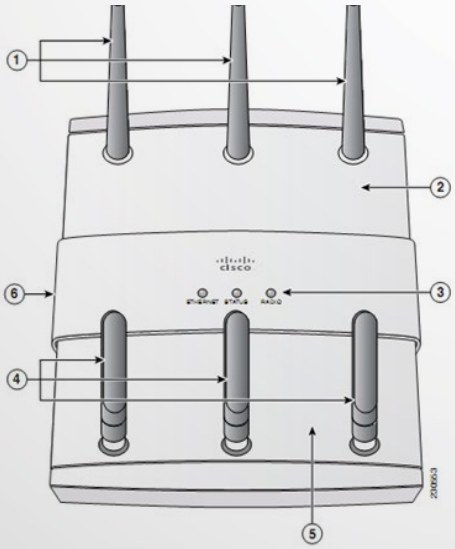
و نظرا لإحتمالية زيادة عدد الأكسس بوينت و لجوء الشركات لزيادة اعتمادها عليه فإنها قد تحتاج الي تغيير أجهزتها Standalone الي Lightweight و هذا يتطلب ميزانية جديدة و لهذا عملت سيسكو علي ايجاد وسيلة لتحويل الأكسس بوينت من الوضع Standalone الي Lightweight بدون الحاجة لتغيير الأجهزة و العكس و هذه هي أنواع الأجهزة التي تدعم عمل النمطين عبر عمليات upgrade و downgrade

Cisco Aironet **1250** AG Series Access Points
Cisco Aironet **1240** AG Series Access Points
Cisco Aironet **1230** AG Series Access Points
Cisco Aironet **1200** Series Access Points
Cisco Aironet **1130** AG Series Access Points
Cisco Aironet **1100** Series Access Points

و هذه الأجهزة لا تعمل في نمط lightweight الا في وجود كنترولر و لابد أن يكون الكنترولر يدعم عمل هذه الأجهزة

و تستطيع أن تحول الجهاز للعمل بين النمطين ليتوائم ومتطلبات شبكتك و ذلك تبعا لنوع الجهاز و مدي دعم سيسكو لهذا التحويل في الجهاز و تسمي عملية التحويل من النمط المنفرد الي المتكامل بعملية Upgrade و أما العملية العكسية فتسمي Downgrade

و سنتعامل هنا مع جهاز Cisco Aironet **1250** AG Series Access Points و الذي تراه في الشكل التالي



1	2.4-GHz radio antenna	4	5-GHz radio antenna
2	Module slot 0 (2.4-GHz radio module shown)	5	Module slot 1 (5-GHz radio module shown)
3	LEDs	6	PC cable security slot

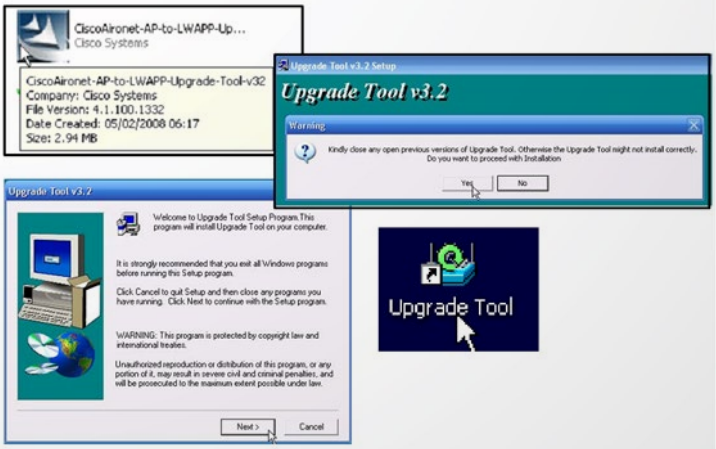
التحويل من IOS الي LWAPP

تستطيع تحويل Standalone AP الي وضع Lightweight AP اي عمل Upgrade بعدة طرق

أحدهما أداة التحويل CISCO IOS-to-LWAPP و هو برنامج صغير يعمل علي ويندوز
و الطريقة الثانية هي بإستخدام سيرفر WCS من سيسكو و الذي يراقب و يتحكم في جميع أجهزة الكنترولر في الشبكة
و أما الثالثة فهي بإستخدام موجه الأوامر CLI
و اما الرابعة فبإستخدام واجهة الويب المرئية GUI

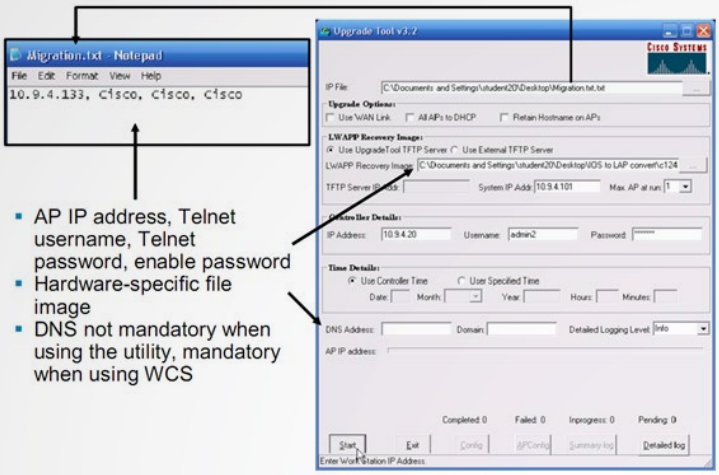
و لتحويل الأكسس بوينت من وضع IOS الي وضع LWAPP فإنه لابد أن يتوفر التالي
أولا لابد أن يكون نظام تشغيل الأكسس بوينت لا يقل عن JA 12.3(7)
ثانيا سيرفر سيسكو WCS لابد أن يكون من النسخة 3.1 علي الأقل
ثالثا نسخة نظام تشغيل الكنترولر لا يقل اصدارها عن 3.1 علي الأقل

عند تمام الترقية فإن الأكسس بوينت يفقد القدرة علي امكانية اعداده بواسطة Console كذلك لن يستطيع العمل في الوضع autonomous بالإضافة لذلك فإنه سيدعم فقط Layer 3 LWAPP



و لترقية الأكسس بوينت قم بالخطوات التالية

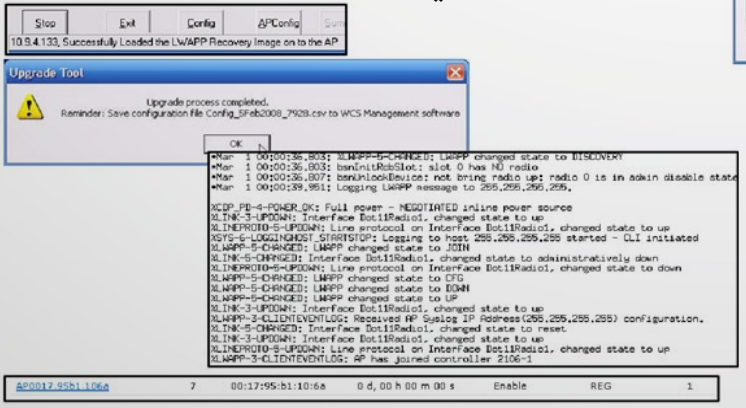
- لابد أن يتخطي الأكسس بوينت المتطلبات الرئيسية و التي ذكرناها مسبقا و لابد أن يكون في نفس subnet مع الكنترولر علي الأقل عند انتهاء عملية الترقية و ذلك كي يوازن نسخة نظام تشغيله من الكنترولر
- قم بتفعيل اتصالات Telnet في الكنترولر من خلال التبويب Management>Telnet-SSH
- قم بالتأكد من توافق إعدادات وقت الكنترولر مع إعدادات و قت جهاز الكمبيوتر الذي تقوم بترقية النسخة منه و قم أيضا بالتأكد من عدم وجود اي فايروول يعمل أو علي الأقل يحجب اتصال TFTP
- قم بفتح البرنامج اداة التحويل Cisco IOS-to-LWAPP و الذي سيحتوي علي الخيارات التي تراها



- في الخانة IP File تستطيع ان تضع ملف به أكثر من IP لأكثر من أكسس بوينت لتقوم بترقية أكثر من أكسس بوينت في نفس الوقت و هذا الملف يكون نصي txt كما تري في الشكل السابق و كل أكسس بوينت توضع في سطر حيث يحتوي كل سطر علي عنوان IP و اسم و باسورد telnet و وضع enable هكذا

ap-ip-address,telnet-username,telnet-user-password,enable-password
ap-ip-address,telnet-username,telnet-user-password,enable-password

- قم بتحميل نسخة IOS الخاصة بالأكسس بوينت الخاصة بك و استخدم سيرفر TFTP الخاص بالبرنامج أو قم بتحميل برنامج سيرفر TFTP آخر ثم اختر النسخة و اضغط start
- سيقوم بعدها البرنامج بالبدء في عملية الترقية بالشكل الذي تراه

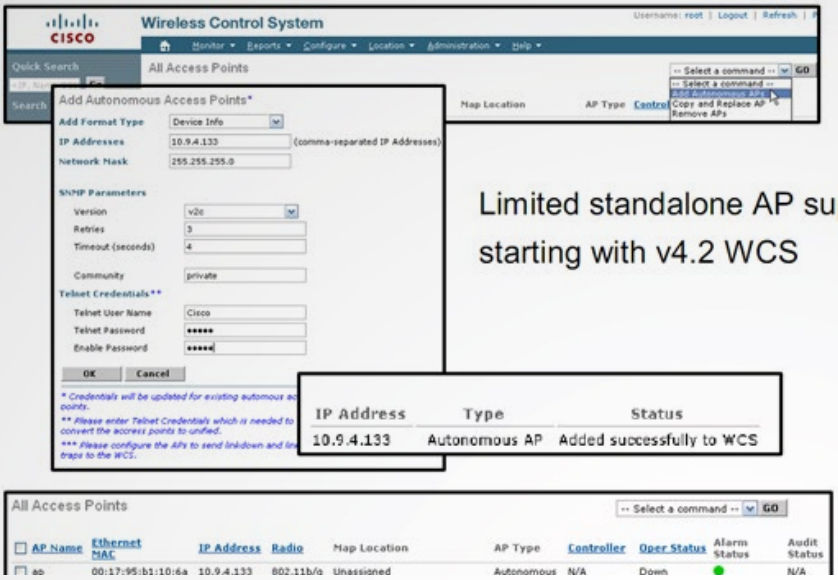


- عند اكتمال الترقية يعيد تشغيل الأكسس بوينت تصبح Lightweight AP ثم تبدأ في البحث عن الكنترولر و عندما تجده و توثق نفسها لديه تجلب منه نسخة اعداداتها و تبدأ في العمل ضمن فريقه

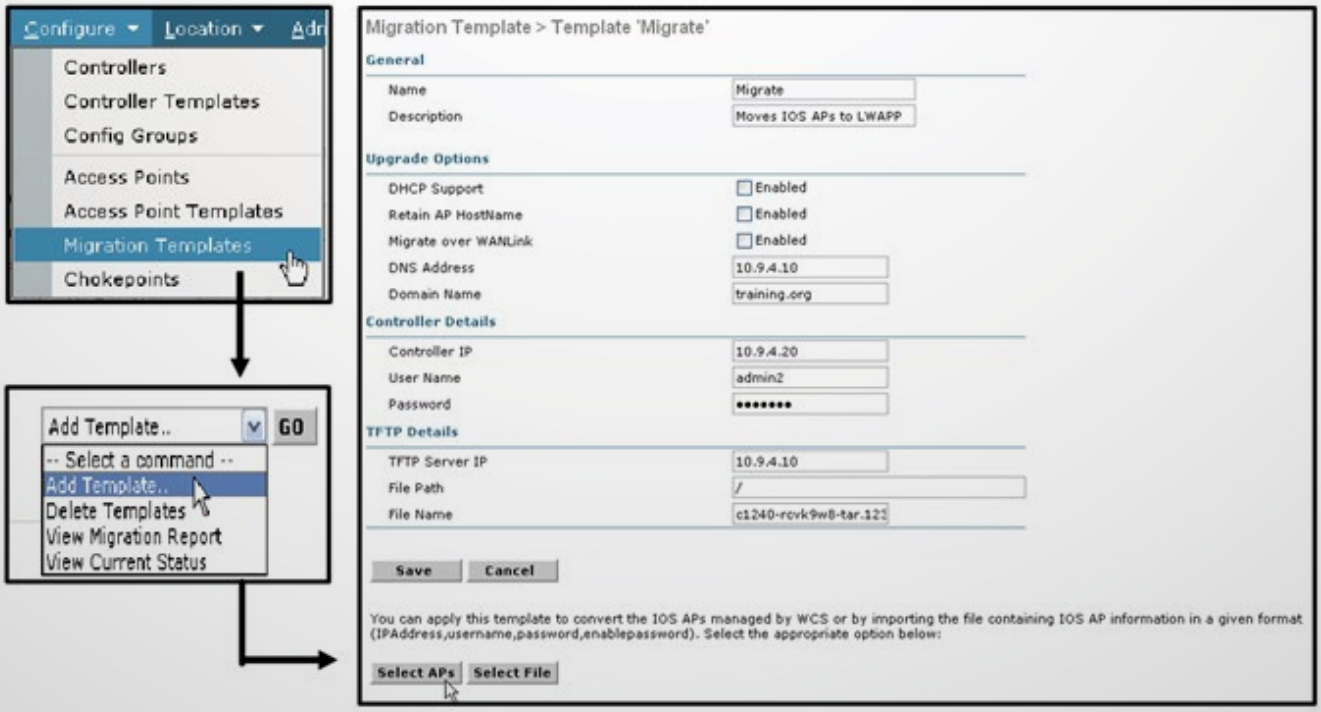
الطريقة الثانية بإستخدام WCS

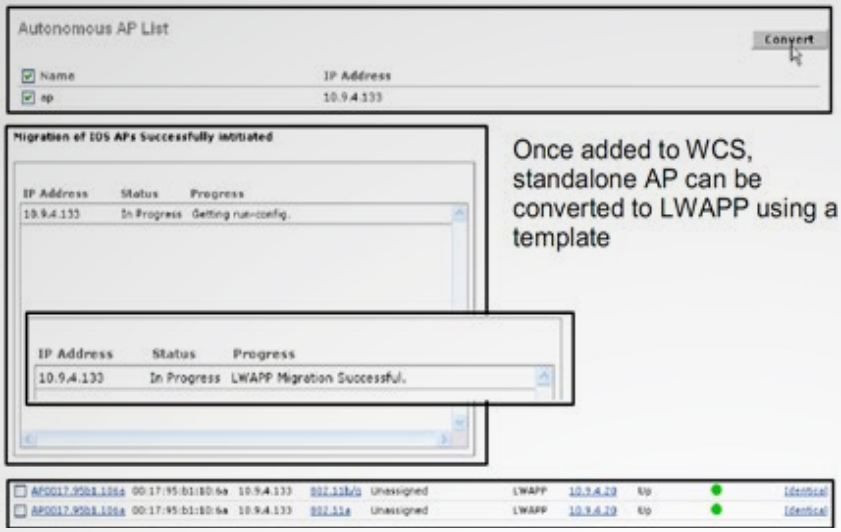
سيرفر Wireless Control System هو المتحكم العام في الشبكة اللاسلكية و يستخدم في الشبكات الكبيرة جدا و التي قد تتعدي أجهزة الكنترولر بها العشرات و سنشرح مستقبلا بإذن الله و بشيء من التفصيل هذا البرنامج الجبار من سيسكو و الذي يستطيع ان يعمل علي أكثر من منصة للسيرفرات مثل Linux Red hat و Windows Server

من الإصدار 4.2 و الذي يليه فقد تم اضافة امكانية أجهزة الأكسس بوينت في الوضع standalone مع وجود بعض القيود طبعا و بما انه تم ادارتها من خلال هذا السيرفر فإننا نستطيع ايضا أن نجري عليها بعض العمليات و منها ترقيتها upgrade



- من الصفحة الرئيسة لسيرفر WCS قم بالدخول علي Configuration>Access Points ثم قم من القائمة التي علي يسار البرنامج بإضافة Autonomous AP ثم Go
- قم بإدخال بيانات الأكسس بوينت و كلمات المرور و غيرها مما يخص الأكسس بوينت ثم OK
- عند نجاح العملية سيتم اضافة الأكسس بوينت لتظهر كما تري في الشكل السابق
- بمجرد أن يتعرف WCS علي الأكسس بوينت تستطيع حينها ترقيته الي LWAP من Configure>Migration template ثم قم بـ Add Template و GO
- ستظهر لك صفحة جديدة قم بإدخال وصف للعملية التي تريدها كما تري في الصورة ثم احفظ ما صنعت ليظهر بعدها زر لإختيار الأكسس بوينت التي تريد العمل عليها





- قم بإختيار الأكسس بوينت التي تريدها ثم Convert
- سيقوم WCS بالإتصال بالكنترولر الذي سيستضيف الأكسس بوينت بعد تحويله ثم يتصل بـ TFTP server و بالأكسس بوينت ثم يقوم بالتحويل مع ظهور شاشة تبين تقدم العملية

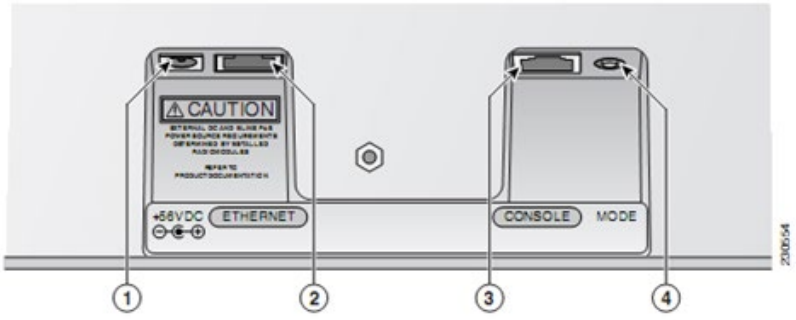
بمجرد الإنتهاء من هذا الأمر تصلك رسالة تخبرك بنجاح العملية و عند حدوث أخطاء تخبرك بما يجب عليك عمله

التحويل من LWAPP الي IOS

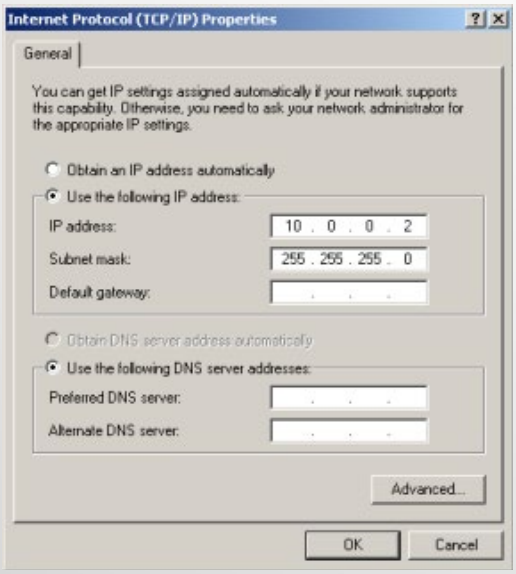
تستطيع التحويل أيضا من Lightweight AP الي Standalone AP أي عمل Downgrade بعدة طرق تعتمد علي حالة الأكسس بوينت فإن كانت الأكسس بوينت متصلة مسبقا

أولا بإستخدام الزر Mode

لأن الأكسس بوينت متصل بالكنترولر فإنه لابد عند تحويله أن يتم تجاهل النسخة الموجودة فيه و لا يتم ذلك الا عند اعادة تشغيله و الضغط على الزر mode و الذى يوجد متخفيا تقريبا بجوار مخارج الأكسس بوينت 1250 مثلا

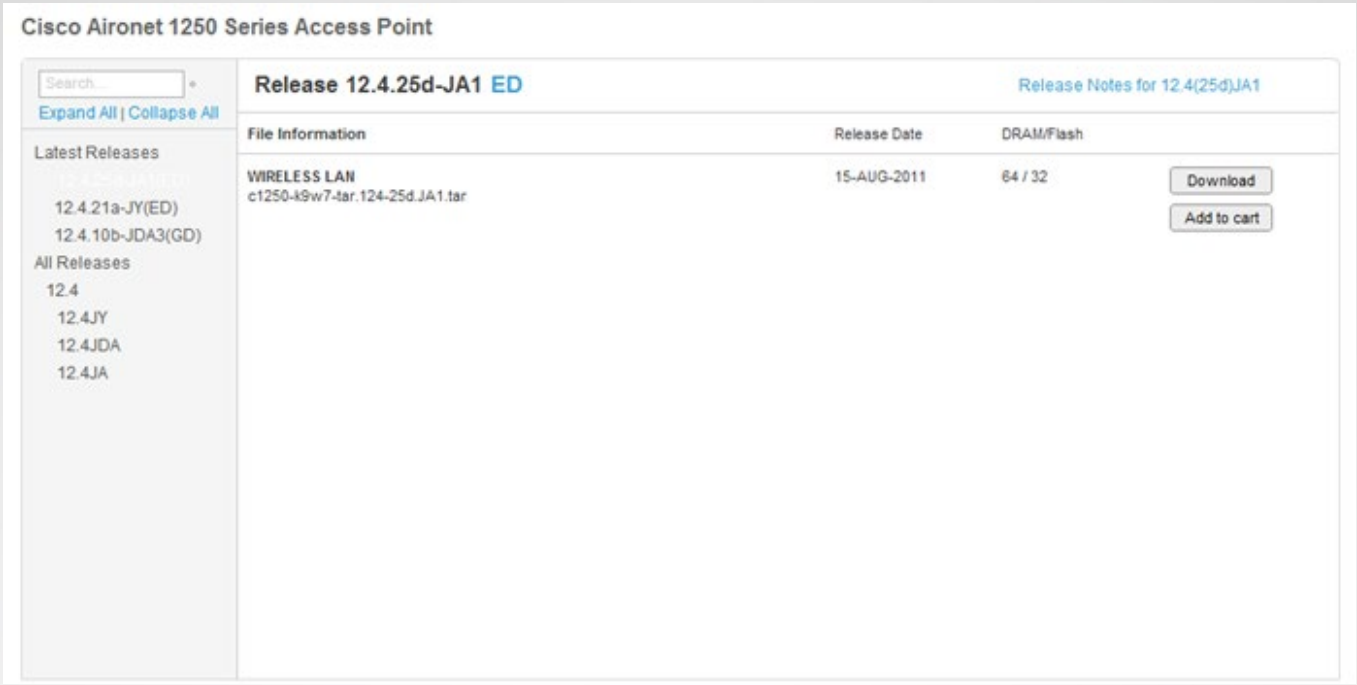


1	DC power connector (+56 VDC)	3	Console port (RJ-45)
2	Ethernet port (RJ-45)	4	MODE button



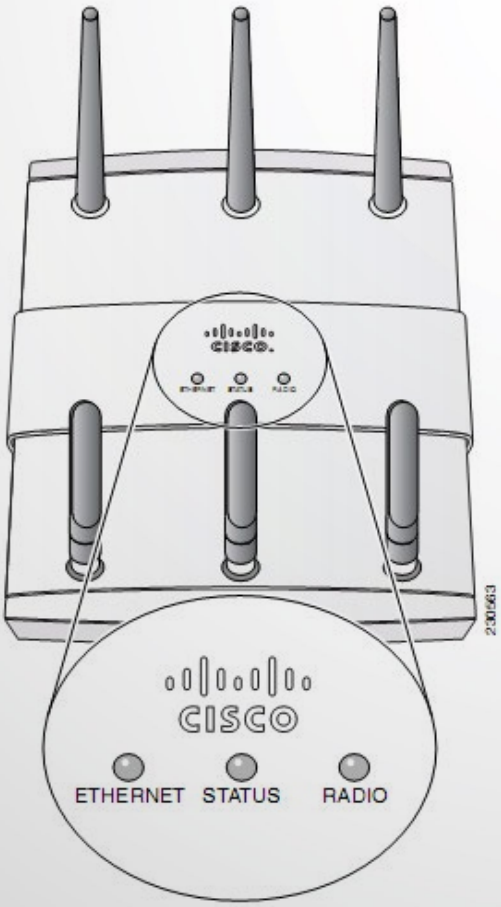
قم في البداية بإعداد جهاز كسيرفر TFTP بأحد البرمجيات المعروفة مثل SolarWinds free TFTP server أو TFTP server recommended by Cisco ثم قم بعمل اي بي ثابت له ضمن هذا المجال 10.0.0.2 – 10.0.0.30 هكذا مثلا

تأكد من أن الجهاز يحتوي علي نسخة من نظام تشغيل الأكسس بيونت وضعها في المجلد الخاص بالسيرفر TFTP و تستطيع تحميلها من موقع سيسكو مثل 25d.-c1250-k9w7-tar.124 JA1.tar



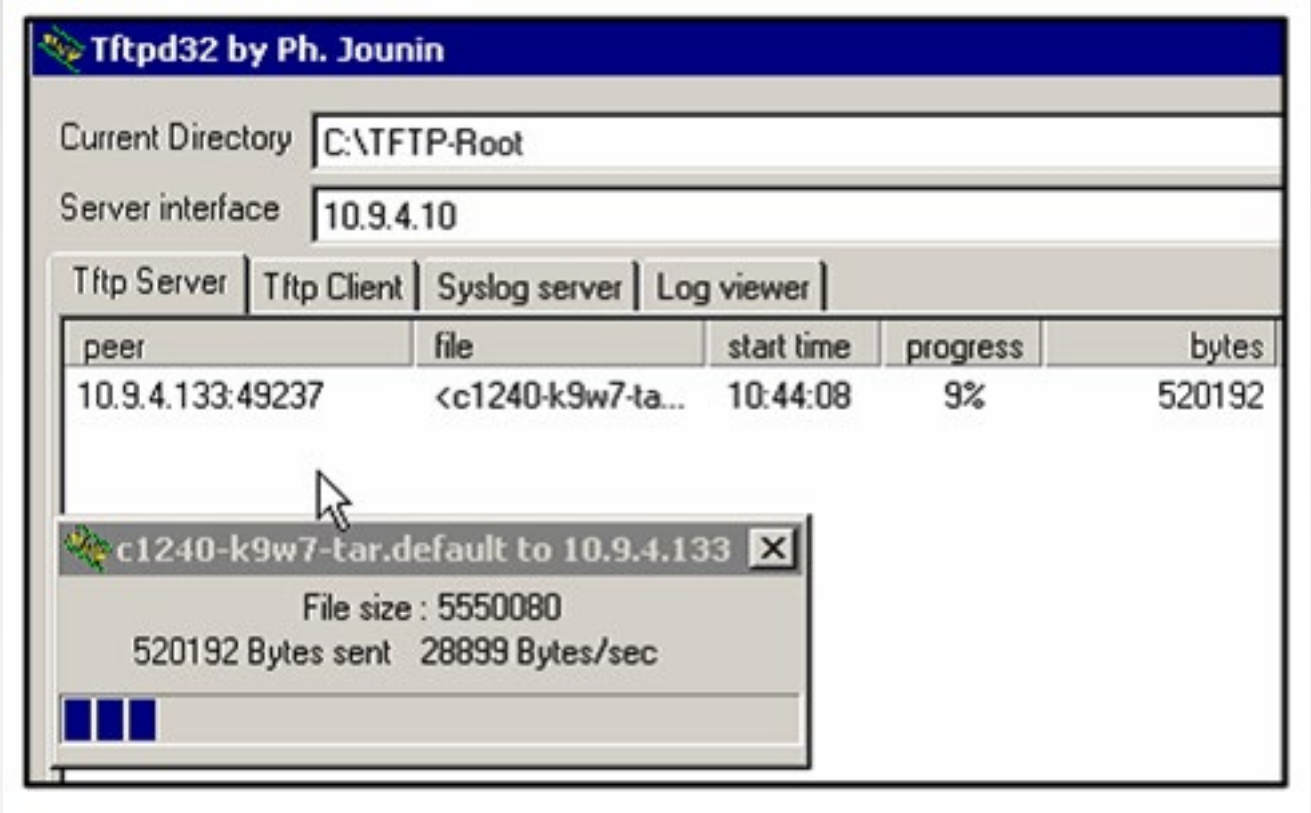
قم بتغيير اسم النسخة الي الإسم الخاص بـ الأكس بوينت هكذا

c1200-k9w7-tar.default for a 1200 series access point
c1130-k9w7-tar.default for an 1130 series access point
c1240-k9w7-tar.default for a 1240 series access point
c1250-k9w7-tar.default for a 1250 series access point



- ثم قم بتشغيل برنامج TFTP مع اختيار مكان النسخة
- وصل الأكسس بوينت بالكمبيوتر مع عدم تشغيل الأكسس بوينت و هنا يجب تنبيهك الي شيء ما ففي حالة استخدام كابل الشبكة كمغذي للطاقة عبر POE فإنه يجب استخدام سويتش يدعم نقل الطاقة عبر مخارجه و يتم توصيل الكمبيوتر به أيضا ليتم عمل اتصال الأكسس بوينت بالكمبيوتر و أفضل سويتش لهذه العملية هو 3750X
- اضغط علي زر mode أثناء اعادتك تشغيل الكهرباء للأكسس بوينت لمدة عشرون او ثلاثون ثانية حتي تحمر مؤشرات الأكسس بوينت LED

- ثم اترك الزر ثم دع النسخة يتم تحميلها و ستري ذلك في شاشة Console و TFTP



- قم بعدها بضبط اعدادات الأكسس بوينت من واجهة الويب بالشكل الذي تريده

الطريقة الثانية بإستخدام Controller CLI

- حمل نسخة IOS الخاصة بالأكسس بوينت و اعد تسميتها بالشكل الذي شرحناه مسبقا و ضعها علي TFTP server
- قم بالدخول علي الواجهة النصية للكنترولر CLI ثم اكتب التالي

- بعد انتهاء التحميل سيقوم الأكسس بوينت بالعمل منفردا و بدون الكنترولر و كأنه أكسس بوينت عادي

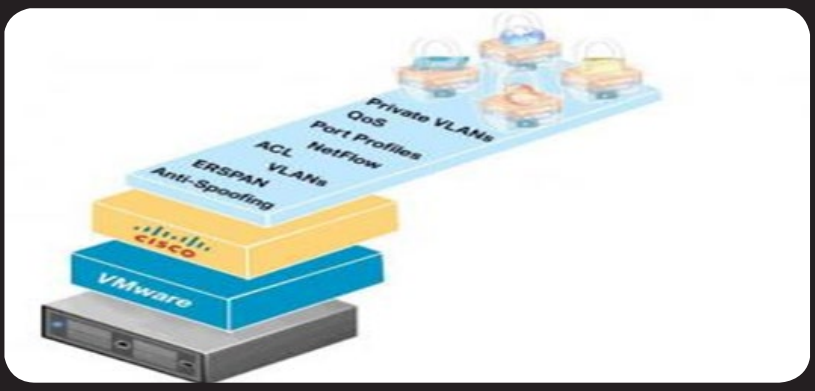
مدخل الى عالم الشبكات فى الـ virtualization Technology

فى خضم التطور السريع فى التكنولوجيا التخيلية وانتشارها السريع على المستوى الاقليمى والعالمى كان لزاما علينا ان نتعرف على عالم الشبكات داخل هذة التكنولوجيا الجديدة الشبكات فى العالم التخيلي تعتبر مشابة بشكل كبير لعالم الشبكات فى العالم الحقيقى لكن يوجد بعض الاختلافات والاختلاف هنا هو فى طريقة ادارة الشبكات نفسها وصيانتها ومتابعتها . لانك فى النهاية لن ترى اى (Switch or Router or NIC or Cable) فى عالم التكنولوجيا التخيلية مع انهم موجودين امامك وتديرهم بنفسك.

كيف ذلك ؟ انها التكنولوجيا التخيلية فماذا تنتظر منها.

يوجد العديد من الشركات العاملة فى التكنولوجيا التخيلية وكل شركة لها اسلوب فى بناء الشبكات داخل سيرفراتها التخيلية لكن الاساس يعتبر واحد ولكن يوجد بعض الشركات تتميز عن شركات اخرى فى التكنولوجيا والمميزات .

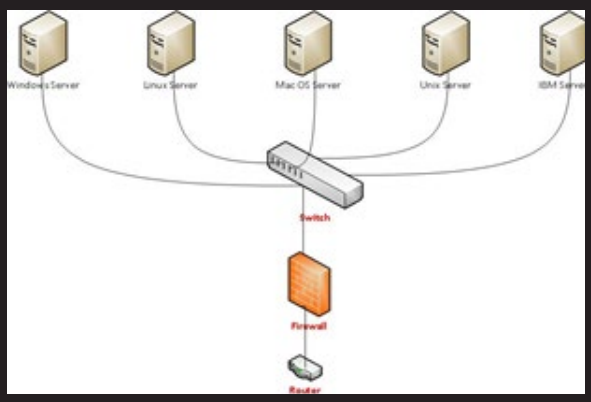
لكن شركة VMware مميزة جدا فى هذة الجزئية عن باقى الشركات لذلك سوف نركز على تكنولوجيا الشبكات عندها تكنولوجيا الشبكات فى عالم التكنولوجيا التخيلية ليس مقتصر على الشركات التى تقوم بعمل السيرفرات التخيلية فقط وانما يوجد شركات متخصصة فى الشبكات قامت بعمل شبكات خاصة بالكتولوجيا التخيلية مثل شركات Cisco قامت بعمل Switch تخيلية Nexus 1000 للعمل داخل سيرفرات VMware



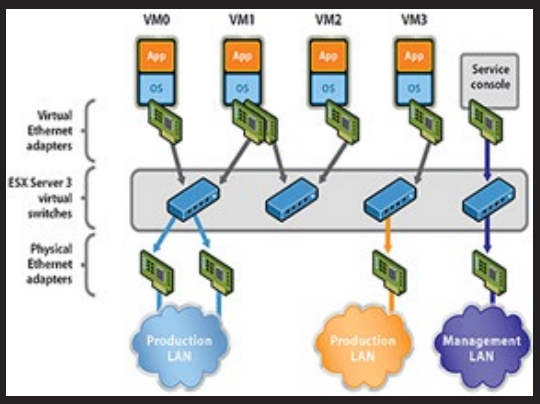
وشركات اخرى قامت بعمل Router & Firewall وكل معدات الشبكات وايضا شركة VMware عندها برنامج للحماية يسمى VShield

كما نرى ان الموضوع ليس بسيط انما لك تفرعات كثيرة وشركات كثيرة تعمل فيه لذلك سوف يكون مقالنا هذا هوا بداية سلسلة من عدة حلقات خاصة بتكنولوجيا الشبكات فى التكنولوجيا التخيلية ، سوف نتكلم فى مقالنا الاول هذا فى الافكار الاساسية فى عالم الشبكات التخيلية ونركز على تطبيقاتها عند شركة VMware

كما ذكرنا ان الشبكات التخيلية تتشابة بنسبة كبيرة فى اسلوب العمل مع الشبكات فى التكنولوجيا التخيلية مثلا يوجد فى الاثنان (Switch – Router – NIC – Firewall – Cable)
لكن الفرق بين مكونات الشبكة هذة فى الشبكات الحقيقية كلها اجزاء ملومسة لكن فى التكنولوجيا التخيلية كل هذة المكونات غير ملموسة انما هى عبارة عن سوفت وير داخل السيرفرات الوهمية نديرة من خلالها
شكل يوضح الفرق بين الاثنين



تصميم لشبكة حقيقية

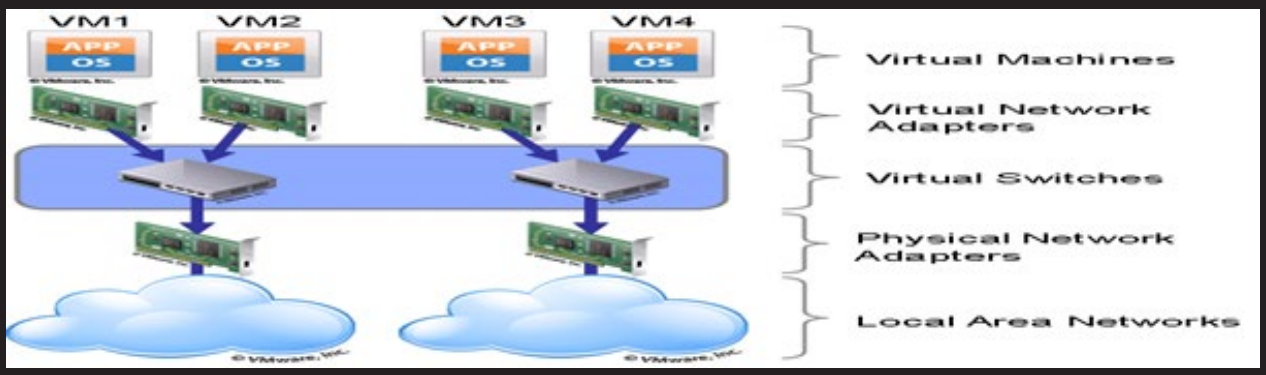


تصميم لشبكة تخيلية

فكرة الشبكات فى السيرفرات التخيلية عبارة عن ان السيرفر الحقيقى التى يتم اعداد عليه VMware Host يكون فية كروت نتورك حقيقية متصلة Switch حقيقى
ومن خلال نظام تشتغيل التخيلى VMware host يتم عمل Switch تخيلية وبورتات تخيلية تتصل بالكارت الحقيقى الخاص بالسيرفر المتصل Switch الحقيقى عن طريق Cable
ثم نبنى على ال vmware host انظمة التشغيل الخاصة بنا ال Virtual Machine وتكون متصلة بال host عن طريق السوتش الوهمى وبذلك تستطيع ال Virtual Machine الاتصال بالعالم الخارجى

ترتيب الاتصال

Switch حقيقى متصل بكابل بالكارت الحقيقى بالسيرفر. السيرفر الحقيقى مبنى على ال Vmware ESXi host ويقوم بعمل علية Switch وهمى يتصل بال Virtual Machine من خلال البورتات الوهمية التى بة والكروت الوهمية الموجودة فى ال Virtual Machine

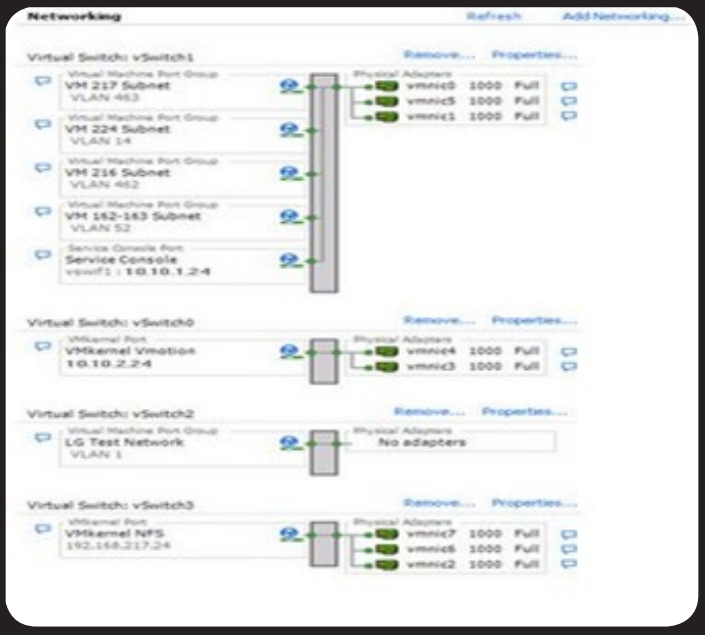


شكل يوضح اسلوب اتصال ال Virtual Machine بالعالم الخارجى عن طريق الشبكة التخيلية

اظن ان الموضوع بداء فى الايضاح بعض الشئ مثل الشبكات الحقيقية يوجد بورتات فى السوتشات وكروت نتورك فى Virtual Machine ويمكن عمل اكتر من كارت
هذة بعض الارقام التى تحدد الحد الاقصى للشبكات عند VMware

Device	Maximum Number
Virtual Ethernet adapters per virtual machine	4
Virtual switch ports per host	4096
Virtual switch ports per switch	1016
Virtual switches per host	248
Uplinks per virtual switch	32
Uplinks per host	32
Virtual switch port groups per host	512
Physical e1000 Ethernet adapters per host	32 (maximum tested)
Physical Broadcom Ethernet adapters per host	20 (maximum tested)
Physical e100 Ethernet adapters per host	26 (maximum tested)

كروت النتورك عند ال Vmware ESXI Host نوعان:



صورة توضح شكل السوتشات والبورتات الكروت الوهمية فى الشبكات التخيلية

1 - VM Network
2 - VMKernel

VM Network : هذة عبارة عن الكروت التى يتصل بها ال VM

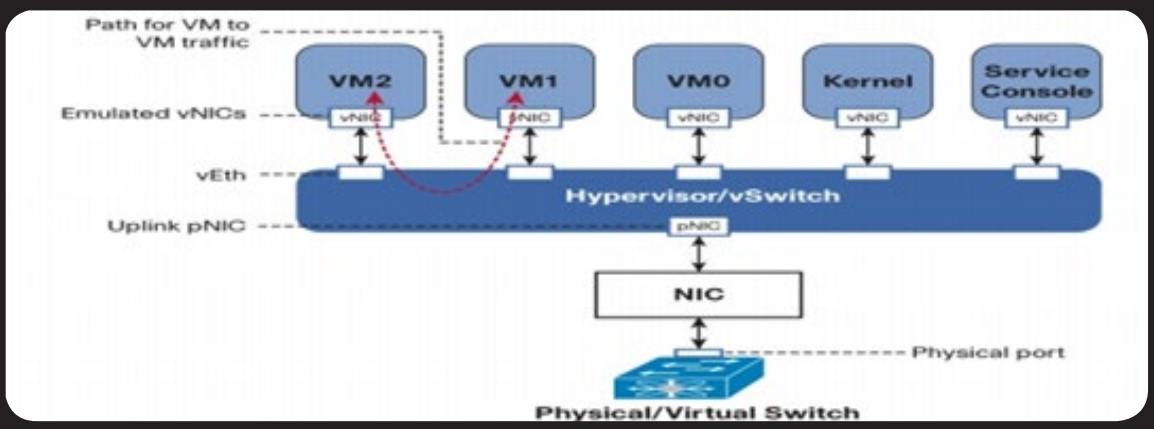
VMkernel : عبارة عن الكروت التى نتصل من خلالها بال SAN and ISCSI and VMotion and Management

انواع السوتشات عند VMware

1 - (Virtual Stander Switch (VSS
2 - (Virtual Distributed switch(VDS

Virtual Stander Switch

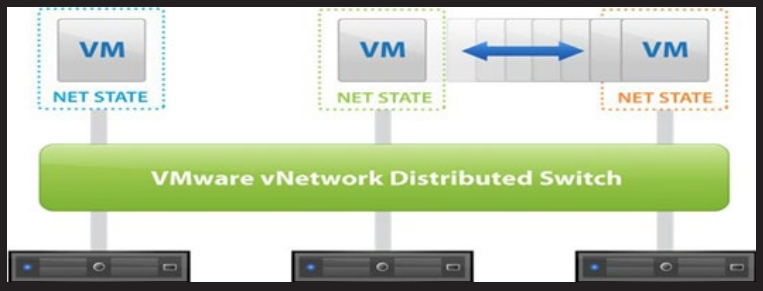
هو عبارة عن Switch يعمل على مستوى سيرفر واحدVMware Host ويربط بين Virtual Machine على مستوى السيرفر الواحد فقط .



صورة توضح ل VSS

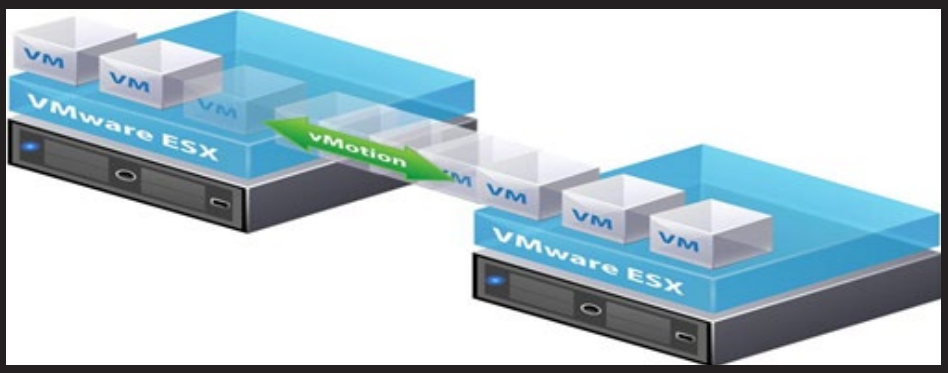
Virtual Disturbed Switch

عبارة عن Switch يعمل على مستوى عدة سيرفرت VMware Hostsويربط بين كل Virtual Machine الموجودعلى هذة السيرفرت .



صورة توضح شكل VDS

هذا تعريف بسيط لانواع Switch عند VMware لكن ما الفائدة عند استخدام الاول عن الثانى او العكس يوجد بالطبع فوائد عدة عند استخدامنا للنوع الثانى وهوا ال VDS
وهوا ان Switch هذا يعمل على مستوى عدة سيرفرات ويعملٍ Switch واحد تتصل بة كل Virtual Machine وهذا يساعد فى عملية ال HA and Vmotion (هذة مصطلحات خاصه VMware وتعبر عن القدرة على تنقل Virtual Machine بين السيرفرات فى حاله ان السيرفر التى تعمل علية يوجد فية مشكلة)



يساعد ال (VDS) الVirtual Machine التى سوف تنقل من سيرفر لاخر فى انها لن تحتاج الى تغير Switch المتصلة بة من السيرفر القديم الى السيرفرالجديد لان السيرفرات كلها تعمل بواسطة Switch واحد

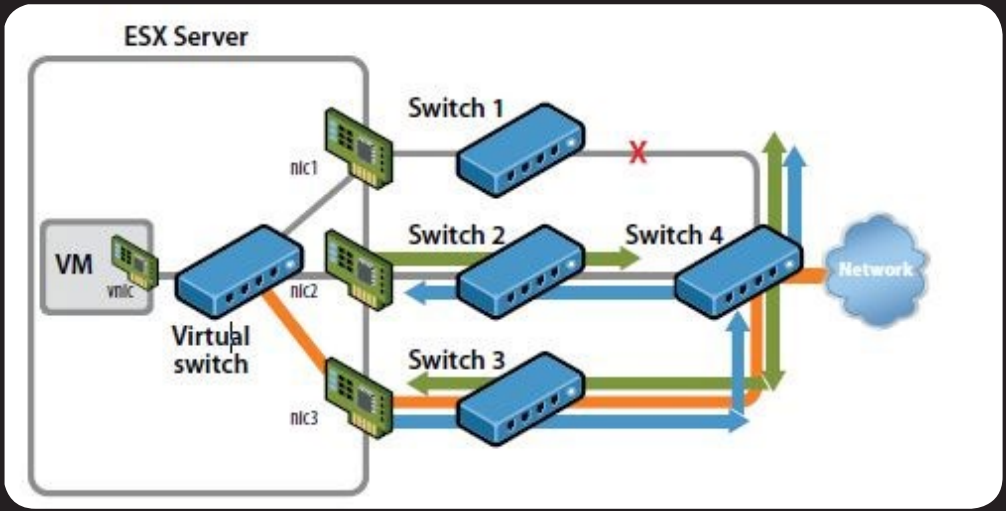
هذه الحالة كانت سوف تفشل فى حالة استخدام السوتش من نوع ال Virtual stander switch لانه عندما تنتقل Virtual Machine من السيرفر الاول وتنتقل الى سيرفر اخر وكان اسم Switch مختلف بين سيرفرين ففى هذا الحالة تتوقف Virtual Machine عن الاتصال بالخارج (البعض يقوم بعمل نفس اسم Switch موحد على مستوى السيرفرات حتى لا تحدث هذة المشكلة)

توجد ايضا بعض المميزات الاخر الموجود فى السوتشات من نوع ال VDS عن ال VSS

1 - Network Policy
2 - Primary and Secondary Vlan
3 - Net flow
4 - Port mirroring

يمكن عمل VLAN على كلا النوعين من ال Switch's وهى شبيه بال VLAN فى الشبكات الحقيقية

يوجد خاصية Network Team والتى نستفاد منها لعمل HA and Load Balance for Network وهى عباره عن ان Switch الوهمى يمكن ان يتصل باكتر من كارت حقيقى فى السيرفر الحقيقى وهذة الكروت متصلة باكتر من Switch حقيقى وهذا يفيد فى حالة وجد مشكلة فى الكارت او Switch او الكابل الحقيقى . يعمل Switch الوهمى على كارت اخر بدون ما تتاثر اى VM متصلة بهذا Switch وتفيد ايضا بعمل زيادة للسرعة النقل لان الكروت يمكن ان تقوم بالعمل مع بعضها فى نفس الوقت



لن ندخل فى التفاصيل او الاجزاء الفنية لان هدف هذة المقالات هو التعرف على التكنولوجيا ولكن اذا كنت تريد المتابعة من الناحية الفنية يمكنك ان تتابع السلسلة التعليميه وتشاهد هذا الدرس على موقع:

www.vmman.me

سوف يكون هناك مقال اخر على سوتشات سيسكو وايضا الجدار النارى الخاص بشركة vmware

الاتصال عبر الأقمار الصناعية

الحمد لله رب العلمين بعد أن تحدثنا في المقال السابق عن أنواع الهوائيات وبيناها أحببت أن أوضح في هذا المقال بشكل مبسط عن تقنية الاتصالات عبر الأقمار الصناعية .....

ماذ نعرف عن الأقمار الصناعية, لماذا نستخدمها

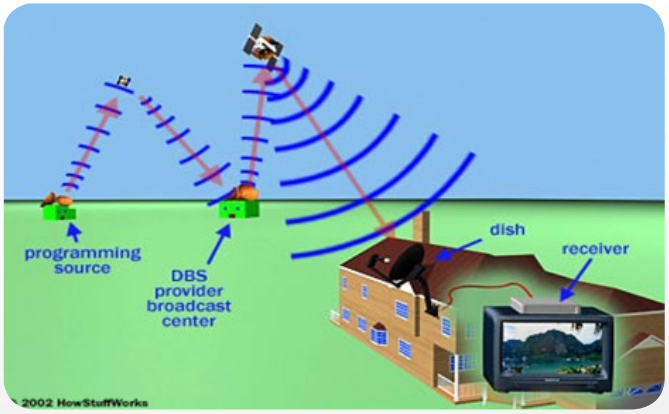
الأقمار عبارة عن محطات تقوية ، تقوم باستقبال أشارة من محطات أرضية معينة وتكبرها ثم تعيد إرسالها باتجاه محطات أرضية أخري وفي هذه الأيام تستخدم هذه الأقمار لنقل الإشارات التلفزيونية بين دول العالم.وفي الأغراض الأمنية والأهداف العلمية والاتصالات من خلال البث الإذاعي .

كيف يتم الاتصال بين محطات الأقمار الصناعية

يتم تبادل المعلومات بين المحطات عن طريق استخدام أقمار صناعية على الأرض ليتم الاتصال بالأقمار الصناعية على الفضاء الخارجي حيث تقوم المحطة المرسلة بإرسال البيانات إلى القمر الفضائي الخاص بعملية الاتصالات

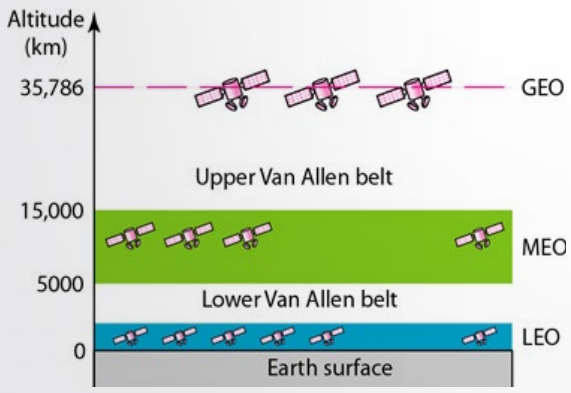
وهذا ما يسمى بعملية (a Uplink) حيث تقوم الأقمار الصناعية (satellite Transponder)

(قابله للإرسال الاستقبال) بتحويل الإشارات المستقبلة وإرسالها إلى محطة الاستقبال على الأرض وتدعى هذه العملية (a Downlink) .....



أنواع الأقمار الصناعية

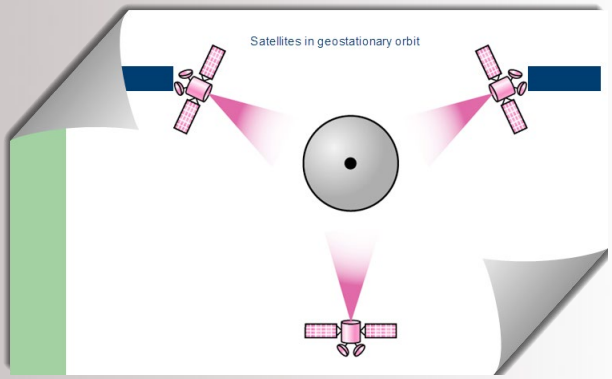
يوجد هنا ك العديد من أنواع الأقمار الصناعية المستخدمة في الاتصالات سنتعرف في مقالنا على نوع واحد هو (Satellite Orbits) يوجد العديد من أنواع هذا القمر الثابت . .



توضح هذه الصور شكل القمر الصناعي في الفضاء الخارجي معا ارتفاعات أقمار Orbits

(Geostationary Earth Orbit (GEO

هذا الأقمار الصناعية في مدار 35,863 KM فوق سطح الأرض على طول خط الاستواء كما أن الأجسام في مدار Geostationary تدور حول الأرض في نفس السرعة عندما الأرض تدور وهذا يعني أن أقمار GEO الصناعية تبقى في نفس الموقع قريب من سطح الأرض .

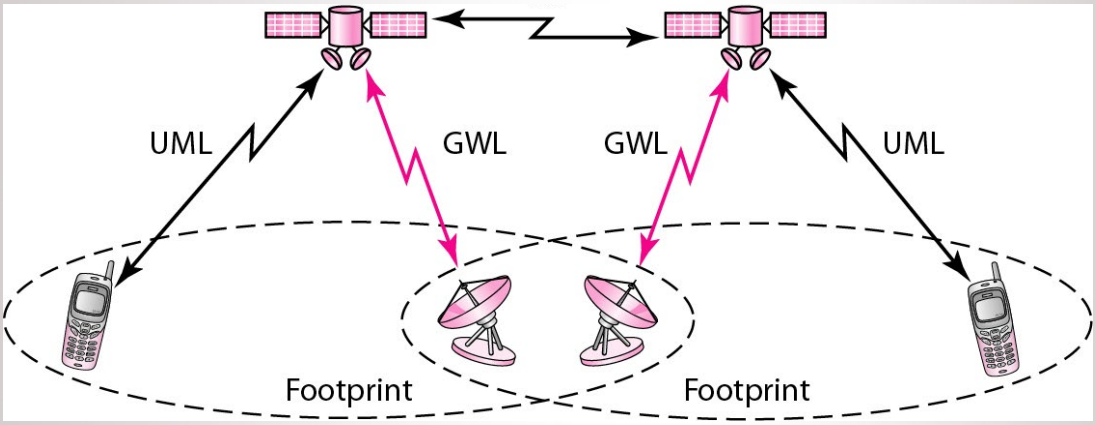


يمتاز قمر GEO إن بعده عن الأرض يعطي تغطية كبير تقريباً ربع سطح الأرض.

من عيوب GEO بعد المسافة عن سطح الأرض مما يسبب ضعف الإشارة و تأخير وقت الإشارة كما أن موقع القمر مركز فوق خط الاستواء يجعله يواجه صعوبة في في عملية نشرا لإشارة broadcasting signals للمناطق القطبية .

(Low Earth Orbit (LEO

أقمار LEO الصناعية أقرب كثير إلى الأرض من أقمار GEO الصناعية يتراوح مداها ما بين 500 إلى 1500 كيلومتر فوق السطح كما أنه لايبقى ثابت في موقعة نسبتاً إلى السطح يمتاز بأن أي قمر LEO قريب إلى الأرض يعطي أشارة قويه وبشكل أفضل معا انخفاض زمن التأخير مقارنةً معا قمر GEO . أقمار LEO تكون غالية الثمن



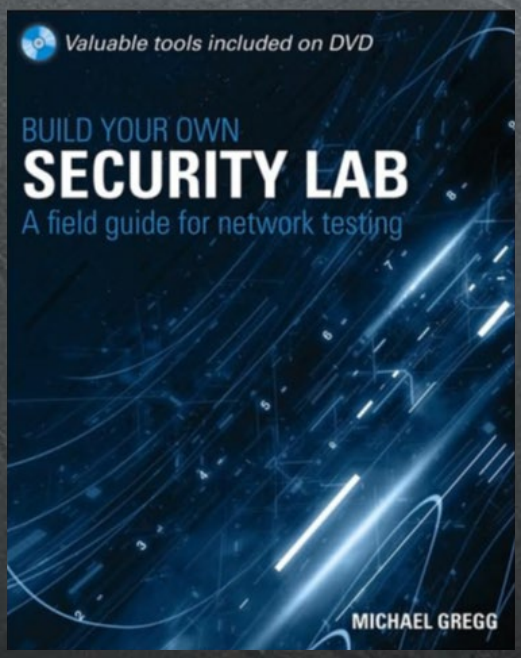
(Medium Earth Orbit (MEO

قمر MEO يقع في مدار ما بين 8000 كيلومتر و18000 كيلومتر فوق سطح الأرض كما أن أقمار MEO مشابهة لأقمار LEO في الوظيفة .تكون هذه الأقمار مرئية لفترات أطول ما بين 2 إلى 8 ساعات كما أن قمار MEO يمتاز بأن لهه منطقة تغطية أكبر من أقمار LEO .من عيوب قمر MEO أنه يعطي زمن طويل للتأخير و أشارة ضعيفة .....

نكون بهذا قد أنهينا جزاء من مقالنا حول الاتصال عبر الأقمار الصناعية أملين أن ينال رضاكم بما قدمناه من معلومات .

كتاب أعجبني

إسم الكتاب :
Build Your Own Security Lab
تأليف : Michael Gregg
دار النشر : Wiley Publishing
اللغة : الانكليزية
عدد الصفحات : 459 صفحة
سنة الاصدار : 2008



عندما نتصفح المواقع والمدونات والمنتديات الخاصة بالشبكات، في بعض الاحيان نبحث عن المواضيع النظرية لمجرد اخذ معلومة سريعة عن الموضوع. ولكن عندما نحتاج الى فهم الموضوع بتعمق، في اغلب الاحيان نفضل المواضيع العملية والتطبيقية. فقد نجد مواضيع متفرقة في صفحات او كتدوينات وتكون غير مكتملة، وكذلك من الصعب ان نجد هذه المواضيع في كتاب وخصوصا عندما تكون مواضيع تغطي العديد من جوانب الشبكات مجتمعة كما في المواضيع النظرية. لهذا ساحاول في هذا المقال تقديم رؤيتي في كتاب اعجبني.

عرفت عن الكتاب من احد الاصدقاء ولكن صراحة لضيق وقتي حاليا لم اطبقه ولكن تصفحته بشكل سريع.. قبل كل شيء سنلقي نظرة سريعة عليه:

كما هو واضح من اسمه فهو كتاب خاص بالسكيورتي، حيث يتيح لك بناء مختبر خاص لعمل تجارب السكيورتي بشقي الاختراق والتامين، اضافة الى انه يقدم الشرح النظري لكل موضوع مع التطبيق العملي. الكتاب يتكون من 11 فصل وهو ينصح به للأشخاص متوسطي الخبرة في مجال الشبكات والسكيورتي بالتحديد. ولكن بشكل عام فهو موجه لكل من يريد فهم طريقة عمل ادوات السكيورتي ولكل من يريد الحصول على شهادة في السكيورتي او التقديم الى وظيفة.

يمكن قراءة الكتاب بأكمله بشكل متسلسل كما يمكن قراءة فصول معينة دون المرور بالفصول السابقة، فمثلا للأشخاص الذين لديهم معرفة بأساسيات الـ IT يمكنهم البدء من الفصل الثالث، ايضا على سبيل المثال الاشخاص الذين يبحثون عن المواضيع الخاصة بطرق التشفير يمكنهم التوجه مباشرة الى الفصل السابع وهكذا وطبعا مع كل فصل تطبيق للموضوع بشكل عملي.. وللتعرف على الكتاب اكثر سأقدم كل فصل مع مواضيعه:

الفصل 1: يشرح كيف تقوم ببناء مختبرك وماهي الادوات التي تحتاجها من معدات وبرامج وانظمة وادوات، وكيف تقوم بتجميعها وربطها وتهيئتها وبعض المعلومات اللازمة للبدء.

الفصل 2: يتطرق الى كيفية تنصيب انظمة التشغيل المختلفة المستخدمة في التجارب بما فيها انظمة الويندوز واللينكس اضافة الى البرامج والادوات الاخرى كالـ VMware وهو موجه للمبتدئين.

الفصل 3: يقدم الطرق المستخدمة في تجميع المعلومات اللازمة للاختراق من تفحص المعدات والانظمة المستخدمة والمعلومات الشخصية وتفحص الـ source code لصفحات المواقع وغيرها.

الفصل 4: يشرح المواضيع النظرية فيما تتعلق بالبروتوكولات اضافة الى طرق تطبيقها مثل ICMP و TCP و HTTP وغيرها وكذلك كيف تعمل بعض الادوات مثلا الـPing والتقنيات المتقدمة المستخدمة في Port Scanning.

الفصل 5: يتعامل مع السكيورتي الخاصة ببروتوكولات الـrouting وادارة الشبكة وانواع الهجوم التي تتعرض لها.

الفصل 6: يقدم الادوات اللازمة لفحص السكيورتي في شبكتك واحتمالية تعرضها للاختراق والتهديدات التي تواجهها.

الفصل 7: يتعامل مع طرق وخوارزميات التشفير والتوثيق المختلفة.

الفصل 8: يتطرق الى الطريقة التي تعمل بها الViruses والTrojans والSpywares والWorms وغيرها من البرامج الخبيثة.

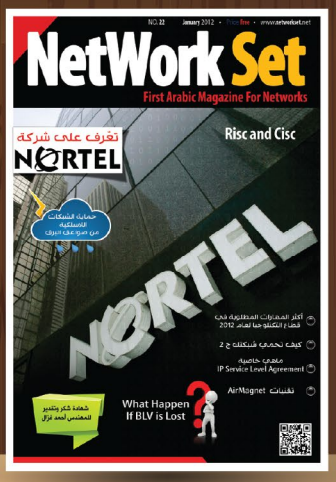
الفصل 9: يشمل كيفية حماية واختراق شبكات الوايرليس.

الفصل 10: يشرح كيف يتم اكتشاف الاختراق في شبكتك (IDS Systems).

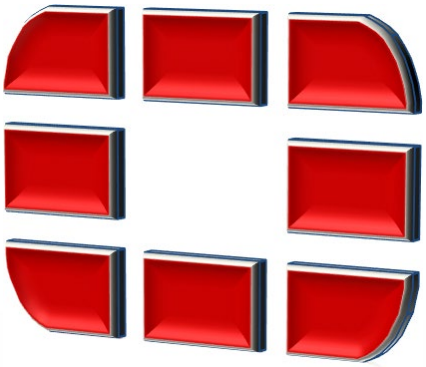
الفصل 11: يوضح الطرق المستخدمة في تعقب وتحليل الاختراقات ومصادرها.

كما شاهدنا فالكتاب يلم اغلب نواحي السكيورتي للمستوى المتوسط، اضافة الى ان اغلب الادوات والبرامج المستخدمة مجانية (مفتوحة المصدر) وهو متوفر على Google books.

Network Set Magazine Gallery



تقرير مفصل عن شركة Fortinet



تعتبر فورتى نت مصدر رئيسي وعالمي لأجهزة أمن المعلومات وتأمين الشبكات وصاحبة مكانة رائدة فى تسويق الاجهزة المسئولة عن إدارة التهديدات والهجمات ضد الشبكة بشكل عام او مايعرف ب «UTM».

منتجات فورتي نت والخدمات المتعلقة بها تقدم حماية على نطاق واسع ومتكامل وعلى مستوي عالي ضد الهجمات المتجددة والتى تهدد امن الشبكة.

يتنوع عملاء فورتي نت مابين المؤسسات الضخمة والشركات المسئولة عن إمداد خدمات الإنترنت «ISP» والمؤسسات الحكومية على مستوى العالم.

يقع مقر الشركة الرئيسي فى مدينة Sunnyvale, Calif.

والتى تأسست عام 2000 بواسطة Ken Xie المؤسس والرئيس والمدير التنفيذي السابق لشركة «NetScreen»تم بيعها بعد ذلك لشركة جونيبر».

تدار الشركة بواسطة فريق إدارة قوي وله خبرة كبيرة جدا فى عالم الشبكات وأمن المعلومات.

ودائما ما تسعى فورتي نت منذ تأسيسها لتثبت جدارتها بأن تكون رائدة فى هذا المجال من خلال بعض النقاط التى تتلخص فيما يلي:-

1 - تبنى او إعتماد كل ماهو جديد فى التكنولوجيا.

2 - جعل الأداء يليق بأن يكون ممثلا لشركة قيادية على مستوى الماركت.

3 - تبسيط السكيورتي لأقصى حد.

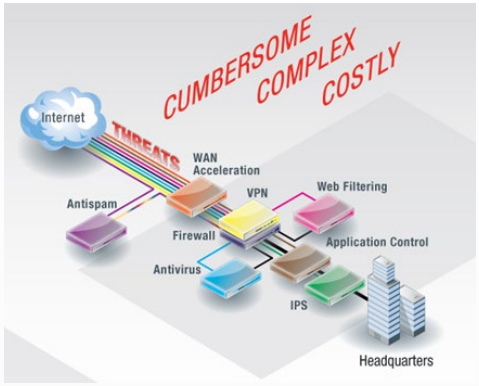
تحقق كل ذلك من خلال رؤية يومية تتمثل فى توقع وإبتكار جديد التكنولوجيا وبالتالى خلق المنافسة التى تضع الشركة فى المقدمة.

- نبذة عن منتجات فورتى نت:

يعتبر الفايروول او مايعرف ب فورتى جيت «fortigate» السمة الاساسية المميزة لفورتى نت حيث انه يقدم سكيورتى متكاملة على اكثر من مرحلة مصممة خصيصا للحماية ضد الهجمات التى تستهدف التطبيقات او الشبكة نفسها.تقدم فورتى نت خط انتاج ضخم للفورتى جيت ليقدم مجموعة من الحلول المتكاملة التى لا تقف عند حدود ال UTM بل تتمتد لتشمل حماية الشركة بأكملها إبتدءا من اجهزة الكمبوتر والمستخدمين ومرورا بال DMZ &Core network مشتملة على التطبيقات وقواعد البيانات.

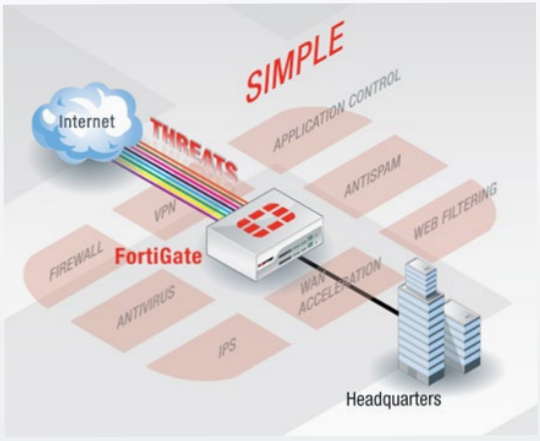
- مقارنة بين فورتى جيت والطرق التقليدية :

الطرق التقليدية لتقديم حلول لتأمين الشبكات
لا تقدم خدمات متكاملة بمعنى ان كل حل مسئول عن

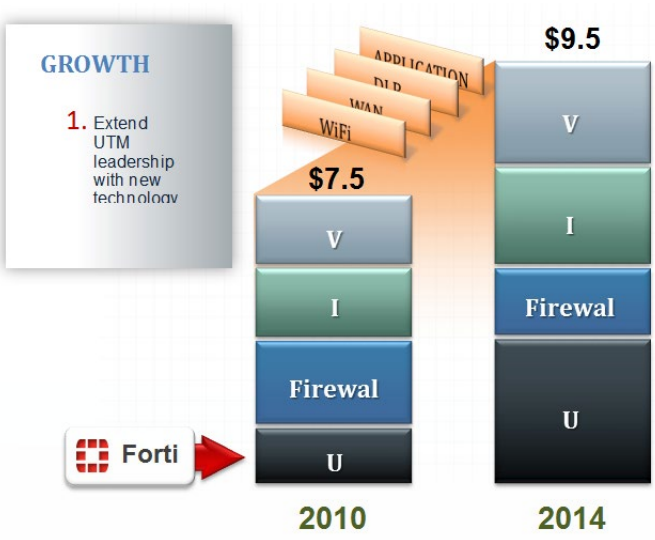


تأمين الشبكة ضد نوع معين من انواع الهجمات وبالتالى لا يوجد حل عام وشامل.
تعتمد على خليط من الاجهزة والتطبيقات تكلفة عالية صعوبة فى التنفيذ والإدارة والإستخدام

حلول فورتى نت:



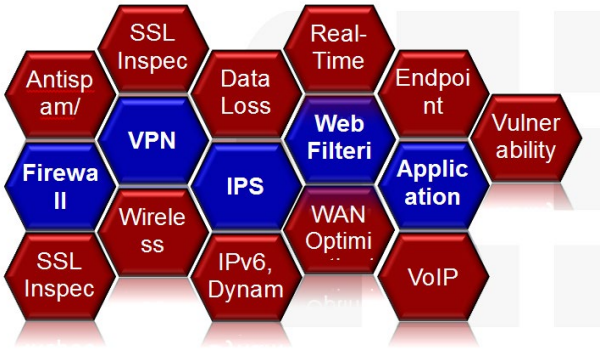
هنا تجد ان كل عيوب الطرق التقليدية تتحول الى مميزات من حيث انها توفر خدمة واحدة متكاملة وتكلفة اقل وتحسن عالى فى الأداء وسهولة فى التنفيذ والإدارة والإستخدام.
جدير بالذكر ان فورتي نت مستمرة فى تطوير الفورتي جيت من خلال خطة تقوم من خلالها بتحسين اداؤه وضم مراحل حماية اضافية



وفى الجدول التالي تجد اهم السمات المميزة لعدد من الفورتي جيت المناسبة للشركات متوسطة الحجم

Product	Firewall	IPSec VPN	Anti Virus (Flow)	IPS (HTTP)
FG-200B	5 Gbps	2.5 Gbps	200 Mbps	650 Mbps
FG-300C	8 Gbps	4.5 Gbps	550 Mbps	1.2 Gbps
FG-600C	16 Gbps	8 Gbps	1.2 Gbps	2.5 Gbps
FG-1000C	20Gbps	8Gbps	1.5 Gbps	3.5 Gbps
FG-1240B	40 Gbps (44 Gbps w/ AMC)	16 Gbps (18.5 Gbps w/ AMC)	1.5 Mbps	5 Gbps

تطور الفايروول:



من الشكل نجد ان الفورتى جيت يجمع بين كل هذه الطرق والأدوات المستخدمة فى حماية الشبكات وتأمين الدخول على شبكة عن بعد

احد مكونات ال utm والتى تستخدم لعمل فلتر على كل التطبيقات المعروفة والمستخدمة يسمح بمرور بعض التطبيقات ويرفض مرور الاخر على حسب الحاجة ورغبة مدير الشبكة وطبيعة العمل.

يقوم بعمل فلتر على جميع مواقع الويب من خلال قاعدة بيانات مخزنة بداخله تحتوى على مجموعات كل واحدة منها خاصة بفئة من المواقع وايضا يمكن الحجب او الفتح على حسب الحاجة ويمكن ايضا غلق فئة بأكملها وفتح موقع محدد يندرج تحت هذه الفئة فهو يقوم بعمل تحكم كامل على كل ما يمكن الدخول عليه .

يستخدم للحماية من هجمات الهاكرز بأنواعها المختلفة فهو يحتفظ ب signature لكل ماهو معروف من انواع الهجمات وبناءا عليه يحدد ما الذى يفعله مع كل نوع منها .كذلك يقوم بعمل مراقبة للوضع الطبيعى لل traffic اليومى وإذا كان هناك ذيادة غير طبيعية فى الحجم او اى إختلاف عن الوضع الطبيعى يعتبر هذا نوع من الهجمات ولكن هذا يحدث فقط فى حالة انه لم يجد تطابق لل signature.

تسهيلا لإستخدام التطبيقات ولكن من خارج المكتب او الشركة عموما ولكنه فى نفس الوقت يضمن الحماية الكاملة ضد اى اختراق اثناء مرور الترافيك من والى المستخدم والفورتى جيت يوفر الأربع أنواع المعروفة من ال VPN

1 - IPSEC VPN يفضل استخدامها فى حالة الربط بين 2 sites كل منها يستخدم فورتى جيت ويمكن ايضا إستخدامها من جهاز كمبوتر عادى عن طريق تسطيب ال agent الخاص بها وهو مايسمى ب forticlient .

2 - SSL-VPN نوع آخر يفضل فى حالة الدخول من لابتوب او موبايل وهناك اكثر من وسيلة للدخول ب SSL-VPN مثلا يمكنك استخدام HTTPS protocol ,RDP,SSH,telnet and etc.

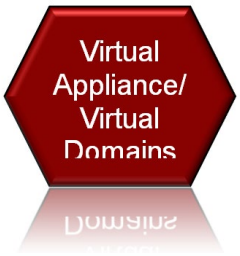
3 - L2TP

4 - PPTP

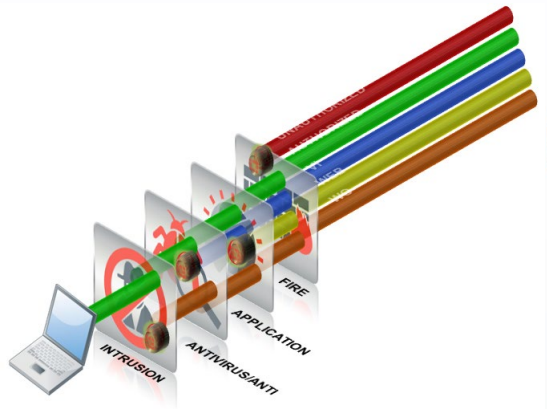
ولكن كلا من 3 و 4 لا يوفران حماية حيث أن اى تيكست يرسل ويستقبل فى صورة plain text ولا يوجد اى نوع من انواع ال encryption وتستطيع فقط عمل configuration من خلال CLI لا يوجد لها GUI interface كنوع من انواع الإستبعاد حيث انه مقرر حذف هذين النوعين ومع ذلك تجد كثير من العملاء يفضلون هذا النوع من ال vpn.

يقوم بعمل سكان على الفيروسات واى نوع من انواع ال infection بناءا على sjgnature كما يحدث فى ال ips . وبشكل عام اى تحيث فى signature or web or application category المسئول عنه هو fortigaurd .

- ماهى تحديثات فورتى جارد:



يمكن تقسيم الفورتى جيت لعدد من ال domains وهى ماتعرف ب V-DOMS or virtual domains حيث أنك تتعامل مع الجهاز الواحد على انه اكثر من جهاز لذيادة السكيورتى وتسهيل الادارة والاعدادات وداخل ال domain الواحد يمكن تقسيمه الى V-LANS .



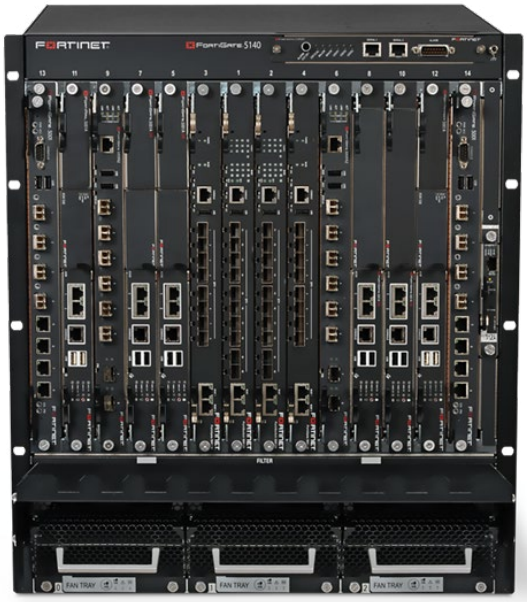
- باقى منتجات فورتى نت:

يختلف نوع المنتج على حسب حجم الشركة وعدد المستخدمين بها وتنقسم الشركات بوجه عام من حسب حجم العمل بها الى اربه انواع كما يلى :

-مزود الانترنت او ما يعرف بال ISP
-الشركات الكبيرة
-الشركات متوسطة العمل
-الشركات الصغيرة

ومن هنا نجد ان كل نوع من الانواع السابقة يناسبه فئة معينة من الفورتى جيت هذه الفئة يوجد بها المواصفات التى تجعلها مؤهلة ومناسبة للإستخدام مع هذا النوع من الشركات وفيما يلى نعرض بعض منها Service provider

FortiGate-5000 series chassis-based



يتميز هذا النوع من الفورتى جيت بدرجة عالية جدا من السكيورتى مع ذيادة السرعة والإعتمادية وفيما يلى بعض المواصفات:

- يمكنه ان يدعم 132 مليون جلسة متزامنة مع480 Gpbs throughput
- يمكن تقسيمه الى عدد من الاجهزة الافتراضية او ما يعرف بال V-DOMS or virtual domains حيث انه يدعم الى ما يقرب من V-DOMS 3000 –به امكانية للعمل مع IPV6
- يمكن توصيله ب fortimanager&fortianalyzer لتحسين ادارته والحصول على تقارير بصورة افضل واسهل

FortiGate-5000 Series Blades

- فى هذا النوع تقل المواصفات بدرجة طفيفة عن النوع السابق حيث نحصل منه على 40Gpbs throughput
- 11 مليون جلسة متزامنة
- V-DOMS 300
- IPV6

FortiSwitch-5000 Series Blades

يقوم بعمل load balancing &traffic routing بين اجهزة الفورتى جيت بسرعة تصل الى 300 - Gbps full duplex
يقوم بعمل سويتشنج على مستوى layer 2 بسرعة 10 GbE backplane &1 GbE fabric
يدعم التكنولوجيا التالية فى حالة Fabric channels static mode layer-2 link aggregation-802.3ad 1 802.1q VLANAS
802.1S multiple spaning tree protocol

FortiGate-3950B

يستخدم مع مزود الانترنت والشركات الكبرى
نحصل منه على 120 Gbps throughput وبالتالى فهو يمثل اسرع فايرول فى الماركت على الاطلاق
اما ان يتكون من 12 ports كل منها يعمل على 10-GbE او 104 ports ولكن كل واحد منهم يعمل عند 1-GbE
به امكانية للتوسع فى المستقبل بحيث يمكنك العمل بالاداء المتطلب فى الوقت الحالى ورفع الاداء فى المستقبل ليلائم متطلباتك واحتياجاتك والتكنولوجيا المستعملة وقتها

FortiGate-3810A

يستخدم ايضا مع ال ISP والشركات الكبرى مثل الفورتى جيت 3950B

يشبه كثيرا النوع السابق من الفورتى جيت الا ان الاختلاف الوحيد بينهم يكمن فى throughput فهو اقل منه نسبيا

FortiGate-3240C

هو الجيل القادم من الفايروول به تحكم كامل وحماية من الهجمات والعديد من التطبيقات حيث يمكنه التحكم فى اكثر من 1900 تطبيق مختلف وفى وقت واحد ضد احدث واخطر التهديدات التى تستهدف التطبيقات والشبكات فى وقت واحد وهى ماتعرف ب APTS or Advanced Persistent Threats
لديه 12 ports كل منها 10-GbE بالإضافة الى 16 ports كل منها 1-GBE وبالتالى فهو يمثل اعلى فايروول كثافة فى عدد ال ports فى هذه الفئة

FortiGate-3140B

يتكون من 10 ports كل منها 10 «1 GbE&12 ports «GbE
به العديد من المواصفات التى تمكنه من حماية الشبكات والمتوقع ان تستخدم تكنولوجيا الجيل القادم فى الشبكات بكل الحلول السابق ذكرها فى الفورتى جيت.

large enterprises

يندرج تحته بعض من الانواع التى سبق ذكرها مع مزود الانترنت مثل
3950B&3810A&3240c&3140B
بالإضافة الى

FortiGate-3040B

يتكون من 8 «1GbE» &10 «10GbE»
40 Gbps throughput

Small business

FortiGate-100D

FortiGate-80C/CM

FortiGate-60C

FortiGate-40C

FortiGate-20C

FortiGate-1240B

Gbps firewall throughput **44**
GbE SFP& **12** GbE interfaces **24**

FortiGate-1000C

Medium enterprises

بالإضافة الى1240B&1000c

FortiGate-600C

FortiGate-300C

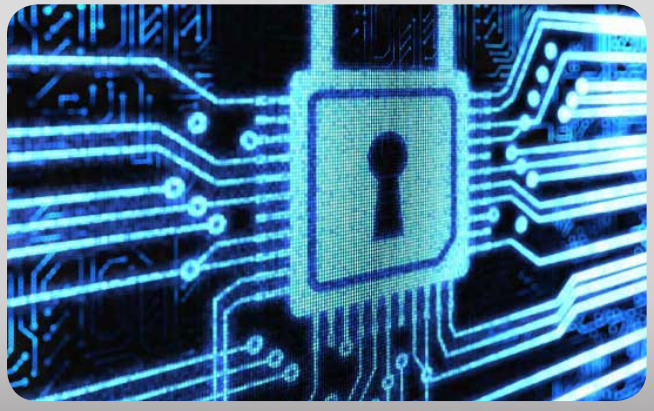
FortiGate-200B/200B-POE

خمس خطوات لتجهيز شبكتك من أجل الـ VOIP

عندما نقرر تبني قرار تفعيل المكالمات الهاتفية عبر الشبكة أو كما يطلق عليها VOIP نبدأ بأكتشاف الكثير من المشاكل بعد تفعيلها كون الداتا الخاصة بها حساسة جدا ولاتحتمل الكثير من الضغوطات كما تتحملها باقي التطبيقات الموجودة على الشبكة , لذلك سوف أقدم لك في هذا المقال خمس أشياء يجب أن تقوم بها على الشبكة لكي تتمكن الشبكة من التعامل مع الترافيك الخاص بي الـ VOIP .

1 - تفعيل خاصية الـ QOS على أجهزة السويتش و الراوتر

تطبيق وتفعل خاصية الـQOS قبل تشغيل الـ VOIP على الأجهزة نقطة في غاية الأهمية وذلك من خلال تفعيل الخاصية على كلا الطرفين (اي بين الجهازان) وسوف نستنتج بعد هذه التهيئة ان حركة الصوت اصبحة لها أولوية اعلى من حركة البيانات وفي هذه الحالة نكون قد قدمنا أفضل حزمة صوت عبر برتكول الVOIP , وأنصحك أيضا بأستخدام بروتوكولات الـ IEEE 802.1q مع بروتوكول الـ IEEE 802.1p من أجل عمل Tag للترافيك مع تفعيل خاصية الـ DSCP على الروترات .



2 - قياس جودة الـ VOIP على الشبكة .

و تتم عن طريق إيجاد وسيلة لقياس جودة حركة الصوت عبر الشبكة ويمكن القيام بذالك بأستخدم أداة يوفرها لنا عادة المصنع للأجهزة التى قررت إستقدامها إلى الشركة او يمكن عن طريق بعض الأدواة التى تستخدم في حل مشاكل الـ VOIP والتى سوف نتحدث عنها في الفقرة القادمة , ولو في حال لم تجد أداة للقياس فأعتد على المستخدمين لديك لتحديد مدى كفاءة الأتصال وطبعا أنا أفضل أن تستخدم أداة أحترافية لهذه العملية لأنك حينها سوف تحصل على نتائج أكثر دقة .

3 - تحديد أداة لحل المشاكل الـ VOIP

وتتم عن طريق العثور على أدواة مخصصة في عملية حل مشاكل VOIP وهي تتوفر عادة في الأماكن التى يباع فيها أداة وبرامج خاصة بالشبكات ومثال عليها أداة NetIQ , لذلك عند تقرر شراء أو أقتناء هذه الأداوت يجب أن تجيب على بعض الأسئلة مسبقا وهي :

- أين سوف أستخدم هذه الأدوات , في الـ LAN أو الـ WAN أو على كل VLAN أم عند أجهزة إدارة الأتصال Call Management ؟
- ماذا سوف أقيس بالضبط ؟
- هل يمكنه أرسال تحذيرات مسبقه لو في حال تدهورة جودة الأتصال ؟

4 - تطوير الاساس الخاص بشبكتك

قبل تطبيق الـVOIP أيضا يتوجب علينا أن نقوم بتحليل الشبكة لتحديد أماكن الأختناق أو bottlenecks, وهذا يتم عن طريق قياس اداء الشبكة اليوم وقبل استخدام الفويس ؟ كما يجب أيضا تحديد المشاكل ونقاط الضعف داخل شبكات الـ LAN والـ WAN. وهذا يتم من خلال طرح تسائل مهم وهو هل لدينا ما يكفي من الباندويث على روابط الـ WAN فجودة الخطوط مهمة من أجل الحصول على مكالمات هاتفية جيدة ويمكنك الأعتماد على آلة حاسبة خاصة بقياس وتحديد كميات الباندويث المطلوبة وبالتالي نستطيع تحديد الأماكن المطلوب منا تطويرها أو تحديثها .

5 - كيف تبقي الـ VOIP سعيدا .

الى جانب معرفتنا بالشبكة يجب ايضا ان نعرف ماذا يحتاج الـVOIP لكي يعمل بشكل جيد لذلك سوف اقدم لك بعض المعلومات السريعة عنه :

- ينبغي أن يكون معدل الـ Jitter مابين 20 ميلي ثانية أو أقل
- ينبغي ان يكون معدل الـ Delay ما بين 80 و 180 مللي ثانية للحصول على جودة صوت جيدة
- يطلق على معيار قياس جودة الـ VOIP على الشبكة أسم PESQ .

التحكم بسرعة الأنترنت حسب وقتٍ معين

الكثير من يبحث عن حل للتحكم بسرعة الأنترنت حسب وقتٍ معين . فقد يكون لديك في الشركة خط أنترنت بسرعة 16Mbps .

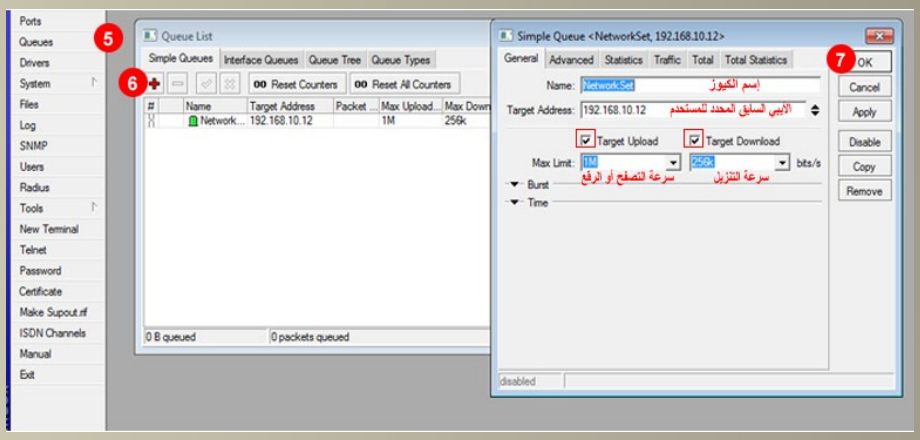
وأغلب الموظفين في الشركة ينجزون أعمالهم بالإعتماد على الأنترنت ولكن المشكلة أن هنالك موظفيين أخرين يقضون معظم وقتهم في مشاهدة اليوتيوب وتنزيل الأفلام وهذا ما يسبب بطء في الشبكة وتأخير الموظفيين عن إنجاز أعمالهم. ولحل هذه المشكلة بتأكيد حلك الفعال خفض سرعة الأنترنت وقت الدوام عن الموظفيين الذين يقومون بسحب السرعة .

ولعمل ذلك أتينا لكم بحل تستطيع من خلاله خفض وزيادة سرعة الأنترنت حسب الوقت الذي تريده وبشكل تلقائي .

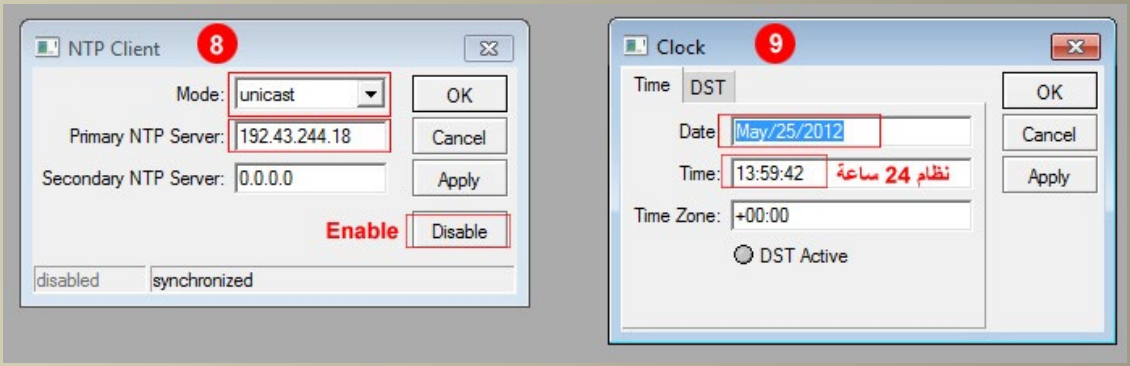
لتطبيق هذه العملية سنستخدم سيرفر المايكروتك الشهير في التحكم بخدمة الأنترنت . ولعمل ذلك سنحتاج أن نحدد Static ip لكل مستخدم أو للعملاء الذين نريد خفض سرعة الانترنت عنهم .

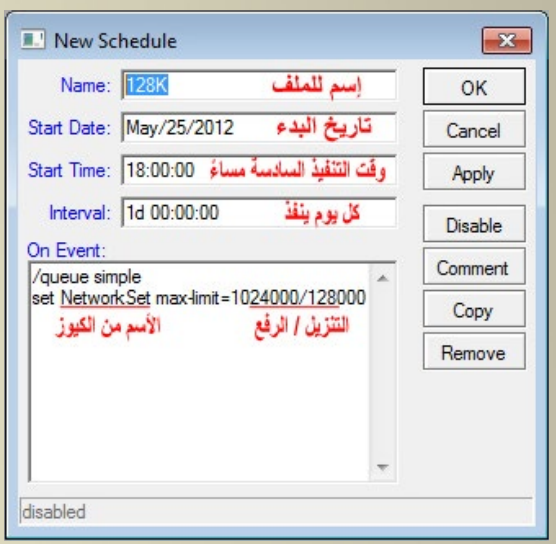
أولاً: نقوم بإنشاء مستخدم على السيرفر وذلك بالتوجة إلى ip ثم hotspot ثم User ثم نضيف مستخدم بيانات المستخدم مع التركيز على Static ip أن يكون ضمن الـ Pool الخاص بكرت خروج الخدمة:

ثانياً: نضيف كيوز للمستخدم بالتوجه لقائمة Queues ونحدد المطلوب:



ثالثاً: نتأكد من ضبط الساعة عن طريق بروتوكول NTP من قائمة System وكذلك نضبط الـ Clock:





رابعاً: نقوم بإضافة Scheduler من قائمة System ونضيف له سكربت والوقت المطلوب لتغير السرعة مع التركيز أن التوقيت بنظام 24 ساعة وإسم المستخدم ينقل نفس ما كتب على الكيوز لأن السكربت حساس لحالة الأحرف :

بالنسبة للـ Interval يقصد بها فترة تنفيذ السكربت ونحن كتبنا 1d يعني كل يوم ينفذ مرة واحدة ويمكنك أيضا تنفيذ سكربت كل 3 ساعات كما يمكننا كتابة 7d أي كل إسبوع مرة واحدة ينفذ السكربت.
كذلك لاحظ سرعة التنزيل والرفع نضيف بعدها 3 أصفار.
لإضافة عدة مستخدميين نفصلهم بعلامة Comma أو فاصلة (,) .
ولترجيع سرعة الموظفيين إلى السرعة الأصلية ننشي Scheduler أخر ونحدد فيه السرعة بالزيادة كما تريد ووقت عودتها للحالة الأصلية .
هنالك طريقة أخرى أسهل عن طريق الـ profile لكن يجب أن ينفصل المستخدم من السيرفر وعندما يدخل مرة أخرى تتفعل السرعة التي نفذها السكربت أما هذه الطريقة مباشرتاً تتطبق عليه السرعة .

هذا ما لدينا لكم في هذا العدد من الملجة وهنالك الكثير والكثير من المميزات في سيرفر المايكروتك نأمل أن نطلعكم عليه في أعداداً لاحقه إن سنحت لنا الفرصة ونتمنى أن نكون قد وفقنا في إفادتكم.

DNS ???

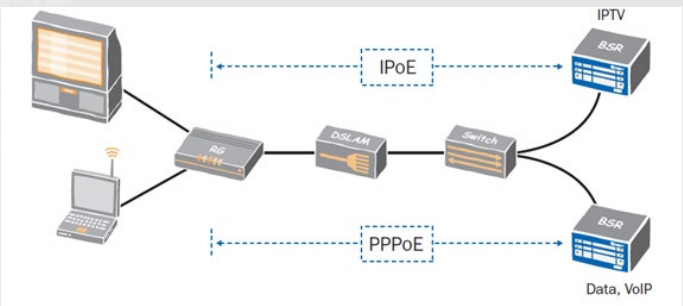
مقارنة بين بروتوكول PPPoE و IPoE

يقوم حاليا معظم موزعي الخدمات (broadband service provider) بتوفير العديد من حزم الخدمات التي تسمح لكل مشترك لتحديد الخدمات التي يريد أن يشترك فيها من قائمة من الخيارات المتاحة. وتشمل هذه الخدمات الأساسية مثل الإنترنت ذو الصبيب العالي (Hish Speed Internet) ، الاتصالات عبر بروتوكول الإنترنت (VoIP) ، البث التلفزيوني عبر الانترنت (IPTV) و الفيديو تحت الطلب(Video on Demand)..... ويشار إلى القدرة على تقديم أي خدمة من الخدمات لأي عميل ب Multiplay services .

تقديم هذه الخدمات المتعددة، يتطلب وجود شبكة تدعم كلا من Multicast بالنسبة للبث التلفزيوني عبر الانترنت (IPTV broadcast services) و Unicast (لكل الخدمات الأخرى). يجب أن تكون هذه الشبكات قادرة على تحديد الأولويات ومنح ال Bandwidth المناسبة لكل خدمة كما هو مطلوب من قبل كل مشترك.

1. فهم TR-101

منتدى ADSL TR-101 حدد رسم شبكة (Ropology network) لدعم الخدمات المتعددة باستخدام شبكات إيثرنت. فقام بدعم IP over Ethernet (IPoE)encapsulation ، هذا الأخير قام بعمل extension لدعم العديد من بروتوكولات LAN ، بما في ذلك DHCP ، للسماح باستخدامه على شبكة الاتصال الواسعة النطاق(broadband network) . يوضح الشكل أسفله رسم الشبكة المحدد من طرف منتدى ADSL TR-101 .



كان بروتوكول PPP هو المهيمن كبروتوكول لمراقبة session في شبكات النطاق العريض السلكية، في شبكات Dial-up وتتطور بعد ذلك لدعم ADSL . حتى وقت قريب، كان PPP آلية النقل الوحيدة المسموح بها من قبل منتدى ADSL . أما الآن فقام هذا المنتدى بالسماح لاستخدام IPoE ، يعتمد IPoE على بروتوكول DHCP لتوفير الكثير من القدرات المتوفرة في PPPoE .

يتم عادة استخدام IPoe / DHCP لدعم البث التلفزيوني عبر الانترنت (IPTV broadcast services) أما PPPoE فهو يستخدم عادة لدعم الإنترنت ذو الصبيب العالي (Hish Speed Internet) و الاتصالات عبر بروتوكول الإنترنت (VoIP) .

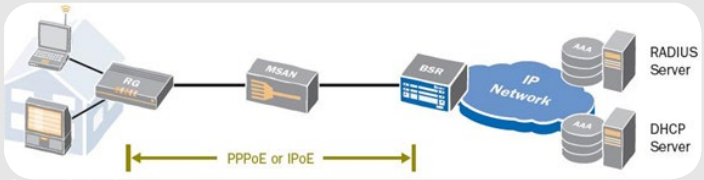
2. متطلبات session

الشرط الأساسي لتقديم خدمة النطاق العريض هو إنشاء session لكل مشترك، والتي يمكن استخدامها للسيطرة على الوصول إلى الشبكة.

تكوين هذه session يتكون من عدة مراحل:

1. عمل Authentication للمشترك : يجب التحقق من هوية المستخدم (authenticated) قبل أن يحق له الوصول إلى الشبكة.
2. إعطاء عنوان IP :بعدما يتم التأكد من هوية المشترك ، لا بد من منحه عنوان IP ليمكنه من الوصول إلى التطبيقات.
3. Access control : يجب على الشبكة أن تحدد الموارد أو الخدمات التي يمكن للمستخدم استعمالها. مثلا تحديد سرعة الوصول إلى الإنترنت على أساس ما اتفق ووقع مع المشترك .
4. مراقبة الاتصال (connection) : يجب أن يراقب كل اتصال للتأكد من أن المشترك لا يزال متصلا مع الشبكة.

IPoE وPPPoE هما التقنيتين الأساسيتين المتاحتين لأداء هذه المهام.IPoE يشار إليه أحيانا باسم DHCP لما من دور رئيسي لهذا البروتوكول أثناء عمل IPoE connection بشكل عام.



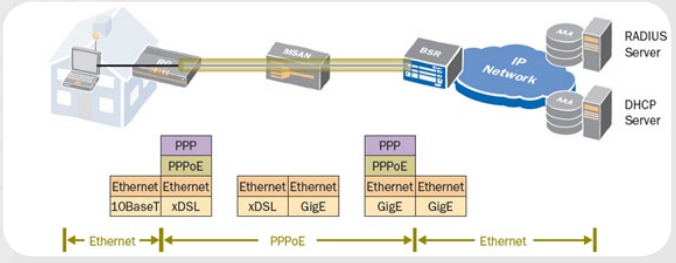
الشكل فوقه يصور رسم بسيط لشبكة واسعة النطاق. يطلق على الجهاز الذي ينهي PPPoE session فقط (Broadband Remote Access Server . (BSR)Broadband Services Router) BRAS) يدعم IPoe session بالإضافة إلى PPPoE session .

3. مقدمة عن PPPoE

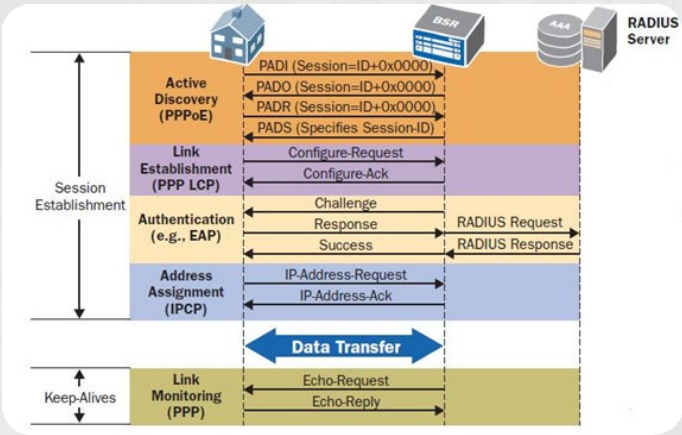
يستخدم PPP للاتصال بين nodes 2 ، مثلا بين عميل (client) وخادم (server) . تم استعماله في الأصل للاتصال المباشر بين جهازين عبر خط مؤجر باستخدام framing ISO 3309 ، حاليا هناك العديد من الطرق لعمل PPP connection عبر media مختلفة. وتشمل PPP over ATM (PPPoA) ، PPPoE ، و PPP over SONET/SDH (POS) .

كان PPPoA هو طريقة الاتصال المحدد أصلا من قبل المنتدى ADSL ، و هو الأسلوب الأكثر شيوعا لربط مستخدمي النطاق العريض في الشبكة. عند نقطة وسيطة مثل multiservice access node (MSAN) ، أو digital subscriber line access multiplexer (DSLAM) أو edge router ، ويتم تجميع المشتركين في ATM uplink واحد.

عندما تحولت الشبكات إلى استخدام إيثرنت،فإن PPPoE هو البديل المناسب لـ PPPoA ،كما هو مبين في الشكل أدناه ، يستخدم PPPoE بين RG/CPE (Residential Gateway) و BSR (Aggregation Router) . الأسماء تختلف من مصنع لأخر.



الشكل أسفله يعطي لمحة عامة عن طريقة عمل PPPoE session ، بالإضافة إلى المراقبة الدورية لـ session aliveness . أولا، يتم إنشاء PPPoE connection عن طريق تبادل عدد من رسائل PPPoE ، في هذه المرحلة يتم تحديد unique session ID. ثانيا ، يتم تأسيس link connection باستخدام (PPP Link Control Protocol (LCP. أثناء هذه المرحلة الاختيارية يتم التفاوض حول حجم الحزمة الأقصى، نوع (CHAP أو(PAP Authentication وعما إذا كان سيتم استخدام الضغط. ثالثا، يتم عمل Authentication للمشترك ، وعادة ما يستخدم Challenge Handshake Authentication Protocol (CHAP) . بدلا من ذلك، يمكن التفاوض حول بروتوكولات Authentication أخرى باستخدام Extensible Authentication Protocol (EAP).في هذه المرحلة يتم التحقق من هوية المشترك والتواصل مع خادم لتحديد نوع الخدمة المسموح بها. أخيرا ، يتم استخدام Internet Protocol Control Protocol (IPCP) لتعيين عنوان IP . عند هذه النقطة يمكن للمشترك الوصول إلى الشبكة. وبالإضافة إلى ذلك، يتضمن PPP وسيلة لتحديد link availability ، سنناقش كل هذه الخطوات تفصيليا في الفقرة التالية .



PPP Link Establishment : وPPPoE Session Establishment

يتضمن PPPoE آلية واضحة للـ host لإيجاد خادم PPPoE الذي سيتواصل معه . يقوم الـ host بإرسال broadcast request لـ session initiation (PADI) ، جميع خوادم PPPoE ترد بعرض (PADO) لتكون مرشحة للعمل كنقطة انتهاء، يقوم الـ host باختيار العرض و يرسل session request (PADR) ، يستجيب الخادم عن طريق تعيين معرف session (session identifier عن طريق رسالة PPP session ID) . (PADS يعرف المشترك، وهولا يتغير طوال حياة session .

تدفقات PPPoE قد تشمل أيضا مرحلة إنشاء PPP link ، في هذه المرحلة يتم التفاوض حول خصائص الخط مثل حجم MTU وبروتوكول Authentication الذي سيستعمل.

عملAuthetication للمشترك :

PPPoEيتحقق من هوية المشترك قبل السماح له بالوصول إلى الشبكة، وعادة عن طريق اشتراط إرسال إسم المستخدم وكلمة السر المخصصة له. يقوم خادمPPPoE بإرسال هذه البيانات إلى خادم Radius، هذا الأخير يتأكد من هوية المشترك و يقوم بإرجاع المعلومات التي تحدد كيفية التعامل مع الترافيك الخاص بهذا المشترك، بما في ذلك المعلومات مثل:

-ما هي الخدمات التي يمكن للمشترك الوصول لها IPTV أوADSL ، سرعة الإنترنت ...

Marking -مناسب فيQoS ، على سبيل المثال، فإن المشترك الذي وقع للحصول على خدمة VOIP سيتم منح الترافيك الخاص به أولوية عالية.

عندما يتم إنشاءsession بنجاح ، سوف تبدأ عملية Radius accounting .

تحديد عنوان IP :

بعد عملAuthentication للمشترك، يرسل IP (Control Protocol (IPCP عنوان IP لPPPoE client .

مراقبة Session :

عن طريق استخدام رسائل PPP keep-alive (echo))، ويمكن لكلا الطرفين مراقبة ما إذا كانت session لا تزال قائمة ومشتغلة . عند فقدان عدد مسبق محدد منkeepalives echos ، سيتم إنهاء session .

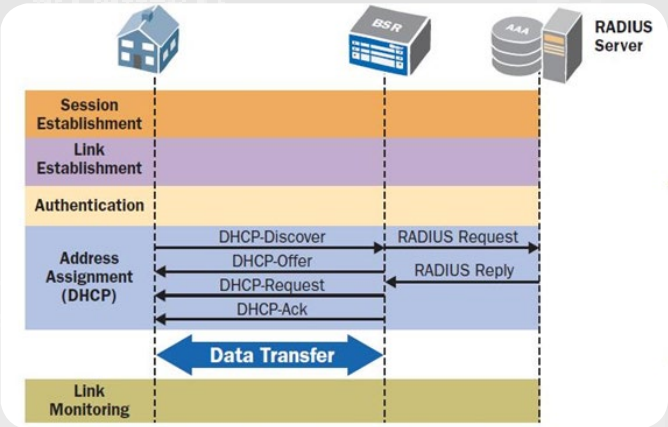
لدىPPPoE اثنين من العيوب. الأول، PPPoE يضيف 8 بايت إلى كل حزمة. هذا يتطلب المزيد منprocessing لإنشاء وفحص وإنهاء كل حزمة PPP أكثر مما هو مطلوب من قبلIPoE .

أكبر عائق أمام PPPoE هو أنه لا يدعم Multicast بكفاءة . البث التلفزيوني(IPTV) هو أول تطبيق يعتمد اعتمادا كبيرا علىmulticast لتسليم الترافيك للعديد من المشتركين .استخدامPPPoE لل multicast يتطلب من جهاز BSR إنهاء session لكل مشترك يود مشاهدة التلفزيون، كما هو مبين في الشكل أدناه. في هذا المثال، يتم إرسال نفس المضمون (قناة تلفزيونية) ثلاث مرات إلىMSAN/DSLAM عبر نفس اللينك لأن كل session لهاUnique ID ، هذا يمنع PPPoE من دعم multicast بكفاءة، هذا الشيء أدى لاستعمال IPoE كذلك في الشبكات ذات النطاق العريض.

IP over Ethernet.4

IPoEهو وسيلة لنقل الترافيك عبر شبكة إيثرنت دون استخدامPPP encapsulation . فهو يعتمد في المقام الأول علىDHCP ، الذي تم تصميمه لتعيين عنوانIP للHosts فيLAN . تم عمل extension لDHCP وبروتوكولات أخرى (مثل بروتوكول Extensible Authentication Protocol) و تم الجمع بينهم وذلك لتوفير قدرات مماثلة ل PPPoE .

الشكل أسفله يلقي نظرة عامة على كيفية إنشاء IPoE session عندما يعملBSR كخادمDHCP وبالتالي يمكنه تعيين عناوينIP .



سيتم شرح كل خطوة في الفقرة التالية .

إنشاءIPoE session :

IPoEلا يقوم بإنشاءsession بينPPPoE client وPPPoe server ، وبالتالي ليس لدى المشترك unique ID ، ولذلك، يجب استخدام عنوانIP لتعريف المشترك.

عملAuthetication للمشترك :

IPoEيفتقر إلى إجرأات لعملauthentication للمشترك مثلCHAP ، لذلك، تستخدم الشبكة معلومات حول شبكة اتصال المشترك لتحديد الخدمات المتاحة. هذا يمكن أن يكون عن طريق تمريرمعلومات من قبلMSAN حول physical connectivity للمشترك (slot ، MSAN node id و port)، أو يمكن أن تعتمد على Ethernet VLAN/ ATM VC الذي أتى منه طلبDHCP .

تحديد عنوان IP :

عندما يتم تشغيل جهاز جديد، فإنه يبث تلقائيا طلبbroadcast لتعيين عنوانIP . خادمDHCP واحد أو أكثر يجيب من خلال تقديم عنوانIP ، يجيب الclient على العرض الذي يرغب في

قبوله، فيقوم خادم المختار بإرسالACK . أحد التحديات يتمثل في أن حزم ترسلbroadcast على شبكة الاتصال. في الواقع يمكن أن يكونBSR لا يمنح عناوينIP ، بل يقوم بإرسال الطلبات إلىDHCP أخر . و هذا مايسمى بـDHCP relay .

مراقبة IPoE Session :

فائدة أخرى من DHCP relay هو أنه يتيح استخدام عملية تجديد عنوان IP كآليةKeep alive . يفعل ذلك عن طريق تعيين وقت تأجير قصير جدا للIP . فعندما يرى RG وقت عقد الإيجار قصير جدا،يصدر باستمرار رسائل طلبDHCP إلىBSR . إذا لم يتم تلقي هذه الحزم لفترة محددة، فإن BSRيفترض أن الجهاز يوجد في حالة downويمسح المعلومات المخزنة.

هناك نقطة ضعف متبقية لDHCP هيIPv6 migration ، يسمح لمزود الخدمة بإنشاء IPv4وIPv6 connection على حد سواء ، مع كل واحدة معرفة بـsession ID الخاص بها، وذلك باستخدام نفس ال VLAN . بينما يتطلب IPoE 2 VLAN منفصلين لنقل IPv4 و Ipv6 .

5. مقارنة بينPPPoE وIPoE

يقدم الجدول أدناه مقارنة بينPPPoE و IPoE عند دعم شبكات النطاق العريض ، يبقى بروتوكولPPPoE القوي والمهيمن لإدارة الاتصالات إلى المشتركين فرادى . إلا أنه يبقى الطريقة الأكثر نضجا لدعم مستخدمي النطاق العريض، بالإضافة إلى ذلك، فإنه يبسط الMigration من IPv4 إلىIPv6 .

تم عملextension للDHCP للسماح للIPoE في أن يكون مفيد في ظروف معينة، إذ يمكن استخدامه اليوم حصرا لدعم البث التلفزيوني عبر الانترنت في شبكات النطاق العريض .

الخاصية	PPPoE	IPoE
إنشاءSession	يعرفPPP session identifier المشترك	connectionless ، يستخدم عنوانIP كمعرف للمشترك
عملAuthetication للمشترك	Triggred عن طريقlogin باستخدام PAP، CHAP أوEAP .	Triggered عن طريق حزمDHCP Discover
خادم Authentication	Radius	DHCP (بعض تطبيقات تسمح باستخدامRadius)
تحديد عنوان IP	DHCP على أساس دخول(login) المشترك	DHCP على أساس physical port VLAN، أوVC
مراقبة Session	LCP echo keep alive	طلباتDHCP لتجديد عقد التأجير
نقط القوة	دعمIPv6	دعم Point-to-multipoint
نقط الضعف	إضافة 8 بايت لكل حزمة	IPv4/IPv6 migration

غالبا ما يتم تشغيلPPPoE وIPoE لتقديم خدمات مختلفة على نفس الشبكة. وبهذا نكون قد انتهينا وشكرا وأتمنى أن ألقاكم في موضوع أخر إن شاء اللّه.حفظكم اللّه.

Magazine

NetworkSet