NO. 30 • October 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

شبكات الجيجا الإيثرنت

CISCO ELECTION DEVICE

MICROSOFT EXCHANGE 2013

الشهادات الجديدة لشركة Vmware

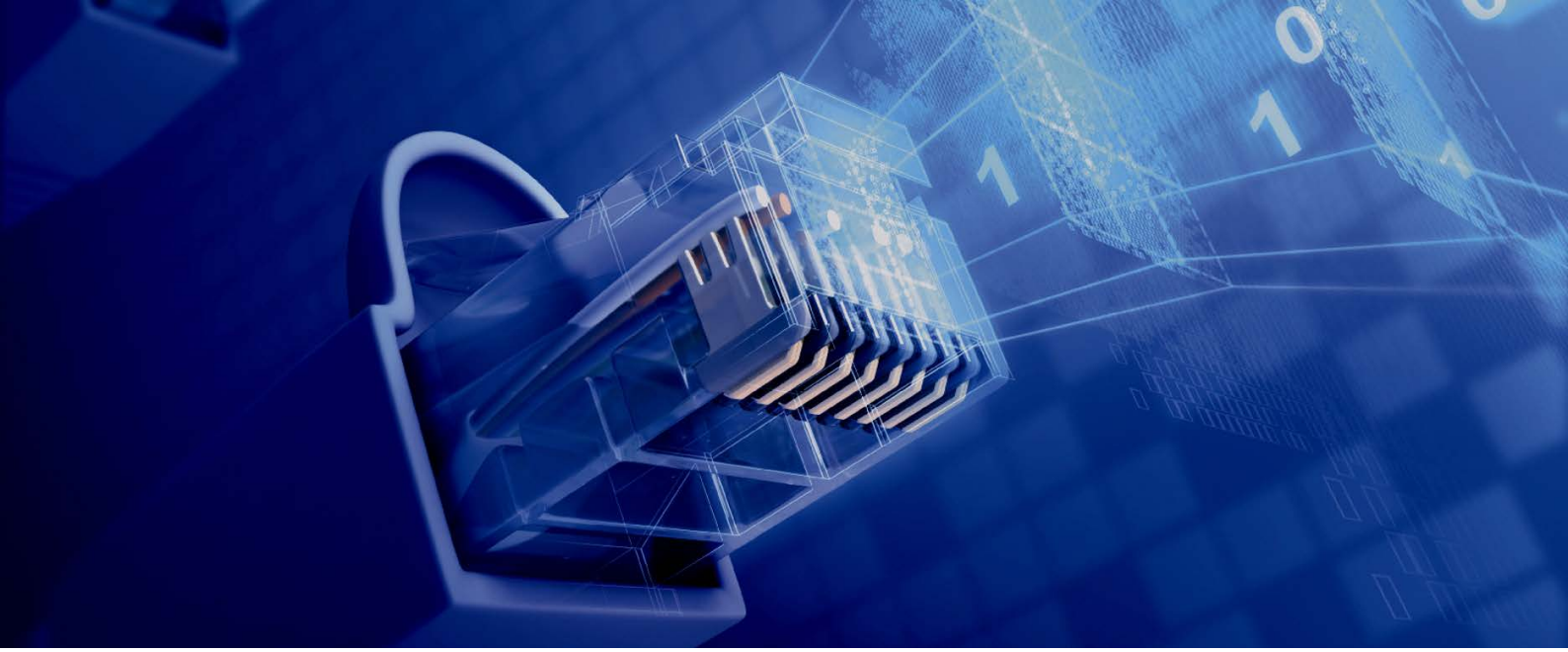
الجيل الثالث من تحكم دخول الشبكة

خمس برامج غير مكلفة للحصول على VPN Clients

السنة الثالثة

في مثل هذه الأيام تقريبا وقبل ثلاث سنوات دخلت مضمار المحتوى العربي على الأنترنت, كتبت الكثير من المقالات وفتحت مشاريع منوعة وصرفت مئات الساعات وأنا أكتب وأكتب وأكتب واليوم اسأل نفسي هل وصلت إلى مبتغاي ؟ هل شعرت بأنك أحدثت نقلة نوعية في مجالك التخصصي على الانترنت ؟
حقيقة وبدون مبالغة أنا غير راضي ابدا عما فعلته وأشعر بأن ماوصلت إليه كان مجرد وقت كان فارغ, كل مافعلته أن وظفت هذا الوقت في أفادة الناس في العلم, وقد يكون سبب إنخفاض المستوى الذي كنت أكتب فيه الآن عن قبل هو الوصول إلى ذلك الشعور بأن ما فعلته وما افعله لا يكفي أو أن أسير في طريق نهايته معروفة بدون الدخول في أرباحنا من نشر العلم عند اللّه فهي أكيد غالية ومهمة لكن نطمح بأرباح أكبر وأهم إن شاء اللّه.
لأطرح عليك نفس السؤال الآن, هل بجد أن راضي عن نفسك ؟ يعني هل جلست مرة وفكرت في حياتك وكم مضى منها, هل ياترى قدمت شيئ مفيد لهذه الدنيا الذي يجمع أغلبنا بأنها دنيا لها هدف أكبر من أن نعيش ونأكل ونشرب ونخلف ونموت, قد تصفني بالشخص المتهور لو قلت لك أن تركت العمل في الشركات لأن لم ارد لحياتي أن تمضي في الروتين الطبيعي لكل أنسان وأتجهت نحو العمل الحر الذي مدخوله عادة مايكون أقل بكثير من عملي في أي شركة فالعمل الروتيني يشعرني بأني أنسان عادي لا أختلف عن المليارات الموجودة في الأرض وخصوصا أن شعور أن تكون زائد على الدنيا هو آخر ما أفضل الشعور به.
كتبت وتحدثت عن هذا الأمر في مقالات كثيرة ولا اعلم لماذا اعود وأذكرك بأن قدراتك وأمكانياتك أكبر بكثير مما تظن, لاتنشغل بالشهادات التقنية وتجعلها آخر همك وطموحك, إرفع رأسك عاليا وأنظر إلى أين الغرب وصلوا وإلى أين نحن وصلنا, نعم وصلنا إلى هذه الدرجة من الأنحطاط بحيث أصبحنا نحقر أنفسنا بأنفسنا ولا نتباها إلا بديننا العظيم الذي والحمد للّه خلقنا وتربينا عليه لكن من الناحية العملية نحن لانساوي شيئ, مجرد أمة لاتعلم ولاتفهم شيئ إلا الأستهلاك, الكل لديه الرغبة في أن يكون شيئ مهم يوما ما لكن نحن ننسى أن تلك المرحلة لاتأتي بيوم وليلة والكل يبدأ فيها صغيرا ويكبر طالما نيته صافية ولديه الرغبة في أحداث ذلك التغيير الذي يخلد أسمه في الدنيا والآخرة, نحن بأختصار أضعنا هذا الحلم لعوامل كثيرة كتعليمنا ومجتمعنا وبخلنا في أن نرسم المستقبل للأجيال القادمة, من منكم يعرف الطفل المصري العبقري محمود وائل ؟ هو ولد في الثالث عشر من عمره الآن, منذ عامان تقريبا قيس معدل ذكائه فوصل إلى 155 (ماشاء اللّه) ذلك الطفل وفي مقابلة متلفزة ذكر بأنه حصل على شهادة CCNA ويحضر لشهادة CCNP وكانت صدمة كبيرة بالنسبة لي أن يرسم مستقبل هذا العبقري كما يرسم المستقبل لكم الآن, شهادات وعمل وراتب ممتاز وتوكل على الرزاق.
بجد, هل أنت راضي عن نفسك, هل تلك الشهادات التى استطيع أن أبيعكم أي شهادة منها بمبلغ مادي يزيد قليلا عن تكلفتها الحقيقة هو هدفك ؟ الدنيا صعبة وكلنا نعاني منها ومن متاعبها لكن لو هي كذلك فلا بأس ان نعاني ونتعب قليلا لأجل شيئ سامي نرضي اللّه وأنفسنا به مع أن غير مقتنع بأن الواحد منا يجب أن يرضى بما عمل مهما كانت قيمته فطالما العقل يفكر والقلب يدق فالطموح يجب أن لايتوقف إلى أن يأخذ اللّه أمانته, أنا غير راضي عن نفسي ابدا فما حالك أنت!!!.... 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.أنس المبروكي
م.أحمد هيكل
م.أحمد خير الدين
م. سامي خالد الرجعي
م.نورس جربوع
م. خالد الدسوقي
م.حسام الدين حشيش
م.رضا عبد الرحمن أحمد فقير
م.عادل محمد شبل
م. غسان محمد ابوجسار

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : أسـامة كـامـل

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

CISCO ELECTION DEVICE

كما في طبيعة البشر من تنافس في الريّادة والزّعامة، ومن بعدها ترشيح وانتخاب، وأفضلية للبعض على الآخر في بعض الأشياء كذلك هناك أفضلية في عملية تشغيل الـDEVICE في CISCO إذا كانت عبارة عن SWITCHES OR ROUTERS فدعنا في هذا المقال أن نتحدث عن الانتخابات في سيسكو و وماهي العملية التي تتم فيها، وسنقوم بتفصيلها بالنسبة إلى SWITCHES OR ROUTERS .

ROUTERS ELECTION'S

سنتحدث عن الـOSPF ففيه توجد عملية انتخاب فيما بين الـROUTERS الموجودة في نفس الـAREA وكما نعلم أنه يمكن في الـAREA الواحدة أن نجد حوالي 50 RECOMMENDED ROUTERS)) فتخيل بالتالي أن تحدث عملية التفضيل والانتخاب فيما بين كل هذا العدد ، إذن الـROUTER صاحب الأفضلية الأعلى هو الذى سيكسب ويصبح السيد أو صاحب الفخامة وتتجه له جميع الأنظار .

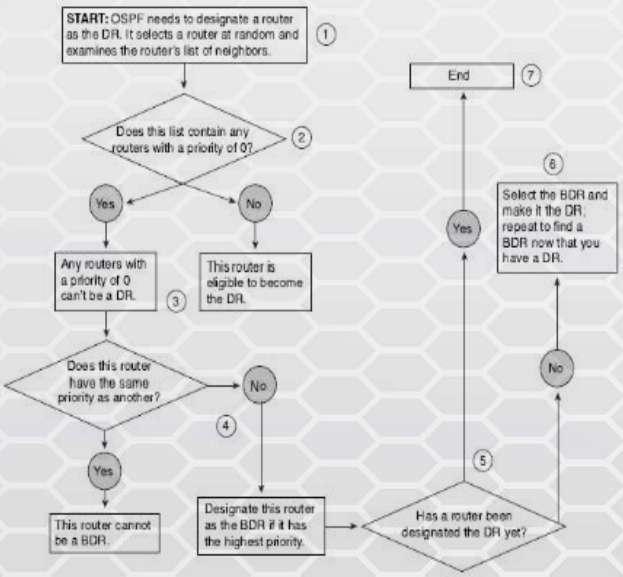
ومن المعلوم أنه كل مازادت الـPRIORITY في الرواتر كل ما كان أفضل من غيره وهو عكس مايتم في الـSWITCH كلما قل (وهنا اقصد الرقم) كل ما كان أفضل من البقية . فمثلا اذا افترضنا أن R1 ذو PRIORITY 5 أما R2 ذو PRIORITY 7 فتصبح R2 هي الأفضل ، يتم الانتخاب لاختيار DR AND BDR وهي DESIGNETD ROUTER , BACKUP وحتى في عملية DESIGNETD ROUTERS الانتخاب هذه تلاحظ أنه يوجد رئيس ونائبه و هما DR AND BDR عند حدوث أي شيء للأول يصبح الثاني هو الرئيس في حالة تساوي الـPRORITY لكل الـSWITCH تصبح عملية الانتخاب بالترتيب التالي :

1 - ROUTERS ID HIGHEST
2 - HIGHEST LOOB BACK INTERFACE
3 - HIGHEST REAL INTERFACE

بالتّتالي، حيث إذا لم يكن رقم 1 نبحث عن الأعلى في رقم 2 أما إن لم نجد الأعلى نبحث عن الأعلى في رقم 3 .

أما في الأسفل، سنرى عملية تثبيت رقم معين بالنسبة للـPRIORITY بالنسبة في OSPF.

```
R#(CONF)#INTERFACE SERIAL 1/ 1
R#(CONF)# IP OSPF PRORITY 0
```



بعد أن يتم اختيار الـDR و BDR تتحول كل الأنظار ويتم إرسال LSA TYPE 2 منهما أما الـROUTERS العادية فترسل ماتسمى LSA TYPE 1 .

في عملية الاختيار نحن نتحدث هنا عن الأغلب في الأمثلة تكون الـPRORITY متساوية في جميع الـ ROUTERS ولذلك نأتي للخطوات في الأعلى :
حيث يتنافسون الأعلى فالأعلى من الكل .
جميع الـROUTERS التي تسمى INTERNAL ROUTER ترسل LSA TYPE 1 للـDR أما هو فيرسل LSA TYPE 2 وكما نعلم فهو يرسلها بالـ ADDRESS 224.0.0.6 أما الـINTERNAL ROUTER ترسلها بـ224.0.0.5

SWITCH ELECTION

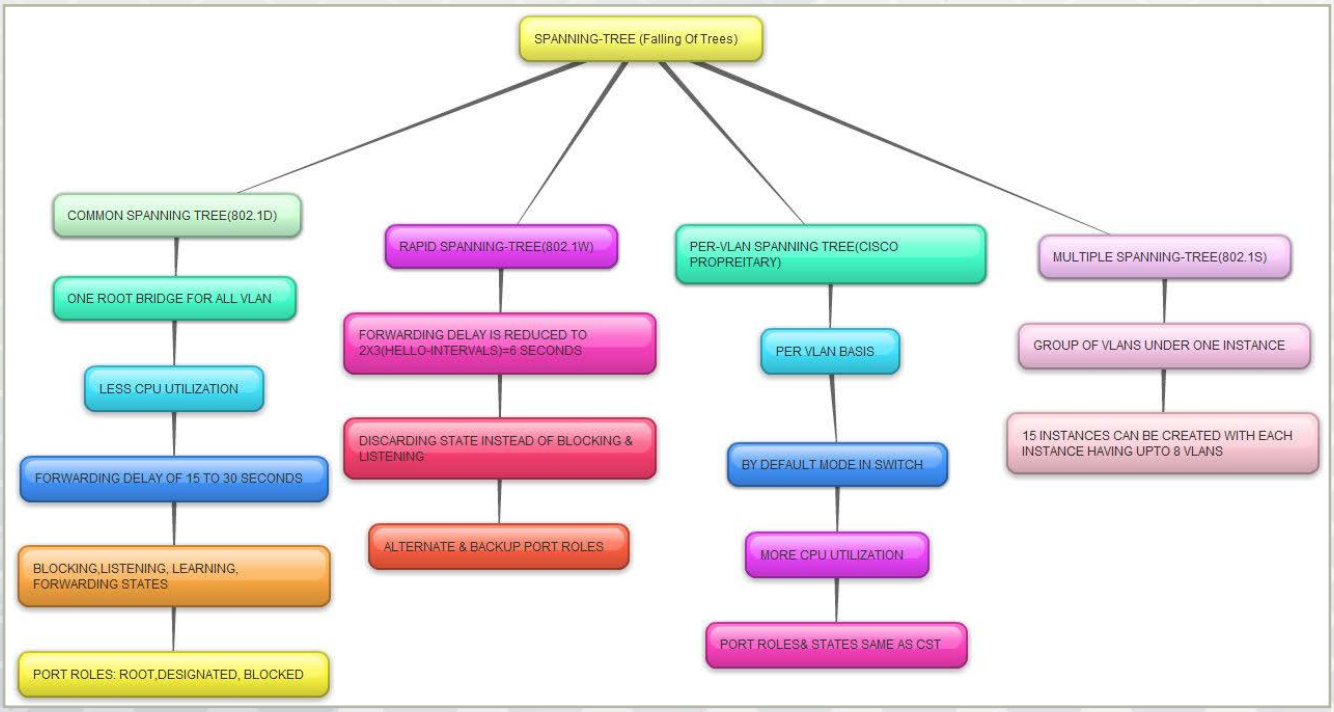
أما في حالة الـSWITCH فتحدث عملية الانتخاب تفاديًا لحدوث عملية دوران البيانات بصورة مستمرة مما يؤدى إلى استهلاك BANDWIDTH والذي معه يؤدي إلى بطء شديد في الشبكة وبالتالي فقدان المعلومة الذي يمنع هذا الـLOOP هو الـSTP IEEE802.1D، تحدث بأن ترسل جميع الـSWITCH مايسمى بـ(BPDU BRIDGE PROTOCOL DATE UNITE وهي عبارة عن رسالة ترسل لتوضيح بعض المعلومات عن الـSWITCH وهي ترسل كل SECOND 2 من بين هذه المعلومات.

PRORITY
MAC ADDRESS

وكما ذكرنا سابقًا هنا في الـSWITCH الأقل هو الذي يكسب الرّهان أما إذا تساوت الـPRORITY لكل الـSWITCH بالتالي يصبح الـMAC في عملية التنافس والسويتش الذي يكسب عملية الانتخاب يسمى بالـROOTBRIDGE .

إذا حدث تغيير من بعد عملية الاختيار وتحديد الـ ROOTBRIDGE فترسل ما تسمى BPDU TCN BRIDGE PROTOCOL DATE UNITE TOPOLOGY CONTROL NOTIFICATION بحيث ترسل في حالة تغيير تم في الـTOPOLOGY ومما يعنى أنه سيتم تغيير الـROOTBRIDGE في أغلب الأحوال .

ومن بعد الـSTP ظهرت العديد من البرتوكولات التي تعمل بصورة أحسن من سابقيها وهي مثلاً كما موضّح في الصورة أدناه: قد نتحدث عنها في مناسبة أخرى :

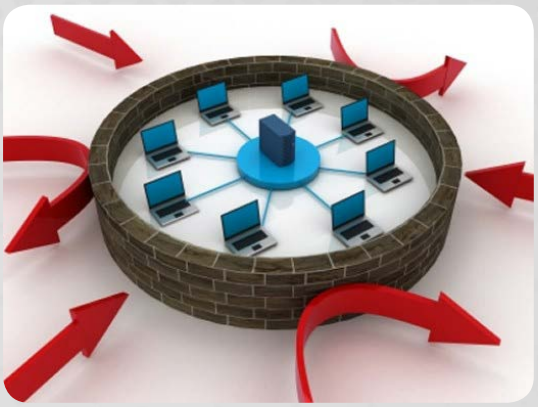


في بادئ الأمر يعتقد كل SWITCH أنه هو ROOTBRIDGE وهو عبارة عن SWITCH يدير دفة سريان البيانات بحيث يصبح هو المنتخب رقم واحد وهو عبارة عن SWITCH ذو PRORITY أفضل .
تتم عملية الانتخابات لتنظيم سريان البيانات بصورة مستمرة وأن يكون هناك تدرّج في ارسال واستقبال البيانات تفاديًا لعمليات تأخر أو ضياعها إلى أن تصل للهدف.

الجيل الثالث من تحكم دخول الشبكة
(3G NAC) Network Admission Control

الجيل الثالث من تحكم دخول الشبكة ((3G NAC
Network Admission Control

جميع الشركات والمؤسسات في العالم ترغب وبشكل كبير بأن تؤسس منظومة أمنية كفيلة بحمايتها من اي مخاطر قد تهدد استمرارية الاعمال فيها. وهذه المخاطر تأتي بالغالب من خارج هذه الشبكة لتضرب استقرارها وتتلاعب بمعطياتها أو تسرقها وقد تطيح بها كليا.

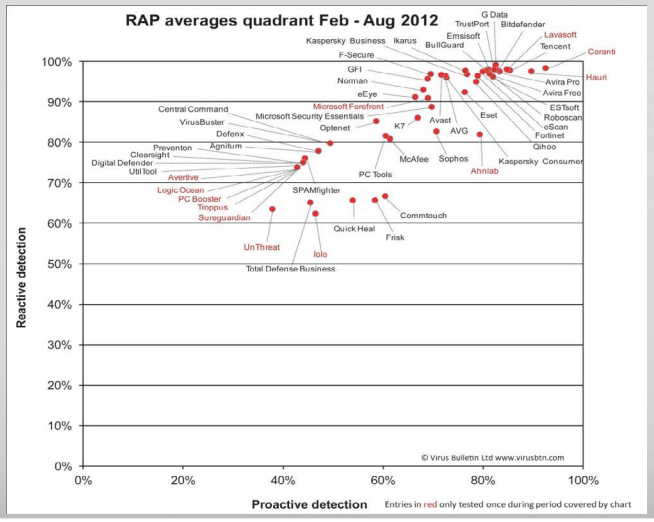


فيقوم وفقا لذلك المتخصصون بمجموعة من التعزيزات التكنولوجية على الحدود الخارجية من الشبكة بوضع انظمة وحلول تحول نوعا ما من ذلك فيقومون بتنصيب ISP's, Deep packet inspection, zero day attack protection, Firewalls ...الخ من المتحكمات التكنولوجية. وتستدعي الحاجة الملحة للعمل بجد لتحصين هذه الحلول بمجموعة من الاعدادات الدقيقة التي تحدد ماهو المطلوب من كل نظام حماية وتفعيل قدرته على استخدام جميع الخيارات المتاحة تقنيا لحماية شبكتنا ومنظوماتنا المعلوماتية.... جميل!

٪20 من الهجمات الالكترونية تتم من داخل الشبكة (خلف جدار الحماية) و ٪80 من الهجمات الناجحة تتم من الداخل ايضا وليس من الخارج, وهذا وفقا لتقارير SANS.org. وبالتالي, حسب USCERT, SANS, FBI وMETRI وبعض مراكز البحوث فإن اكثر من ٪95 من الخروقات الامنية هي نتيجة مباشرة لاستغلال نقاط الضعف الشائعة والتي تسمى ((CVE Common vulnerability and Exposure. فبكل بساطة تستطيع ان تعرف اي ثغرة بأي System أو protocol, Application أوحتى أي Operating system عن طريق البحث في جوجل او في قواعد بيانات ال CVE لتظهر لك آلاف النتائج التي تستطيع ان تستغلها لتنشئ عملية اختراق دقيقة على الانظمة التي لم تجد تحديثا لهذه الثغرات.

هذه الثغرات تتواجد في كل مكان ابتداءا من اجهزة الكومبيوتر الشخصية الى الـServers, Wireless, Application access prints, , وفي كل التطبيقات والاجهزة التي نستخدمها فلا تستغرب ان يكون جهازك المحمول يحتوي عشرات بل مئات من الثغرات التي ممكن ان تستغل لتشكل تهديدا حقيقيا بحال جلبت أو استعملت جهازك بالعمل و أوصلته الى الشبكة الخاصة بالشركة التي تعمل بها.

يعتمد بشكل أساسي الكثيرون على الـ Antivirus لحماية أجهزة المستخدمين من Desktops Laptops, Mobile phones, من اي تهديد قد ينشأ بسبب سوء استخدام هذه الاجهزة أو اي برمجيات خبيثة قد تدخلها من خلال, infected websites USB's أو CD's...ألخ. بالحقيقة فإن ٪70 الى ٪90 من هذه الـ Antiviruses' لا تستطيع ان تكتشف للاسف بعض البرمجيات الخبيثة أو الـMalware. حسب ما هو مبين ادناه. فلذلك لا نستطيع الاعتماد على Antivirus بشكل تام لحماية أجهزة المستخدمين.



ماذا عن Zero-day Malware الجديدة؟ كيف سيتم التعامل معها ؟ هل تستطيع المغامرة بالسماح لأي أحد بأن يتصل بشبكتك قد يحمل في جهازه Malware قد تنفذ الى انظمتك التي قد تحتوي ثغرات لم تسد بعد من قبل المصنع لهذه لانظمة؟ ....هذا اذا افترضنا انهم يعلمون بهذه الثغرة!!!

كيف تستطيع ان تدير المستخدمين الغير مصرح لهم بوبوج الشبكة وكيف يتعلم انهم كمستخدمين عاديين يستخدمون الانترنت فقط ولا يشكلون خطرا بقصد او غير قصد على الشبكة الداخلية للبنية التحتية المعلوماتية وقواعد البيانات....؟

قد تقول بأننا لن نسمح لأحد ان يتصل بشبكتنا و نستطيع ان ندير هذه المشاكل داخليا وان نفرض قيودا إدارية وتقنية تمنع اي احد ان يجلب جهازه وان يشبكه لاننا بالاصل قد اعددنا السويتشات الخاصة بنا لمنع اي MAC address غير معروف ولدينا VLAN's للبينة التحتية منفصلة تماما عن باقي اجزاء الشبكة ولا أحد يستطيع أن يتصل بها....عمل جيد. هل الجميع راضٍ؟

ان التفكير بمنهجية الحماية من الخارج الى الداخل لم تعد تكفي لتلبي احتياجات الاعمال وتطور التكنولوجيا وتعقيدات التهديدات الدائمة التطور بنفس الوقت. ان العمل على منهج الدفاع في العمق (Defense in Depth) يؤسس الإطار العريض لمنهجية الحماية من الداخل الى الخارج الذي يتكون التحكم بولوج الشبكات أساسا لا غنا عنه وليفرض نفسه حلا لا يستغنى عنه في الشبكات الحديثة ومنهجية الحديثة من الحماية.

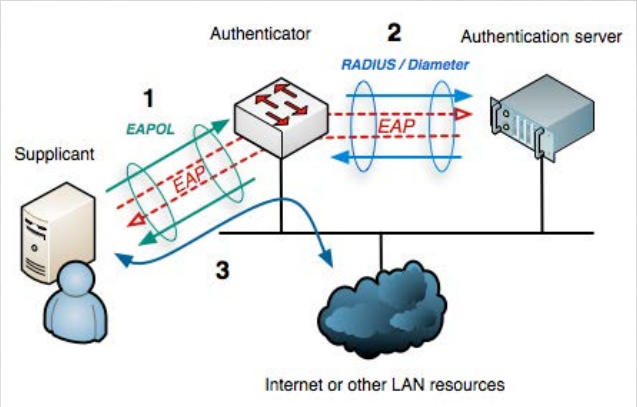
فتطور الاعمال تفرض علينا منهجية عمل مختلفة للحاق بركب هذا التطور الهائل بمجال تسهيل الاعمال والتنقلية. اصبحت الاجهزة المحمولة جزء لا يتجزء من اعمالنا واعمال المستخدمين المسؤولون نحن عنهم بنهاية المطاف. (Bring your own device BYOD) اصبح منهجا شائعا اينما كان, الجميع يستطيعون ان يجلبو اجهزتهم الخاصة بهم من iPads, iPhone,. Blackberryفمن المعضلات الكبرى هي التحكم بهذا الكم الهائل من المستخدمين الذين يريدون ان يستفيدو من بعض خدمات الشركة أو المؤسسة بشكل أو بآخر كالإنترنت مثلا او بعض قواعد البينات كعلامات طلاب الجامعات وجداول المحاضرات والفعاليات...مثلا. وكله يتم لا سلكيا على الاغلب.

فكيف Mr. NAC سيحل لنا هذه المعضلات جميعها؟.....حسناً.

قدم الكثير من المصنعين مثل Cisco و Juniper حلول للتحكم بولوج الشبكات الذي يعتبر احد سياسات تحكم الطبقة الثانية. لذلك اعتمدو بشكل أساسي على بروتوكول 802.1X الذي شكل العامود الفقري لهذه التكنولوجيا. 802.1X هو منهج لتطبيق (EAP) Extendable Authentication Protocol والذي بالأصل يدعى (EAPOL) EAP over LAN. كثير من ال بروتوكولات تعتمد على EAPOL كالـ PPP, RADUS, TACACS+ و طبعا 802.1X للقيام بعملية الـAuthentication مع السيرفير لتحديد ان كان المستخدم مخول بالدخول ام لا. جدير بالذكر هنا بأن EAPOL صمم بالتحديد من اجل دعم PPP لعدم قدرة الـ PAP و CHAP للتواصل مع الـ Authentication سيرفير.

NAC هو ما تدعوه Cisco (IBNS) Identity Based Network Security, والذي هو عمليا 802.1X بالنهاية. تعتمد مثل هذه الشركات اساسيا على ربط

هذه التقنية بالـ Physical Port و الـ MAC Address بتصديق المستخدم عن طريق اسم المستخدم وكلمة السر حيث ترسل للسيرفر المسؤول عن عملية تصديق المستخدمين.



هذه التقنية القديمة ليست كافية وعملية بالاطلاق وخصوصا بعد تطور اساليب الاختراق وبلأخص اثبات أن 802.1X سهل الاختراق ويمكن خداع السيرفر باستخدام بعض الادوات المتوافرة حاليا على الانترنت لا تكلف 250$. بالاضافة الانه يتوجب على جميع المستخدمين تنصيب Local Agent على اجهزتهم ليكونو قادرين على ولوج الشبكة.

الاصدارات القديمة من هذه التقنية لا توفر القدرة على تحديد اذا كانت هذه الاجهزة تمتثل للسياسات الامنية المطبقة من قبل الشركة مثلا (OS محدث, Antivirus محدث, USB Ports غير مفعلة....الخ) وكذلك عدم القدرة على معرفة اذا كان لدى هذا المستخدم اي Malware أو Active Malicious تنشط على منافذ بطاقة الشبكة للمستخدم سلكية كانت ام لاسلكية.

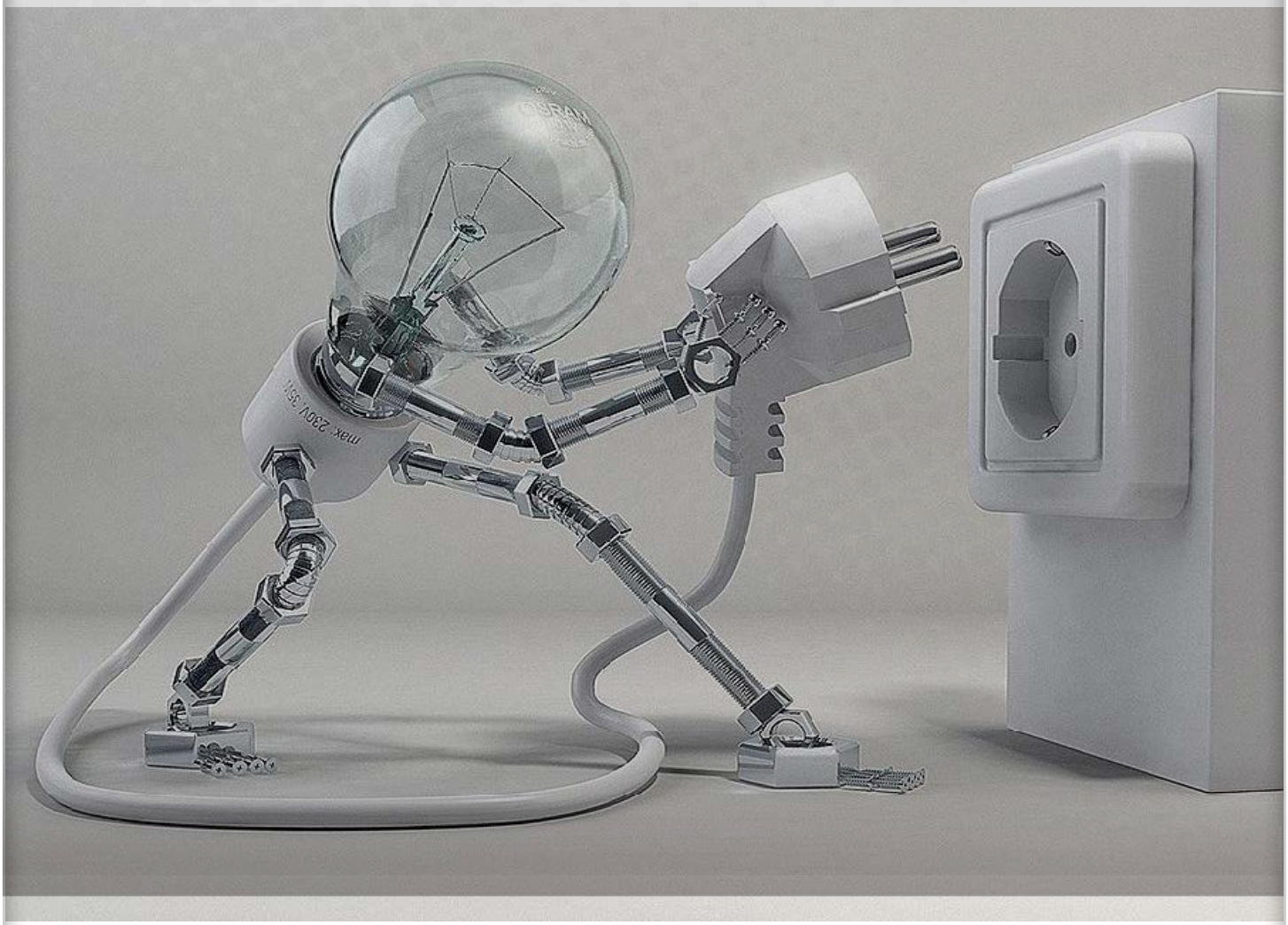
الجيل الحديث من NAC والذي سمي بالجيل الثالث يقدم حلول رائعة لتتماشى مع متطلبات الاعمال وتوفر سهولة بالتعامل مع جميع المستخدمين واجهزتهم أيا كانت منصة التشغيل لديهم. يعتمد الجيل الجديد على بروتوكول 802.1q او VLAN trucking أوVLAN Tagging ليعطي القدرة على التعامل مع المستخدمين المؤقتين أو Guests ومراقبة اي مستخدم جديد قد يتصل بالشبكة. وفي حال الاشتباه بأي مستخدم بأنه قد يضر بباقي المستخدمين عن او الكشف عن عملية Port scanning أو تزوير للـ MAC Address يقوم الـ NAC بفصله بـ VLAN منفصلة اوتوماتيكيا وعزله عن الشبكة مع إبقاء القدرة على الاتصال بالانترنت وتستطيع ارسال رسالة للمستخدم اوتوماتيكيا بأنه تم عزله للأسباب التالية. بالإضافة لإمكانية التحكم بالوقت المسموح لدخول الشبكة فمثلا يمكنك ان تخصص ساعة فقط للزوار لأن يستخدموا الانترنت او ان تمنع الموظفين من استخدام الشبكة قبل ساعة العمل المحددة أو أيام العطل مهما غيروا من اجهزة ثابتة كانت او محمولة أو حاولوا ان يحتالو على النظام عن طريق عناوين شبكة مزورة اوغيرها من طرق وأن تستثني بعض المستخدمين بنفس الوقت.

يتمتع الجيل الثالث بالقدرة على معرفة بصمة نظام التشغيل وتمييز المستخدمين عن طريق الـ User ID, OS finger print MAC Address, IP address. وقدرة كبيرة على اكتشاف الثغرات (CVE) Common vulnerability and Exposure وفصل Zero-day Malware أو مستخدم اي جهاز يحمل هذه الثغرات بـ VLAN منفصلة منعا لأي حوادث اختراق وبدون اي حاجة لتثبيت اي Agent أو Softwareعلى اجهزة المستخدمين لذلك فهو يعمل كـ Agentless NAC.

في حال اصبح الـNAC خارج الخدمة بسبب عطل ما لا يؤدي الى تعطل دخول المستخدمين بعكس الاصدارات القديمة منه التي تسبب الى منع جميع المستخدمين من استخدام الشبكة. ايضا يساعد الجيل الثالث في عملية احصاء الـ Assets ومعرفة من يعمل حاليا على الشبكة ومن هو خارج الاتصال.

الامتثال لمعايير أمن المعلومات امر هام وضروري بالنسبة للمؤسسات والشركات مثل معايير:,ISO27001:2005, HIPAA, PCI/DSS SOX,. 3rd Generation NAC System يساهم في دعم عملية الامتثال لهذه المعايير وإثبات الامتثال عبر التقارير للمدققين الامنيين والمدراء التنفيذيين عن طريق اجبار أجهزة المستخدمين ان يكونو ممتثلين لتوصيات المعيار وسياسات المؤسسة المتبعة وإذا لم يكونو كذلك فلن يتم السماح لهم بالوصول الى الشبكة او منعهم من الوصول لمصادر معينة. يستطيع الـNAC اصدار تقارير حول حالة الاجهزة والمستخدمين لفترة محددة مع اعطاء تفاصيل التجاوزات التي حصلت لكل مستخدم. وهنا تستطيع الشركة اتخاذ التدابير المناسبة لمراقبة ومنع اي تحركات مشبوهة من قبل المستخدمين موظفين كانو أم زوار.

وبذلك يكون الجيل الجديد من الـNAC قد حل جميع المشاكل التي قد تواجه اي مؤسسة بالتعامل مع المستخدمين بمختلف مستوياتهم وحقوق وصولهم لمصادر معلومات ومعطيات المؤسسة وبشكل فعال يتوافق ويتماشى مع توصيات المعايير الدولية لأمن المعلومات ويضمن بذلك تقليل من نسبة الخسائر الناجمة عن الوصول الغير الشرعي للشبكة التي قد تؤدي في بعض الحالات الى توقف العمل او حتى انهيار المؤسسة ككل بسبب عدم قدرة الادارات التنفيذية على التواصل الصحيح أو ربما توفير الدعم اللازم لادارة تقنية المعلومات المسؤولة عن سلامة وسرية وتوافرية المعلومات.



DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

واحد من أشهر البرتوكولات التي يتعرف عليها جميع الدراسين في بداية دراستهم في مجال تكنولوجيا المعلومات خاصة الشبكات، والكل يعتقد أنه فقط يمكن تطبيقه على الراوتر ولكن هل يصلح أن يكون السيرفر الموجود عليه نظام تشغيل مثل الويندوز أو اللينكس واليونكس أن يحل محل الراوتر فى مثل هذه الوظيفة؟

الإجابة هي بالطبع نعم.

DHCP هو عبارة عن خدمة كل وظيفتها توزيع NETWORK CONFIGURATION على الأجهزة الموجودة في الشبكة وكل ما تحتاجه لتقديم هذه الخدمة هو وجود RANGE من IP'S صالح للتوزيع على الأجهزة الموجودة في الشبكة سواء كانت الخدمة على راوتر أو على نظام تشغيل فهي تعمل بنفس الطريقة.

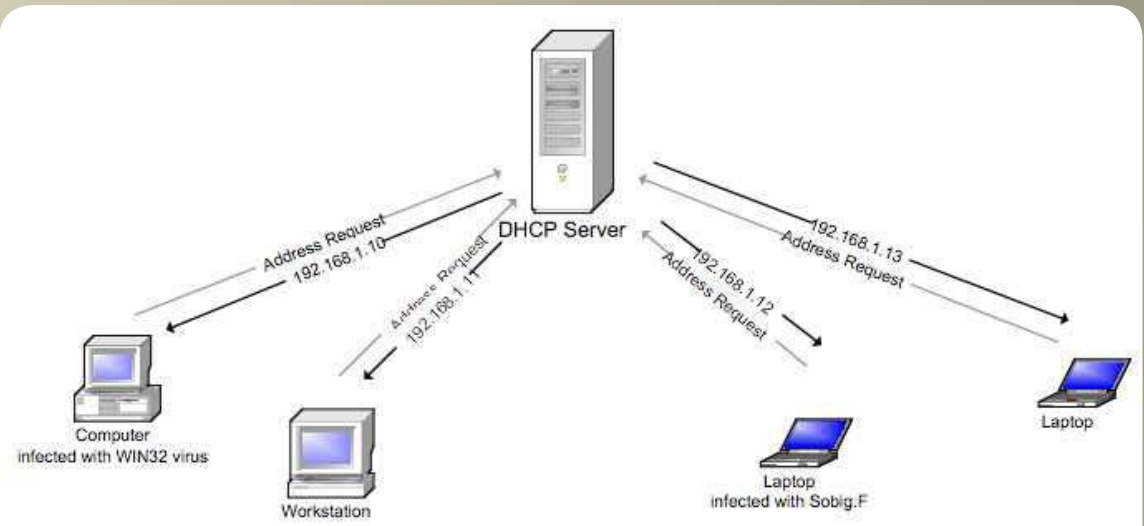


Figure 1: Standard DHCP provides IP addresses to all machines

إذن كيف تعمل هذه الخدمة على اللينكس ريدهات؟

1 - يجب عليك أولاً التأكد من وجود PACKAGE على السيرفر حتى تستطيع تقديم هذه الخدمة بالأمر التالي:

RPM -QA | GREP DHCP

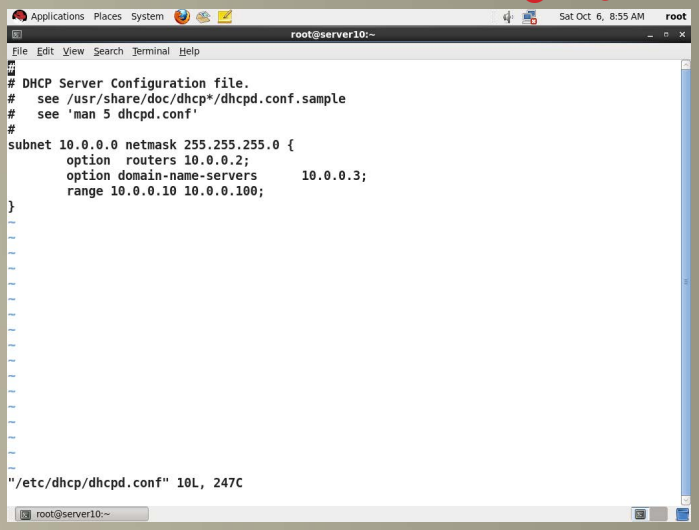
إذا لم تكن PACKAGE موجودة تستطيع تنصيبها عن طريق الأمر التالي:

YUM INSTALL DHCP

وهذه PACKAGE هي التي تجعل السيرفر يفهم كيفية عمل DHCP SERVER وبالتالي تستطيع من خلالها أن تقوم بتوزيع IP'S على الأجهزة الموجودة في الشبكة.

2 - عند تنصيب هذه PACKAGE ينزل معها الملف الآتي /ETC/DHCP/DHCPD.CONF وهو الملف الذي سيتم كتابة CONFIGURATION الخاصة DHCP به بجانب أنه أيضًا توجد DHCP SERVICE وهي المسؤولة عن توزيع CONFIGURATION على الأجهزة المختلفة، حيث أنها تفتح PORT NUMBER 67 والذي يستقبل عليه السيرفر REQUESTS الخاصة بـ DHCP من الأجهزة المختلفة.

مثال على CONFIGURATION :



والآن لنقوم بشرح هذا المثال:

1 - SUBNET 10.0.0.0 NETMASK 255.255.255.0

وهذا معناه أنه الشبكة التي ستقوم بتوزيع NETWORK CONFIGURATION هى 10.0.0.0 و SUBNET MASK الخاص بها هو 255.255.255.0

2 - OPTION ROUTER 10.0.0.2

وهذا معناه أنه GATEWAY IP الذى سيخرج عليه البيانات هو 10.0.0.2

3 - OPTION DOMAIN-NAME-SERVERS 10.0.0.3

وهذا معناه أنه DNS SERVER IP هو 10.0.0.3

4 - RANGE 10.0.0.10 10.0.0.100

هذا معناه أنه RANGE الذي سيقوم بتوزيعه على الأجهزه هو 10.0.0.10 إلى 10.0.0.100 والباقي RESERVED أي أنه STATICS IP'S لن يتم توزيعها ويجب أن يتم كتابتها يدويًا للأجهزة المختلفة في الشّبكة وعلى الأخص للسيرفرات الموجودة في الشبكة التي يجب أن تمتلك STATIC IP لا يتغير.

أيضًا يجب ملاحظة أن كل اختيار منهم يجب أن ينتهي; بهذه العلامه وإلا ستكون خطأ فى كتابة ENTRY الخاص بهذا OPTION .

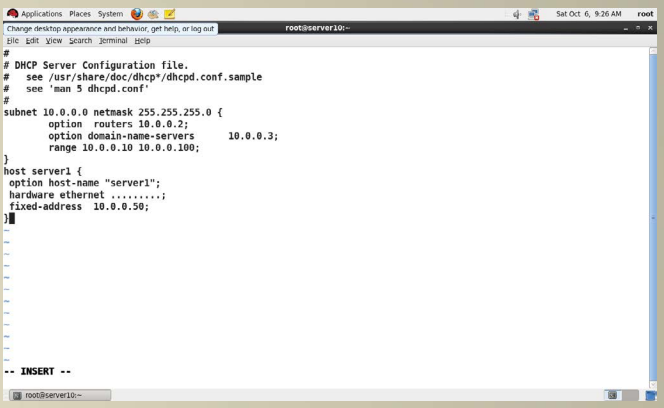
ملاحظة أخرى وهي أنه ليست هذه بالطبع كل OPTIONS المتاحة فهناك العديد من OPTIONS والتي لايوجد وقت لذكرها ولكن لكي تتطّلع عليها يمكن ذلك من خلال الأمر التالي : MAN DHCP-OPTIONS

لكى تجعل هذه CONFIGURATION تعمل يجب أن تقوم بذلك : SERVICE DHCPD START

وبذلك أصبح لديك الآن سيرفر يستطيع توزيع CONFIGURATION على الأجهزة الموجودة لديك في الشبكة.

حالة خاصة :

ماذا إذا أردت أن تقوم بربط جهاز معين على الشبكة بـ IP معين أي أنه كلّما يطلب هذا الجهاز IP من السيرفر فإنه يأخذ نفس IP كل مرة . لعمل ذلك تحتاج إلى اسم الجهاز و MAC ADDRESS لكارت الشبكة الموجودة به وأيضا عليك أن تكتب CONFIGURATION التالية:



هنا كل ماعليك فعله هو أن تعرف اسم الجهاز والماك الخاص بكارت الشبكة، وعندها عندما يصل REQUEST من هذا الجهاز إلى السيرفر سيكون به الماك الخاص بهذا الجهاز لذلك يأخذ نفس IP كل مرة كأنه STATIC IP.

فى النهاية يجب عليك ملاحظة أنه عند أي تغير في الملف /ETC/DHCP/DHCPD.CONF فإنه يجب عليك أن تعيد تشغيل DHCP SERVICE عن طريق الأمر التالي: SERVICE DHCPD RESTART.

وإلى اللّقاء في مقال قادم إن شاء اللّه.

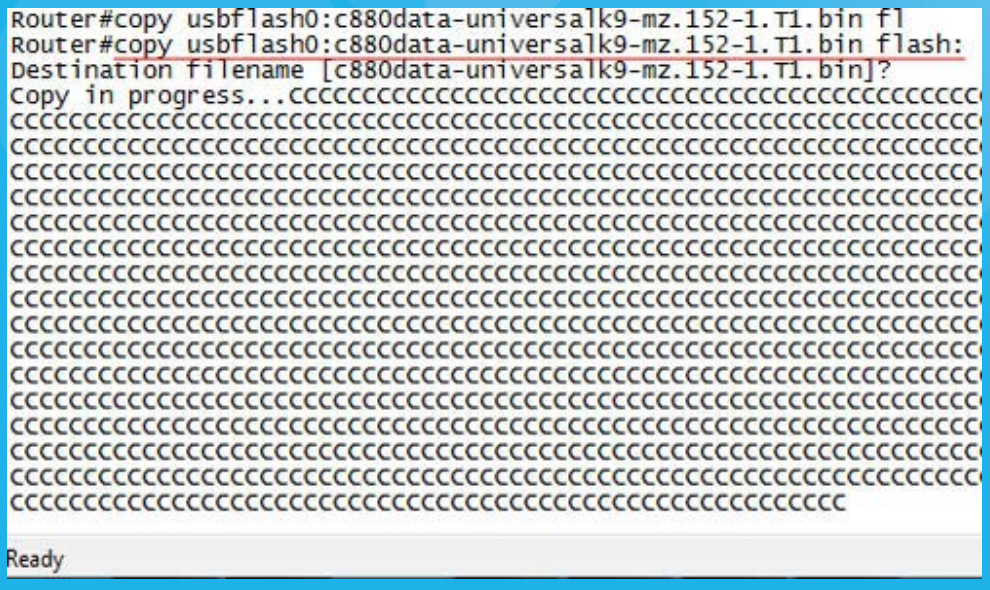
كيفية استخدام الـ USB في أجهزة سيسكو

مرت معي منذ فترة حادثة صغيرة حينما أكتشفت وجود عطل في نظام التشغيل الخاص بسيسكو وكان الحل الوحيد المتاح هو تحديث نظام التشغيل وقد أعتمدت على طريقة جديدة غير الطرق المذكورة من قبل وتحديدا عن طريق الـ USB .

بعد عملية مخاض طويلة مع أحد الروترات (C880) أكتشفت وجود مشكلة في نظام التشغيل وكان الحل الوحيد هو التحديث , وكانت حلول نقل النسخة إلى الروتر كثيرة ومن بينها التلنت والـ TFTP لكن مع وجود فتحة USB في الروتر أستغنيت عن تلك الحلول الطويلة , فقمت أولا بنسخ نظام التشغيل الجديد إلى الـUSB وبعدها قمت بكتابة الامر التالي وهو لنقل نظام الشغيل من الفلاشة إلى الروتر :

```
Router#copy usbflash0:c880data-universalk-9mz.1-152.T1.bin flash:
```

وبعدها نجد عملية النسخ إلى الروتر قد بدأت كما هو موضح في الصورة القادمة



خطوتنا القادمة هي أهم خطوة وهي جعل الروتر يقلع من النظام الجديد من خلال الأمر التالي :

```
Router#conf t
Router(config)#boot system flash c880data-universalk-9mz.1-152.T1.bin
```

```
33273984 bytes copied in 99.436 secs (334627 bytes/sec)

Router#sh
Router#show fl
Router#show fla
Router#show flash:
-#- --length-- -----date/time------ path
1      30552244 Mar 1 1984 00:01:00 +00:00 c880data-universalk9-mz.151-2.T1.bin
2          1001 Aug 25 2011 18:51:24 +00:00 CCPBackup2011-08-25_09_50_11
3         96395 Aug 27 2011 17:37:58 +00:00 vdsllog.bin
4      33273984 Oct 10 2011 22:04:26 +00:00 c880data-universalk9-mz.152-1.T.bin
5      33273984 Oct 16 2011 16:22:52 +00:00 c880data-universalk9-mz.152-1.T1.bin

31633408 bytes available (97210368 bytes used)

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#boot system flash
Router(config)#boot system flash c880data-universalk9-mz.152-1.T1.bin
Router(config)#

Ready
```

وآخيرا نقوم بعملية حفظ الأعدادت ونعيد أقلاع الروتر وأنتهى الأمر , وأكيد أن التدوينة لم تنتهي فأنا أود أن اشير إلى بعض النقاط بخصوص الـ USB .

- سيسكو بدأت دعم أدخال الـ USB مع الروترات من السلاسل التالية : 800 , 1800 , 2800 , 3800 (على مايبدوا أن سيسكو تتفائل بالرقم 800 مع الـ USB)
- الـ USB يجب أن يكون مبني على نظام FAT32 لأن نظام التشغيل لايدعم الـ NTFS
- الـ USB عادة تكون 2.0

- بعض الأوامر المفيدة مع الـ USB ,
- dir usbflash0
- show usb device
- show usb controllers
- show usb driver
- show usb port

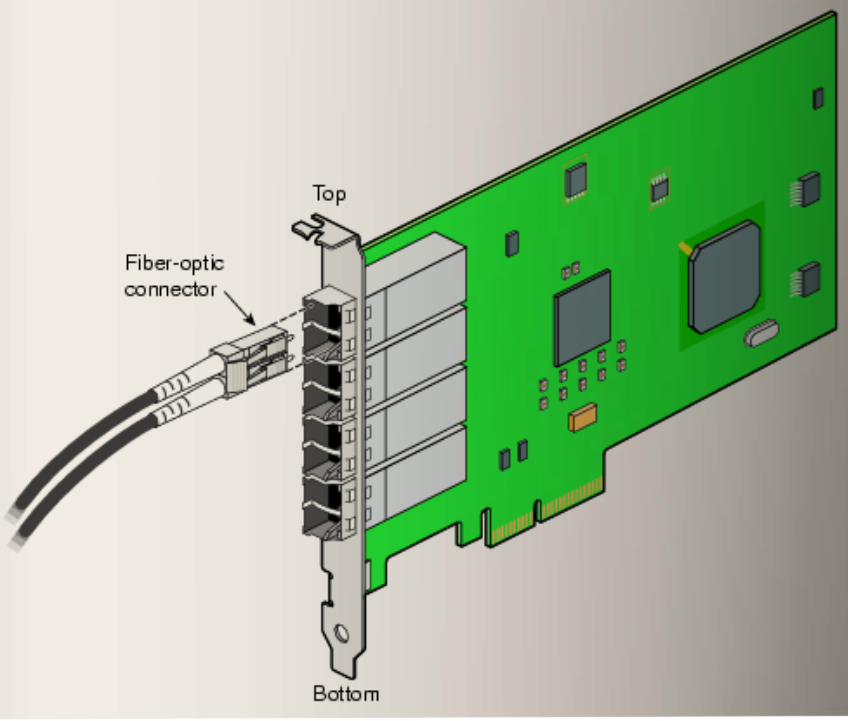
وتجربتي مع الـ USB كانت جيدة ووفرت الكثير من الوقت وخصوصا أن المساحة المتاحة لديك كبيرة ويمكنك تخزين كل ماتريده على الروتر من انظمة تشغيل أو أعدادت سابقة وبل يمكنك الأقلاع من خلالها وتحميل الأعدادت أيضا لكن يتوجب عليك التلاعب بأمر الـ Boot الذي وضحته في بداية المقال , أتمنى ان تكونوا قد أستفدتوا من معلومة جديدة ولو كانت بسيطة فهي في الآخر مفيدة إن شاء الله ودمتم بود .

في شبكات الكمبيوتر يعتبر Gigabit Ethernet GbE أو 1 GigEهو المصطلح المعبر عن تقنية إرسال الفريمات بسرعة الف ميجا بت لكل ثانية (1,000,000,000 bits per second), طبقا لمعيار IEEE 802.3 المعدل في سنة 2008 و تم بدء التفكير في هذا المعيار مبكرا في 1999 و أصبح شائع الإستخدام جدا مع حلول 2010 و استخدم هذا المعيار بالأساس لتمكين التراسل full-duplex و لكنه أيضا يدعم الطريقة الأسبق Half-duplex

بدأت تكنولوجيا الإيثرنت بواسطة شركة زيروكس الشهيرة Xerox و ذلك بسرعة 10 Mbit/s ثم تطورت الي سرعة 100 Mb/s بما يعرف بـ fastethernet , بعدها بدأت الحاجة الي وجودة سرعات أكبر و هنا بدأ التفكير في امكانية تطوير السرعة لتصل الي 1000 Mb/s أو ما يسمي بـ Gigethernet

خرج الي النور أول معيار يحدد مواصفاته من منظمة IEEE في يونيو 1998 بما يسمي بـ IEEE 802.3z أو تجاريا بما يسمي 1000BASE-X حيث X معامل يتغير طبقا لأنواع سنتعرف عليها مثل LX , SX , CX و التي تعبر عن أنواع موصلات الفايبر مثل Single Mode للمسافات الطويلة أكثر من كيلو متر و Multimode أقل من كيلو متر كذلك تم تخصيص هذا المعيار لموصلات الكابلات المحورية التي تنقل الموجات الميكروويف الشبكية عبر الجيجا ايثرنت

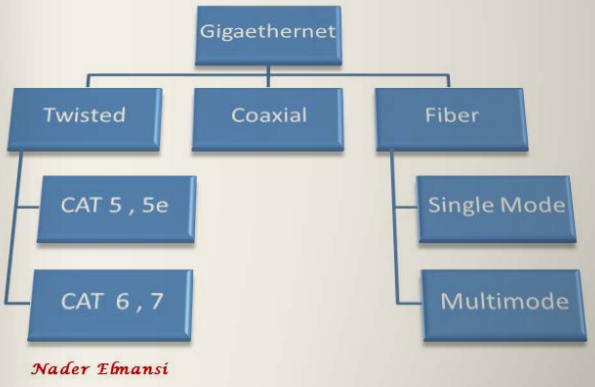
بعد ذلك بسنة و في عام 1999 تم تطويره IEEE 802.3ab و الذي مكن Gigabit Ethernet من نقل هذه السرعة عبر الكابلات المجدولة (unshielded twisted pair (UTP من نوع 6 , 5e , 5 CAT و تم تسمية هذا المعيار تجاريا بـ 1000BASE-T و هنا انتقل الإيثرنت من كونه تقنية ربط شبكات فقط backbone network الي تقنية ربط أجهزة أيضا desktop technology و يعتبر العام 2000 هو العام الفعلي لتشغيل 1000BASE-T desktop technology مع الأجهزة الشخصية حيث تمكنت شركة أبل من استخدام هذه التقنية لربط أجهزتها و ذلك مع الجيلين Apple's Power Mac G4 و PowerBook G4



في عام 2004 تم تطوير معيار جديد للجيجا ايثرنت هو IEEE 802.3ah حيث تم قابلية استخدام نوعين جديد من موصلات الفايبر و هما 1000BASE-LX10 و 1000BASE-BX10 و الذي يسمي أيضا Ethernet in the First Mile

مع حلول 2006 كانت السرعة 10Gb Ethernet جاهزة كبديل لـ 1Gb في شبكات backbone و سنتكلم عنها لاحقا في مقالة أخري

و هذا الشكل يبين اختصار لهذه الأنواع



و هذا جدول يبين تفصيل هذه الأنواع مع الكابلات المناسبة و أطوالها القصوي

Name	Medium	Specified distance
1000BASE-CX	Twinaxial cabling	25 meters
1000BASE-SX	Multi-mode fiber	220 to 550 meters dependent on fiber diameter and bandwidth
1000BASE-LX	Multi-mode fiber	550 meters
1000BASE-LX	Single-mode fiber	5 km
1000BASE-LX10	Single-mode fiber using 1,310 nm wavelength	10 km
1000BASE-EX	Single-mode fiber at 1,310 nm wavelength	~ 40 km
1000BASE-ZX	Single-mode fiber at 1,550 nm wavelength	~ 70 km
1000BASE-BX10	Single-mode fiber, over single-strand fiber: 1,490 nm downstream 1,310 nm upstream	10 km
1000BASE-T	Twisted-pair cabling (Cat-5, Cat-5e, Cat-6, or Cat-7)	100 meters
1000BASE-TX	Twisted-pair cabling (Cat-6, Cat-7)	100 meters

متطلبات استخدام الجيجا ايثرنت

لعمل أي منظومة شبكية أو هندسية لابد أن يكون لديك ثلاثة مكونات أولها المكون المادي ثانيها هو الطاقة ثالثها هو المكون المعرفي

المكون المادي هو المكونات المطلوبة لعمل شبكة جيجا ايثرنت و أما المكون المعرفي فهي المعلومات اللازمة لعمل هذه الشبكة و أما الطاقة فهي رغبة الشخص للعمل

المكون المادي لشبكات الجيجا ايثرنت :

بالنسبة للمكون المادي فلإستخدام هذه التقنية نحتاج أربعة أشياء أساسية لا غني عنهم أولهم جهاز شبكي يدعم الجيجا ايثرنت و ثانيهم كابل Cable و غالبا ما يكون الفايبر و ثالثهم هو الموصل Connector و هو رأس الكابل أما الرابع فهو محول Transceiver أو ما يسمي بـ GBIC أو (SFP (Mini-GBICs و هو الذي يوضع في السويتش لتركيب رأس الكابل به

هناك أشياء ثانوية أحيانا أتغاضي عن استخدامهم مثل Patch Panel Fiber و هو بحجم السويتش يستخدم لترتيب أسلاك الفايبر و يوضع به Transceiver و الثاني هو Patch cord fiber و هو كابل قصير يربط بين Patch Panel والسويتش الفايبر

و سيكون كلامنا علي المنظومة المستخدم فيها كابلات الفايبر رغم أن الجيجا ايثرنت أيضا يصلح للكابلات المجدولة و المحورية

أولا السويتشات التي تدعم الجيجا ايثرنت

سنستخدم سويتشات سيسكو و هذه بعض السويتشات التي تدعم هذه التقنية

Catalyst 6500/6000 Series Switch
Catalyst 5500/5000 Series Switch
Catalyst 4500/4000 Series Switch
Catalyst 3550 Series Switch
Catalyst 3750 Series Switch
Catalyst 3750 Metro Series Switch
Catalyst 2900 XL/Catalyst 3500 XL Series Switch
Catalyst 2940 Series Switch
Catalyst 2950 Series Switch
Catalyst 2955 Series Switch
Catalyst 2970 Series Switch
Catalyst 2948G L34908/G L34840/G Switch
Catalyst 8500 Series Switch Router

و يختلف كل سويش عن تلآخر في عدد البورتات التي يدعمها للجيجا ايثرنت

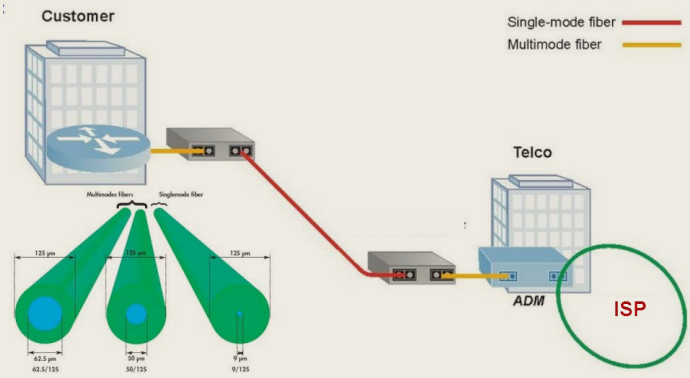
ثانيا كابل الفايبر

لدينا نوعان من الألياف البصرية هما single mode و multimode

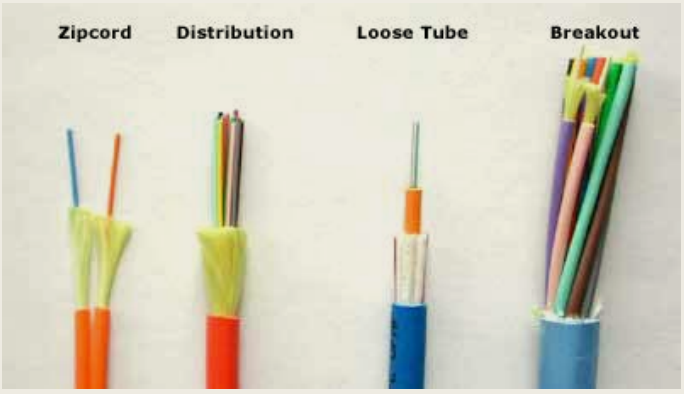
فأما Single-Mode Fiber و يسمي احيانا monomode شائع الإستخدام في المسافات الطويلة و التي تستخدم ككابلات اساسية backbone cable للربط بين الشبكات في حدود أكبر من 1 كيلومتر

و أما Multimode فيستخدم للربط بين السويتشات في الشبكة الواحدة للمسافات القصيرة في حدود أقل من 1 كيلومتر –غالبا-

و الشكل التالي يبين بعض الفروقات بين النوعين



و يأتي الكابل الواحد به أكثر من فايبر كل اثنين يمثلان خط واحد مرسل و مستقبل لنفس الجهة و تتنوع الكابلات حسب العدد و أقلها يأتي بخط واحد «اتنين فايبر» و هو patch cord و الشكل التالي يبين الفرق بين هذه الأنواع



و يعتبر العائق الأساسي في مد كابلات الفايبر هو ارتفاع ثمنها و قلة الأيدي العاملة الفنية التي تتعامل معها فالشبكية التي سيتم استبدالها او تركيبها لتتوائم مع الكابلات سيتم تبديل سويتشاتها و مكونات كبائنها و هذا يعني ان تكلفة تركيب الألياف البصرية تزيد بمقدار 50 ٪ عن الألياف العادية

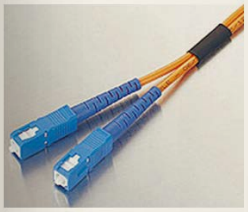
بعض هذه السويتشات تكون بورتات الفايبر فيها مدمجة و أخري موضوعه علي هيئة موديول مستقل تستطيع تغييره اذا لزم الأمر كما بالشكل الذي يخص سويتشات 3750X المشهورة في عالم الشبكات اللاسلكية لسيسكو

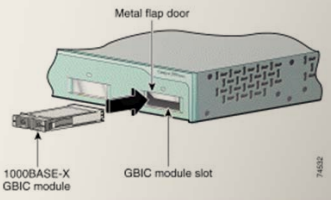
ثالثا الموائمات Transceiver

تسمي GBIC - Gigabit interface converter حيث يأتي السويتش الذي يدعم الجيجا ايثرنت غالبا ببورتات فارغة و لذلك نحتاج الي موائمات GBIC و هذه الموائمات تقوم بشيئين أولهما هو موائمة السويتش ليتم تركيب الموصل المناسب به و ثانيهما لتحويل الإشارة الكهربية في السويتش الي اشارة ضوئية لنقلها داخل كابل الفايبر – في حال استخدام كابل فايبر -

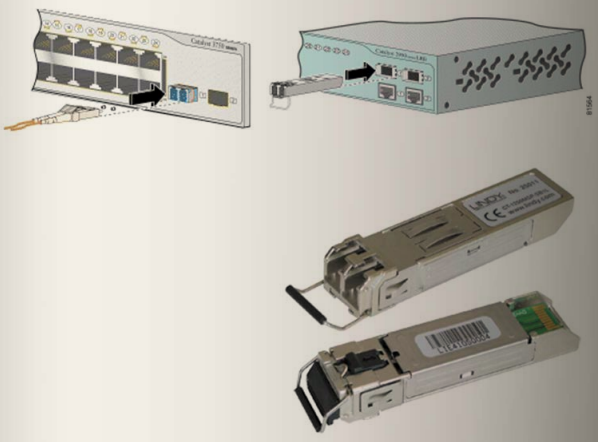
و نستخدم في سويتشات سيسكو الحالية نوعين هما GBIC و Mini-GBICs

فأما GBIC فهو أقدم النوعين و هو محولات لموصلات فايبر من نوع SC مثل هذه

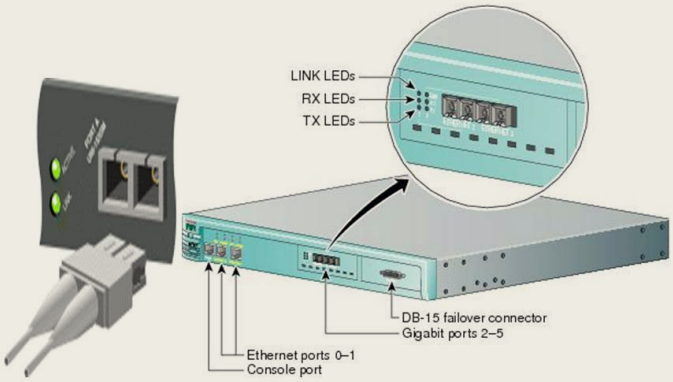




النوع الآخر من المحولات و هو الأحدث و هو Mini-GBICs المسماة (SFP (Small Form Factor لموصلات فايبر من نوع LC مثل هذه

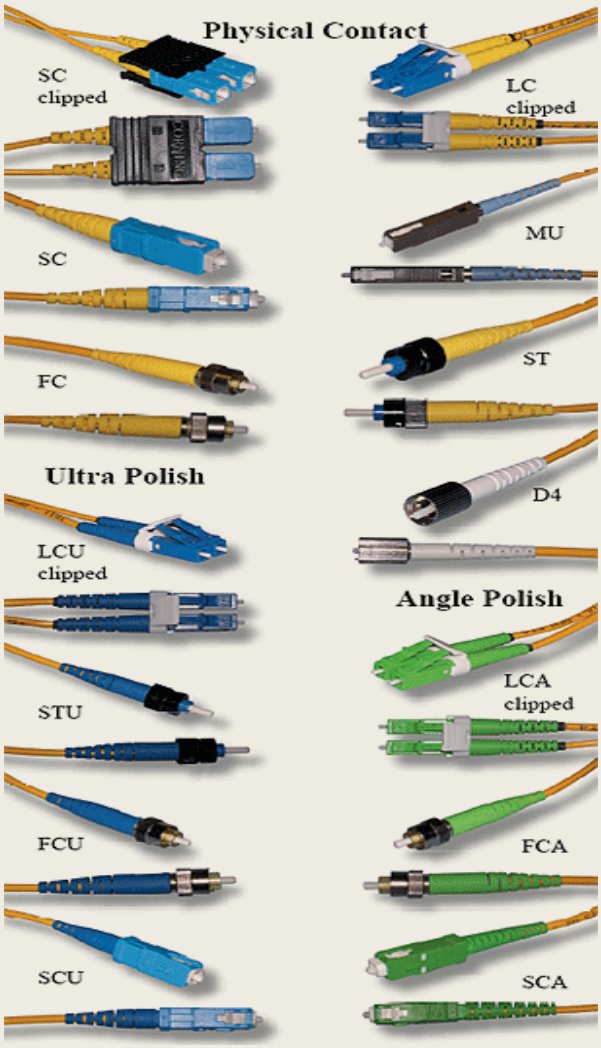


في السويتشات القديمة من سيسكو مثل 2900 و 2970 لا يعوزك لإستخدام المحول GBIC و يتم قبس الكابل الفايبر في السويتش مباشرة كما تري



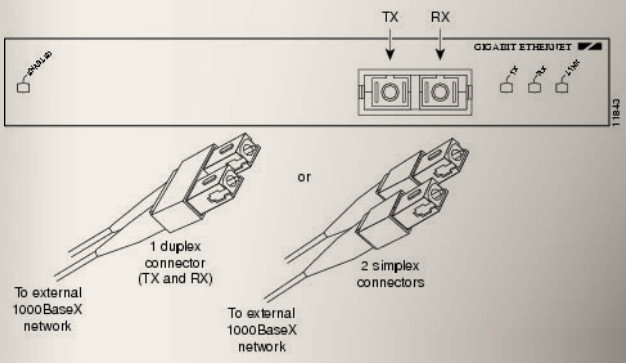
رابعا الموصلات Connectors

و هي نهايات الكابلات التي توضع في GBIC و تتلائم مع نوع و شكل GBIC و لدينا أنواع عديدة يمثلهم الشكل التالي



و أغلب ما نستخدمه هما النوعين LC و SC فأما LC فهو الأحدث و المستخدم مع Mini GBIC و SFP و النوع الأقدم هو SC المستخدم مع GBIC و أحيانا نحتاج في بعض الأحيان الي كابلات إحدي طرفيها من النوع LC و الطرف الآخر SC و ذلك عند توصيل سويتشين مختلفين في GBIC مثل هذه

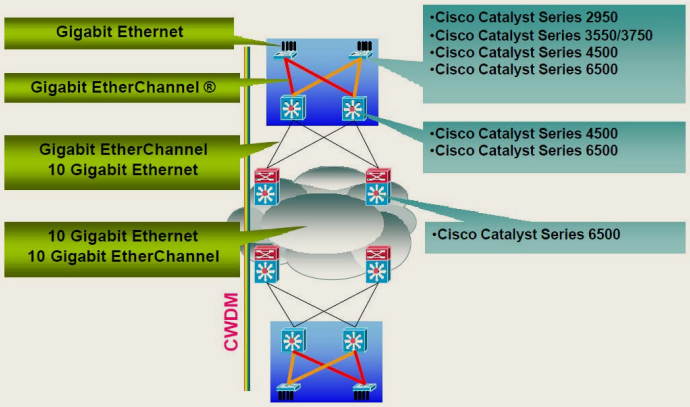
و قد تكون الموصلات بشكل مفرد أو بشكل مزدوج هكذا



ثانيا المكون المعرفي أو تصميم الشبكة

تأتي سويتشات الفايبر من سيسكو بأكثر من بورت جيجا ايثرنت تصل الي أربع بورتات كل منها يستخدم غالبا لربط Uplink بين السويتشات و الا فتستطيع أيضا أن تربطها بأجهزة حاسوب ان توفر لها كروت شبكية بها بورتات فايبر

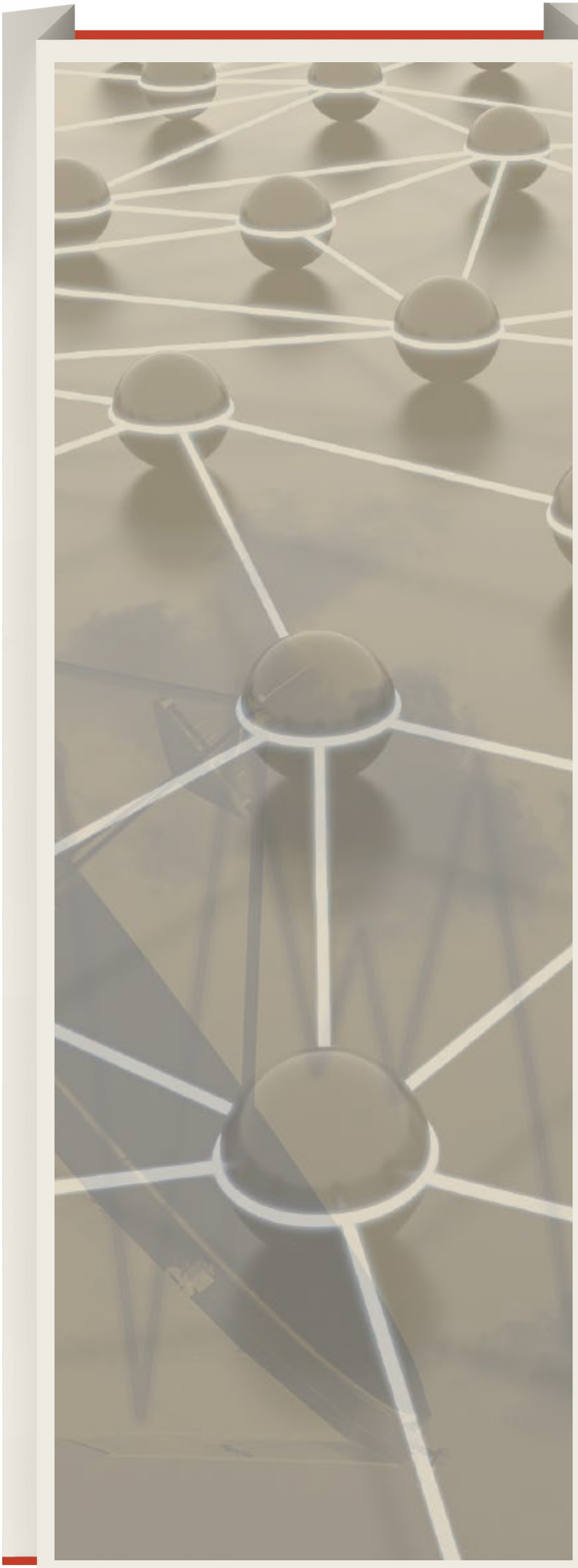
في الشبكة التالية ثلاث طبقات من الشبكة بدءا من ISP و هم Core و توجد في قمة السلم الهرمي لشبكتك و أحيانا تكون في ISP الذي تنتمي له ثم Distribution و توجد في قمة السلم الهرمي لشبكتك الخاصة ثم Acsess و هي تحتوي علي السويتشات التي ترتبط بها بشكل مباشر



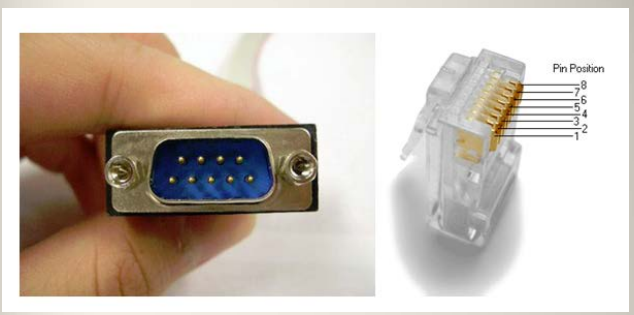
و لعمل ربط فايبر طبقا لأنواع السويتشات التالية فأنت ستستخدم موديولات GBIC تناسب كل سويتش و نهايات فايبر تناسب كل موديول كما هو موضح في الجدول التالي

Cisco Catalyst Series	1 GE Uplinks	10/100/1000 Ports	10 GE Ports	1GE fiber (GBIC & SFP)
2950	2 ✓	2/module ✓	✗	2/module (GBIC) ✓
3550	2 ✓	10/module ✓ 50/stack	✗	10/module (GBIC) ✓ 50/stack
3750	4 ✓	24/module ✓ 216/stack	✗	4 SFP uplinks ✓
4500	2/sup ✓	48/blade ✓ 240/chasis	✗	48/blade (SFP) 18/blade (GBIC) ✓ 240/chasis
6500	2/sup ✓	48/blade ✓ 384/chasis	4/blade (Xenpak) ✓ 32/chasis	48/blade (SFP) 16/blade (GBIC) ✓ 384/chasis

بقي أن نتكلم قليلا عن المقياس 1000BASE-CX و هو يختص بنقل البيانات بهذه السرعة عبر الكابلات المحورية twinaxial cabling لمسافة 25 متر فيستخدم موصلات من نوع DE-9 و التي تشبه المستخدمة في Console و موصلات 8P8C connector و التي تشبه موصلات RJ و هذه هي GBIC المستخدمة



و هذه هي Connectors المستخدمة



و تستخدم هذه الأنواع في IBM BladeCenter
حيث تتوفر هذا الأنواع من الموصلات

ثالثا مكون «الطاقة» في شبكات الجيجا ايثرنت

هي بشكل مختصر رغبتك لعمل هذه الشبكة و التي تشبه رغبتي لكتابة هذا المقال و هو مكون مهم جدا في بناء أي منظومة هندسية أضاف لها بعدا بشريا فقد يكون لديك أجهزيتك و لديك المعرفة و لكن يعوزك الحماس و الرغبة و التحفيز بل ربما القدرة المادية و المالية لعمل ذلك

و استخدمت ثلاثية مكونات المنظومات الهندسية بشكل عام لدرء نظرية داروين الخاصة بنشئة الخلق حيث افتقرت النظرية للمكون المعرفي و بعض مكون الطاقة فليس معني أن لدي كل مكونات خلق الكون أن يخلق الكون من نفسه صدفة

MICROSOFT EXCHANGE 2013

مايكروسوفت كعادتها تفاجئنا بسرعة التطورات الجديدة في عالمها من إبداعات وتقنيات رائعة.
وحديثنا اليوم عن البرنامج أو الخدمة التي أصبحت حجر أساسي في بناء الشّبكات في الشّركات المتوسّطة والكبيرة وهو MICROSOFT EXCHANGE SERVER الغني عن التعريف ولكن بإصداره الجديد 2013.
البريد الإلكتروني وهو الشيء الذي أصبح من أساسيّات الموظفين وليس من الكماليات لأن اعتمادنا على التوثيق والمتابعات في إرسال الرسائل أصبحت من بعض أسسْ نجاحات الشركة أو المؤسسة .
يؤمن لنا EXCHANGE SERVER إنشاء حسابات للمستخدمين باسم النطاق الذي نريد من أجل أن يتم تبادل البريد الإلكتروني بينهم بشكل موثوق وآمن وأخذ النسخ الاحتياطية للحسابات بشكل يومي دون الحاجة لإنشاء حسابات على مخدمات مثل الهوتميل أو الياهو التي تحتاج إلى إنترنت وتكون نسبة الأمان ضئيلة لأصحاب المعلومات المهمة الموجودة خارجاً .
بعد ظهور MICROSOFT EXCHANGE 2010 في عام 2009 وتحقيقه نجاح رائع أكثر من إصدار 2007.
الآن مايكروسوفت تصدر EXCHANGE SERVER 2013 مع مواكبتها لظهور:

WINDOWS 8 – WINDOWS SERVER 2012 – MICROSOFT SHAREPOINT 2013 – MICROSOFT OFFICE 2013

وسنتطرق اليوم عن عملية التثبيت وأهم المزايا والفروقات عن غيرها من الإصدارات :

أولاً : مرحلة التّحضير:

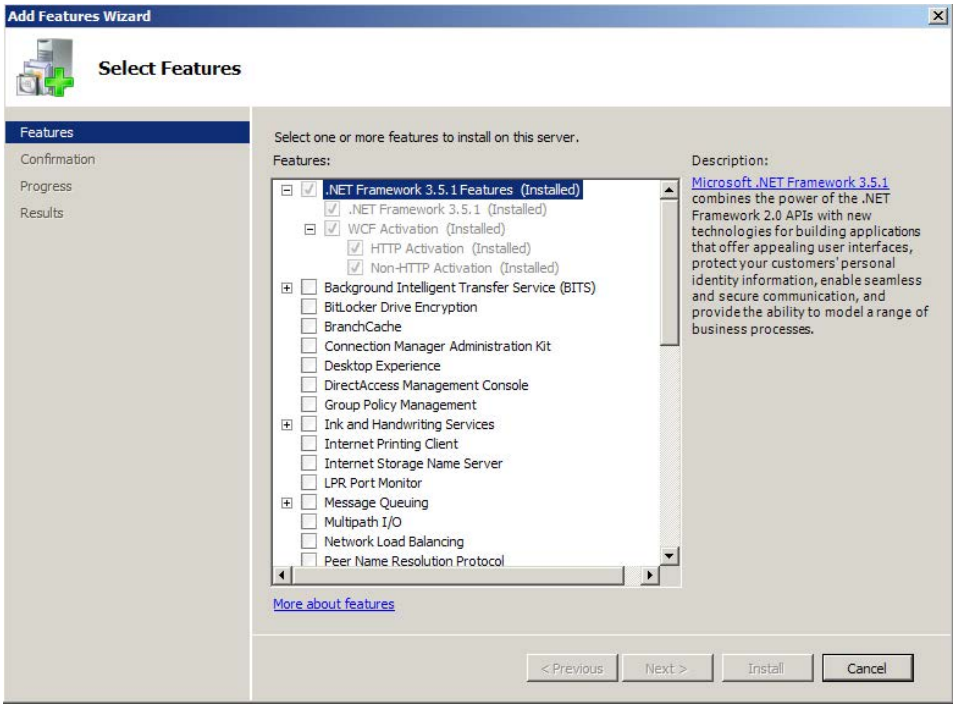
يمكننا تثبيت البرنامج على WINDOWS SERVER 2008 R2 , أوWINDOWS SERVER 2012 وهو سيكون الأسهل بسبب التوافقية الأكثر له.

مثال :

على اعتبار أنني أملك الجهاز WIN 2008 R2 و عضو في الـ DOMAIN و لتهيئة النظام قبل عملية الإعداد نتبع الخطوات التّالية:

1 - تثبيت المزايا (FEATURES):

INSTALL-WINDOWSFEATURE AS-HTTP-ACTIVATION, DESKTOP-EXPERIENCE, NET-FRAMEWORK-45-FEATURES, RPC-OVER-HTTP-PROXY, RSAT-CLUSTERING, WEB-MGMT-CONSOLE, WAS-PROCESS-MODEL, WEB-ASP-NET45, WEB-BASIC-AUTH, WEB-CLIENT-AUTH, WEB-DIGEST-AUTH, WEB-DIR-BROWSING, WEB-DYN-COMPRESSION, WEB-HTTP-ERRORS, WEB-HTTP-LOGGING, WEB-HTTP-REDIRECT, WEB-HTTP-TRACING, WEB-ISAPI-EXT, WEB-ISAPI-FILTER, WEB-LGCY-MGMT-CONSOLE, WEB-METABASE, WEB-MGMT-CONSOLE, WEB-MGMT-SERVICE, WEB-NET-EXT45, WEB-REQUEST-MONITOR, WEB-SERVER, WEB-STAT-COMPRESSION, WEB-STATIC-CONTENT, WEB-WINDOWS-AUTH, WEB-WMI, WINDOWS-IDENTITY-FOUNDATION

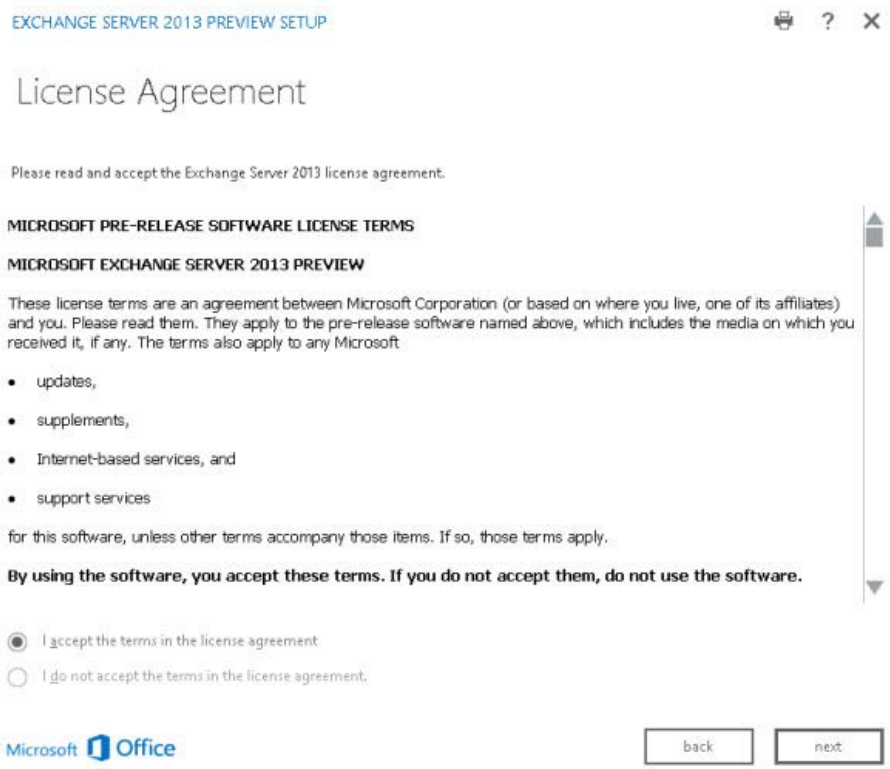


2 - إزالة VISUALC++ 11 BETA REDISTRIBUTABLE من FEATURES.

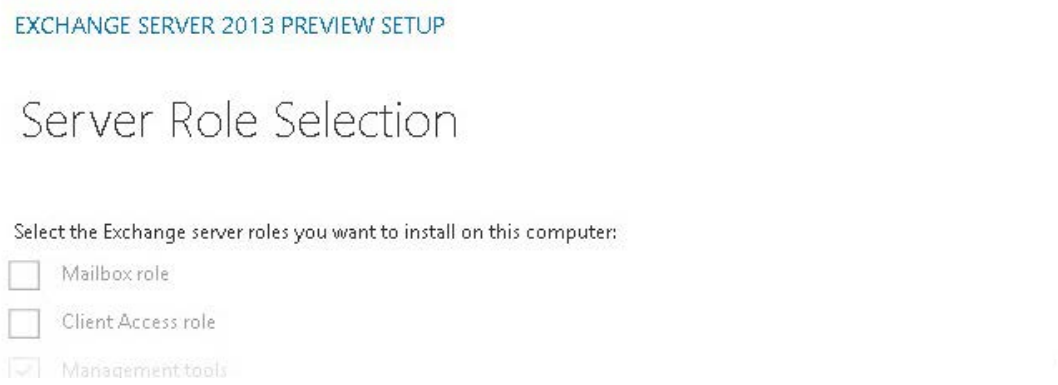
ثانياً : مرحلة الإعداد:

التغيرات التي حدثت في عملية الإعداد هي واجهات مايكروسوفت الحديثة لعمليّات التنصيب التي تدعى بـ METRO INTERFACE وهي الواجهة التي أصبحت متواجدة في جميع منتجات مايكروسوفت الحديثة منها:

MICROSOFT OFFICE **2013** , WINDOWS **8** , WINDOWS SERVER **2012**



وعلى عكس الاصدارات السابقة يحتوي هذا الأصار على ROLE 2 فقط وهما :



- MAILBOX ROLE

يتألف من قسمين أساسيين:

1 - HUB TRANSPORT SERVICE : تقوم هذه الـ ROLE بتوجيه الرسائل بين المستخدمين و من و إلى الإنترنت

أي يستطيع أن يرسل الرسائل إلى الإنترنت مع الـ SEND & RECEIVE CONNECTOR.

2 - MAILBOX TRANSPORT SERVICE : المسؤولة عن توصيل الإيميلات من HUB TRANSPORT الى MAILBOX DATABASE.

يحمل هذا الـ ROLE وظيفة تخزين الـ MAILBOXES أو صناديق بريد المستخدمين فى قواعد بيانات MAILBOX DATABASES .

- CLIENT ACCESS ROLE

سوف يتكون من جزئين فقط وهما:

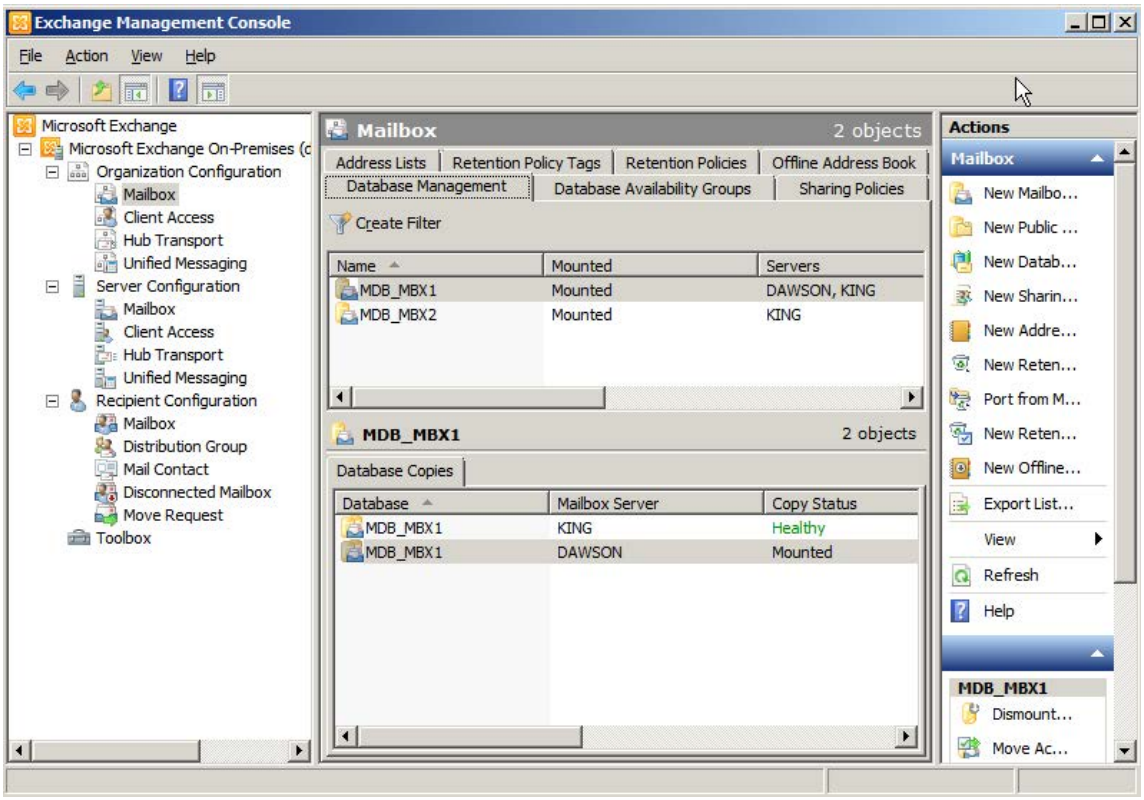
1 - CLIENT ACCESS SERVICE: يستقبل جميع الاتصالات القادمة من قبل الـ CLIENTS و يدعم

POP3,IMAP,RPC OVER HTTPS, MAPI و يجب أن يكون أيضا عضو فى الـ DOMAIN .

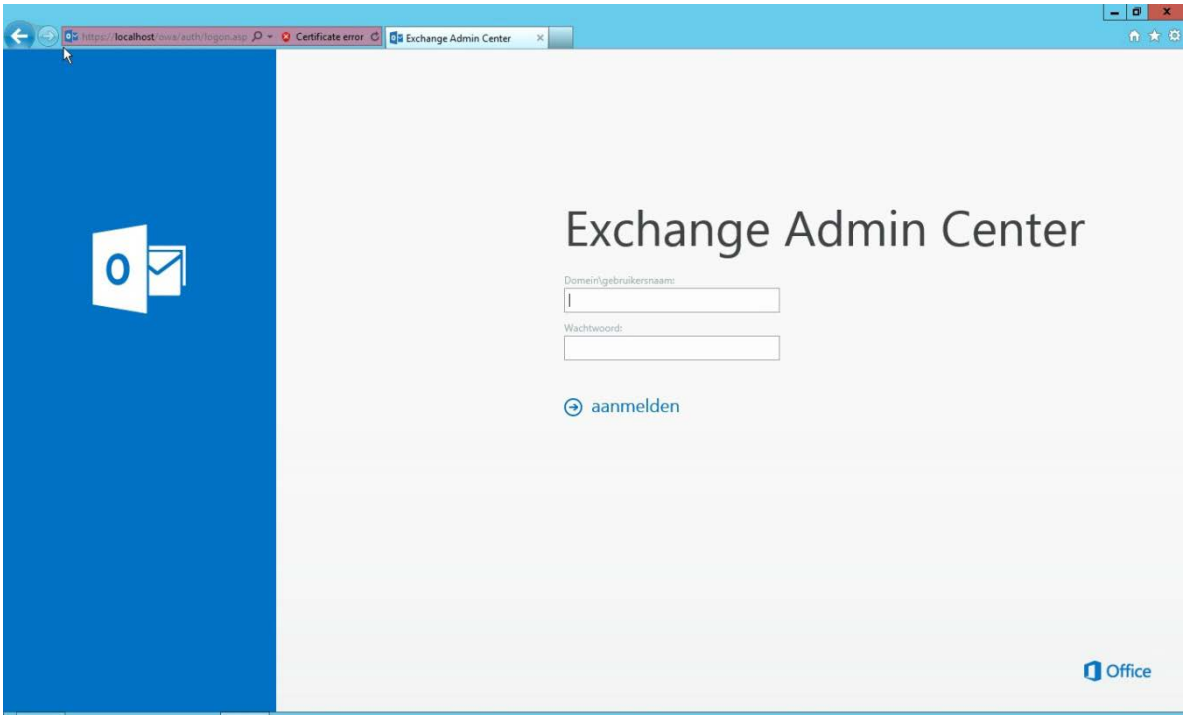
2- FRONT END TRANSPORT SERVICE وهي المسؤولة عن عملية فلترة الرسائل والتعرف على SPAM داخل وخارج المؤسسة.

ثالثاً : الواجهات:

EMC) EXCHANGE MANAGEMENT CONSOLE) وهي الواجهة المعروفة لاستخدام EXCHANGE SERVER في الاصدارات 2007 و 2010 والتي كنا نعاني أحيانا من مرونة هذه الواجهة .

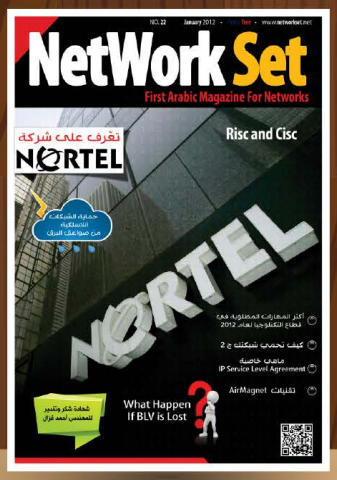


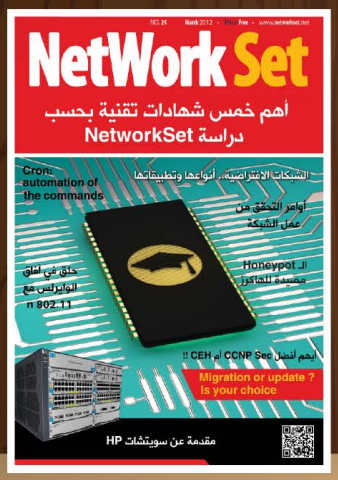
ولكن في الاصدار الجديد تم استبدالها بـ EAC(EXCHANGE ADMINISTRATION CENTER) وهي صفحة يتم الدخول بها عن طريق الويب مثل SHAREPOINT و LYNC أي من كل مكان إن كان في داخل الشركة أو في خارجها لسهولة ضبط الاعدادات دون الحاجة للدخول إلى السرفر أو تنزيل كونسل مخصصاً لدينا وتم إلغاء EMC .

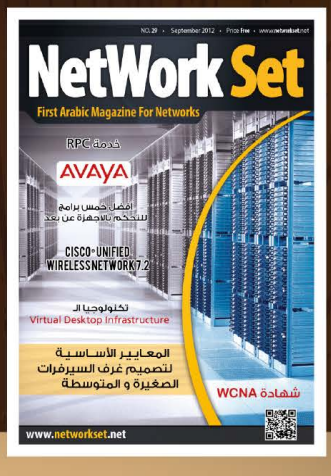


وبهذا القدر أكون قد وافيتكم بأهم المزايا والتطّورات إلى حد الآن الموجودة في الإصدار الجديد EXCHANGE 2013

Network Set Magazine Gallery







بروتوكولات اكتشاف الأجهزة
مقارنة بين بروتكول LLD-MED و CDP

بروتوكولات اكتشاف الأجهزة (DEVICE DISCOVERY PROTOCOLS) تمكّن الأجهزة المتّصلة مباشرة من اكتشاف معلومات حول بعضها البعض. فهي ترسل معلومات حول الجهاز على كل واجهة، وتسمح لأي جهاز في الشبكة بمعرفة كل شيء عن الجهاز المتصل به.

أمثلة على التطبيقات التي تستخدم هذه المعلومات التي تم نقلها عن طريق هذه البروتوكولات تشمل:

- رسم الشبكة : يمكن لـ NETWORK MANAGEMENT SYSTEM (NMS) أن يمثّل بدقة خريطة لـNETWORK TOPOLOGY .
- يمكن لـMANAGEMENT SYSTEM من إرسال QUERY لمعرفة المزيد عن جميع الأجهزة المتصلة بـSWITCH ما.
- في حالات الطوارئ يمكن تحديد موقع هاتف ما من خلال منفذ الـSWITCH الذي يتصل به.
- إعداد الـ VLAN : يمكن لـSWITCH من إعلام الهاتف بالـ VLAN المستخدم للصوت.
- التفاوض حولPOWER : إذ يمكن للهاتف وSWITCH التفاوض حول كمية POWER التي يمكن أن تستهلك من قبل الهاتف.

قدمت CISCO SYSTEMS بروتوكول®CISCO (DISCOVERY PROTOCOL (CDP سنة 1994 لتوفير آلية لـ MANAGEMENT SYSTEM من المعرفة التلقائية للأجهزة المتصلة بالشبكة.

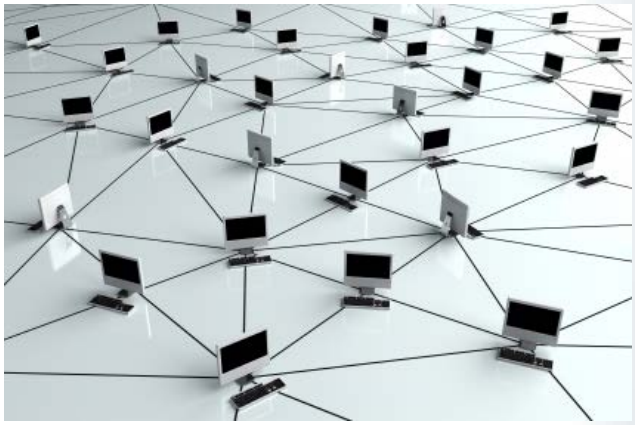
بروتوكولCDP يعمل على أجهزة سيسكو (ROUTERS وSWITCHS والهواتف، الخ) وقامت سيسكو أيضا بالترخيص لبعض الشركات الأخرى بتشغيله على أجهزتها ، باستخدام CDP تقوم أجهزة الشبكة بإرسال المعلومات الخاصة بها إلى عنوانMULTICAST وذلك بشكل دوري ، مما يجعلها متاحة لأي جهاز أو تطبيق يريد استعمالها أو استلامها.

لأن الاكتشاف التلقائي للأجهزة مفيد جدًا لإدارة الشبكة، قامت العديد من الشركات في وقت لاحق من إصدار بروتوكولات اكتشاف الأجهزة الخاصة بها. يقوم الجدول أسفله بسرد بعض بروتوكولات اكتشاف الشبكة الخاصة :

الإسم	الاختصار	الشركة
CISCO DISCOVERY PROTOCOL	CDP	CISCO SYSTEMS
ABLETRON DISCOVERY PROTOCOL	CDP	ENTERASYS
EXTREME DISCOVERY PROTOCOL	EDP	EXTREME
FOUNDRY DISCOVERY PROTOCOL	FDP	FOUNDRY
NORTEL DISCOVERY PROTOCOL	NDP	NORTEL

مع مرور الوقت، تم إجراء تحسينات على هذه البروتوكولات وذلك لتوفير قدرات أكثر . أصبحت التطبيقات (مثل الصوت) تعتمد على هذه القدرات للعمل بشكل صحيح، هذا الشيء أدّى إلى وجود مشاكل في التوافق بين البائعين.

لذلك، لإتاحة العمل المشترك بين معدات مصنوعة من طرف شركات مختلفة، فقد أصبح من الضروري أن يكون هناك بروتوكول اكتشاف موحد. قامت سيسكو بالعمل مع الشركات الرائدة في المجال و IEEE بتطوير بروتوكول جديد تحت إسم LINK LAYER DISCOVERY PROTOCOL (LLDP) ، 802.1AB ، الذي حدّد قدرات الاكتشاف الأساسية. تم تعزيز هذا البروتوكول تحديدًا لمعالجة تطبيق الصوت ، وهذا ما يسمى بـ LLDP) LLD-MED FOR MEDIA ENDPOINT DEVICES) ، تجدر الإشارة إلى أنLLDP أوLLDP-MED ، ولكن ليس كلاهما ، يمكن استخدامه في أي وقت من الأوقات على واجهة بين جهازين.



هذا المقال يقارن بينCDP وLLDP-MED تحديدًا من حيث صلتهما بالهواتف وSWITCHS.

1. HISTORY :

1.1. CISCO DISCOVERY PROTOCOL :

اخترع في سيسكو من قبل KEITH MCCLOGHRIE و DINO FARINACCI ، و قدم على منتجات سيسكو في عام 1994. هذا البروتوكول يعمل الآن على عشرات الملايين من أجهزة سيسكو في جميع أنحاء العالم. في البداية قام بدعم مجموعة محدودة من الميزات التي كانت تستخدم أساسًا لاكتشاف الأجهزة. وتستند هذه الميزات على TYPE وLENGTH وVALUE ، ويشار إليها بـ TLVS .

ودعمت TLVS في البداية ما يلي :

- ID الجهاز .
- عنوان IP.
- القدرات (مثلSWITCH ، ROUTER ، وBRIDGE ، الخ.)
- إصدار برنامج.
- PLATFORM (على سبيل المثال، SWITCH 6500)
- الواجهة. (INTERFACE)
- PORT ID.

في عام 1996 أضافت شركة سيسكو لـ CDP ميزة أخرى ليشمل دعم ON-DEMAND ROUTING (ODR)) ، الذي بسّط الإعدادات بالنسبة لـ STUB ROUTERS . هذه الميزة هي:

- NETWORK PREFIX

في عام 1997 نقلت شركة سيسكو بروتوكول من الإصدار 1 إلى الإصدار 2 وشمل هذا الإصدار الجديد TLVS التالية:

- PROTOCOL HELLO : تم السماح لبروتوكولات أخرى بنقل حزم الـHELLO الخاصة بهم على متن بروتوكولCDP .
- VLAN TRUNKING PROTOCOL (VTP) إسم الـ : MANAGEMENT DOMAIN MANAGEMENT DOMAIN .
- NATIVE VLAN : يشير إلى رقم NATIVE VLAN
- FULL أو HALF DUPLEX : يشير إلى إذا ما كانت الواجهة تعمل HALF أوFULL DUPLEX .

في عام 1999 أضافت سيسكو ميزات لدعم الصوت عبر بروتوكولVOIP (IP) . وشمل هذا التغييرTLVS التالية:

- APPLIANCE VLAN : يشير إلىVOICE VLAN
- TRIGGER : يوفر القدرة على إلزام الجهاز الموجود في الجهة المقابلة على إرسال حزمةCDP فورًا.
- POWER : يضيف القدرة على التفاوض حول POWER المطلوبة .
- EXTENDED TRUST وCLASS OF (SERVICE (COS : يوفر القدرة على تحديد ما إذا كان منفذ PC الموصول بالهاتفTRUST

أو لا ، وبماذا يعلمCOS BITS الموجود في حزم L2 القادمة من PC.

في عام 2000 أضاف سيسكو TLVS على النحو التالي:

- SYSNAME : يشير إلى FULLY QUALIFIED DOMAIN NAME (FQDN) للجهاز في RFC 1907 .
- SYSOBJECTID : يعطي OBJECT IDENTIFIER (OID) في RFC 1907 .
- MANAGEMENT ADDRESS : يشير إلى عنوانIP الذي يقبل الجهاز منه رسائل بروتوكول SNMP .
- PHYSICAL LOCATION: يرسل كلمة تمثل الموقع الجغرافي للجهاز.

في عام 2001 أضافت سيسكو الدعم لـ TLVS التالية:

- EXTERNAL PORT ID: تعريف الـPHYSICAL FIBER .

وأخيرا، في عام 2003 أضافت سيسكو الميّزات التّالية في بروتوكولCDP :

- الطاقة المطلوبة :تحديد مقدار الطاقة المطلوبة.
- الطاقة المتاحة : تحديد مقدار الطاقة المتاحة.
- PORT UNIDIRECTIONAL MODE : تحدّد على أن حركة المرور على هذا المنفذ هي في اتجاه واحد .

2.1. LLDP-MED :

في سبتمبر 2000، سيسكو عملت مع IEEE لإنشاء LLDP ، هذا الأخير نشر في مايو 2005. يوفر هذا البروتوكول معايير اكتشاف الأجهزة بين أجهزة شركات مختلفة .

كان من المسلّم به أن هناك حاجة إلى قدرات إضافية محددة لنقل الصوت، لهذا قامت رابطة TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA) بتطويرLLDP-MED ، الذي يحدد ملحقات لـ LLDP . تم تحديد-LLDP MED ليعمل فقط بين الأجهزة مثل الهواتف وأجهزة مثلSWITCHS .

2. مقارنة بين LLDP-MED وCISCO DISCOVERY PROTOCOL

LLDP و CDP هما بروتوكولين ذات صلة ، ولهما عدة أوجه متشابهة ، بما في ذلك طريقة تشغيلهما و المعلومات المنقولة من طرفهما. تناقش الفقرة التالية قدرات البروتوكولين معا ، وأوجه اختلافهما وتشابههما

- اكتشاف القدرات: (CAPABILITIES DISCOVERY)

اكتشاف القدرات يسمح بتحديد نوع الجهاز المتصل في الجهة المقابلة، يمكن استخدامها للإشارة إلى ما إذا كان الجهاز المتصل هو هاتف، راوتر، ، الخ.

اكتشاف هذه القدرات الأساسية مدعوم من قبل البروتوكولين CDP وLLDP . بالإضافة إلى اكتشاف القدرات الأساسية، LLDP يتضمن وظيفة إضافيّة لتحديد القدرات المفعّلة في الجهاز. على سبيل المثال، CDP يقر بأن الجهاز المتصل هو الهاتف، في حين أن LLDP يمكنه الكشف على أن الجهاز هو هاتف مع PC PORT مفعّل أو غير مفعّل.

- سرعةLAN و اكتشافDUPLEX :

هذه القدرة مهمة لأنها تسمح باكتشاف أي سرعة أو DUPLEX غير متطابق قد يحدث بين جهازين. على سبيل المثال، يمكن لـSWITCH إرسالTRAP إذا كشف أن هناكDUPLEX غير متطابق بينه و بين الجهاز المقابل. يدعم LLDP اكتشاف السرعة أو الـ DUPLEX بينما يدعمCDP اكتشاف DUPLEX فقط.

- اكتشاف NETWORK POLICY :

هذه القدرة هي واحدة من أهم القدرات لأنها توفر آلية لـSWITCH لإعلام الهاتف بالـ VLAN الذي ينبغي استخدامه. يمكن للهاتف الاتصال مع أيSWITCH والحصول على رقمVLAN ، ثم يبدأ الاتصال.

اكتشافNETWORK POLICY يحل اليوم مشكلة كبيرة بين هواتفTHIRD-PARTY التي تعمل معSWITCH سيسكو وكذلك هواتف سيسكو التي تعمل معTHIRD-PARTY SWITCHS . في كلتا هذين الحالتين ، مشكلة في الـ INTER-WORKING تحدث إشكالية فيDEPLOYEMENT

- هواتفTHIRD-PARTY التي تعمل مع SWITCH سيسكو:

بعض هذه الهواتف تستقبل معلومات الـ VLAN من خلال بروتوكولDHCP ، وهذا يعني أن هذه الهواتف يجب عليها عملBOOT أول ، والحصول على عنوان IP عن طريقNATIVE VLAN ، والحصول على VOICE VLAN من خادمDHCP ، ومن ثم إعادة الـBOOT مرة أخرى باستخدامVOICE VLAN .

في حالات أخرى يجب إعداد الهواتف بشكل فردي لمنحها رقم الVOICE VLAN .

- هواتف سيسكو التي تعمل مع : THIRD-PARTY SWITCHS

في هذه الحالة، لا بد من إعداد هواتف سيسكو بشكل فردي من خلال واجهة الهاتف بشكل فردي بالVOICE VLAN .

o- اكتشاف الطاقة :

اكتشاف الطاقة يسمح للهواتف و الـSIWTCH بنقل كمية الطاقة المحتاجة و تستخدم هذه الخاصية مع بروتوكولPOE (POWER OVER ETHERNET) .
يوفرLLDP معلومات متعلقة بكيفية تشغيل الجهاز (من الخط، من مصدر احتياطي، من مصدر طاقة خارجي، وما إلى ذلك)، وأولوية الحصول على الطاقة ومقدار الطاقة المحتاج.
بينما CDP يتضمن TLVS منفصلة واحدة خاصة بالطاقة المطلوبة وأخرى خاصة بكمية الطاقة المتاحة، مما يسمح لـ SWITCH والهاتف بالتفاوض بكمية الطاقة المستخدمة .

o- اكتشاف الINVENTORY :

CDPو LLDP يسمحان للهاتف بإبلاغ SWITCH عن سماته مثل رقم الـ MODEL و رقم SERIAL ، ونسخة البرنامج وغير ذلك وهذا أمر مهم لأن هناك العديد من الهواتف لا تدعم واجهةSNMP .

o- تمديد نطاقTRUST :

يوفرCDP قدرة إضافية لا توجد في LLDP إذ يسمح بتمديد نطاق الثقة إلى الهاتف. في هذه الحالة، يتم الوثوق بالهاتف حيث يقوم بتعليم الحزم الواردة على منفذ الـ PC. هذه الميزة تخفف الحمل على SWITCH.

وبهذا نكون قد انتهينا و أتمنى أن أكون قد وفقت، ألقاكم قريبًا إن شاء الله والسلام عليكم.

USB

مع كثرة استخدام وسائل نقل البيانات وخاصة الفلاشات وغيرها مع كثرة انواع الفيروسات التى تنتشر من خلال هذة الوسائل تحديدا والتى اصبحت اسهل وسيلة لنقل هذة الفيروسات والديدان عبر اجهزة الكمبيوتر

هذة الفيروسات قد تنتقل الى حاسوبك بمجرد توصيل فلاش ميمورى معطوب بأحد هذة الفيروسات لذلك سنتخذ مجموعة من الاجراءات لتفادى اصابة الكمبيوتر بمثل هذة الفيروسات والتروجنات

- أولا: ايقاف خاصيتي Auto play و Auto Run :

ولكن ما هاتين الخاصيتين وما فائدتهما وما الفرق بينهما؟

Auto play

هذة الخاصية التى تمكن نظام التشغيل من اكتشاف نوع البيانات المخزنة داخل Removable device مثل الفلاشات أو الاسطوانات وغيرها ليقوم بعرض برنامج تشغيلها اتوماتيكيا مثل الفيديوهات أو الصور وغيرها أو سيقوم بفتح الفلاش او الاسطوانة تلقائيا وهذا قد يسبب انتشار مثل هذة الفيروسات بمجرد فتح الفلاش او الاسطوانة

Auto Run

هذة الخاصية تمكن النظام من تنفيذ أوامر معينه موجودة داخل ملف autorun.inf والموجود داخل الاسطوانة أو الفلاش مباشرة بمجرد فتحها سواء يدويا أو من خلال خاصية ال auto play
فقد نستطيع مثلا وضع صورة أو icon للاسطوانه بإضافة الامر icon=path حيث يشير ال path الى مسار الصورة

ايضا يمكن تشغيل ملف معين سواء ملف تنفيذى او غير ذلك بمجرد فتح الاسطوانة باضافة السطر open=path وايضا هنا ال path هو مسار هذا الملف مع العلم ان هذا الامر يستخدم مع الاسطوانات فقط أما مع الفلاش ميمورى يستبدل بالامر

shellexcute=path

وقد كان وظيفة هذة الخاصية هى تسهيل عمل اسطوانات الالعاب او البرامج التى تحتوى على العديد من الملفات حيث بمجرد ان يضع المستخدم الاسطوانة يشير ملف ال autorun الى ملف ال setup او ملف تشغيل اللعبة

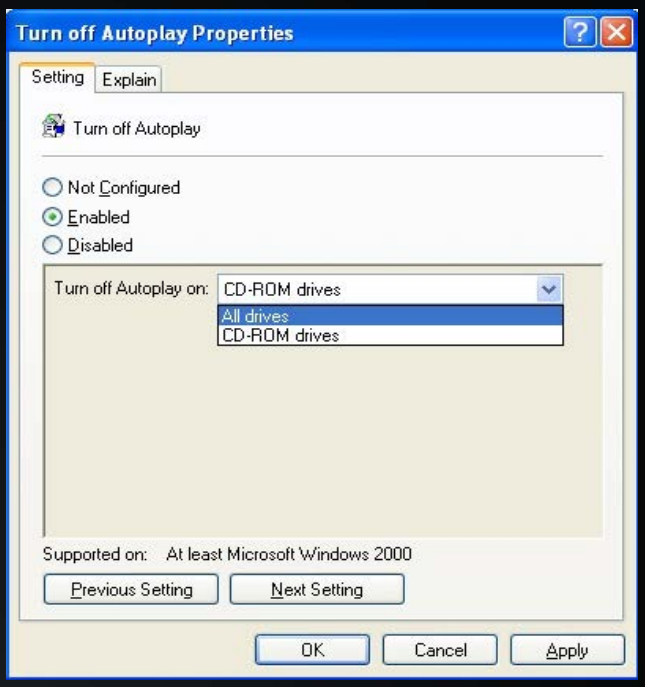
الان ومع انتشار استخدام الفلاش ميمورى تم استخدام خاصية ال Autorun لتشغيل الفيروس بمجرد فتح الفلاش
إذا الخطوة الاولى ستكون إيقاف هاتين الخاصيتين فى وندوز 7 نذهب الى run ونكتب:
gpedit.msc

ثم :
user configuration\administrative templates\windows components\autoplay polices

ومن هنا نوقف عمل خاصيتى Auto play و autorun فى وندوز xp نوقف خاصية ال Auto play بالذهاب الى run ثم gpedit.msc ثم :

user configuration\ administrative templates\system

ثم نختار Turn off autoplay ونختار enabled وهنا ممكن نحتار ايقافها فقط على الاسطوانات ام على جميع ال Drives



لوقف خاصية ال Auto run على xp نستخدم هذا الامر :

reg add «HKLM\SOFTWaRE\Microsoft\ Windows NT\CurrentVersion\IniFileMapping\ autorun.inf» /ve /d «@SYS:DoesNotExist» /f

• **ثانيا: استخدام أحد برامج ال anti-virus القوية :** مثل Avira أو Eset smart security 5 والتى تقوم تلقائيا بحماية منفذ ال USB من انتشار الفيروسات واى ملفات خبيثه من خلالة مع الحرص على تحديث هذة البرامج اولا بأول

• **ثالثا: استخدام أداة مثل myusbonly :** والتى تمنع توصيل اى فلاش ميمورى الى جهازك بدون علمك او بدون موافقتك حيث تمنع هذة الاداة عمل اى فلاش ميمورى على النظام الا بعد ادخال كلمة مرور انت تحددها مع العلم ان الاداة لا تغلق المنفذ نهائيا لكن تسمح لأى مكونات اخرى بالعمل على المنفذ تلقائيا بدون اى اعاقة مثل mouse او keyboard او camera انما فقط تمنع الفلاش ميمورى

هذة الاداة يمكن تحميلها من موقعها:
www.myusbonly.com

VIRTUAL FIREWALLS ON CISCO ASA

في البداية كما يعلم الأغلبية أن كل شبكة في العالم مهدّدة بالهجوم عليها واستغلالها إما بطريقة شرعية من قبل الـ PENETRATION TESTING أو غير شرعية من قبل الناس المخربين BLACK HAT HACKER ، وأيضًا أغلب الناس قد سمع عن الجهاز المسمّى بالجدار الناري FIREWALL ومن أشهر الجدران النارية هو جهاز ASA (ADAPTIVE SECURITY APPLIANCE) المقدّم من شركة CISCO ، وهناك طبعًا أجهزة أخرى مقدمة من شركات عالمية تعمل بنفس المفهوم .

ولكن هنا نحن سنتحدث عن جهاز الـ ASA وهذا الجهاز عبارة عن حائط صد للهجمات التي قد تصيب شبكتك و القادمة من الشّبكات الغير موثوق بها UNTRUSTED NETWORK ومن ضمن مميزاته هي STATEFUL ، PACKET FILTERING ، NETWORK ADDRESS FILTERING ، VPN SUPPORT ، HIGH TRANSLATION ، AAA SUPPORT ، AVAILABILITY ومميزات أخرى كثيرة ..

ولكن هنا من الممكن أن نعمل أكثر من جدار ناري وهمي على جهاز ASA واحد !
نعم تمامًا كما قرأت، واعتقد أن أكثر الناس قد تعاملوا مع برنامج الـ VMWARE الشهير بعمل أجهزة وهمية على جهاز كمبيوتر واحد والتدريب عليها ، وهنا من الممكن أن نعمل جهاز ASA وهمي داخل جهاز ASA حقيقي وموضوعنا لهذا العدد هو كيفية إعداد هذا الشيء .

في البداية عندما نعمل جدار ناري ASA وهمي داخل الـ ASA الحقيقي كل جهاز وهمي يسمى SECURITY CONTEXTS وكل SECURITY CONTEXTS يعمل كجدار ناري منفصل مع سياسات الأمن وإعدادات الـ INTERFACES الخاصة به ، ولكن هناك بعض الخصائص التي لا تعمل على الجدار الناري الوهمي مثل IPSEC AND SSL VPN ، DYNAMIC ROUTING PROTOCOLS ، MULTICAST .
كل الموديلات الخاصة بالـ ASA (ماعدا موديل الـ 5505) يدعموا MULTIPLE SECURITY CONTEXTS وكل SECURITY CONTEXTS تقوم بإنشائه على الـ ASA الحقيقي يحتوي على ملف إعداداته الخاص به (FILENAME.CFG) والمخزن في الـ FLASH ، وهذا الملف يحتوي على سياسات الأمن وإعدادات المنافذ وإعدادات SECURITY CONTEXTS الخاص به .

من المفترض BY DEFAULT أن يكون هناك ADMIN CONTEXT موجود دائمًا ولديه ملف إعدادات يسمى بالـ ADMIN.CFG وهذا الـ CONTEXT مثل أي CONTEXT موجود على الجهاز ولكن الفرق هنا أن أي شخص يدخل على هذا الـ CONTEXT يكون لديه كل الصلاحيات حتى صلاحيات الدخول على الـ CONTEXT الأخرى (مثل حساب الـ ADMINISTRATOR في الويندوز) .

ولكي نعرف ماهي الـ CONTEXT الموجودة حاليا على الـ ASA الحقيقي نكتب الأمر التالي :

```
ciscoasa(config)# show context
Context Name      Class      Interfaces          URL

Total active Security Contexts: 0
ciscoasa(config)#
```

وكما نلاحظ أنه لا يوجد أي CONTEXT تم إنشائها من قبل .
عندما نريد من الـ ASA الحقيقي أن يقوم باستضافة CONTEXT وهمية نقوم بكتابة الأمر التالي :-

```
ciscoasa(config)# mode m
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
```

وبعد كتابة الأمر سيعمل الجهاز RELOAD . وعند الانتهاء يقوم الـ ASA بتحويل الإعدادات الحالية RUNNING CONFIGURATION إلى ملفين ملف جديد يحتوى على إعدادات الإقلاع STARTUP CONFIGURATION ويضم داخله إعدادات النظام SYSTEM CONFIGURATION وملف الـ ADMIN.CFG الذي تكلمنا عنة سابقًا والذي يضم الـ ADMIN CONTEXT الموجود في ذاكرة الـ FLASH ، والملف الثاني هو الإعدادات القديمة ويحفظ في ذاكرة الـ FLASH ولكن باسم OLD_RUNNING.CFG .
ولإنشاء SECURITY CONTEXT جديدة نقوم بكتابة الأمر التالي :

```
ciscoasa(config)# admin
ciscoasa(config)# admin-context ?

configure mode commands/options:
  WORD  Name of administrative context
ciscoasa(config)# admin-context administrator
Creating context 'administrator'... Done. (1)
ciscoasa(config)#
```

ولإعطاء موارد معينة لـ CONTEXT معين على سبيل المثال G1 AND G2 نكتب الأوامر التالية :-

```
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# all
ciscoasa(config-ctx)# allocate-in
ciscoasa(config-ctx)# allocate-interface g1
ciscoasa(config-ctx)# all
ciscoasa(config-ctx)# allocate-in
ciscoasa(config-ctx)# allocate-interface g2
ciscoasa(config-ctx)# con
ciscoasa(config-ctx)# conf
ciscoasa(config-ctx)# config-url
ciscoasa(config-ctx)# config-url flas
ciscoasa(config-ctx)# config-url flash:/admin.cfg
INFO: Converting flash:/admin.cfg to disk0:/admin.cfg
```

وللتأكد من إعطاء الموارد للـ CONTEXT المعين نكتب الأمر التالي وسنلاحظ أنه بالفعل G1 AND G2 ينتموا لهذا الـ CONTEXT :-

```
ciscoasa(config)# show context
Context Name      Class      Interfaces          URL
*administrator    default    GigabitEthernet1,   disk0:/admin.cfg
                             GigabitEthernet2

Total active Security Contexts: 1
```

سنقوم الآن بإنشاء CONTEXT جديد من أجل التحقق في الآخر أن كل شيء يعمل جيداً وبالشكل المطلوب سننشئ CONTEXT باسم CUSTOMERA وسنسند له الـ G3 AND G4 لكي يكونوا ضمن هذا الـ CONTEXT :

```
ciscoasa(config)# context customerA
Creating context 'customerA'... Done. (2)
ciscoasa(config-ctx)# alloc
ciscoasa(config-ctx)# allocate-in
ciscoasa(config-ctx)# allocate-interface g3
ciscoasa(config-ctx)# alloc
ciscoasa(config-ctx)# allocate-in
ciscoasa(config-ctx)# allocate-interface g4
ciscoasa(config-ctx)# conf
ciscoasa(config-ctx)# config-url
ciscoasa(config-ctx)# config-url flash
ciscoasa(config-ctx)# config-url flash:/customerA.cfg
INFO: Converting flash:/customerA.cfg to disk0:/customerA.cfg
```

إلى هنا نكون قد أنشأنا 2 CONTEXT وأسندنا لهم الموارد المطلوبة ، لكن عندما تدخل على الـ ASA الحقيقي عن طريق الـ CONSOLE CABLE ستدخل على إعدادات النظام SYSTEM CONFIGURATION أو كما يطلق عليها البعض SYSTEM EXECUTION SPACE وهذا الوضع هو الوضع العام للجهاز والذي من خلاله تستطيع الدخول على أي SECURITY CONTEXT آخر ، وعند الدخول إلى هذا الوضع وكتابة أمر SHOW RUN هنا المخرجات ستكون فقط إعدادات الـ GLOBAL SYSTEM CONFIGURATION وليس إعدادات الـ SECURITY CONTEXT الآخر لأنه كما قلنا سابقًا أن لكل SECURITY CONTEXT ملف إعدادات خاص به ومن أجل أن ترى إعدادات SECURITY CONTEXT معينة يجب عليك أولاً الدخول عليه ومن ثم كتابة الأوامر المطلوبة .

وللتغير مابين الـ SYSTEM EXECUTION SPACE و الـ CONTEXT أو مابين الـ CONTEXT نفسهم يجب نكتب الأوامر التالية :-

للتحول إلى الـ CONTEXT المسمى CUSTOMERA نكتب الأمر التالي وسنلاحظ بعد كتابة الأمر SHOW INTERFACE IP BRIEF أنه يوجد فقط G3 AND G4 ينتموا له ويحق لهذا الـ CONTEXT التعامل معهم فقط وليس غيرهم :

```
ciscoasa# changeto context customerA
ciscoasa/customerA# show
ciscoasa/customerA# show inter
ciscoasa/customerA# show interface ip br
ciscoasa/customerA# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet3           unassigned      YES unset  down                  down
GigabitEthernet4           unassigned      YES unset  down                  down
ciscoasa/customerA#
```

وللعودة مرة أخرى إلى وضع الـ SYSTEM EXECUTION SPACE نكتب الأمر التالي وأيضاً سنلاحظ هنا بعد كتابة أمر الـ SHOW INTERFACE IP BRIEF أن هذا الوضع لديه كافة الصلاحيات على الـ ASA وهو الـ ADMIN الذي تحدثنا عنه سابقا ..

أتمنى لكم الاستفادة من الموضوع وتحياتي لكم ونلتقى في العدد القادم إن شاء الله ..

SIP TRUNKING وفوائده الاقتصادية

هل تذكر عزيزي القارئ الهواتف السلكية عندما كانت جميع المكالمات الهاتفية تذهب فوق الشبكة الهاتفية العامة المبدلات او المقاسم Public Switched Telephony Network (PSTN) وكانت شركات الأعمال تشتري خطوط خاصة أو تستأجرها trunks لربط شبكتها الهاتفية الفرعية بالشّبكة العامة وكانت كلّها خطوط أنالوج ؟ليوم أصبح النموذج الجديد من الربط هو («trunking to IP) وقد أدّى إلى خفض تكاليف الاتصالت الهاتفية وأصبح هناك عائد سريع على الاستثمار بالاضافة إلى تحسين ا الاتصالات داخل المؤسسة الواحدة

وتحسين اتصالاتها مع الموردبين والشركاء والعملاء والأفرع الخارجية. SIP trunk هو خدمة تقدمها (Internet Telephony Service Provider (ITSP التي تستخدم sip لإنشاء اتصال بين المقاسم الفرعية الخاصة للمؤسسات PBX وبين ITSP هذا الترنك يشمل multiple voice sessions ليلبي حاجات المؤسسات.

SIP trunking مع بروتكولها تلبي جميع حاجات الاتصالات من بداية الاتصال إلى نهايته real-time communications بمافي ذلك التراسل الفوري وتطبيقات الاتصال المرئي والتطبيقات التشاركية ... إلخ.
والعائد السريع من الاستثمارفي هذا المجال هوالمحرك الرئيسي للتطوير في SIP trunk.

وأهم فوائد SIP trunking :

1) تلغي تكاليف BRIs (Basic Rate Interfaces) و PRIs (Primary Rate Interfaces) services وخدماتها .
2) عند تطور المؤسسة وزيادة استثماراتها تلغي الحاجة لإضافة PSTN gateway جديدة.
3) يقلل المصروفات الرأسمالية فالحواسيب المكتبية وخطوطها تُستعمل لاتصالات الهاتف دون الحاجة لخطوط pstn .
4) يحسن من استخدام bandwidth عند استخدام نفس الخط للاتصال الصوتي ونقل البيانات في نفس الوقت.
5) يزيد من المرونة في الاستخدام وضبط أبعاد الخطوط المستخدمة وسعاتها بتجنب شراء خطوط بسعات عالية دون الحاجة لها كشراء (30 lines) E1)

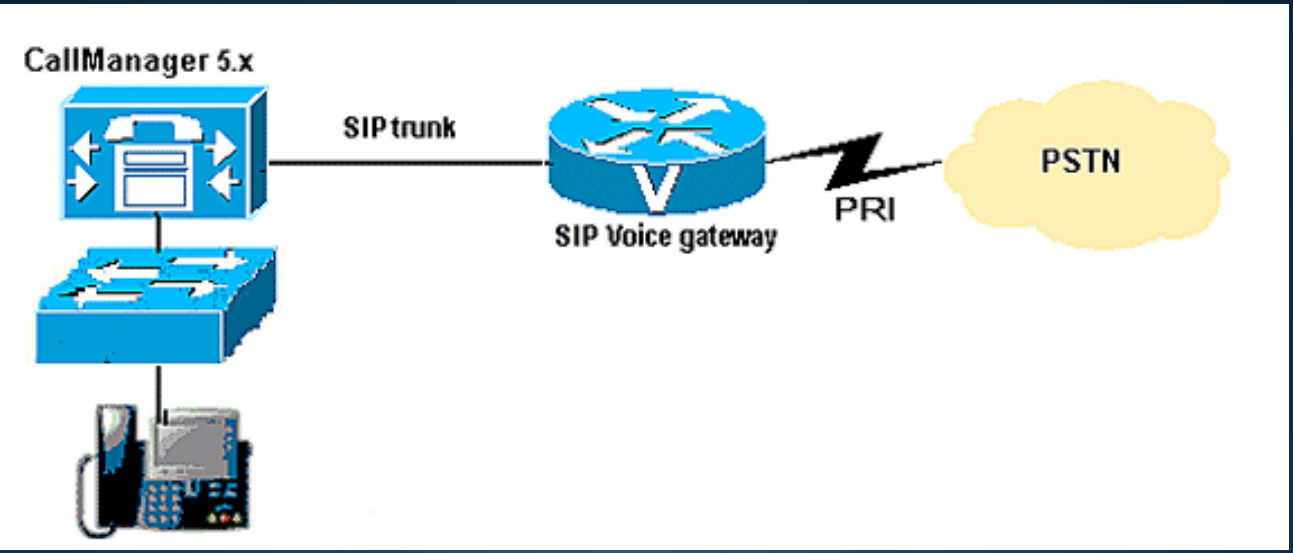
في حين يمكن استخدام 10E1 .

6) تقدم اتصالات عالمية بسعر المكالمات المحلية.

7) توفر اتصال مع مقدمي الخدمات المتعددة.

هناك عناصر ضرورية لنجاح الـ SIP TRUNKING

IP-PBX with a SIP-enabled trunk interface,
Enterprise edge device that supports SIP
Internet telephony or SIP trunking service
provider ITSP



الفوائد الإنتاجية التي تأتي من SIP TRUNKING مهمة جدًا من خلال توسيع قدرات SIP إلى خارج الشبكة المحلية لتصل إلى جميع أنحاء العالم وتوصيلها بالأقمار الصناعية للاتصال مع العاملين في المناطق النائية واستخدامها على الصعيد التجاري في الاتصالات لعمل اتصال في وقته الحقيقي وكسر الحواجز ونقل البيانات.

خمس برامج غير مكلفة للحصول على VPN Clients

هناك العديد من الشركات تعتمد بشكل حيوي على الوصول الى مخدماتها، الملفات و البيانات الخاصة بالعمل وذلك من مواقع متعددة و غير ثابتة احيانا و الكثير اعتمد على الفائدة الكبيرة التي تقدمها تكنولوجيا الـ VPN. الا انه عادة ما يترافق مع قلق شديد و خوف من مرور بياناتهم عبر الانترنت مثلا، لان هذه التكنولوجيا تعد تغيير في طريقة الاتصال مع المخدمات و البيانات التي يعرفونها و التي اعتادوا عليها وهذا التغيير يبعث بالشك و عدم الثقة و الذي ترتفع حدته بأرتفاع اهمية البيانات المطوب الولوج اليها. تجدر الملاحظة الى ان ختيار الـ VPN client المناسب هو مفتاح الحل لهذا الشعور في جعل هذه التقنية امنة، كما يشار الى ان هناك العديد من الـ VPN Serversمثل (Sonicwall and Fortinet) تتطلب منك استخدام الـ VPN Client الخاص بمخدماتها. ولكن هنالك العديد من المخدمات الاخرى تسمح باستخدام VPN client لطرف ثالث، بعضها مجاني بالمطلق و بعضها رخيص وبعضها يستحق ان تعرف عنه اكثر،لذلك لقد اعددت خمس انواع من الـ VPN clients و التي اؤمن انها سوف تعجبك و تثير اهتمامك فيما يتعلق باتصال الـ VPN Client – Server . بعضها ربما يلبي احتياجاتك و البعض الاخر ربما لا يتوافق مع ما تريد وهذا يعتمد على الـ VPN Servers التي تعمل عليه، الا ان كل VPN Client يقدم لك الكثير من المزايا و مستويات متعددة من السهولة و التعقيد بما يناسب المستخدم النهائي.

لنبدأ مع الاداة الاولى والأشهر وهي:

- OpenVPN Client

OpenVPN Client هو عميل يتمتع بمواصفات الـ SSL VPN Cleint وهو مدمج بشكل سهل و بسيط مع OpenVPN server، يتصف بالسهولة في الاعداد و الاستخدام و يقوم بالاتصال بالمخدم بشكل

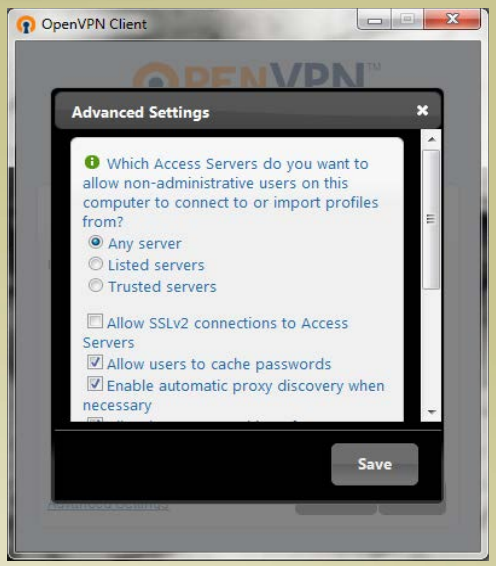
سريع جدا ومجاني و متوافق مع Windows, Mac, Linux ، متوافق مع جميع اصدارات Windows .

وبدأ دعم أنظمة أندرويد مؤخرا, وفي النهاية الـ OpenVPN Client يعمل مع OpenVPN server بكل سهولة و سرعة و آمان.

يعتمد الـ OpenVPN في عملية الـ Authenticate بين الطرفان على عدة تقنيات من بينها pre-shared secret key, certificates, username/password أما عملية التشفير فهي تعتمد على مكتبة تدعى OpenSSL وهي مشروع مفتوح المصدر ومنفصل تماما عن OpenVPN يقوم بالتشفير إعتمادا على بروتوكول الـ SSL والـ TLS, الأداة بشكل عام جيدة وعملها مستقر والأهم من كل هذا أنها مجانية بشكل كامل ويوجد إصدارات خاصة بالـ Virtual Machine, ولتحميل الأداة والتعرف على المزيد من المعلومات راجع الموقع الرسمي لهم على العنوان الآتي https:// /openvpn.net

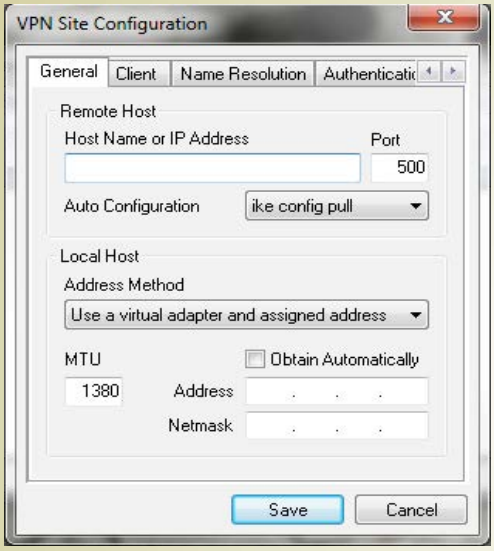
Shrew Soft VPN Client - 3

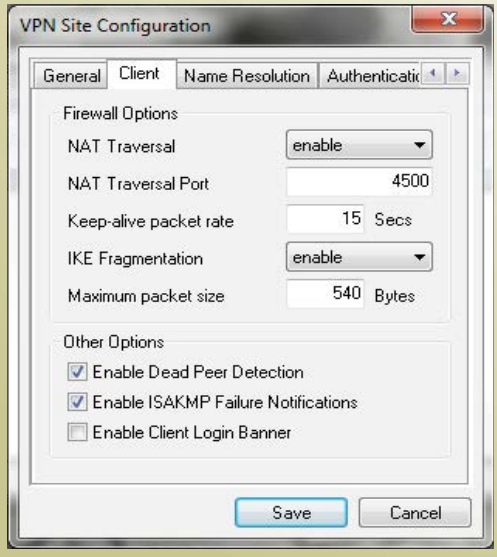
اداة سهلة الاستخدام و مجانية، وتعمل على تأمين اتصالVPN الى السيرفر الذي يعتمد على بروتوكل الـ IP sec في عملية الأتصال، وهي متوقرة لانظمة تشغيل Windows 7, Vista, XP, 2000 (32bit, 64bit) ، كما انه يعمل على Linux platform ، صممت هذه الاداة بالاصل للاتصال على السرفرات المفتوحة المصدر كا FreeSWAN و OpenSWAN اما الان فهي تنشأ اتصال VPN من خلال Cisco, Juniper, Checkpoint, Fortinet, Netgear, Linksys, Zywall و الكثير ايضا.

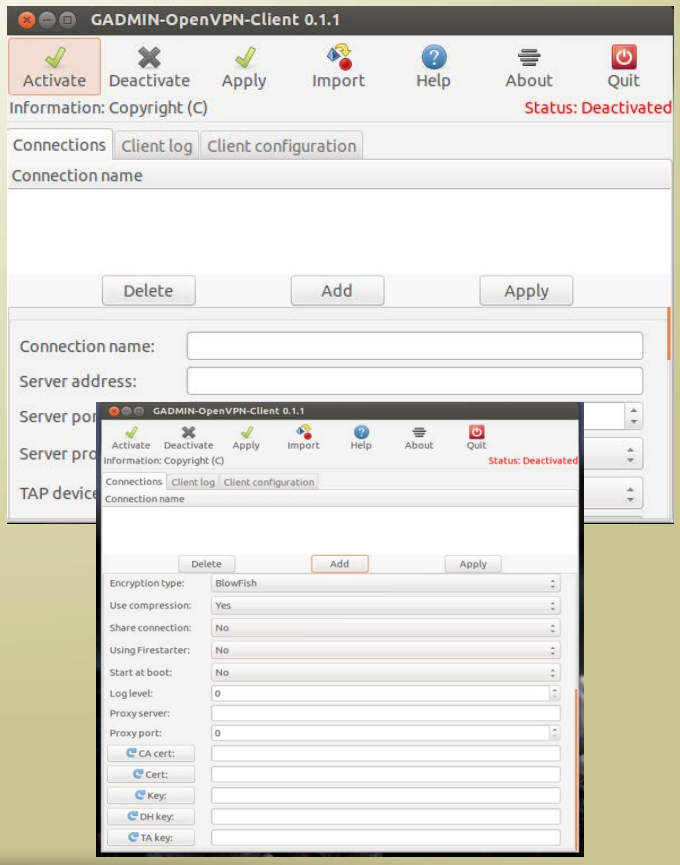


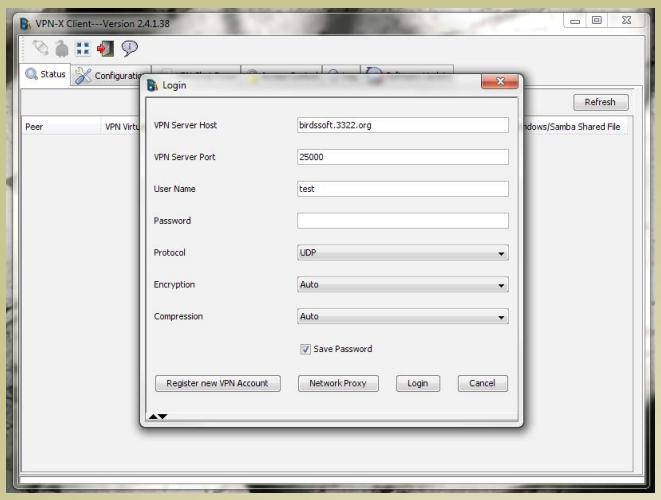
Gadmin VPN Client - 2

هذه الاداة تمثل وسيلة اخرى للاتصال بـ OpenVPN server ، كما تمثل جزء من مجموعة أدوات لادارة الاتصال مع مخدم الواجهة الرسومية التي تسهل كثيرا العمل مع OpenVPN server ، الا ان هذه الاداة صممت بالتحديد للعمل مع Linux فقط، وهي تقدم الكثير والكثير جدا من الخيارات، وهذا ما يجعلها غير مناسبة للمستخدمين ذو الخبرة المتواضعة في التعامل مع VPN Connections , فهي تسمح لمدير الشبكة بالتحكم بكل الأرقام والأحداثيات الخاصة بالأتصال الخاص بي الـ VPN وهذا يشمل البروتوكول المستخدم ورقم المنفذ ونوع التشفير والضغط والكثير من الخيارات الآخرى.



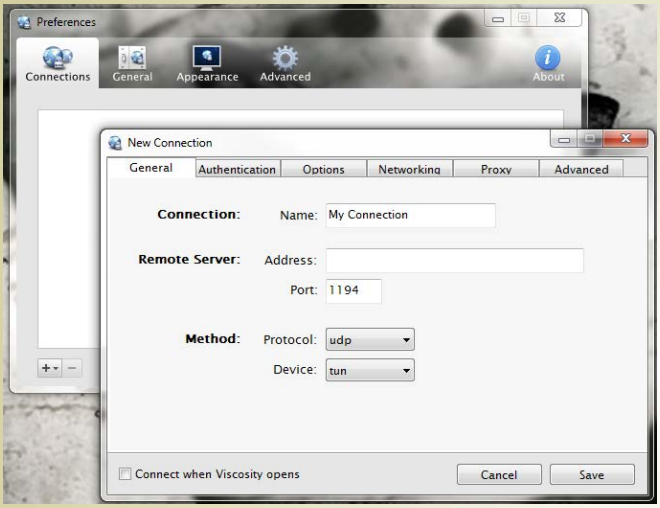






VPN X Client - 4

هذه الاداة غير مجانية، و سعرها يتوقف على عدد النسخ المطلوبة، كما ان VPN X Client مخصص للاتصال بـ VPN X server بشكل خاص و الذي يتمتع بسهولة الاعداد ومدعوم من كافة الأنظمة الموجودة, الـ VPN-X يعتمد على بروتوكول الـ SSL/TLS, الأداة يمكن أن تكون مجانية لكن في حالة الأستخدام الشخصي فقط وهي محدودة بخياراتها ومميزاتها عن الأداة المدفوعة,



Viscosity VPN Client - 5

تعمل هذه الاداة على انظمة Mac ،windowsو يقوم بتأسيس اتصال في غاية السهولة الى OpenVPN server ، يشار الى انه ليس مجاني، وتكلفته في حدود الـ 9 دولار. تعتبر هذه الاداة متوافقة مع OS X's advanced DNS system ، و تعمل مع و AppleScript Batch/Vbs scripts ، كما وتقدم الدعم الكامل لـ , multiple connections, proxy (integration IPv6,Smartcar/token (PKCS#11 واكثر.

الخمس ادوات انفة الذكر تعمل مع VPN servers مختلفة و تعطيك خيارات و اسعة من السهولة والتعقيد وتكاليف بسيطة جدا، واذا كنت تبحث عن VPN client جديد او تسعى لستبدال ما لديك. ما عليك سوى ان تنتقي المناسب لشبكتك

أنواع الـ VLAN

وصلتني منذ فترة على الخاص طلب من أحد زوار المدونة حول توفير مقال خاص حول أنواع الـ Vlan وكيف يتم تقسيمها وفقا لوظيفتها

عندما طرح علي السؤال أمر, أستغربت من السؤال فأنا لم أسمع من قبل أن للـ VLAN هناك أنواع, قررت البحث أكثر عن الموضوع فوجدت أن المقصود بها هي ليس الأنواع بمفهومها العام, الفكرة ببساطة تعتمد على نوع الترافيك الذي يمر من خلال هذه الـ VLAN وهو مايعبر عنه بأنواع

لكن بشكل عام الأنواع تكون عندما تكون لديك اشياء ثابتة تختار أنت منها, أما هنا فهي بحسب رغبتك فأما أن تجعل شبكتك تعمل كلها في VLAN واحدة أو تقوم بتقسيمها وعزل كل شيئ على حدا, وهي خمس أنواع , Data Vlan, Management Vlan, Voice Vlan, Default Vlan, Native Vlan

سوف أتحدث عنهم بطريقة مختصرة وتعريفية.

Data Vlan

تعتبر الـ Data Vlan الممر الأساسي لمرور المعلومات الخاصة بالمستخديمن على الشبكة لذلك يطلق عليها أحيانا User Vlan,

عادة ما تكون هذه الـ VLAN في الشبكات الصغيرة هي لكل شيئ للادارة والفويس, لكن في الشبكات الكبيرة والاحترافية تكون مخصصة للمعلومات فقط أو لنقل لتبادل الملفات وتصفح الأنترنت ولا مانع أن يكون في الشبكة أكثر من Data Vlan.

Management VLAN

تعتبر الـ Management Vlan الممر الخاص بأدارة السويتش والتى عادة تستخدم من أجل أكثر من شيئ يخص أدارة الشبكة من خلال أحد البروتوكولات المخصصة مثل HTTP, Telnet, SSH وعملية الأتصال مع السويتش أو من أجل مراقبة الشبكة من خلال بروتوكول الـ SNMP .

Voice VLAN

تعتبر الـ Voice Vlan الممر الخاص بالترافيك الخاص بالفويس أو كما نسميه أحيانا VOIP, فكرة عزل الداتا عن الفويس تعتبر مسألة مهمة جدا لأن المكالمات الهاتفية لايمكنها الأنتظار كالداتا العادية كعملية التصفح أو عملية مشاهدة الفيدوهات على الأنترنت. وتسمح عملية العزل هذه بالتلاعب بالباندويث الموجود على الشبكة وإعطاء أولويات أعلى بأستخدام أحد بروتوكولات الـ QoS.

Default Vlan

عادة ماتكون هذه الـ Vlan هي الرقم واحد والتى تنتمي إليها كل المنافذ فأي منفذ لاينتمي إلى أي Vlan يكون عادة في الـ Default Vlan, تستخدم هذه الـ Vlan من قبل عدة بروتوكولات مثل بروتوكول الـ STP, CDP, VTP, Pagp, UDLD, BPDU, هذه الـ VLAN لايمكن حذفها أو إعادة تسميتها كون وجود بروتوكولات كما قرانا مسبقا تعتمد عليها.

Native Vlan

تعتبر الـ Native Vlan هي نفسها الـ Default Vlan وهي خاصة ببروتوكول الـ 802.1Q وفيها ينتقل الترافيك بدون وجود أي Tags عليه وللمزيد حول هذا الموضوع راجع الرابط التالي جيث تحدث المهندسين عن هذا الموضوع بأسهاب في قسم الأسئلة والأجوبة وخصوصا أن الموضوع طويل وتفاصيله كثيرة.

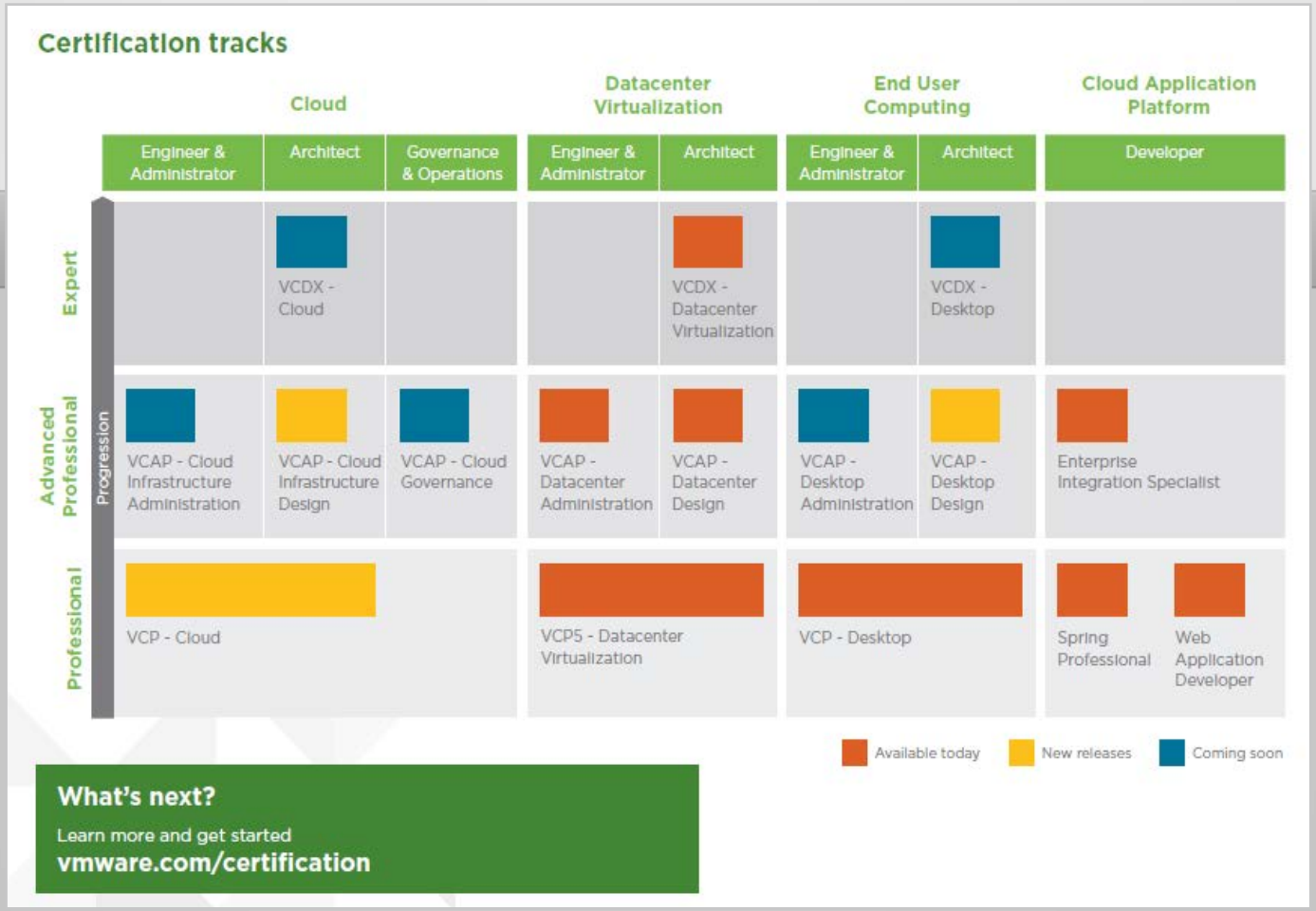
إلى هنا أكون قد عرفت هذه الأنواع ولو كان الأمر مختصرا وهو بالفعل لايحوي الكثير من الكلام بأستثاء النوع الآخير, وطبعا التصنيفات تكون أما على نوع الترافيك المار وأما بوطيفته في الشكبة, أتمنى أن لاتنسونا من دعوة صالحة بالتوفيق والتيسير وبأن يتقبل الله عملنا لوجه الكريم ودمتم بود.

الشهادات الجديدة لشركة VMware

تكلمنا فى مقالا سابق منذ شهور قليلة عن شهادات شركة VMware وتقسيماتها
لكن خلال هذة الشهور القليلة الماضية حدث تغيير كبير في تقسيمات الشهادات وظهرت شهادات جديدة للشركة .
تم الاعلان عن هذة الشهادات الجديدة خلال مؤتمر VMware VMworld 2012 الذى انعقد خلال شهر اغسطس الماضي في الولايات المتحدة

اهم معالم هذة التغييرات في الشهادات هي انهم قاموا بعمل تقسيم جديد للمتخصصين فى ال Cloud Computing وايضا اضافوا قسم للمتخصصين في المطورين والمبرمجين لهذة التكنولوجيا

فيما يلى صورة توضح التقسيم الجديد :



كما نرى في التقسيم الجديد للشهادات فقد تم تقسيمها الى اربع تقسيمات اساسية :

1 - Cloud :

وهو تقسيم جديد تم الاعلان عنة في المؤتمر وهو مصمم خصيصا للمتخصصين في تكنولوجيا الCould Computing بانواعها
وهي مقسمة الى ثلاث مستويات – Professional Advanced Professional – Expert) (لكى تغطي كل مستويات العاملين في هذا المجال الجديد

اسم الشهادة (VCP-Cloud)

هذا القسم الجديد من الشهادات كنا في احتياج له منذ فترة طويلة ليكي يكون هناك فرق بين العاملين فى التكنولوجيا التخيلية بصفة عامة وبين العاملين فى ال Cloud Computing

2 - Data Center Virtualization :

لا يعتبر هذا القسم جديد ولكن تم التغيير فى الاسم فقط وهذا القسم يعطي شهادات للمتخصصين فى تكنولوجيا VMware Virtualization على منتجاتها مثل ال vSphere and vCenter
وهذه اشهر شهادة لدى شركة VMware
وهي شهادة مقسمة الى ثلاث مستويات وهي لم تتغير في مستوياتها عن الماضى

اسم الشهادة (VCP-DV)

3 - End User – Computing :

من التقسيمات القديمة لكن تم اضافة مستوى المحترفين فيها Expert والذي لم يكن موجود فى الماضي
وهذة الشهادة كما نعرف متخصصة للعاملين في تكنولوجيا ال VDI من خلال برامج VMware View and VMware ThinApp

اسم الشهادة (VCP – Desktop)

4 - Cloud Application Platform :

تقسم جديد في شهادة VMware وهو خاص للمبرومجين والمطويرين لتطبيقات ال Cloud Computing وهي اول شهادة متخصصة في هذا المجال الجديد وهم مختصون بعمل بيئات عمل لل Cloud وتطبيقات عليها من خلال برامج ال VMware vFabric وبيئات جافا

مما سبق نستنتج ان شركة VMware اضافة قسمان جديدان في الشهادات لديها وتحديدا في التكنولوجيا الجديدة وهي ال Cloud Computing
وهذا كان شئ متوقع ومنتظر منها ومن شركات اخرى مثل مايكروسوفت التى قامت باصدار شهادة تسمى ال MCSE Private Cloud

وهذا نتيجه الاقبال الكبير على هذة التكنولوجيا وعلى تعلمها ولم يكن لها اسم شهادة او تخصص معين يندرجوا تحته

الجدير بالذكر : يوجد شركات تقوم بعمل شهادات متخصصة فى هذة التكنولوجيا فقط وهى كورسات وامتحانات ولا تنتج اى تطبيقات مثل شركة: Cloud School

NetWork Set

First Arabic Magazine For Networks