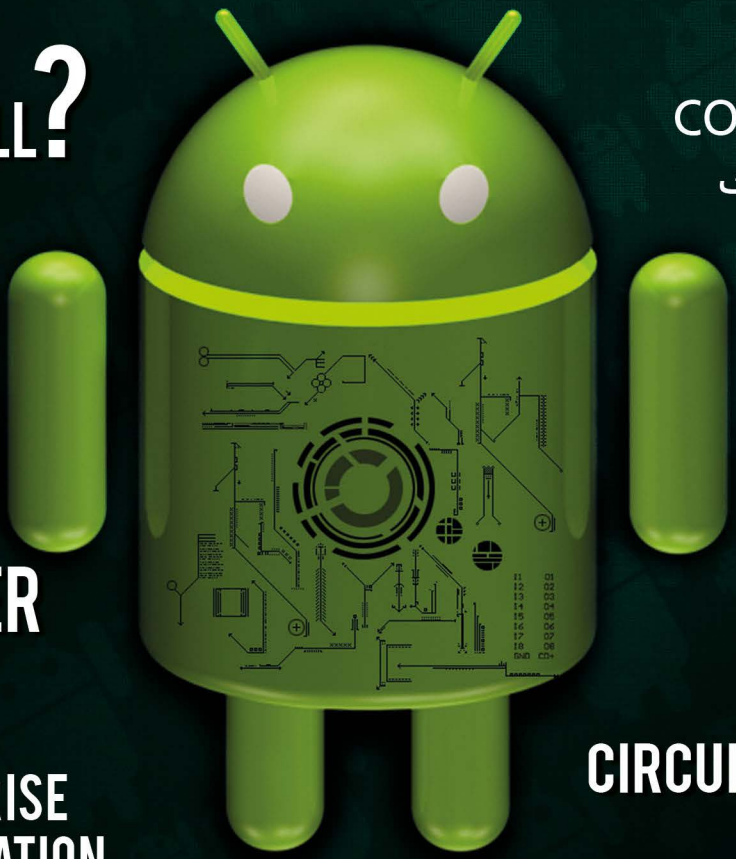
NO. 31 • December 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

15 NETWORK ADMIN APPS FOR ANDROID



WHY FIREWALL?

FCOE

LYNC SERVER 2010

HUAWEI ENTERPRISE NETWORK SIMULATION PLATFORM(ENSP)

عمل CONFIGURE للراوتر الخاص بك للكشف عن URL LOGGING الموجود على الشّبكة

CIRCUIT SWITCHING VS PACKET SWITCHING

عشرة أفكار مفيدة لتحسين أمان الشبكة وأجهزة الكمبيوتر

قوة الثقة بالنفس

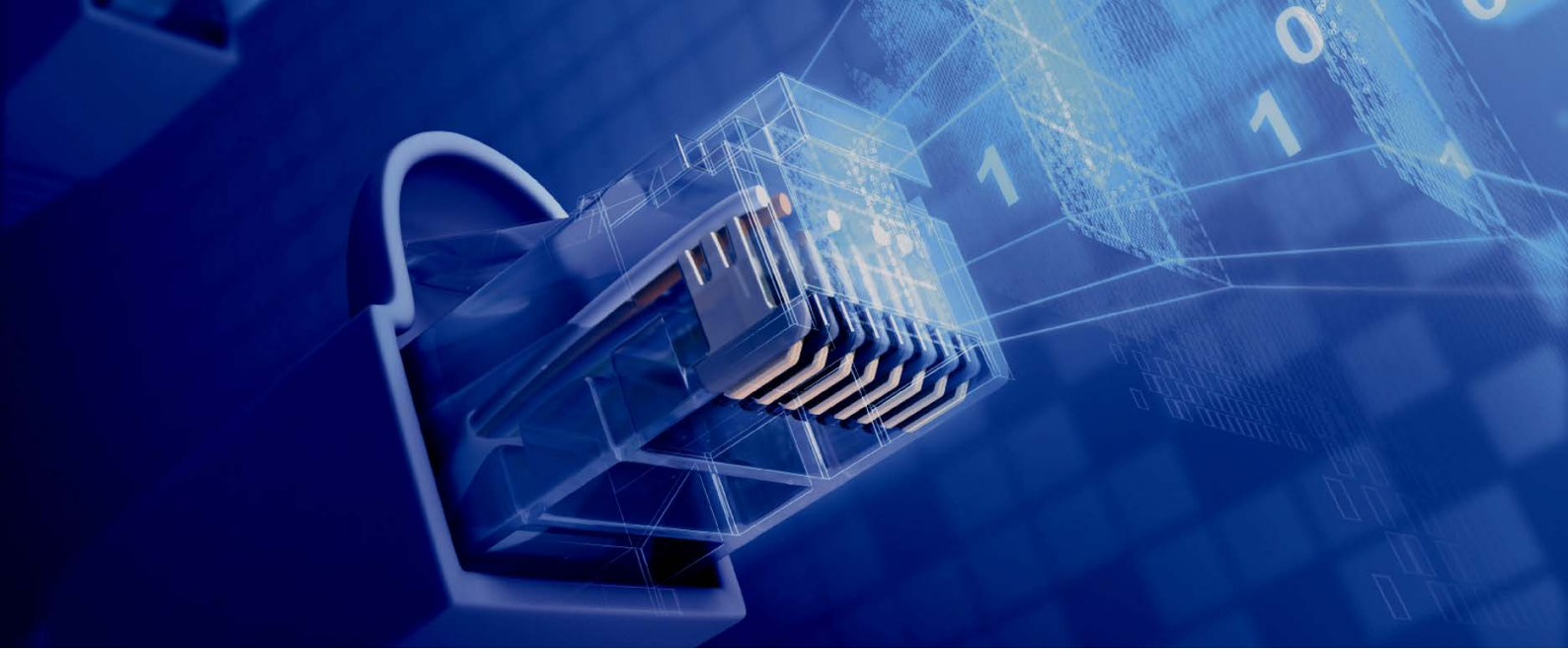
لا أفضل عادة أن يتم فهم مقالاتي التى افتتح بها أعداد المجلة مثل حب الأسبرين, مفعوله مؤقت ويختفي بعد وقت قصير جدا, لذلك أحاول دائما أن أكون واقعيا اكثر من أن أكون كاتبا يصنع الحماس الكاذب لك ويوهمك بأنك الرجل الذي يستطيع أن يغير العالم لو أراد. فعادة ما أقدم لك الواقعية في مقالاتي من خلال التجارب التى أعيشها والتى تعكس الواقع الموجود على الأرض والذي هو فعلا من الأمور الصعبة جدا تصويرها للقارئ فأنا أقع بين نارين, الاولى تقول لي لاتحبط الناس بكلامك عن الواقع والثانية تقول لي من واجبك إظهار الحقيقة مهما كان الثمن, فلو قلت لك أن زمن شهادات سيسكو والأحلام الذهبية لعالم الشهادات بدأ يختفي تدريجيا فالهدف ليس احباطك بقدر ماهو أعطائك الصورة الحقيقة لما هو موجود لذلك لاتعتبرني شخصا متشائما وهذه المقدمة أقولها لمن راسلني بهذا الخصوص.

منذ فترة تحدثت على الفايس بوك عن موضوع الذاكرة وقلت فيها حرفيا أن ذاكرتي في الآونة الآخيرة اصبحت سيئة جدا وبالكاد أتذكر أمور درستها وتعلمتها وبل كتبت عنها عدة مقالات لكن لاحظت في أحد المرات أن ذاكرتي في مسألة معينة قوية جدا وتحفظ لعدة شهور وربما لسنين ومن هنا شعرت ان الأمر هو نفسي جدا ويعتمد على القرارات التى يبدأ عقلي بأتخاذها أحيانا كأن أقول أن ذاكرتي ضعيفة ولاتحفظ الامور التقنية التى أتعلمها وكلما زدت قناعتي بالامر زادت حالة ذاكرتي سوءا ومن هنا عدت إلى فكرة الثقة بالنفس وبأن ثقة في ذاكرتي هي السبب في ضعف ذاكرتي وطبعا بدون أن أتناسى بعض العوامل الخارجية مثل تطور التكنلوجيا السريع والسلبي في أغلب الأحيان.

مسألة الثقة بالنفس مسألة كتب عنها الكثير وأغلب من كتب عنها كان يركز عليك مباشرة ويركز على عقلك ويحاول أن يعلمك بعض الطرق والأساليب لتخدع عقلك وتبث الحماس فيه والذي كما جربه أكثركم مفعوله جيد لكن لايطول, لماذا لا يطول ؟ كتب تحفيز النفس أو أي كتاب يدخل ضمن البرمجة اللغوية العصبية يقدم لك أول مرة طاقة تلاحظها في نفسك جيدا وتجعلك تدمن هذه الكتب حتى تصل إلى يوم تصبح طاقتك متعلقة بهذه الكتب فكلما نقصت ركضت باحثا عن كتب جديدة حتى تصل إلى يوم تكره فيه هذه الكتب وتعتبر أنها كانت مضيعة من الوقت وهذا الأمر هو عن تجربة شخصية وتجارب بعض الأصدقاء, والحقيقة خسارتك أكبر مما تتصور وهي ليست فقط مع الوقت ولن تشعر بها ابدا إلا لو دققت جيدا, عندما تقرأ قصص النجاح أو اي كتب نفسية من هذا النوع سوف ترتفع الطاقة لديك إلى مستويات عالية وتبدأ فعليا بمحاولة عمل شيئ جديد بناءا على تلك الطاقة والتى قوتها تكون في البداية كافية لان تمنحك شعور بأنك بيل غيتس العرب, أغلب تلك المحاولات تبوء بالفشل وبدون الدخول في الأسباب, أما النتيجة الحقيقة أن ذلك المستوى من الطاقة لن تعد تحلم فيه ابدا ولو وصلت إليه مرة آخرى فأنا أؤكد لك أن ثالث مرة لن تصل إليه, بعد كل مرة تخسر تلك الطاقة تعود للبحث عن كاتب أو كتاب يمنحك تلك الطاقة وتعود لتخسرها وتخسر المستويات القياسية في مسألة رد الفعل المصاحب حتى تصل إلى يوم يصبح لديك مناعة ضد كل كتب التحفيز الموجودة على الأرض.

أين أجد التحفيز والثقة في النفس إذا ؟ وهو السؤال الذي أرغب بالأجابة عليه في هذا المقال, مايدفعنا دائما للبحث عن تلك الكتب أو المقالات هو شيئ واحد وهو الكسل بأن نصنع الثقة بأنفسنا, ودعوني أخبركم بتجربتي, فبعد الحمد لله على كل شيئ أقول, القراء والمتابعين هم من أعطاني الثقة بنفسي وبأمكانياتي حتى وصلت إلى يوم أقول فيه علناً أن على أستعداد لكي أبسط أي شيئ يخطر على بالك في عالم الشبكات ووصلت أيضا إلى يوم أقول فيه بأن قادر في أي لحظة على تغيير مجالي 180 درجة ومستعد أيضا للأبداع فيه, لكن كيف وصلت إلى هذه الثقة برائيك؟ تلك الثقة بدأت بمشوار صعب وطويل, بدأت من المنتدى ومن حل المشاكل وأنتقلت بعدها إلى التدوين والكتابة وفي كل مرة أحسن الاجابة في المنتدى أو في أختيار موضوع مميز للكتابة عنه بطريقة جيدة أحصل على جزء بسيط من تلك الثقة لكن لاتتصور أن الموضوع بتلك البساطة, فالحصول على الثقة بالنفس شيئ ليس بالهين ابدا وكلما تعبت وبذلت جهد أكبر كلما زادت علامات الثقة الممنوحة لك, فالله يقول لكم «إن الله لايضيع أجر من أحسن عملا», والأجر لاياتي بالمجان فأنا لو لم أتعب في الكتابة وفي أختيار العناوين لما حصدت ثقة الناس والاهم من كل هذا لاتستعجل في الحصول على الثقة فأنا جلست مرة, أسبوعا كاملا وأنا أكتب في تدوينة وبعد طرحها عدد مشاهديها لم يتجاوز 17 بعد أسبوع كامل, وآخيرا أختم بشيئ صغير لاتشحذوا الثقة من الكتب أو من الكتاب مثلي, أصنعوها بأنفسكم وكونوا خير أمة أخرجت للناس 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.أنس المبروكي	م. شيماء الرازق	م.غسان محمد أبو جسار
م.حسام الدين حشيش	م.عبد العزيز صبرة	م.محمد عماد الجغصي
م.خالد الدسوقي	م. عباس موسى عودة	---
م. أحمد خير الدين	م.أحمد فتح الله	---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : عثمان اسماعيل

www.networkset.net

NetWork Set

معنى جديد لعالم الشبكات
في سماء اللغة العربية

الموسوعة

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

GO زيارة الصفحة

المجلة

أول مجلة عربية متخصصة
في مجال الشبكات

GO زيارة الصفحة

المدونة

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

GO زيارة الصفحة

(س) و (ج)

قسم خاص
بالأسئلة والاجوبة

GO زيارة الصفحة

القناة

YouTube

قناة المدونة
على موقع يو تيوب

GO زيارة الصفحة

ترجم

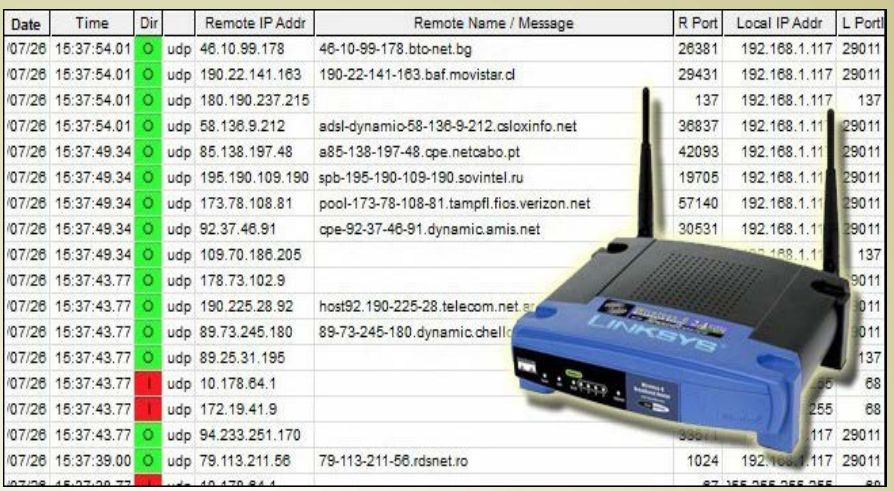
أول مشروع عربي لترجمة
المواد العلمية و التقنية

GO زيارة الصفحة

Email: networkset@Bhotmail.com | www.networkset.net

عمل CONFIGURE للراوتر الخاص بك للكشف عن URL LOGGING الموجود على الشبكة

Identification
غسان محمد ابو جسار
الجنسية : الأردن
حاصل على دبلوم هندسة اتصالات وبكالوريوس علم حاسوب مبرمج بلغة الجافا فني اتصالات لاسلكية وفني شبكات حاسوب
ghajassar@gmail.com
JORDAN



Date	Time	Dir		Remote IP Addr	Remote Name / Message	R Port	Local IP Addr	L Port
/07/26	15:37:54.01	O	udp	46.10.99.178	46-10-99-178.bto-net.bg	26381	192.168.1.117	29011
/07/26	15:37:54.01	O	udp	190.22.141.163	190-22-141-163.baf.movistar.cl	29431	192.168.1.117	29011
/07/26	15:37:54.01	O	udp	180.190.237.215		137	192.168.1.117	137
/07/26	15:37:54.01	O	udp	58.136.9.212	adsl-dynamic-58-136-9-212.csloxinfo.net	36837	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	85.138.197.48	a85-138-197-48.cpe.netcabo.pt	42093	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	195.190.109.190	spb-195-190-109-190.sovintel.ru	19705	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	173.78.108.81	pool-173-78-108-81.tampfl.fios.verizon.net	57140	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	92.37.46.91	cpe-92-37-46-91.dynamic.amis.net	30531	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	109.70.186.205				137
/07/26	15:37:43.77	O	udp	178.73.102.9				9011
/07/26	15:37:43.77	O	udp	190.225.28.92	host92.190-225-28.telecom.net.ar			011
/07/26	15:37:43.77	O	udp	89.73.245.180	89-73-245-180.dynamic.chell			011
/07/26	15:37:43.77	O	udp	89.25.31.195				137
/07/26	15:37:43.77	I	udp	10.178.64.1			68	68
/07/26	15:37:43.77	I	udp	172.19.41.9			255	68
/07/26	15:37:43.77	O	udp	94.233.251.170			117	29011
/07/26	15:37:39.00	O	udp	79.113.211.56	79-113-211-56.rdsnet.ro	1024	192.168.1.117	29011

حتى تتمكن من مراقبة الأشخاص الذين يستخدمون شبكتك اللاسلكية ومراقبة أولادك على الشبكة فانت تستطيع مراقبة كل طلبات الـ URL العالمية الناشئة والطّلبات الصادرة من المستخدمين الفرديين على الشّبكة.

ماذا تحتاج لتمكين URL LOGING :

هذا الأسلوب يتكون من شقين سوف نقسّم الاحتياجات إلى جزئين أولا إذا كنت مهتمًا فقط GLOBAL LOGGING لحفظ سجلات كل زيارات الـ URL من اتصال الانترنت الخاص بك دون التركيز على معرفة أي الاجهزة على الشبكة التي قامت بطلب URL وهنا تحتاج للأمور التالية :

1) راوتر يسمح لك بإعداد DNS SERVERS خاصة به .
2) حساب OPENDNS مجاني.

أما إذا كنت ترغب في الحصول على عرض أدق من الطلبات URL على شبكة الاتصال ولا تمانع من بذل جهد إضافي ستحتاج :

1) جهاز راوتر يسمح لك بالتسجيل ALLOWS LOGGING معظمها يفعل ذلك.
2) نسخة مجانية من WALLWATCHER تجدها على الرابط التالي .
/HTTP://WWW.WALLWATCHER1.COM

الأسلوب الأول أسهل، ويحتاج إلى دقائق قليلة لتنصيبه والجانب السلبي الأول له أن الراوتر مع طريقة OPENDNS تسمح لك برؤية الطلبات التي حصلت للـ URL دون معرفة من قام بهذه الطلبات من شبكتك. أما الجانب السلبي الآخر أنه لايعطيك السجلات المحدّثة للـ URL في وقتها الحقيقي بل عليك الانتظار يوم تقريبًا لمراجعة السجلات المحدثة.

الطريقة الثانية يدخل فيها عملية الـ SYS LOG في جهاز الراوتر الخاص بك وسحب هذه الـ LOG وإدخالها في برنامج تحليلي ويقوم بالكشف عن جميع الـ IP ADDRESS والمواقع التي دخلوها ، وهي تقنية توضح لك الجهاز الذي استعمل الشبكة في أي وقت وماهي المواقع التي دخلها ، والخَيار يرجع إليك عزيزي القارئ في استخدام أي من الطّريقتين.

إعداد الراوتر ليستخدم الـ OPEN DNS :

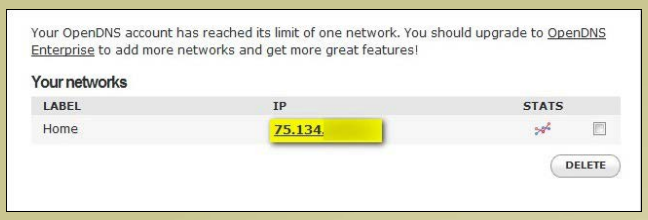
أولا عليك بزيارة موقع HTTP:// OPENDNS WWW.OPENDNS.COM/HOME والاشتراك بحساب المستخدم المنزلي وهو مجاني.

ضع بريدك الإلكتروني واختر كلمة سر قوية وتفقد بريدك الإلكتروني للتأكيد على هوية المستخدم وتنشيط حسابك.

وبعد تنشيط الحساب يجب عليك أن تضع عنوان IP المنزلي الخاص بك في صفحة الموقع وبعد ذلك سيقوم OPENDNS بالتّعرف على شبكتك، قم بتسمية الاتصال المنزلي للشّبكة لديك التي تخطّط لعمل LOGGING URL فيها.

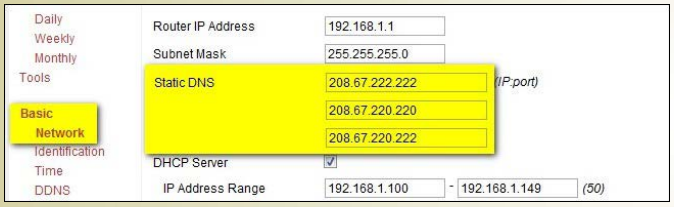
انقر فوق ADD لإضافة الشّبكة في لوحة المعلومات الخاصة بك على OPENDNS وقم بعمل تأكيد على عنوان IP المنزلي الخاص بك المستَخدم للاتصال بالانترنت.

عند الانتهاء، إذا لم يتم نقلك تلقائيًا للقائمة الفَرعية لإعدادات لوحة المعلومات SETTINGS اضغط على علامة التبويب لتنتقل لوحدك ستجد شبكة جديدة قمت بها ومسجلة بالاسم الذي وضعته وعنوان الـ IP الخاص بك وانقر على عنوان IP للوصول إلى إعدادت تلك الشبكة.



ومن داخل إعدادات القائمة اضغط على STATS AND LOGS عند العامود الذي يوجد على جهة اليسار ومن STATS AND LOGS MENU حدد مربع ENABLE STATS AND LOGS وثم اضغط APPLY وبذلك انت تخبر OPENDNS أن يقوم بمراقبة اتصالك والآن يتم تشغيل DNS SERVERS على راوترك ليرصد الحركة عليه.

في هذا المثال نحن نستخدم راوتر من نوع LINKSYS والذي يحتوي على فريم وير عادي TOMATO ، وللذّهاب إلى DNS SETTINGS ندخل على الراوتر LOGIN ثم الى BASIC ثم NETWORK ثم STATIC DNS وهكذا .



من المفترض أن يحتوي الراوتر الذي تمتلكه على قائمة مشابهة وللحصول على معلومات عن الراوتر الذي تستعمله وهل يلبّي الغرض لتلك العملية أم لا قم بزيارة الموقع OPENDNS ROUTER GUIDE من الرابط التّالي:

HTTPS://STORE.OPENDNS.COM/SETUP/
/ROUTER

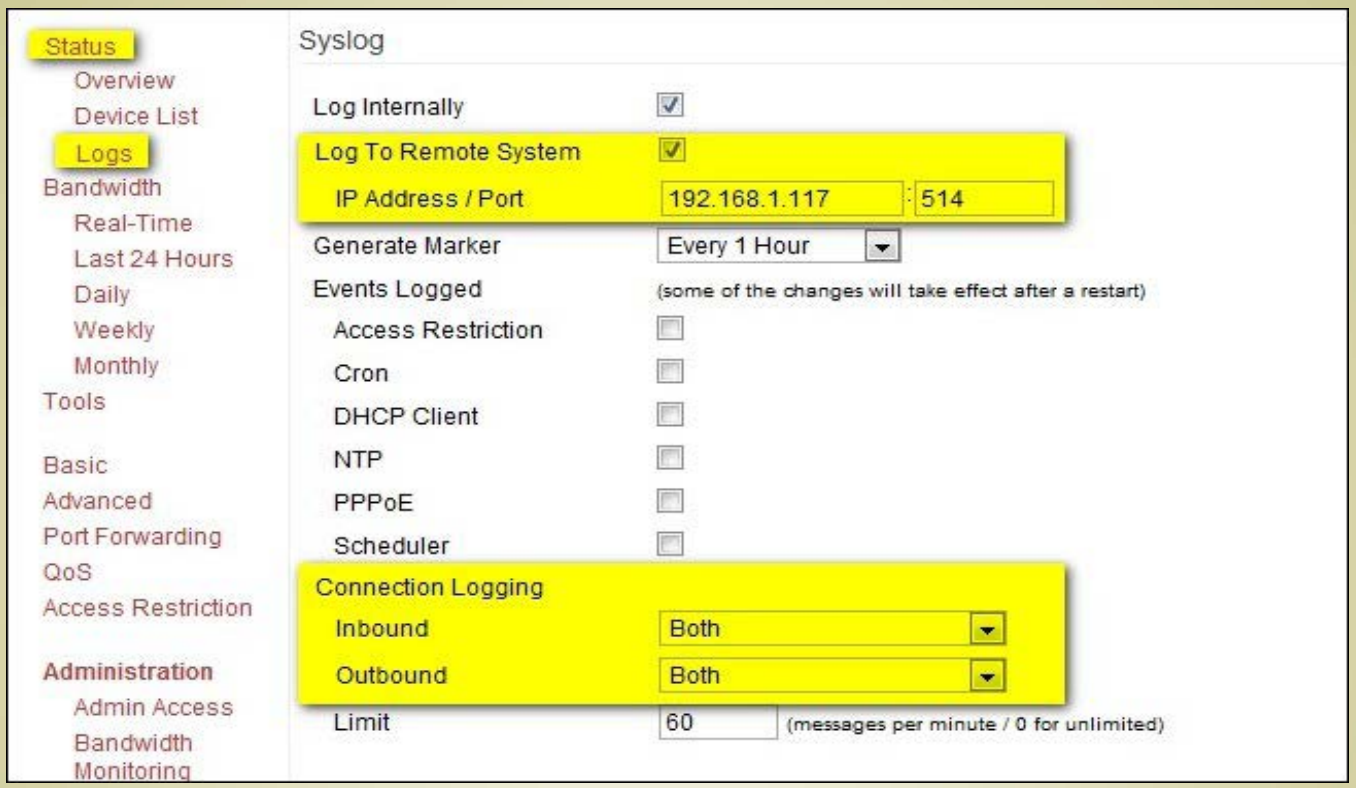
واعتمادًا على جهاز الراوتر لديك والـ FIRMWARE المحمل عليه فأنت تمتلك خانات من 2 الى 4 عناوين DNSSERVER وإملاء الخانات بالعناوين بالترتيب التالي:

208.67.222.222
208.67.220.220
208.67.220.222
208.67.222.220

بمجرد إضافتك إلى DNS SERVERS إلى الراوتر احرص على القيام بحفظ الإعدادات ومن هذه النقطة إلى الأمام سوف يقوم OPENDNS سيقوم بتسجيل كافة الطلبات URL القادمة من الشبكة المنزلية.
ولمشاهدتهم كل ماعليك ببساطة هو الدخول إلى حسابك في OPENDNS اضغط على STATS وقم بمراجعة البيانات DOMAINS ومن الجدير بالذكر أنه لا يتم تحديث الإحصائيات في الوقت الحقيقي، ويجب أن تتوقع مالا يقل عن 24 ساعة من زيارة الموقع إلى أن يظهر في صفحة الحالات STATS .
واحرص على زيارة الموقع التالي HTTPS://WWW.OPENDNS.COM/DASHBOARD/SUPPORT/
للحصول على معلومات أكثر عن OPENDNS مثل FREE CONTENT FILTERING وهو أكثر من مجرد DNS SERVERS .

ENABLING ROUTER LOGGING AND LOG ANALYSIS

تحليل URL LOGGING بطريقة أكثر دقة :



كما علمنا أن OPENDNS طريقة بسيطة إذا كنت لاتهتم بالوقت الحقيقي للـ LOGGING ومن قام بالدخول إلى هذه المواقع، ولكن عند الحاجة لتفاصيل اكثر فأنت تحتاج لعمل أكثر وهنا سنقوم بشرح طريقة استخدام برنامج WALL WATCHER وهو برنامج مجاني لتحليل LOGS وما هي المواقع التي تم الدخول إليها و من قام بالدخول إلى المواقع بوقتها الحقيقي فلا تحتاج لانتظار وقت معين لتحصل على هذه LOGS فأنت تأخذها REAL TIME .

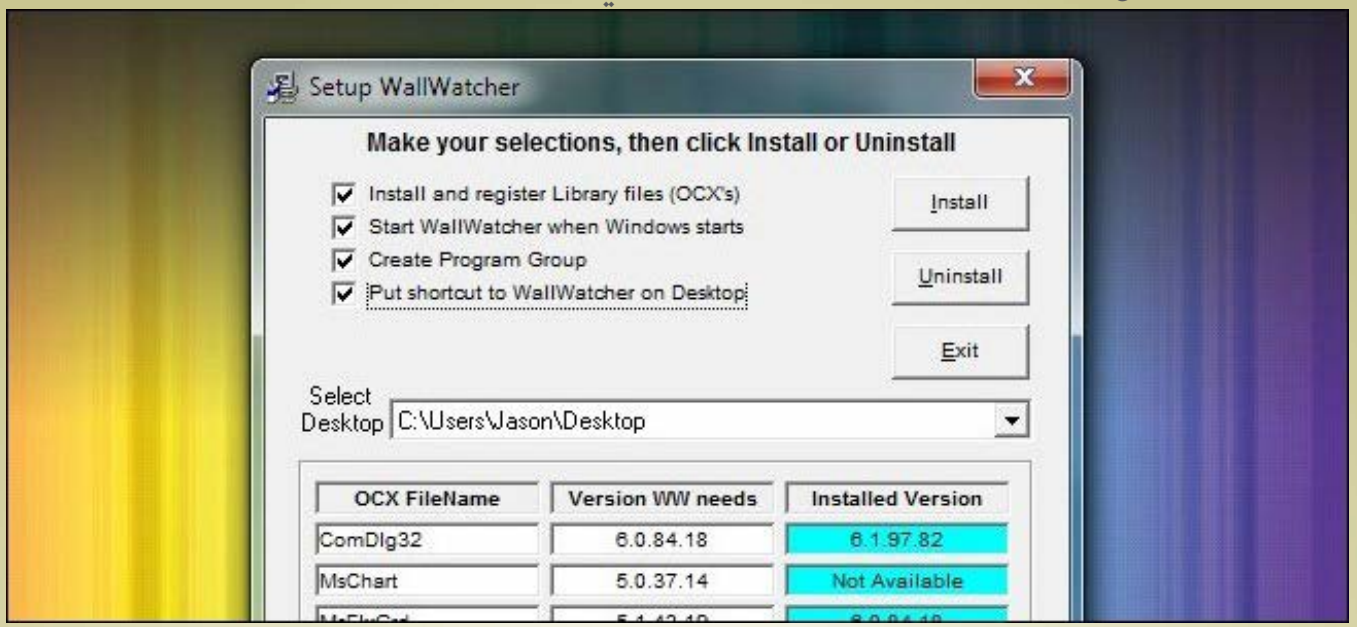
أولا أنت بحاجة لعمل تسجيل الدخول LOGGING على الراوتر مثال على ذلك راوتر اللينكسيس وفريم وير التوماتو الموجود عليه فتدخل على: STATUS >>> LOGS >>> LOGGING ثم قم باختيار LOG CONFIGURATION ثم قم بوضع الـ IP TO REMOTE SYSTEM ADDRESS لجهاز الكمبيوتر المراد تنزيل برنامج الـ WALL WATCHER عليه وهو عنوان داخلي على الشبكة لجهاز موصول داخل الـ LAN وفي مثالنا هو 192.168.1.117 وبعد ذلك نذهب إلى قطاع CONNECTION LOGGING ونثبت INBOUND AND OUTBOUND TRAFFIC ونضغط SAVE بعدها عند الانتقال للاسفل.
والآن الراوتر يقوم بعمل تسجيل LOGGING ويبث هذا التسجيل BROADCASTING THE LOGS على الشبكة ليصل لجهاز الكمبيوتر الذي قمنا بتنزيل برنامج الـ WALL WATCHER عليه ولتنزيل البرنامج عليك اتباع الرابط التالي: HTTP://WWW.WALLWATCHER1.COM/DOWNLOADS/WALLWATCHER.ZIP
قم بفك ضغط البرنامج وقم بتشغيل ملف RUN SETUP.EXE اذا واجهتك مشكلة

MISSING VISUAL BASIC FILE

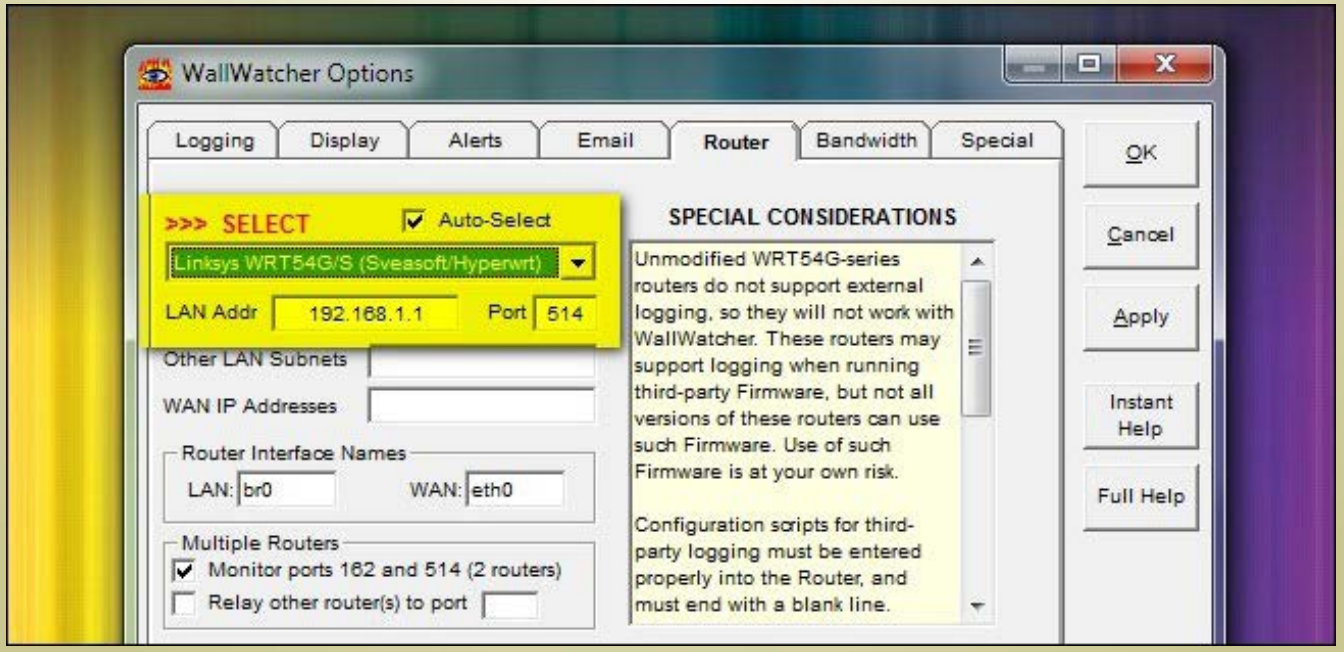
قم بتنزيل الملفات الناقصة لديك من هنا:

HTTP://SUPPORT.MICROSOFT.COM/KB/**180071**

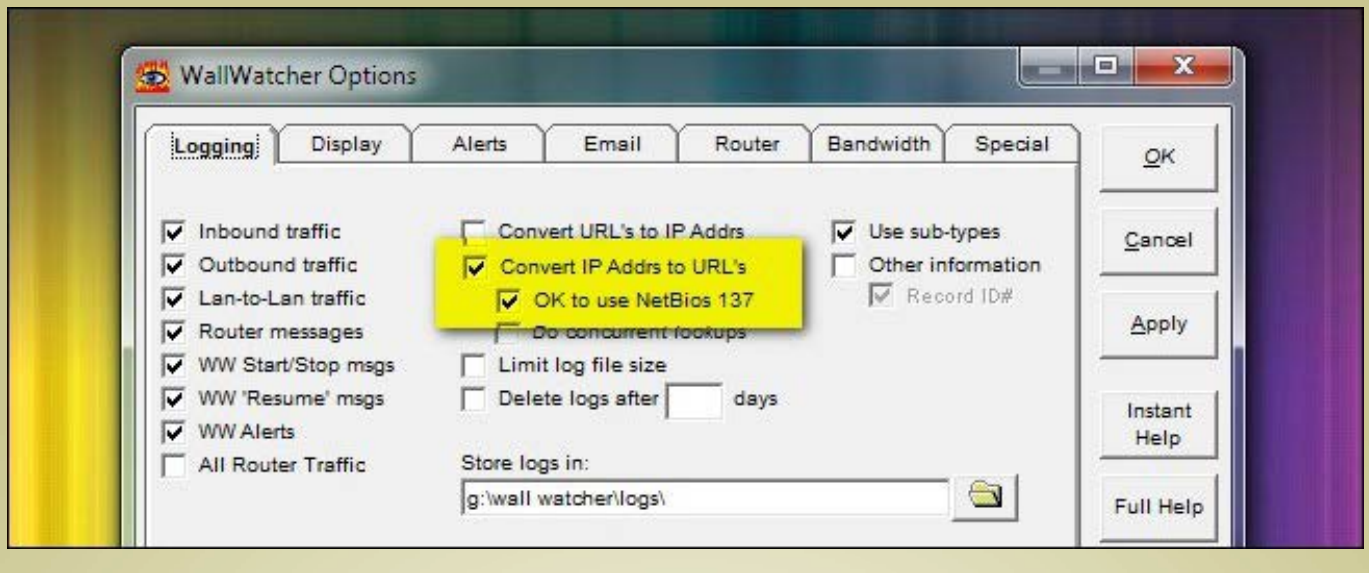
وعند تنزيل البرنامج لأول مرة سيظهر لك صندوق الحوار التالي:



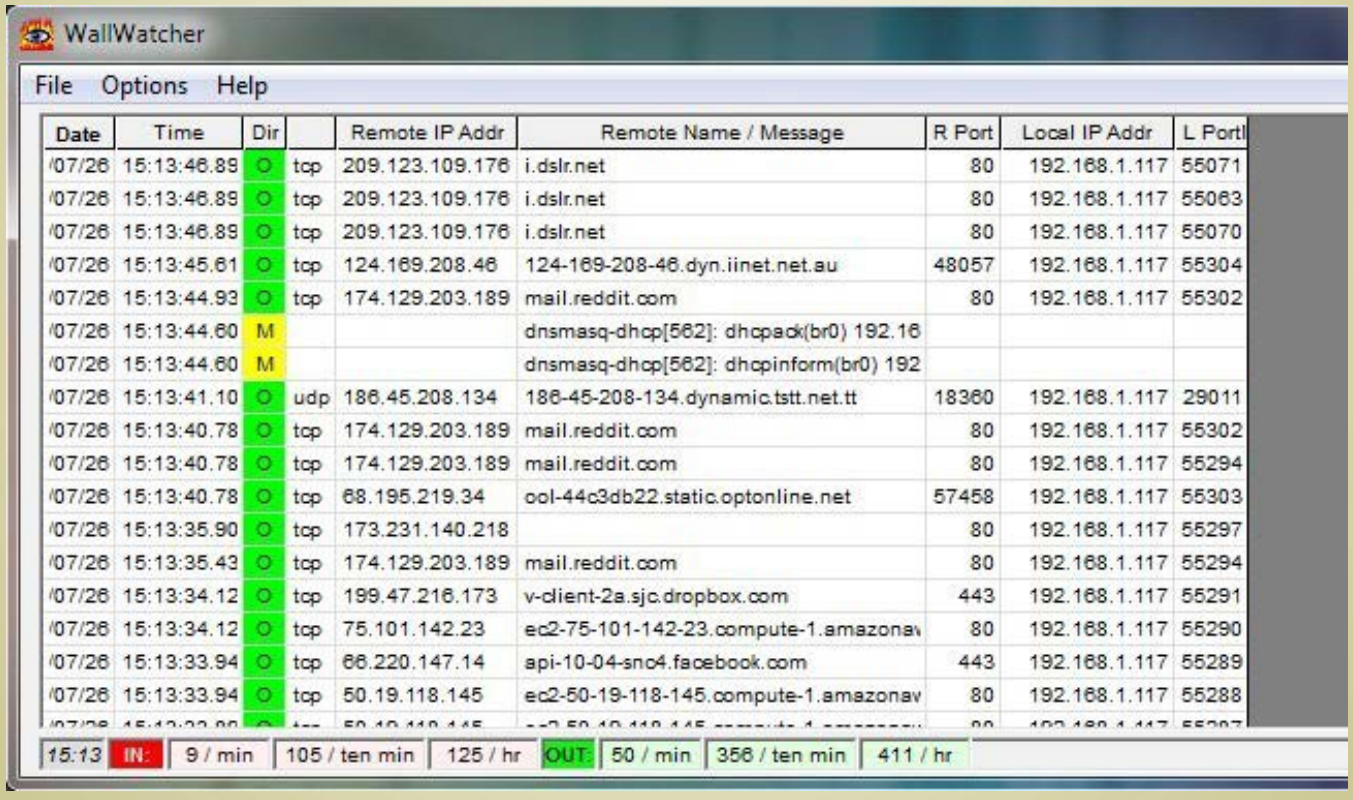
عليك بوضع إشارة صح أمام الخيارات الأربعة كما هو واضح وخصوصًا الخيار الأول INSTALL AND REGISTER LIBRARY FILES تخطي هذه الخطوة يؤدي حتمًا إلى أخطاء فعليك توخي الحذر.



عند أول تشغيل للبرنامج سيتطلب منك تحديد جهاز الراوتر الخاص بك إذا اخترت تحديد تلقائي سيقوم برنامج WALL WATCHER بتجريب كل سجلات الراوتر مخزنة على قاعدة بيانته لمطابقتها مع الراوتر الذي تستخدمه فإذا كنت تعرف نوع الروتر لديك اختره من القائمة لتوفير الوقت وبامكانك الاختيار من اسم FIRMWARE إذا كنت تعرفه ثم اضغط OK .



اضغط على LOGGING >>> OPTIONS في MENU BAR ومن LOGGING MENU اختر IP ADDRS TO URLS وضع صح أيضًا بجانب OK TO USE NETBIOS 137 اضغط OK ثم ارجع الى صفحة WALLWATCHER الرئيسية وبجانب كل IP ADDRESS ترى URLS ووقتها إلى ذلك.



الطريقة الثانية أكثر أهمية لأنها تقوم برصدٍ كاملٍ للعناوين المحليّة للأجهزة، فهي تُظهر جميع URL وجميع الحركات على الشّبكة ويتم رصدها من جهاز الكمبيوتر *.117 و بوقتها الحقيقي تظهر الزيارات للمواقع ويتم تسجيلها .

انتهى موضوعنا هذا، ولكن ملاحظة عزيزي القارئ يمكن تفعيل هذه الطريقة على أجهزة لينوكس أيضًا ولكن هنا تم شرحها باستخدام مايكروسوفت فقط.

كيفية أختيار السرعة المناسبة Clock Rate في كوابل السيريال

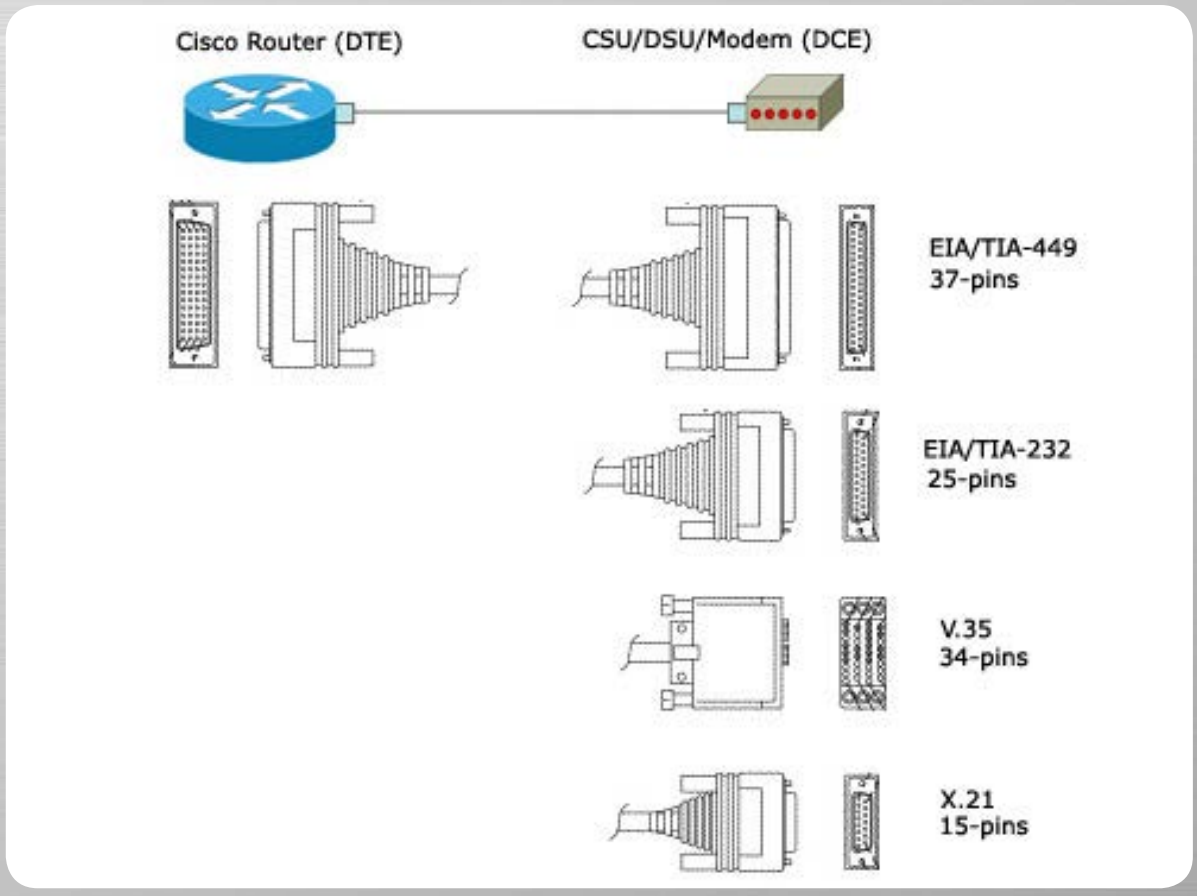
تلقيت منذ بضعة أيام سؤال بخصوص الـ Clock Rate الموجود في اجهزة سيسكو والخاص بكوابل السيريال , كيف نختار الرقم المناسب وهل كلما زدنا الرقم زادت السرعة وماهو المبدا العام في الأختيار, كل هذه الأسئلة سوف أطرحها في مقالاتي لهذا العدد.

في البداية أسمحولي أن أوضح نقطة صغيرة عن هذا الأمر, هذا السؤال لو بحثنا عليه على الأنترنت لوجدناه مكرر مئات المرات وطرح علي عشرات المرات ولكن ما لاحظته أن طارحي هذا السؤال هم فقط طلاب جدد في عالم الشبكات أو طلاب الـ CCNA حصرا, بينما لانجد أي احد دخل سوق العمل يطرح هذا النوع من الأسئلة وسوف أوضح السبب إن شاء الله.

أول شيئ يجب أن نعلمه أن تقنية السيريال تقريبا أنقرضت ولم يعد أحد يستخدمها في عالمنا العربي أو الغربي وهي تطبق وتشرح فقط في الكورسات العلمية كمادة تثقيفية لا أكثر, أما في الحياة العملية لاتساوي شيئا لأن عصر المودمات أنتهى الآن ولم يعد هناك مودمات تدعم هذه التقنية, لكن لنجيب على السؤال ماهي أنسب سرعة وكيف أقوم بعملية الأختيار.ىعادة مايقوم أغلب المدرسين والأنستركتور في المعاهد والمراكز التعليمية بأختيار سرعة 64000 بينما نجد أن هناك سرعات أكثر متاحة مثل أن نكتب في موجه الاوامر الأمر التالي فنجد :

```
Cisco's
? R3(config-if)#clock rate
(Speed (bits per second
300
1200
2400
4800
9600
14400
19200
28800
32000
38400
48000
56000
57600
64000
72000
115200
```

فكرة الاختيار لو رجعنا إلى أيام السيريال سوف نجد أن لها عدة نقاط يجب أخذها بالحسبان وأنا هنا أتحدث عن إستخدام التقنية مع مودمات الأنترنت القديمة وتحديدا مع خطوط الـ Leased Line والتى كانت ترتبط مع مقدم الخدمة ISP, وحينها كانت أقصى سرعة موجودة أو السرعة التى كانت متاحة عند أغلب المستخدمين هي 64 كيلو وهي تساوي الرقم الذي يستخدمه الجميع بشكل تلقائي 64000 بدون تحديد سبب أختيار هذا الرقم لذلك فالعملية هي عملية توريث من شخص لآخر.

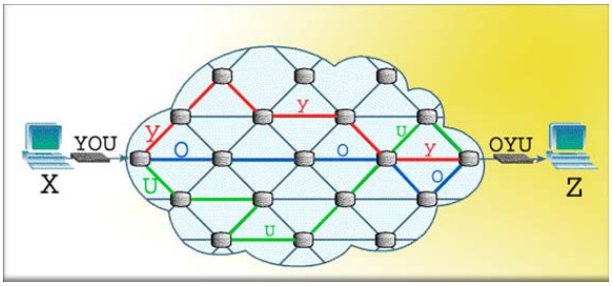


لكن بشكل عام لو تحدثنا عن التقنية داخليا وبين الروترات فالأمر مختلف هنا ويمكن وضع معدلات أكبر من 64 بكثير لكن يجب أن نراعي هنا عدة نقاط أول نقطة هي السرعات التى يدعمها المنفذ نفسه فهناك من يدعم حتى أثنان ميغا وهناك من يدعم حتى ثمانية ميغا والنقطة الثانية ماهو كبل السيريل المستخدم وهو موضح بالصورة الجانبية وماهي السرعات التى يدعمها وآخيرا كم طول الكايبل المستخدم , هذه هي النقاط بشكل عام وأعود وأقول لا تتعب نفسك كثيرا مع هذه التقنية فأنت لن تراها بعد أن تخرج من لاب المعهد الذي تدرس فيه إلا نادرا لأن سرعتها محدودة مقارنة بكوابل الأيثرنت التى أصبحت تتمتع بسرعات مضاعفة عن السرعات المدعومة في تقنية السيريال . أتمنى أن تكون المقالة قد اجابة على أستفساراتكم ولاتنسونا من دعواتكم ودمتم بود.

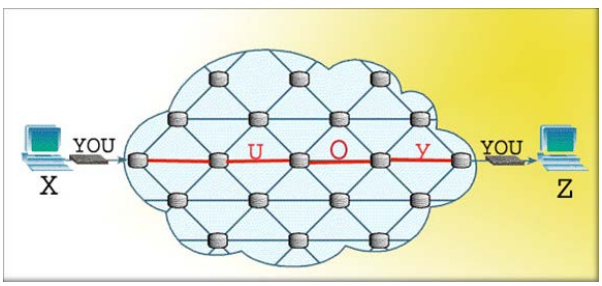
Circuit Switching VS Packet Switching

هل قرّرتَ يومًا أن تربط فروع شركتك الموزّعة جغرافيًا مع بعضها البعض؟؟
هل سألت نفسك يومًا لماذا تقدم وزارة الاتصالات خدمة ربط بكلفة 50 $ شهريًا ولماذا تقدم خدمة ربط بكلفة 500$ وبذات عرض الحزمة؟؟!! أليست البنية التّحتية هي نفسها ؟؟ أليست الأسلاك التي ستربط فروع الشركة بكلتا الحالتين هي نفسها؟؟ والكثير من التساؤلات.
كل هذه الأسئلة سنجيب عليها اليوم من خلال حديثنا عن التقنيات الأساسية المستخدمة في نقل المعطيات على الشبكة، حيث سنتحدّث في هذا العدد عن التقنيات المستخدمة في هذه الحالات ،ماهي؟ما هو مبدأ عملها؟؟ماهي ميزاتها ومساوئها؟؟

فلنفترض أن لدينا الفرعين Z و Xونريد أن نرسل رسالة نصية «YOU» مثلا من X إلى Z.



نلاحظ أن الرسالة في الشكل السابق تسلك طرق مختلفة عبر العقد الواصلة بين الطرفين وقد تصل غير مرتبة إلى المستقبل، تسمى الطريقة السابقة Packet Switching.
لنرى الآن الشكل الآخر لنقل المعطيات على الشبكة والرسالة ذاتها « YOU »



نلاحظ الآن من الشكل أن المعلومات تسلك طريق واحد وستصل مرتبّة حتمًا بنفس تسلسل ترتيب الإرسال، تسمى هذه الطريقة Circuit Switching.

بهذه البساطة تعتمد أغلب البيانات في عمليّة انتقالها عبر الشبكة الموسعة.
والتي سوف أدعوكم اليوم للتعرف على تفاصيل كل واحدة منها في هذه المقارنة والتي تجمع تقنية Packet Switching و تقنية Circuit Switching.

Circuit Switching

التبديل عبر الدارات، تمثل هذه التقنية تقنية البنية التحتية الخاصة بمؤسسات الاتصالات حيث استُخدمت أول مرة عام 1878 ضمن المكالمات الهاتفية.

تعتمد هذه التقنية على حجز قناة اتصال خاصة بين المرسل والمستقبل يتم تبادل البيانات من خلالها، تبقى هذه القناة خاصة بالاتصال القائم لحين إنهائه، حيث لا يستطيع أحد المشاركة عبرها أو استخدامها، وبالتّالي عند استخدام هذه التقنية لإجراء مكالمة هاتفية بين شخص من الصين مع شخص من افريقيا فإن قناة فيزيائية خاصة سيتم تسخيرها لإقامة الاتصال بين الشخصين، حيث ستبقى هذه القناة قائمة

ما دام الاتصال قائم وهذا ما يفسر ارتفاع كلفة الاتصال الهاتفي الدولي ، ناهيكم عن أن عدد هذه القنوات محدود حسب إمكانيات المقاسم الهاتفية وقدرتها على تأمين خط خاص لكل مكالمة، ومن هنا نشأت المشكلة، لماذا يتم حجز خط كامل بين شرق الأرض وغربها لإجراء اتصال ونقل البيانات؟؟؟

فكان الحل هو ما يسمى بتقنية الـ Packet Switching

Packet Switching

التبديل عبر الطرود ,ويعتبره البعض «المسمسار الأول في نعش شركات الاتصالات»

يتم في هذه التقنية تقسيم الرسالة إلى عدة أجزاء، كل جزء يسمى Packet أو طرد ومن ثم يتم إرسال هذه الطرود عبر الشبكة العالمية باستخدام بروتوكول الانترنت IP ، الآن ليس من الضروري أن تسلك كل الطرود طريق واحد فتكون الرسالة قد تم إرسالها عبر خط واحد وإنما يتم إرسال كل طرد من طريق مختلف وذلك تبعًا لمشغولية الطريق وليس لقصره ، من الممكن أن يسلك عدة طرود الطريق ذاته، لكن ذلك ليس بالضرورة

من الناحية الأخرى عند المستقبل تبدأ الطرود بالوصول ولكن هذه المرة الطرود تصل بشكل عشوائي الطرد الأول قد يصل أولا وقد يصل في النهاية وذلك تبعًا للطريق الذي سلكه. وبالتّالي المستقبل هنا بحاجة إلى آلية ليرتب هذه الطرود وهنا يأتَي دور المرسل حيث يقوم المرسل قبل إرسال أي طرد بتزويده بعنوان الوجهة والعدد الكلي للطرود الخاص برسالته المرسل ضمنها كما يقوم بإعطائه رقمًا تسلسليًا ضمن الرسالة التي تم تجزيئها إلى عدة طرود، وبالتّالي المستقبل يعمل على ترتيب هذه الطرود وفق الأرقام التسلسلية لها ، وإن لاحظ نقص في طرد ما فإنه يعاود طلب الطرد الناقص من المرسل من جديد.

لنرى الآن جدول لمقارنة سريعة بين أهم الخصائص بين التقنيتين وأمثلة على الشّبكات التي تستخدمها:

	Circuit	Packet
السرعة	أسرع	أبطئ
الوثوقية	أعلى	أقل
الكلفة	مرتفعة	منخفضة
نقل الصوت	مفضل	غير مفضل
بيانات غير صوتية	غير مفضل	مفضل
مسار النقل	يحدد مسبقا	يحدد أثناء النقل
عرض الحزمة	استغلال كامل للمجال المتاح	ليس بالضرورة
تستخدم في	Leased Line	DSL , Frame relay

بهذه المقارنة نكون قد تعرفنا على هاتين التقنيتين الأساسيتين في النقل عبر الشّبكات الواسعة.

FCOE

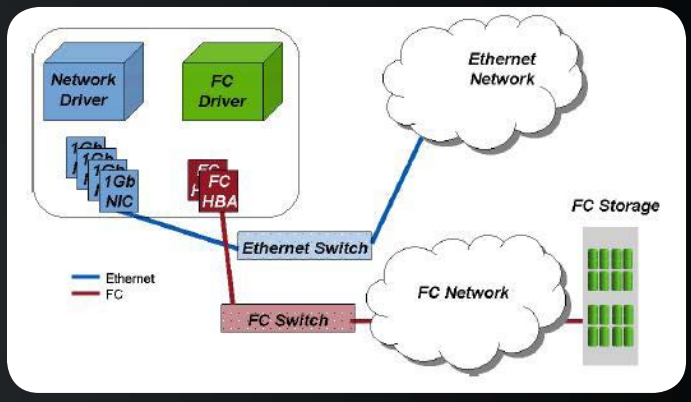
سوف نستعرض اليوم تكنولوجيا وبروتوكول للاتصال في عالم الشبكات والسيرفرات ووحدات التخزين, وما علاقة وحدات التخزين الـ (Storage) مع الشبكات والسيرفرات ! .

فمعظمنا يعرف أنّ الدّاتا سنتر تتكون من بعض القطع الأساسية (Servers – Switch - Storage).

ملحوظة: المقصود بوحدات التخزين الـ SAN Storage التي تتصل بالسيرفرات بالـ Fiber Optical.

للتوضيح أكثر: يتم اتصال السيرفرات فيما بينها وبين المستخدمين عن طريق Switch Cable and .
ويتم الاتصال بالـ SAN Storage فيما بينها وبين السيرفرات عن طريق الـ Fiber Optical عن طريق سويتش Fabric Switch.

ملحوظة : حالياً يمكن أن تتصل الـ SAN Storage بالسيرفرات عن طريق Ethernet بالكلابات والسويتشات العادية بواسطة بروتوكلات الـ iSCSI and NFS لكن الأفضل والأسرع هو الـ Fiber Optical.



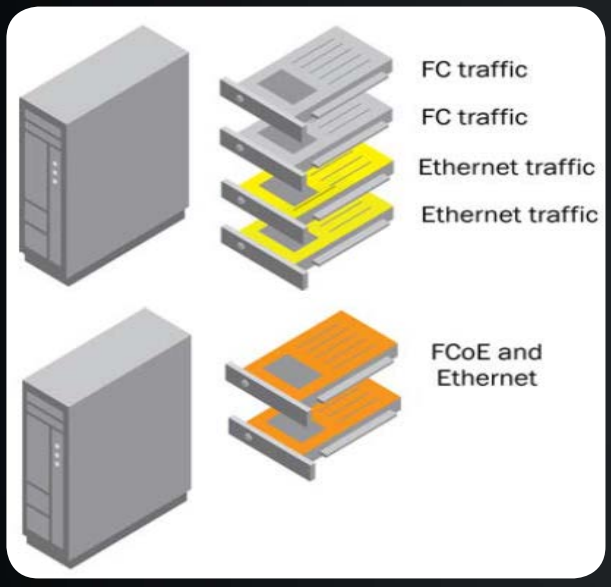
شكل توضيحي للاتصال بالشكل التقليدي

ما هى تكنولوجيا الـ Fiber Channel Over Ethernet : FCoE

بالوضع الحالي في الداتا سنتر يكون فى كل Server نوعان من كروت الاتصال كارت Ethernet وكارت HBA لكي يستطيع أن يقوم بالاتصال بالشبكة العادية عن طريق السويتش العادي والكابلات الـ RG45 والكارت الآخر HBA يستخدمه في الاتصال بـ SAN Storage بواسطة كابلات فايبر وعن طريق سوتش فايبر.
بهذا الوضع لا يوجد مشاكل فى السرعة أو شيء لكن يوجد مشكلة في كثرة الكابلات في الداتا سنتر وكروت النيتوورك وكروت الفايبر والسويتشات.

ملحوظة : دائمًا ما يكون هناك كارتين HBA وبين 2 إلى 4 كروت Ethernet في كل سيرفر.

لاحظوا حجم الكبل الضخم الذي يسوف يستخدمه كل سيرفر للاتصال بالـ SAN and Network ويكون لديه Load Balance
وعدد السويتشات أيضًا التي سوف نستخدمها.



لذلك جاءت فكرة أن نقوم بعمل بروتوكول نستطيع من خلاله عمل دور الـ Ethernet and Fiber Optical Connection
وذلك من خلال كرت واحد. فقاموا بتسمية هذا الكرت بالـ (Converged network adapter) CNA والبروتوكل الذي يعمل به هو FCoE.

هذة التكنولوجيا بدأت أواخر التسعينيات وتحديدًا في عام 1997 قامت منظمة الـ IEEE بوضع معيار أساسي لكل الشركات التي سوف تنتج هذه الكروت والسويتشات التي سوف تعمل معها وأيضا لأنظمة التشغيل.

وحتى الآن يوجد 3 شركات فقط تنتج هذه الكروت (Brocade – Qlogic – Cisco) .


Figure 1 - STAND UP CNA (iSCSI, FCoE or NIC)

صورة توضح كرت الـ CAN

وشركتان فقط هي التي تقوم بإنتاج السويتشات الخاصة بهذه التكنولوجيا (Brocade and Cisco)

صورة توضح FCoE Switch

وأغلب أنظمة التشغيل الخاصة بالسيرفرات أصبحت تدعم هذه التكنولوجيا وأيضًا الـ VMware vSphere and Citrix Xen Server.

لتوضيح أكثر لهذه التكنولوجيا وكيفية عملها :

يعمل كرت الـ CNA الموجود في السيرفر بنقل للداتا الخاصة بالـ SAN وأيضًا الداتا الخاصة بالـ Ethernet وذلك عن طريق الكابلات وهي نوعان :
إما كابلات فايبر التقليدية، أو كابلات خاصة لهذه الكروت:


Figure 3 –SFP+ Direct Attach Copper Transceiver and Cable all in one

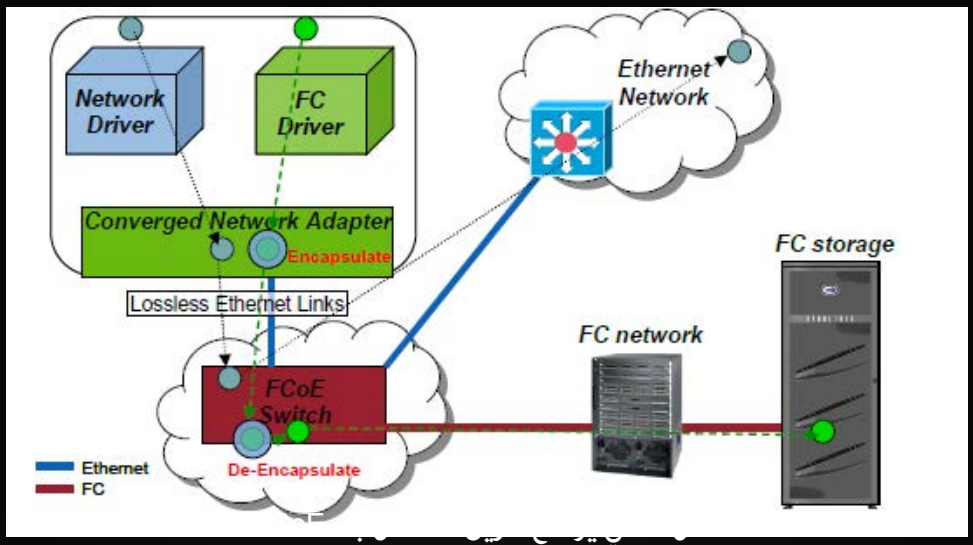
صورة توضّح الكرت الخاص بـ FCoE

وسواءً استخدمنا أي من هذه الكابلات سوف يتم توصيل هذه الكابلات بسويتشات خاصة بهذه التكنولوجيا وليست أي سويتشات عادية

لكن ما يميز هذة السويتشات أنها يمكنها أن تتعامل مع كل بروتوكولات الاتصال سواءً Fiber , Ethernet , FCoE)).

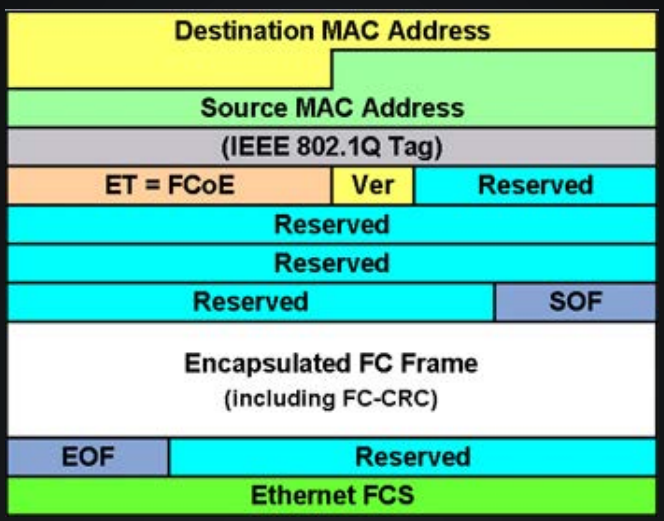
فبهذا نكون قمنا بتوفير شيئين حتى الآن وهما: الكروت الكثيرة والكابلات والسويتشات التي كنا نستخدمها في الوضع السابق.

فائدة أخرى وهي السرعة التي تصل إلى 10 Gbits وهي السرعة الحالية لهذه البروتوكلات وهي سرعة عالية للغاية لا تتوفر في الـ Ethernet ولا في أغلب الـ Fiber Optical.



ملحوظة مهمة: هذة التكنولوجيا مصمّمة خصّيصًا للربط بين السيرفرات ووحدات التخزين والشبكات العادية والكابلات الخاصة بها محدودة الطول.

لذلك هي لن تستخدم في الاتصال بين عدة سويتشات أو بين مستخدمين عاديين.
وحاليًا هذة التكنولوجيا لا تطورها فقط الشركات الخاصة بالشّبكات من أمثال سيسكو وغيرها، وإنما الداعم الأول لها هي شركات الـ Storage مثل شركات HP– IBM – NetApp – EMC وشركات الـ Virtualization مثل VMware – Citrix.
لأنهم أكثر الشركات التي تحتاج لهذه التكنولوجيا لأنها تقوم بتسهيل الإدارة وتعطي سرعة عالية في الاتصال.



صورة توضيحية لكيفية عمل البورتوكول FCoE Fram

هذة التكنولوجيا وهذا الأسلوب الجديد في الاتصال لم ينتشر كثيرًا حتى الآن وبرأيي بسبب:

1 - عدم دراية الغالبية العظمى من العاملين فى حقل تكنولوجيا المعلومات بهذه التكنولوجيا وأنا منهم حتى وقت قريب.
2 - قلة عدد الشركات التي تنتج الهاردوير الخاصة بهذة التكنولوجيا.

لكن من المتوقع لهذه التكنولوجيا النجاح الكبير في المستقبل القريب.

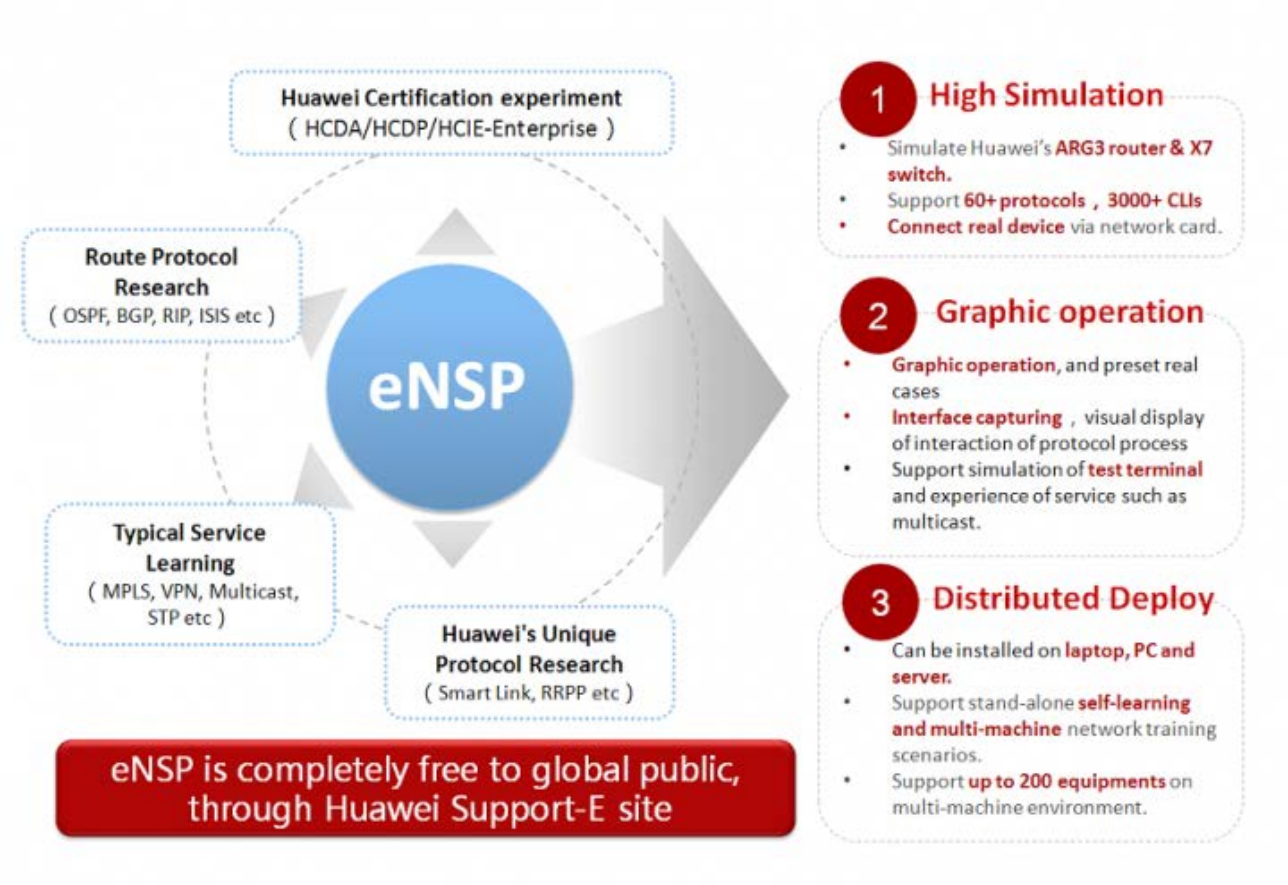
Huawei enterprise network simulation platform (eNSP)

أعلنت شركة هواوي، الشركة العالمية الرائدة في المعلومات وتكنولوجيا الاتصالات، مؤخرًا عن إطلاق برنامج محاكاة الشبكة الخاص بأجهزتها واسمه هو Huawei enterprise network (simulation platform (eNSP . هذا البرنامج يمكِنه محاكاة بعض الراوترات و السويتشات وذلك من أجل فهم كيفية تشغيل منتجات شركة الهواوي.

هذا البرنامج يدير نظام تشغيل الشركة المسمى (Huawei's Versatile Routing Platform (VRP ، ويمكنه محاكاة العديد من الإعدادات قبل إدخالها على أجهزة حقيقية كما يدعم الربط بينه وبين أجهزة حقيقية، وعلاوة على ذلك، فهذه الأداة تسمح لك بالإستعداد لاجتياز شهادات شركة هواوي:

- Huawei Certified Datacom Associate (HCDA),
- Huawei Certified Datacom Professional (HCDP)-Enterprise,
- Huawei Certified Internetwork Expert (HCIE)-Enterprise.

بالأضافة إلى دعمه للكثير من البروتوكولات، والقدرة أيضًا على مراقبة الباكيت ومشاهدة محتوياتها لحظيًا وفي الـ Info graphic التالي سوف تجد أهم مميزات هذا البرنامج.



هذا البرنامج مجاني ، عليك فقط التسجيل في موقع هواوي (أنظر أسفله) ، أما استعماله فيشبه إلى حد كبير برامج المحاكاة الآخرى، لتحميل البرنامج يتوجب عليك التسجيل أولاً على الرابط التالي :

http://support.huawei.com/enterprise/softdownload.action?pid=9017384&idAbsPath=fixn7C9017384&fastLocation=fastLocation٪7C7923123٪7C7919712٪7C7919710٪ode01

وللمزيد حول البرنامج ومشاهدة بعض الشروحات على اليوتيوب شاهد الرابط التالي :

http://www.youtube.com/watch?v=iYQ_njjDRW8

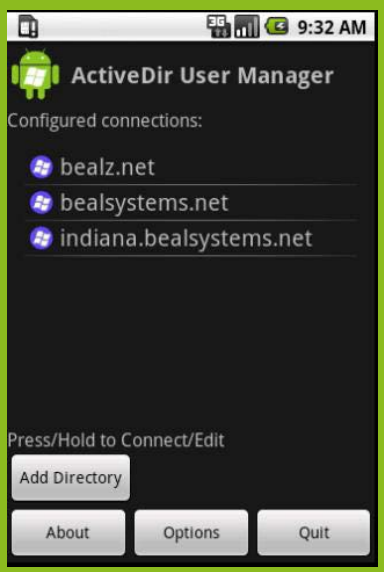
15 Network Admin Apps for Android

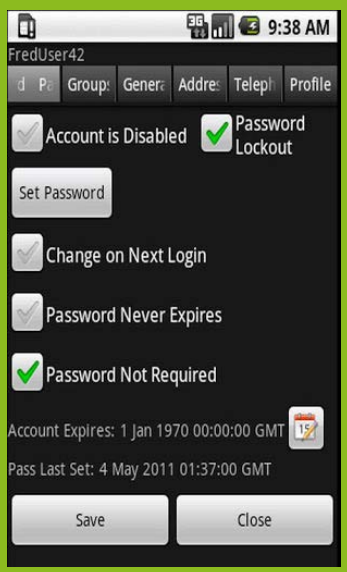
نظرًا لسيطرة أنظمة الـ (ANDROID) وهيمنتها على سوق أجهزة (MOBILE & TABLET) كان لابد من إلقاء نظرة على أهم التطبيقات التي تساعدك على إدارة شبكتك. حيث تم تسليط الضوء على أهم تطبيق مختلف يعمل على هذا النظام الرائع. تقدم هذه التطبيقات العديد من الخدمات من حيث اكتشاف ومراقبة الأجهزة المتصلة بالشبكة وخدمات الشبكة المختلفة وقواعد البيانات. وغيرها الكثير من الخدمات وكل هذا من خلال هاتفك النقال آو جهازك اللوحي (TABLET) وكذلك تمثل مرجع سريع مثل برنامج (IP Calculator).

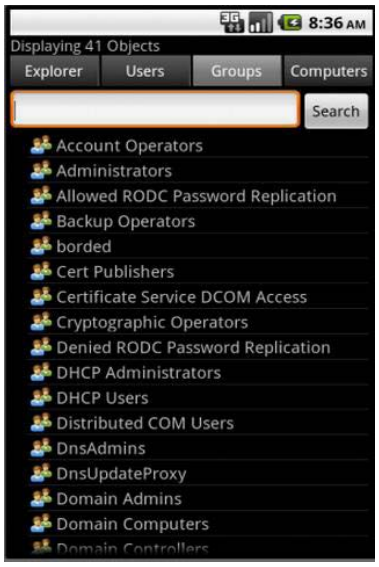
1 ActiveDir Manager

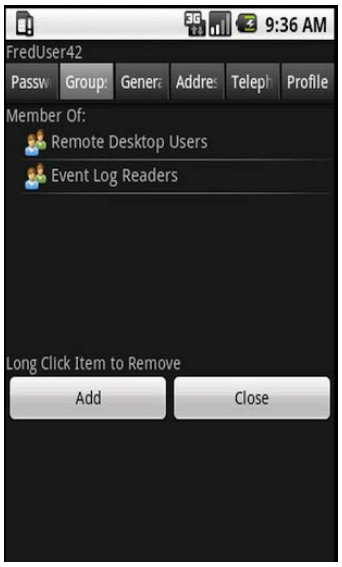
Rate : 4.4

License : Free & 4.99 $









يقدّم هذا التطبيق أدوات الإدارة الأساسية للـ (Windows Active Directory Domain) من متابعة وإدارة المستخدمين والمجموعات والأجهزة المتصلة حيث من خلاله تستطيع تعديل وحذف المستخدمين والمجموعات والكثير من الأدوات المرفقة معه .

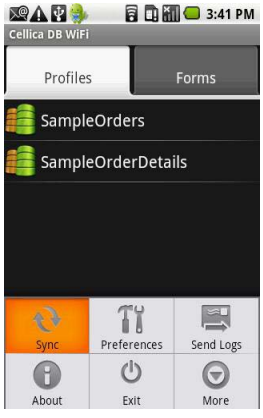
يدعم (Windows Server 2000, 2003, 2008, and later with StartTLS, SSL) والإصدارات الأقدم .حيث تمكنك من الولوج إلى السيرفر مباشرة بدون أية برامج مساعدة على السيرفر ويتم الاتصال عن طريق AD من خلال (WIFI & VPN) .

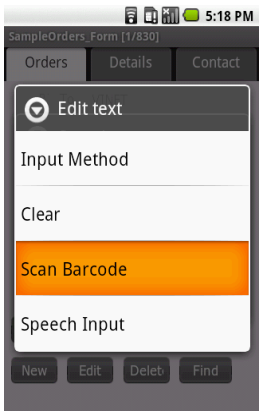
---

2 Cellica Database for Android

Rate : 4.0

License : Free





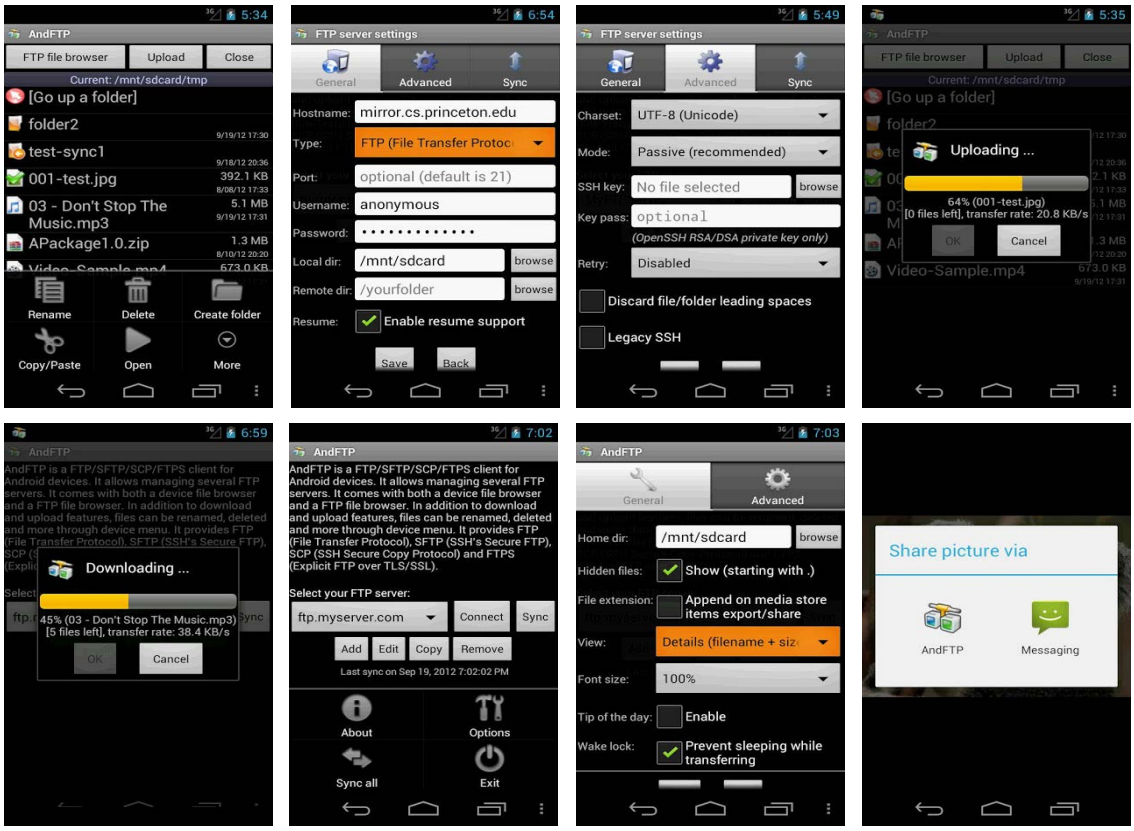
من خلال هذا التطبيق تستطيع إدراة قواعد البيانات الموجودة على حاسبك الشخصي من خلال هاتفك عن طريق الاتصال (3G ,WIFI) حيث تستطيع إنشاء قاعدة بيانات جديدة وترتيب وتعديل الحقول وعمل تصفيه وتطبيق SQL .

ويدعم (Microsoft Access, Access 2007, Microsoft Excel, Excel 2007, Oracle, SQL Server, DB2, MySQL, PostgreSQL, FoxPro, dBase, R:BASE and any ODBC Compliant Database) ولا يحتاج إلى برامج مساعدة للتنصب على الحاسب والتي تودي إلى تفعيل (the remote administration secured with 128 bit AES encryption)

3 AndFTP

Rate : 4.5

License : Free



كما هو واضح من اسمه حيث يعمل كـ (FTP client) مع دعم للـ FTPS and SFTP with SSH (RSA/DSA keys) حيث تستطيع رفع وتحميل الملفات مع دعم لاستئناف التحميل ويمكنك أيضًا من مشاركة الملفات من خلال (email, messaging, Bluetooth, etc) وإضافة إلى ذلك يقدم الخدمات الأساسية من تحرير وإعادة تسمية الملفات وتحديث الأذونات وإدارة الأوامر المخصصة . والإصدار الإحترافي يدعم بروتوكول (SCP) ومزامنة الملفات.

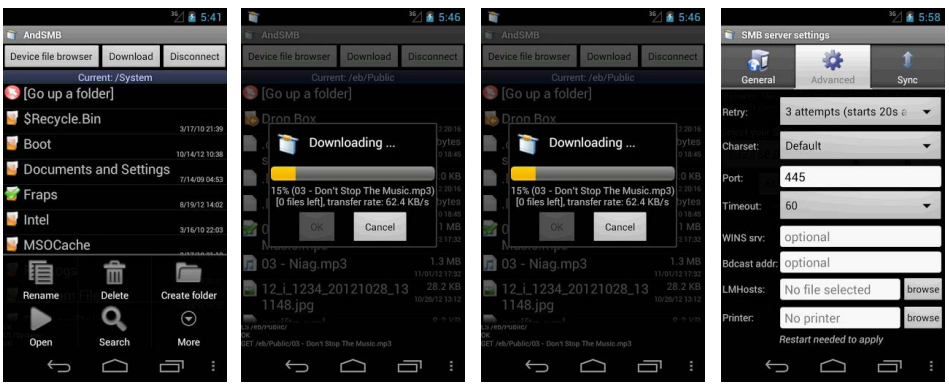
---

4 AndSMB

Rate : 4.4

License : Free

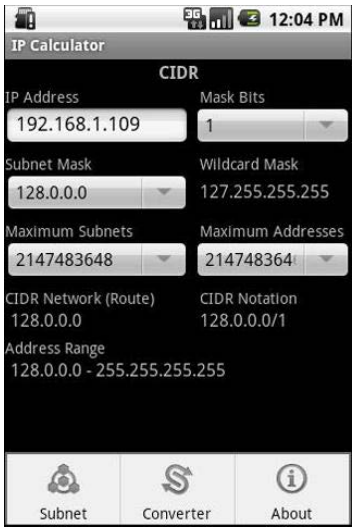
يمثل (SMB client) حيث تستطيع الاتصال بـ(Windows shares) من خلال Wi-Fi and 3G/4G,
حيث يوفر القدرة على التصفح ورفع وتحميل الملفات وانشاء وحذف المجلدات وله القدرة على مزامنة الملفات والمجلدات وإرسال الملفات إلى shared printer وغيرها الكثير من الإمكانيات.

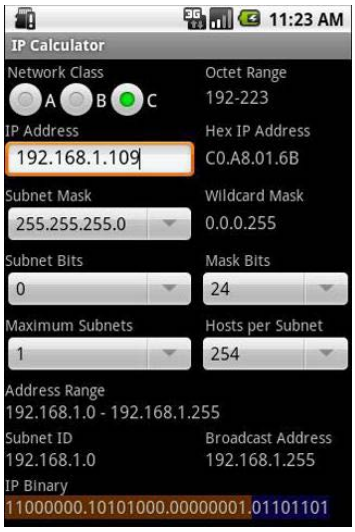


5 IP Subnet/Supernet Calculator

Rate : 4.2

License : Free





يساعدك على حساب subnet and supernet information .

وعند إدخال (IP address, subnet mask and bits maximum subnets, and hosts per subnet) ويزودك هذا البرنامج بالمعلوات التالية.

the address range, subnet) ID, broadcast address,and the IP binary. Classless Inter-Domain Routing ((CIDR) addresses

وأيضا يدعم التحويل بين الأنظمة الرقمية

decimal, binary, octal and) .(hexadecimal numbers

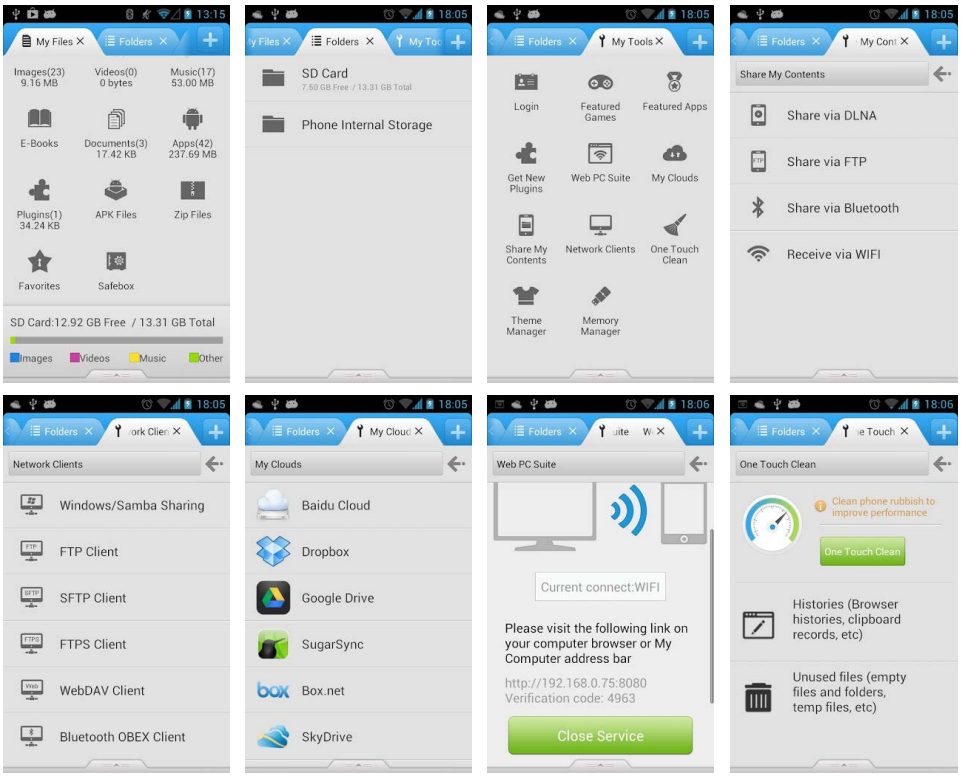
---

6 File Expert

Rate : 4.4

License : Free

يعد من أقوى برامج إدارة الملفات لما يحتويه من إضافات قوية ومميزة . إضافة الى تأديته المهام الأساسية من (Copy, Paste, Move, Create, etc) فهو أيضًا يدعم thumbnails للوسائط المتعدده وفتح ملفات النصوص ومشاهدة الصور , وله القدرة على ضغط وفتح الملفات المضغوطة . (ZIP, RAR, GZIP, TAR, TGZ, and BZ) ويتضمن أيضا مدير تطبيقات يساعدك على إلغاء تثبيت بدفعة واحدة وبسرعة كبيرة .ويعمل أيضًا كـ web and FTP sharing على الشبكة الداخلية . ويساعدك على الاتصال من خلال جهاز آخر على نفس الشبكة بجهازك وتصفح

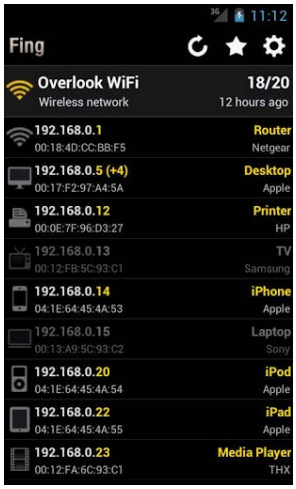


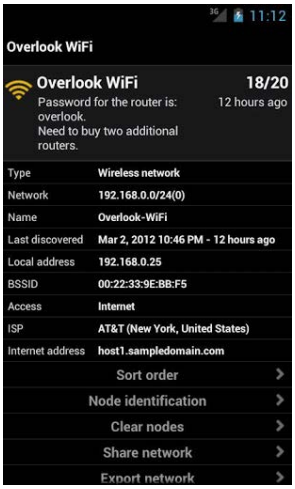
ملفاتك ونقل وإدارة الملفات . ومن مميزاته أنه يعمل أيضًا كـ SMB client حيث يتصل بـ Windows shares. و FTP client حيث يتصل مع FTP server .

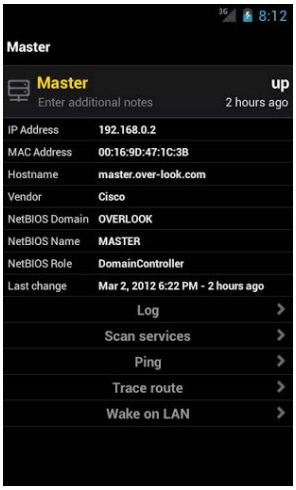
7 Overlook Fing

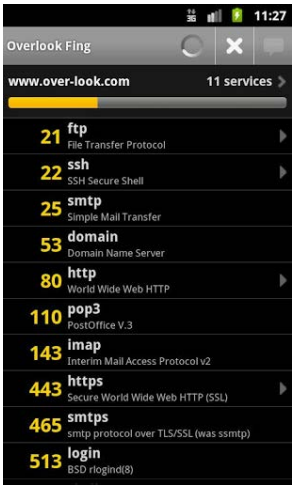
Rate : 4.8

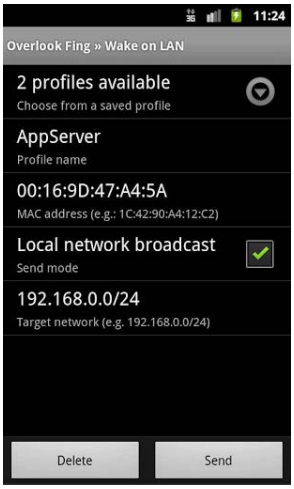
License : Free











يعد من تطبيقات اكتشاف الشبكة من خلال (TCP port scanning, pinging, traceroute, and DNS lookups) على الشبكة من خلال الWIFI .

للوهلة الأولى ترى تفاصيل الاتصال الخاصة بك.
((SSID, IP details, and speed) وقائمة من أجهزة المتصله بالشبكة بالإضافة إلى معلوماتهم
(MAC address, IP and vendor))

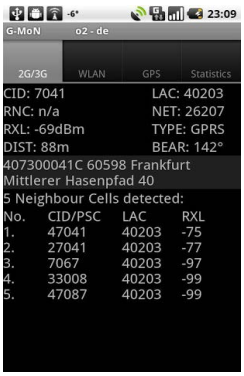
وله القدرة على عمل (port scan or ping) وتغير اسم جهاز معين على الشبكة والـ Icon الخاصة به وإضافة ملاحظات لكل جهاز .

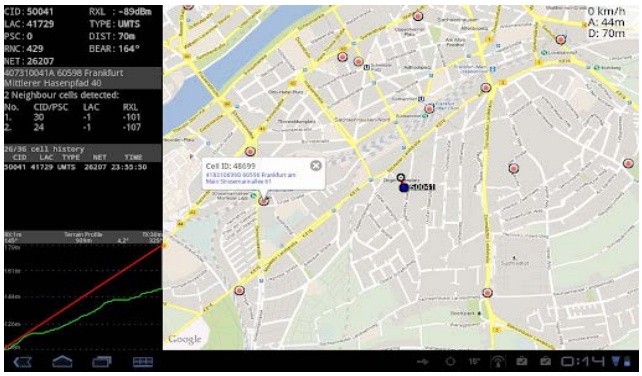
ويحتوي على العديد من الأدوات المرفقة معه من third-party apps الخاصة بـ SSH, Telnet, FTP, FTPS, SFTP, SCP, HTTP, HTTPS, and SMB.

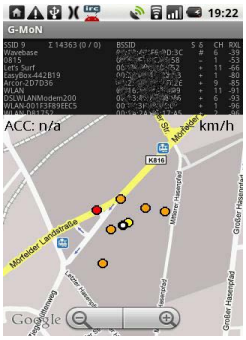
8 G-MoN for Android 2.x

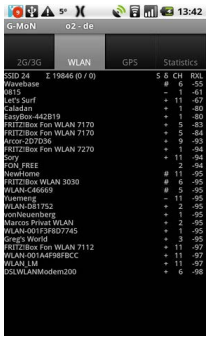
Rate : 4.3

License : Free









إنه Wi-Fi and GSM/UMTS scanner مع دعم لـ GPS يعد من أروع البرامج الخاصة لرسم الخرائط الخاصة بمواقع الـ Wi-Fi access points and/or cell towers في منطقة معينه.

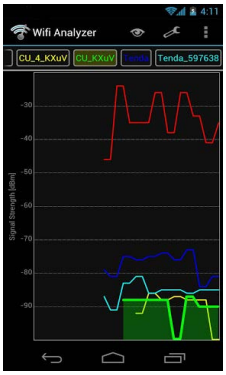
حيث يعرض موقع معلومات عن كل access points مثل:
encryption, channel, and signal strength
وله القدرة على إنشاء KML file for Google Earth

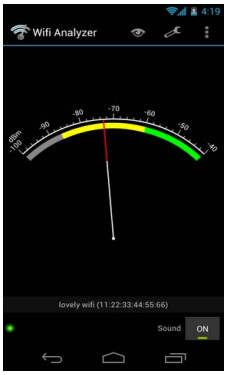
---

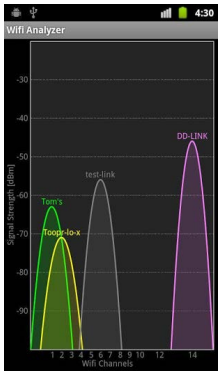
9 Wi-Fi Analyzer

Rate : 4.6

License : Free







يعد من البرامج المتقدمة في تحليل شبكات الـ WI FI ويساعدك في التحليل عند إنشاء Aps حيث يقوم بتحليل الشبكة واكتشاف الأخطاء وإصلاحها .

عند التشغيل لأول مره سوف يظهر معلومات على شبكتك مثل (SSID, ومعلومات الشبكة (MAC, and IP من SSID, MAC, supported) وقوة الإشارة (encryption, channel وتستطيع أخذ لقطة من الشاشة و تصديرها .

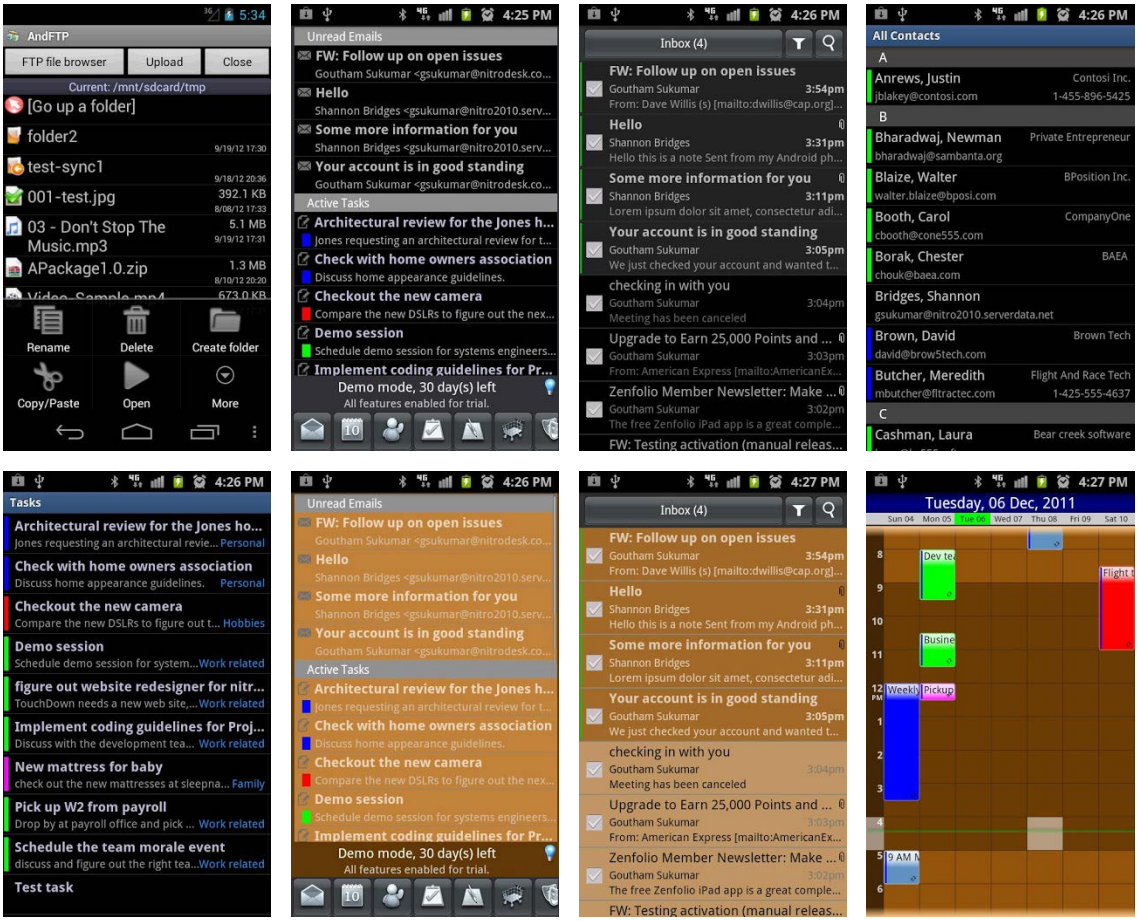
ويقدم أيضًا العديد من الأدوات مثل channel graph حيث يعرض أي الـ AP أقرب وأيضًا time graph حيث يقدم نفس المعلومات خلال فتره زمنية معينة و channel rating chart يقدم أية أفضل القنوات. و signal meter يساعدك على تحديد موقع AP من خلال مؤشر مرئي وصوتي .

Exchange by Touchdown

Rate :

License : $19.99

10



يقدم خدمات Exchange email من أسماء وتقويم وتبادل رسائل وإنشاء مهمات للمستخدمين، و يقدم تحسينات أمنية وتشفير على بيانات وملفات الـ Exchange .

ConnectBot

Rate : 4.7

License : Free

11

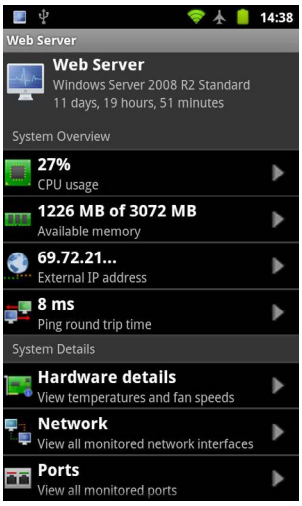
ويمثل أحد أروع البرامج والتي استخدمها شخصيًا بكثرة حيث يشابه عمله عمل برنامج PUTTY حيث أنه عبارة عن (SSH client) ويدعم أيضا Telnet and local connections .

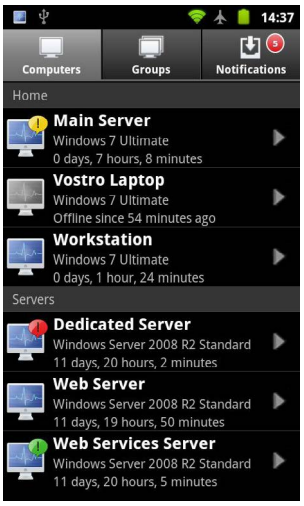
ويعتبر أروع أداة لمستخدمي UNIX SERVER والأجهزة التي تقبل الاتصالات البعيدة ومن مميزاته توليد مفاتيح خاصة تشغيل أكثر من SSH sessions خلال وقت واحد دعم لخاصية copy/paste

12 PC Monitor

Rate : 4.7

License : 3 Pc Free and up 100 PC paid





يمكّنك من مراقبة وإدارة أجهزة ويندوز والسيرفرات بشكل آمن .حيث أن الإصدار المجاني منه يدعم ثلاث أجهزة والمدفوع يدعم أكثر من 100 جهاز حيث يمكنك من مراقبة أداء حاسوبك منstatus and uptime CPU and memory usage, and info on events, hardware, network, and hard disks

وكذلك تستطيع إدارة الخدمات والبرامج ودخول المستخدمين وغيرها الكثير من مميزات .

وكذلك يدعم إدارة الحسابات للـ Active Directory . ويحتاج برنامج مساعد يتم تنزيله على الحاسب الشخصي وتخصيص كلمة مرور محددة لكل حاسب وإرسال تنبيهات إلى بريدك عند حدوث أي تغيرات أو دخول غير مرخص لحاسبك .

13 Server Monitor

Rate : 3.6

License : Free

هذا هو التطبيق مراقبة بسيطة للحصول على تنبيهات صوتية أو الإهتزاز اعتمادًا على :

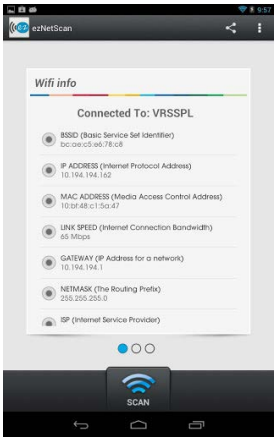
TCP connections and SSH tunnels

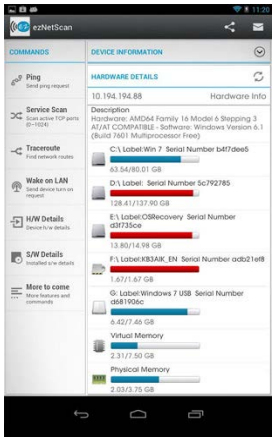
وهو وسيلة بسيطة ومجانية لمراقبة أجهزة الكمبيوتر المحدّدة أو السيرفرات. ويمكنك أيضًا تحديد polling frequency بالدقائق.

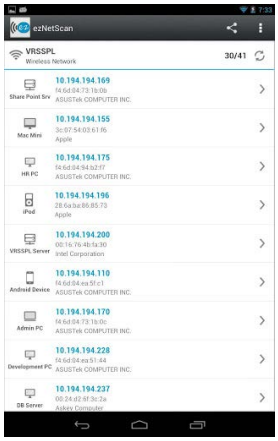
14 ezNetScan

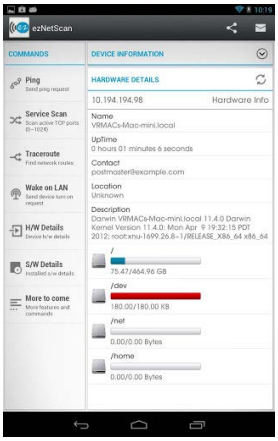
Rate : 4.3

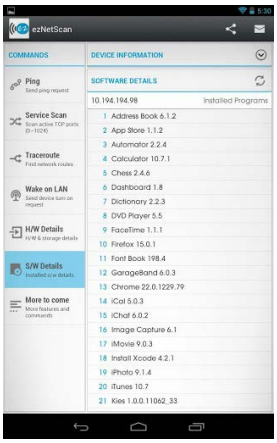
License : Free

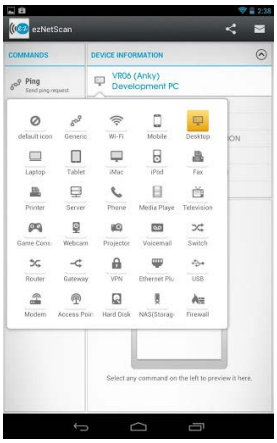


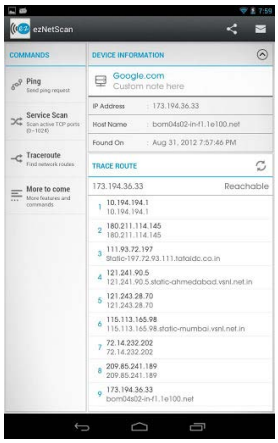


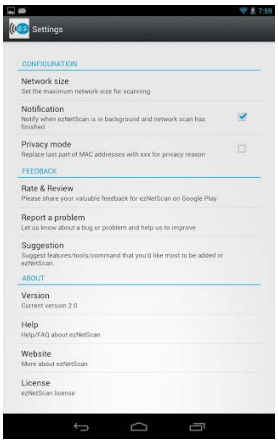












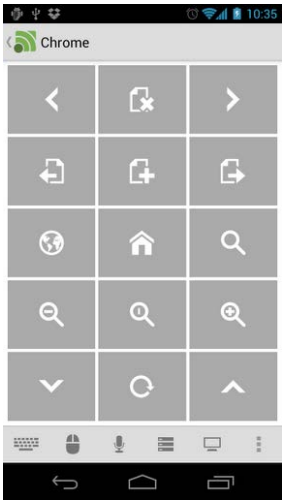
يعتبر من أفضل الأدوات لمدراء الشبكات فيمكن من خلاله عمل بحث على الشبكة وتسجيل جميع الأجهزة المتصلة وكذلك يمكنك من تحديد مظهر جهاز معين وتسجيل الملاحظات وغيرها الكثير وكذلك يقدم العديد من الأدوات منها :

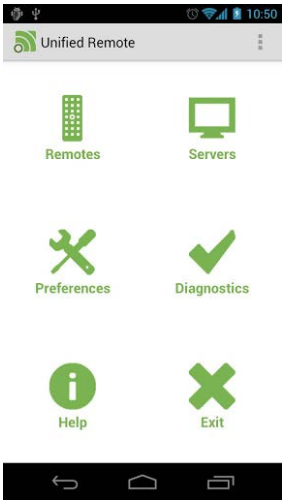
- Ping
- Service Scan
- Traceroute
- Wake on LAN
- DNS lookup
- NetBios Name
- Scan TCP Service
- Device IP Address, MAC Address and Manufacture Name
- Custom device name and icons
- Installed Software & Hardware details (It will work for SNMP enabled devices)

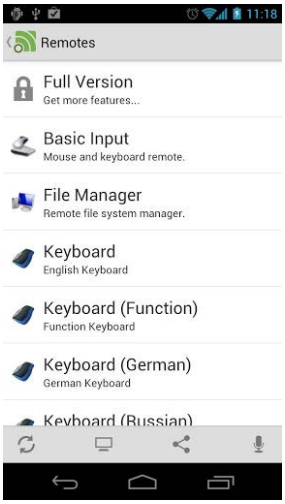
15 Unified Remote

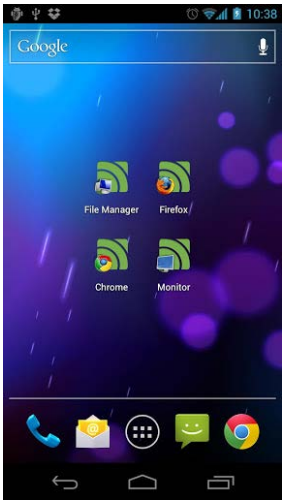
Rate : 4.5

License : Free & Paid





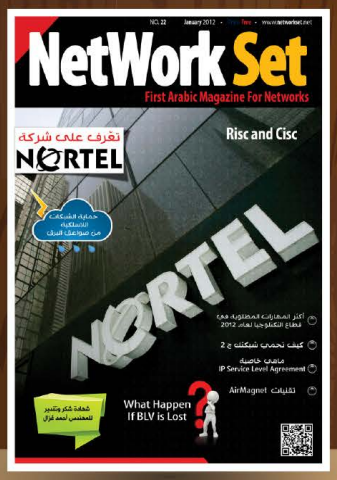


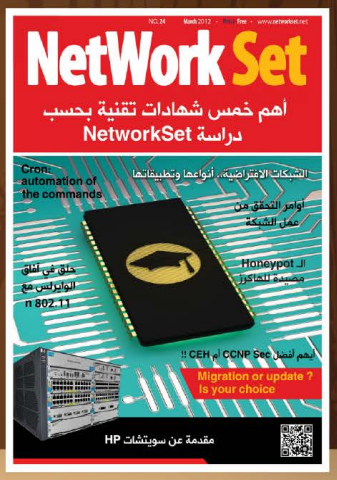


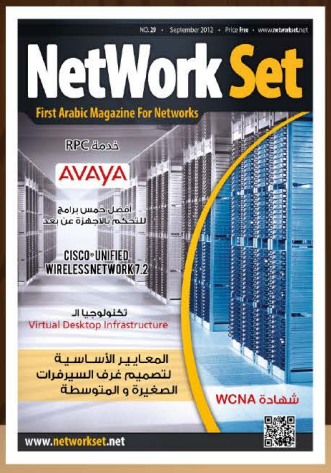
يمثل أفضل البرامج الموجودة حاليًا للتّحكم في الـ PC لما يقدمه من خدمات وتحكم في برامجك المفضّلة لما فيه من مميزات من اتصال خلال الـ WIFI & BLUETOOTH.

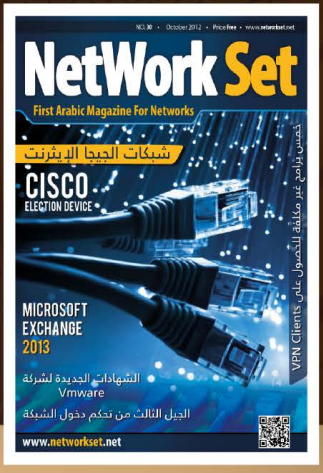
وتشفير وتحديد البرامج التي ترغب في التحكم فيها وبحث آلي عن السيرفر والتحكم بالصوت وسهولة في تغيير السيرفر (إذا كان لديك اكثر من جهاز متصل).

Network Set Magazine Gallery





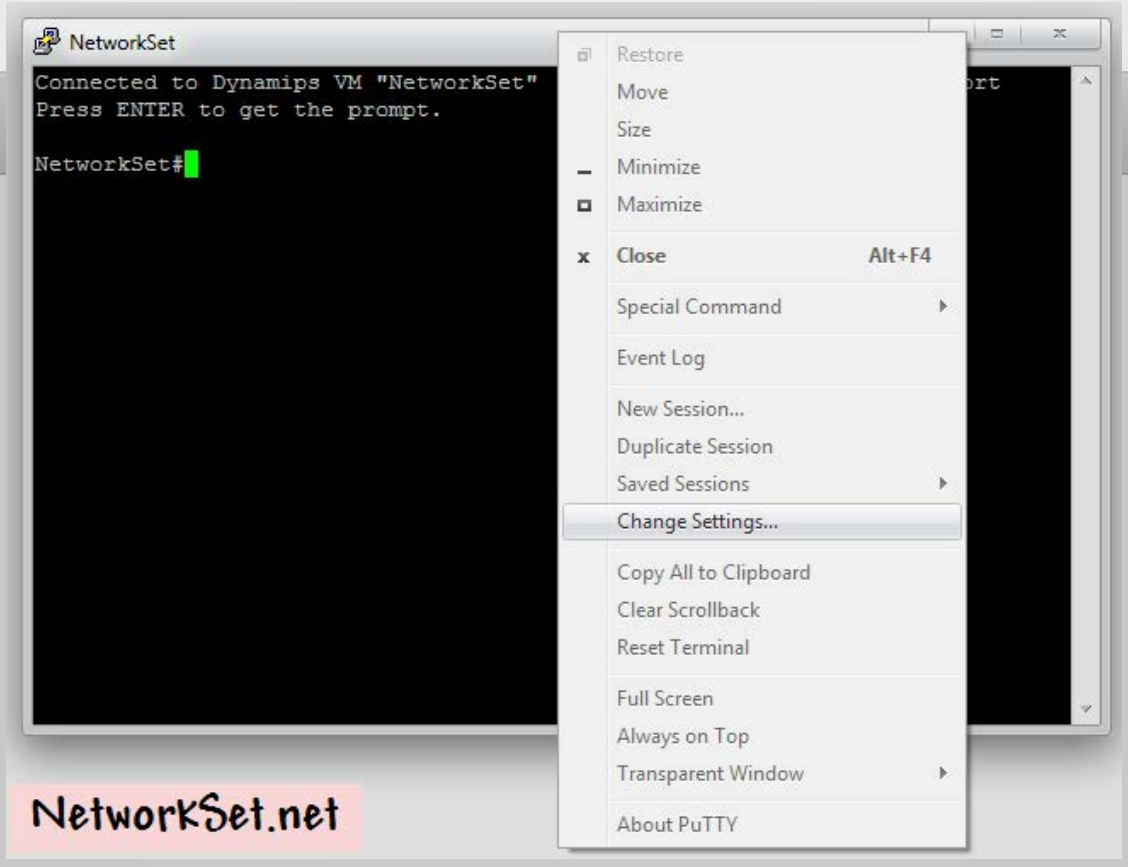


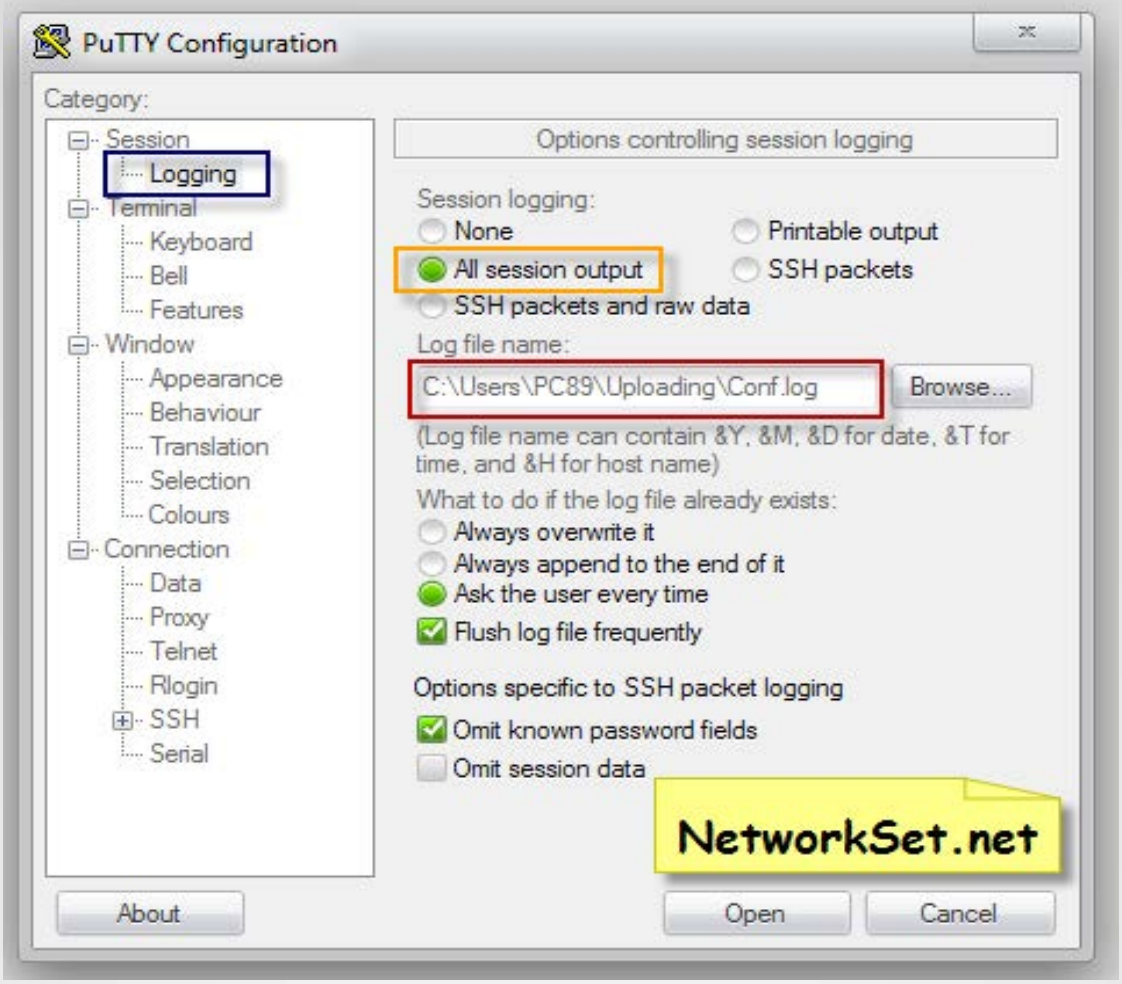


كيفية إلتقاط الأعدادات وحفظ النسخ الاحتياطية الخاصة عن طريق برنامج Putty

عادة مايستخدم الكثير من مديري الشبكات والمسؤولين عن أجهزتها برنامج PUTTY للتحكم بالأجهزة الموجودة على الشبكة من راوترات وسويتشات وفايروول، في هذا المقال الخفيف سوف أوضح بشكل سريع طريقةً نستطيع من خلالها حفظ الإعدادات الخاصة بالراوتر أو أي جهاز أخر نقوم بعمل Configuration له مهما كان نوعه، عن طريق برنامج PUTTY،فهو يدعم أنواع كثيرة من الاتصالات مثل الـ SSH, Telnet, RLogin & RAW.

فلو كنت متصل بفايروول من شركة جونيبر أو راوتر - سويتش من شركة سيسكو فأنك بالتأكيد ستستخدم برنامج يدعم الـ SSH أو الـ Telnet وعندما تنتهي من عملك وبعد حفظ الإعدادات فلابد من أخذ نسخة أحتياطية من هذه الإعدادات وحفظها في مكان آمن مثل FTP سيرفر أو حتى على جهازك الشخصي ولفعل ذلك بسهولة فعليك أن تستخدم برنامج PUTTY وتدخل على Change Settings ثم Loggingوتقوم بتغير بسيط وهو أن تجعل البرنامج يقوم بتسجيل كل ما تقوم به من أوامر في ملف text.log وتحدد المكان الذي سيخزن فيه الإعدادات ثم تضغط موافق كما هو موضح في الصور الظاهرة أمامك وبذلك تنتهي من عمل الإعدادات المطلوبة للبرنامج :





فإذا كنت تريد عمل حفظ نسخة إحتياطية (Backup Configuration) من الإعدادات الموجودة في نظام تشغيل الراوترات أو سويتشات الخاص بـ شركة سيسكو فما عليك إلا عمل التالي :-

```
NetworkSet# term len 0
NetworkSet # sh running-config
```

أما إذا كنت تريد عمل حفظ لـ الإعدادات Startup configurationفسوف تقوم بعمل التالي :

```
NetworkSet# sh startup-config
```

أما في حالة الفايروول الخاص بشركة جونيبر فكل ما عليك أن تفعله هو التالي :

```
admin> get config
```

وكما قلت سابقاً هذه الخطوات تعمل على جميع الأنواع وليس سيسكو وجونيبر فقط وكل ما ستحتاجه هو عمل إعداد البرنامج فقط دون أضافة أي أمر في الجهاز الذي ستقوم بعمل Configuration له.

Microsoft® Lync™ Server 2010

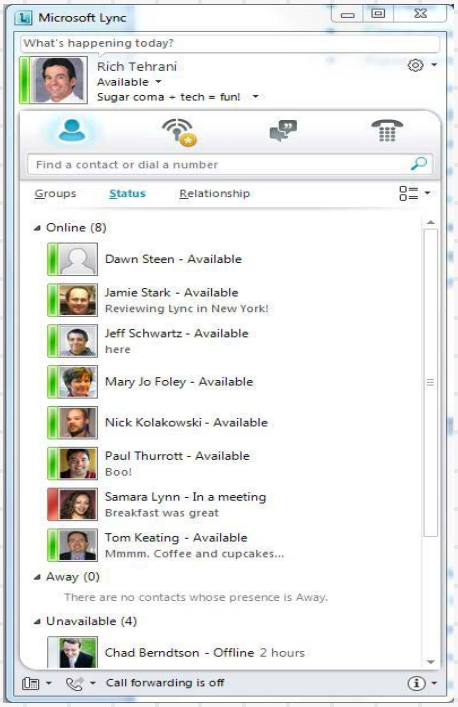
مع التطور المتسارع لتكنولوجيا المعلومات الذي هدفه تطوير الشركات في العمل والمتابعات لحظة بلحظة مع الموظفين وإبقائنا على التواصل مع الشركات الأخرى.

مقالنا في هذا العدد يسعى لنضع القراء بأحدث هذه التطورات ليتم استخدامها في جميع أحجام الشركات الصغيرة منها والكبيرة.

برنامج Microsoft Lync 2010 الذي كان يعرف في السنوات السابقة بـ Office Communicator 2005/2007 .

جميعنا يعلم الـ Windows Live Messenger الذي يوفر لنا المحادثة ونقل الملفات و المكالمات الصوتية وعرض المحاضرات مع الأشخاص التي تتم إضافتهم في حسابنا.

ما رأيك أن تكون إدارة الأشخاص وإتمام صلاحيات الاستخدام بشكل مركزي من مخدماتنا الخاصة؟



و يعتبر برنامج Lync 2010 اتصالاً ظاهريًا بينك وبين الأشخاص الآخرين الذين تعمل معهم وهو يمكّنك من التّحدث معهم ، ومشاركتهم سطح المكتب وتطبيقات (Word , Excel ,.....)، والعمل معهم في الوقت الفعلي مباشرةً من الكمبيوتر الخاص بك.

إن Microsoft Lync 2010 يؤمن لك جميع مزايا Windows Live Messenger وبالإضافة إلى ميزات عديدة تختص في مجال الاعمال.

نحن نتحدث عن منتج يتألف من فئتين :

1 - أون لاين

- الاشتراك عن طريق مايكروسوفت بالـ Office 365 الذي يوفر لك خدمة البريد الإلكتروني وخدمة اللينك سيرفر التي يتم الاشتراك بها على حسب عدد المستخدمين، والدفع شهري .

2 - داخلي

- النسخة المجانية المقدمة من مايكروسوفت ليتم تنصيبها على مخدم و نسخة ويندوز سيرفر 2008 حصراً ويكون عضواً في الدومين لدينا .
- جعل المسنجر الداخلي خارجي، وذلك عند السماح للأشخاص من خارج الشركة بالدخول إلى المخدّم واستخدام الماسنجر، وبهذه الحالة أصبح الماسنجر خارجياً مثله كمثل اللايف مسنجر.
- إنشاء الشهادة الخاصة بالبرنامج ليتم العمل بشكل أمن Certificate SSL

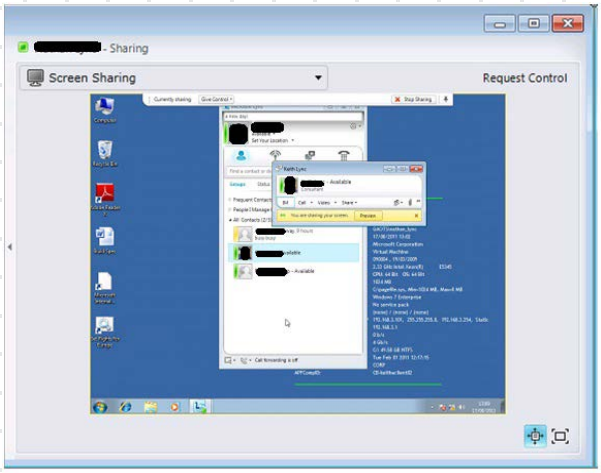
تنصيب نسخة الـ Client ، أيضاً مجانية ويتم الدخول بها باسم المستخدم وكلمة المرور المخصصة لدى الموظّف في الـ Active Directory .

- **لقد تم إضافة الخدمات التالية :**

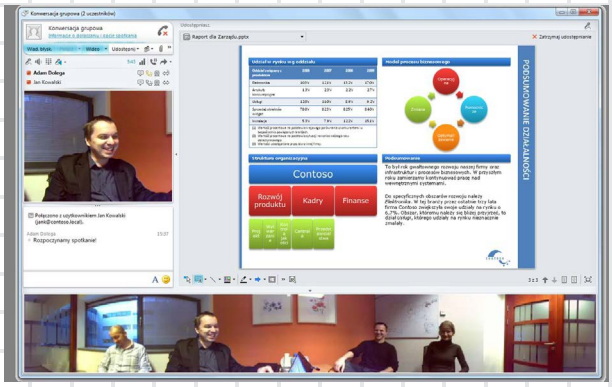
1 - عند توفر الـ Exchange Server يتم إنشاء وبشكل تلقائي ملف اسمه: Conversation History تتم بواسطته حفظ جميع المحادثات التي تمت بينك وبين شخص آخر.

2 - اتصال Audio ، Video.

3 - مشاركة سطح المكتب ليتم إجراء إصلاح أخطاء أو الأسئلة عن بعد مع قسم الدعم الفني.



4 - مشاركة ملفات الـ Presentation مثل ملفات الـ Power Point لمناقشها مع جميع الموظفين في خارج وداخل نطاق الشركة.



5 - الاتصال بالعديد من شبكات المراسلة الفورية العامة، بما في ذلك MSN وWindows Live وYahoo! وAOL.

6 - استخدام الرنين المتزامن لـ Lync 2010 لتلقي المكالمات الواردة تلقائيًا على الهاتف الجوال أو الهاتف المنزلي أو أي رقم هاتفي آخر، بالإضافة إلى عميل سطح المكتب والكثير من الخدمات الرائعة والهامة في مجال الأعمال.

فمن خلال واجهة مستخدم محدّثة، يجمع Lync 2010 معًا أدوات الاتصال التي تعمل بطريقة الاستخدام التي اعتدنا عليها.

Why Firewalls

ماذا ستفعل لو اضطررت لترك سيارتك أو منزلك لفترة من الوقت؟هل ستقوم بغلق الأبواب ؟بالطبع نعم، لأن ذلك يعطيك الإحساس بالأمان ويضع ممتلكاتك بعيدًا عن اللصوص.

نفس الشيء بالنسبة للكمبيوتر حيث أن اتصالك بشبكة الانترنت يجعلك عرضة لمحاولات الإختراق من قبل العديد من الهاكرز الذين يسعون دائما للوصول إلى بياناتك الشخصية أو المالية.
يرسل الهاكر فيروسات أو ديدان ضارة تضر الشركة ابتداءً من تشويه سمعتها وصولا لتدمير نظم التشغيل.

لكن السؤال هنا هو كيف تقوم بتأمين هذه الأبواب أو المداخل المؤدية لأي كمبيوتر فى الشبكة مع إستمرارية الدخول للإنترنت والوصول إلى هذه الاجهزة من الخارج؟

هنا تتجلى أهمية الفايروول لأن دوره الأساسي يتلخص في منع الدخلاء من الوصول للشبكة فهو يضمن لك اتصال آمن بالعالم الخارجي في الوقت الذي يمنع فيه أي اتصال من أي جهاز خارج الشبكة أو يحدد من لهم الحق في ذلك بناءً على احتياجات العمل والتي يحدّدها مدير الشبكة.
وبشكل عام لكي تدرك أهمية شيء لابد وأن تعرف أولا ما حجم الخسائر التي يمكن أن تتعرض لها بدون هذا الشيء. لذلك إليك بعض المخاطر لتعرف ماذا يوجد على المحك.

- فقدان الداتا أو التلاعب بها Data loss and manipulation

إذا كان لديك عملك الخاص هذا يعني أنك تتعامل يوميًا مع أطنان من الداتا منها ماهو خاص بشركتك أو ماهو خاص بالعملاء.مثل هذا النوع من البيانات يكون حساسًا جدًا وضياعها قد يتسبب في انهيار الشركة أو وقوعها في العديد من المشكلات .
ماذا ستفعل لو اختفت جميع البيانات الموجودة على النظام أو ذات صباح اكتشفت أن كل الأجهزة خالية تمامًا من كل الداتا التي كانت بها أمس؟

-البيانات السرية وأسرار العمل confidential data

طبيعة أي عمل تقتضى أن يكون لديك مخططات خاصة بمستقبل العمل مثل الخطط الخاصة بالإصدارات الجديدة من البرامج التي تعمل بها الشركة أو مشروعات مستقبلية قيد البحث والتطوير .

كل هذه المخططات من الممكن الإحتفاظ بها داخل أي جهاز من أجهزة الشبكة ولكن هل لديك فكرة عن كيفية إيقاف أي شخص لنقل مثلا هاكر أو منافس أو أي شخص أيًا كان من الدخول للنظام؟

ماذا لو تمكن أحدهم من الحصول على قائمة خاصة بأسماء العملاء أو خطط العمل السرية أو أسرار تكنولوجيا خاصة بالشركة أو خط إنتاج أو غيرها.
من كل هذا يتضح لماذا تنفق الشركات أموالاً طائلة لشراء الفايروول أو غيره من الأجهزة الخاصة بالنيتورك سكيورتي.

-الإستيلاء على الشبكة Hijacking the network

هذا الأمر ليس ببعيد حيث يتمكن أحدهم من التلاعب بالشبكة فيسهل عليه اقتحامها والإضرار بنظم التشغيل وإخضاع النظام بالكامل لإستعماله الخاص، والذي يكون في الغالب استعمال ضار أو غير قانوني ولكن كل هذا يكون بدون علم مدير الشبكة أو أي مستخدم فكل الأدوات المستخدمة في ذلك عادة ما تعمل في خلفية نظم التشغيل بحيث تكون مختفية تمامًا عن الأنظار حتى عن أنظار مضادات الفيروسات.
مثال لذلك مخطط إرهابي يتم الإعداد له بالكامل من خلال شبكة ما وبعد تنفيذه ووقوع الكارثة ومع بدء التحقيقات القانونية على من سيتم إلقاء المسؤولية؟

-إهدار الوقت Down time

بما أن الوقت مساو للمال فإن إهدار الوقت يعتبر بمثابة إهدار للمال وعملية اختراق الشبكة ليست بالضرورة أن تكون من أجل إهدار للوقت الذي يتحول إلى خسائر مالية، ولكن تتنوع الأهداف من الاختراق فمن الهاكرز من يقوم بذلك من أجل الاستمتاع وآخر لجذب الانتباه وآخر من أجل الإنتقام ولكن يبقى أخطرهم هو من يفعل ذلك من أجل تعطيل السيرفرات بالكامل أو تجميدها عن العمل مما يتسبب في توقف جميع الأجهزة والمواقع المتصلة بهذه السيرفرات وأشهر الهجمات المستخدمة فى ذلك ما يعرف DOS»denial of service» or «DDOS»distributed denial of service

- تشويه السمعة Reputation loss

ماذا لو كنت فى موقف فقدت فيه بيانات العملاء أو أسرار العمل الذي يؤثر بشكل كبير على استمرار نجاح عملك؟ بماذا ستجيب تساؤلات من يهمّهم الأمر أو الشركاء أو العملاء أو حتى هيئة العاملين بالمكان؟ مثل هذه الاسئلة لا مفر من الإجابة عنها ومن المؤكد أن أي إجابة سواءً كانت حقيقية أم لا ستؤثر سلبًا على سمعة المكان والعمل به .

إعرف المزيد عن(Category 7 (Cat7
Category 7A (Cat7A)

تعتبر من أحدث معايير كبلات الشبكات و التي تم تطويرها لانتاج سرعة أكبر في نقل البيانات و تأثر أقل بالمحيط من حقول و تشويش بما يعادل إلى حد معين الـ fiber optic .

مع التصنيف الجديد (Cat7) سوف يكون التأثر بالحقول الكهربائية و المغناطيسية و الكهرومغناطيسية بحده الأدنى ذلك لأن هذه الحقول تؤثر بشكل كبير و ملحوظ على جودة نقل البيانات في الكبل، وقد تم هذا من خلال تصميم جديد كليًا للكبل و باختلاف ملحوظ عن (Cat6).

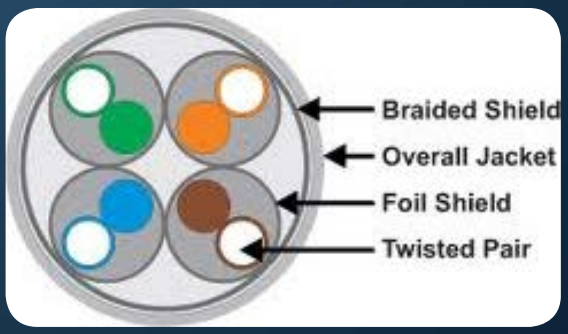
فقد تكوّن الكبل في التصنيف الجديد من:

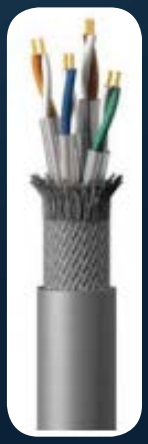
1 - أربعة أزواج مجدولة من الأسلاك النحاسية.

2 - لف كل زوج من هذه الأسلاك بطبقة قصديرية للحماية من crosstalk and EMI.

3 - لُفت الأزواج الأربعة بشبكة من الأسلاك الحديدية الصغيرة لزيادة الحماية أيضًا.

4 - لُفت الشبكة بالطّبقة الخارجية للكبل و هي التي نراها و يكتب عليها التصنيف.





كل الذي سبق أدى إلى زيادة السرعة في نقل البيانات بشكل كبيرجدًا في هذا التصنيف بمعدل 10 Gigabit في الـ 100 مترالواحد.

عادةً ما يستخدم التصنيف Cat7 & Cat7a مع GG45 connector و المتوافق مع RG45 connector .

GG45 connector له أربعة أنماط لتخديم ترددات أعلى من 600 MHz وذلك باستخدام Cat 7 و ترددات أعلى من 1000 MHz باستخدام Cat 7a ، السرعة القصوى التي يخدمها الكبل من التصنيف Cat 7 هي 10 gigabit .

متى نستخدم Cat 7 & Cat7a :

لكي نأخذ الفائدة المرجوة من هذا التصنيف، يجب وضعه في المكان الصحيح في الشبكة، مثلا أنا لا استفيد منه بالشكل النموذجي عندما أضعه لكمبيوتر معين دون سواه و ذلك لقناعتي أن هذا سوف يسرع من أداء الشبكة على هذا الكمبيوتر. لكن يكون الاستخدام النموذجي لهذا النوع من الكبلات في الـ Data centers بين السيرفرات الرئيسية في الشبكة و التي يكون الطلب عليها كبير و ذلك لأنه يدعم السرعات العالية كما سبق وذكرنا.

هل Cat 7 يحل مكان الـ fiber optic :

يمثل Cat 7 بديلاً مناسبًا لكبلات الـ fiber optic و ذلك لعدة أسباب:

- يمثل بديل مقبول جدًا من حيث السرعات العالية و الأداء و الفعالية المطلوبة والتي يحققها الـ fiber optic .

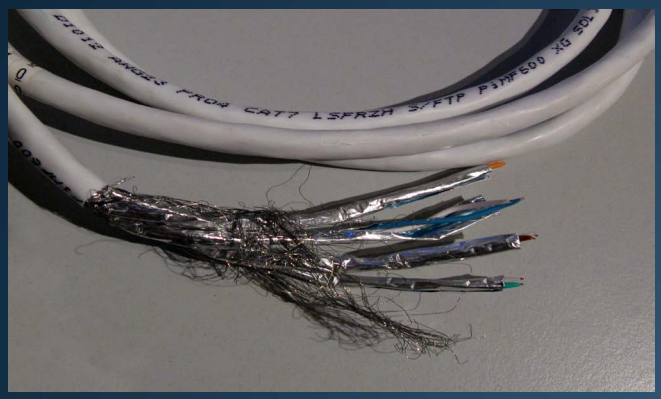
- عندما تقوم باستخدام fiber optic في شبكتك أنت بحاجة إلى عدد من المتطلبات التي يحتاجها هذا النوع من الكبلات كالـ router modules, NIC, switch modules لذا ستكون تكلفة استخدامه مكلفة جدًا مقارنة مع Cat 7 الذي يتوافق مع معظم التجهيزات الشبكية و لا يحتاج إلى متطلبات خاصة به.

- عندما تقوم باستخدام Cat 7 هذا يعني أنك تتعامل مع كبل من النحاس و هو طبعًا ليس بهشاشة الـ fiber optic ممّا يعطيك سهولة في التمديد و التركيب و التشغيل.

هل Cat 7 مستخدمة بشكل واسع النطاق:

نستطيع القول أنها ليست مستخدمة بشكل واسع في الوقت الحاضر و ذلك لأن Cat5e and Cat6 تقدم حلول جيدة فيما يتعلق بالسرعة التي تحتاجها كل من data centers, networks, and end users ، إلا أن المستقبل القريب سوف يفرض استخدام Cat 7 بشكل واسع ضمن الـ data centers بشكل خاص.

«إذا كنت تقوم ببناء البنية التحتية لشبكتك اليوم، قم باستخدام هذا النوع لتتفادى الحاجة إليه مستقبلا»



هذه بعض المقارنات للتصنيفات اعتبارا من Cat 5 :

	Frequency Supported *	Ethernet Signal Supported	Shielded	Connector	Conductor Pairs	Applications
Cat 5	1 - 100MHz	10/100Base T	Optional	8p8c RJ45	4	Small office, home office, schools
Cat5e	1 - 100MHz	10/100Base T Gigabit Ethernet	Optional	8p8c RJ45	4	
Cat6	1 – 250MHz	10/100Base T Gigabit Ethernet	Optional	8p8c RJ45	4	Large enterprise, university campuses, high speed applications
Cat6a	1 – 500MHz	10/100Base T Gigabit Ethernet 10Gig Ethernet	Optional	8p8c RJ45	4	
Cat7	1 – 600MHz	10/100Base T Gigabit Ethernet 10Gig Ethernet	Individual Pair & Overall Cable Shield	GG45 TERA	4	Data center backbone, high speed and bandwidth intensive applications
Cat7a	1 - 1000MHz	10/100Base T Gigabit Ethernet 10Gig Ethernet	Individual Pair & Overall Cable Shield	GG45 TERA	4	

10 أفكار مفيدة لتحسين أمان الشبكة وأجهزة الكمبيوتر

يشكّل أمن الشّبكات وأجهزة الكمبيوتر تحديًا كبيرًا لمدير الشبكة، وهو في معركة دائمة معه وكثيرًا ما أدى ذلك التّحدي إلى فقد مدير الشّبكة لوظيفته وأضرار كبيرة للشركة وعملها .
وخاصةً بالنّسبة للشركات الصغيرة محدودة الموارد المالية، فهم أصلاً يجدون صعوبة في معرفة من أين يبدؤون وماذا يستعملون لمواجهة هذا التحدي، لذلك سأقوم في هذه المقالة باقتراح عشرة أدوات وطرق لمساعدتك على الوصول لمستوى أمان أفضل لشبكتك و لأجهزة الكمبيوتر:

1 - استعمل Linux:

حقيقة الأمر تقول بأنه كلما جعلت المستخدمين على الشبكة يستخدمون نظام Linux، فإن ذلك الأمر سيؤدي إلى انخفاض المخاطر الأمنية، فإذا جعلت مثلا ربع المستخدمين يستخدمون Linux فإن ذلك سيؤدي إلى انخفاض المخاطر الأمنية بمقدار الربع .
ولكن قد يسأل البعض ما هم المستخدمون الذين سنجعلهم يستخدمون نظام Linux ؟

فالإجابة ستكون بأنهم المستخدمون الذين لا يملكون برامج تعمل على windows فقط، فمثلا إذا كنا نستعمل الـ Exchange فيمكننا تنصيب الـOWA على الـLinux لجعل المستخدمين يدخلون إلى الـ Web Mail.

2 - منع المستخدمين من تنصيب البرامج:

كثير من الشركات التي تقوم باتخاذ هذا الإجراء، صحيح أن هذا سيؤدي إلى بعض الإزعاج لك كمدير للشبكة ،حيث ستضطر دائمًا كل ما احتاج أحد المستخدمين لتنزيل برنامج ما إلى الذهاب لمكتبه وتنزيل ذلك البرنامج، ولكن إذا نظرنا إلى الفائدة التي سنحقّقها من وراء ذلك فهي كبيرة ،حيث سيؤدي ذلك إلى دخول فيروسات وبرامج خبيثة أقل إلى الأجهزة مقارنة بعدد الفيروسات والبرامج الخبيثة التي ستدخل فيما لو سمحنا للمستخدمين بتنزيل البرامج.

3 - عمل ترقية للـantivirus :

من المهم جدًا أن يكون الـ antivirus دائمًا محدّث ،حيث أنني أشعر بالإنزعاج عندما أرى تطبيق أو antivirus غير محدث ، حيث أن تحديث الـ antivirus والتطبيقات يساعدنا على الحماية من البرامج الخبيثة ونقاط الضّعف الموجودة في البرامج.

4 - تبديل متصفح الانترنت:

لا أريد أن أثير نقاشًا طويلاً ولكن في واقع الأمر فإن متصفح الـ Internet explorer يبقى الأسوأ من ناحية الأمان ،لذلك أنا أنصحك بجعل المستخدمين يستخدمون متصفح الـFirefox بدلاً من الـinternet explorer لأنه يبقى الأحسن من ناحية الأمان.

5 - عدم تفعيل الـadd-ons

كثير من مستخدمي المتصفحات يقومون بإضافة add-ons . حيث أن بعض هذه الـ add-ons جيد وبعضها غير جيد لذلك أنا انصح بشدة بعدم استخدام الإضافات الغير ضرورية ،لأنه على الرغم من أنها تقوم أحيانا بتحسين الأداء، إلا أننا لا نستطيع أن نضمن أنها آمنة ،وكثيرًا ما أدى إضافة بعضها إلى توقف الجهاز عن العمل.

6 - إضافة Hardware-based Firewall

لا يقوم الـ built-in windows firewall بعمل حماية جدية حيث يكون غير فعّال كثيرًا، لذلك إذا أردت حماية حقيقيّة لابد من إضافة firewall على الشّبكة حيث سيصبح هذا الـ Firewall نقطة الدّخول الوحيدة إلى الشّبكة، وسيمنع العديد من محاولات الاختراق، أكثر بكثير من المحاولات التي سيمنعها الـ software-based firewall بالإضافة إلى ذلك فإن الـ hardware-based firewall أكثر مرونة وقابليّة للتخصيص.

7 - تطبيق سياسات صارمة لكلمة المرور:

عليك دائما أن لا تسمح للمستخدمين باختيار كلمات السّر الخاصة بهم بدون قيود، لأنك إذا فعلت ذلك ستجد أن كثيرًا من كلمات السر هي 1 أو 2 أو 12 أو حتى أسوأ من ذلك، لذلك عليك أن تضع شروط صارمة لإدخال كلمة السر. يجب أن تحوي كلمة السر حروفًا كبيرة وصغيرة وأن تحوي رموز وأرقام، ويجب أن لا تنسى أن تضع ضمن القواعد شرط أن تتغير كلمة السر كل 30 يوم، صحيح أن هذه الإجراءات ستزعج المستخدمين لكنها فعالة لزيادة الحماية.

8 - لا تسمح بعمل مشاركة ملفات الشبكة لكل الأشخاص:

صحيح أن إعطاء الكل إمكانية رؤية الملفات المشتركة يوفر عليك كثيرًا من الوقت الذي تحتاجه لمعرفة لماذا بعض المستخدمين لا يمكنهم عمل دخول على ملفات الشبكة ،لكن ذلك يزيد من حماية الشبكة من المشاكل الأمنية المحتمل حدوثها بسبب جعل جميع المستخدمين يملكون إمكانية الوصول لكل الملفات.

9 - استخدام network access control مثل PacketFence:

حيث أن الـ PacketFence هي وحدة من أقوى أدوات الـ NAC التي ستجدها، حيث يمكنك بواسطتها معالجة الدخول والتسجيل. وتعطيك إدارة مركزية سلكية ولاسلكية، وباختصار مع هذه الأدوات يمكنك الاطمئنان إلى أن الأجهزة الخبيثة التي ستحاول الاتصال ستكون فرصتها قليلة بالنجاح ولمزيد من المعلومات راجع الرابط التالي:

http://www.packetfence.org/home.html

10 – القيام بعمل فلترة للمحتوى للحماية من mail ware:

أنا مؤمن أنه من الأفضل أن يتم عمل فلترة للمحتوى من أجل الحماية من الـmail ware حيث يوجد بشكل واضح مجموعة من العبارات والكلمات المفتاحية والروابط التي يجب عمل فلترة لها بالاعتماد على تاريخها في التسبّب بالبرامج الخبيثة.

وأنا لم أقم بوضع أفضل الكلمات الجيدة لفترة البرامج الخبيثة لذلك عليك القيام ببحث بسيط للحصول عليها

NetWork Set

First Arabic Magazine For Networks