

تعرف على تقنية Virtualization



نتائج الاستفتاء

ما هو أفضل منتدى عربي للشبكات ؟

• منتديات عرب هاردوير

87% ☐

• منتديات برامج نت

3% ☐

• منتدى بوابة العرب التعليمية

5% ☐

• منتديات أخرى

5% ☐

- توفير المال والوقت والطاقة
- سهولة في التحكم والأعداد
- أمان وحماية عالي المستوى

تقرير كامل عن محاكي

الشبكات الأول

+

أسرار وحلول

GNS3

تقرأون في هذا العدد

كيف تتم عملية التتبع

Trace Route

من أين وكيف أبدا دراسة الشبكات؟

كيف تقوم بتأسيس شبكة فويس من الصفر

مقارنة بين IPv4 و IPv6

حصاد الشبكة العنكبوتية لعام 2009

والعديد من المواضيع الجديدة والقيمة

شاهدوا أيضا أقسام

مصطلحات تقنية



عتاد ومعلومات



مشاكل وحلول



2

أفتتاحية العدد

أطفال السكورتى!

المحررون الدائمون

- الدكتور محمد التميمي

Yarra_link@yahoo.com

- المهندس أيمن النعيمي

admin@networkset.net

- المهندس أحمد الشحات

warrior10@hotmail.com

- المهندس عادل الحميدي

adel_husni2000@hotmail.com

المحررون الضيوف

- المهندس عثمان أسماعيل

othman_ucmael@yahoo.com

لا أعلم أن كانت هذه صدفة أم أن هذا الشيء هو واقعي ففي كل يوم أتجول فيه على المنتديات العربية أتفاجئ بأن الأغلبية تركض وراء دراسة كورسات السكورتى والأمن مع أنه الطلب على هذا النوع من الوظائف ليس بالكبير في ساحتنا العربية وحتى عندما يحدث بعض الأشخاص عبر الماسنجر أجد نفس الشيء أريد أن أختص بمجال الأمن والسكورتى و.....الهكر....ومن هنا بدأنا ومن هذه النقطة عدنا إلى النقطة الحقيقية وراء وجود الكثير من الأشخاص يهتمهم دراسة هذا الكورس فكما هو معروف عند الأشخاص العاقلين أن 97% من العرب همهم الأول والآخر أن يكون هكر وقرصان زمانه وقد تستغرب إذا قلت لك أن هذه النسبة سوف تزيد لو في حال سألت أي شخص يدخل الأنترنت حول القرصنة وأمور الهكر فالكل سوف يرد عليك بأنه يعرف ويعلم الكثير حول هذه المواضيع وله الكثير من التجارب.

وفي أحد المرات وعلى أحد المنتديات المعروفة وجدت شخص يسأل سؤال حول مستقبله ويقول فيه أرغب في الدخول في مجال الأمن لاني أهوى هذا المجال وأحس نفسي باتي ناجح في هذا المجال ومشكلتي أنني لا أعلم كيف أبدا فبماذا تنصحوني أن أبدا ؟ وطبعاً الشباب لم تقصر معه ومع طموحاته وقامت بوضع سلسلة كورسات قوية ومفيدة في هذا المجال وعندما عاد صاحبنا سأل سؤال في غاية الغباء وهو طيب إذا أنا درسة أول ثلاث كورسات هل أستطيع أن أكون هكر قوي؟؟؟ أو تجد أحدهم يطلب منك كورسات السكورتى التي تفيد في تعلم القرصنة بشكل مباشر

نعم أخي هذه أحد الأمثلة وهناك منها الكثير وبراني أن أتجاه الأشخاص نحو السكورتى والأمن يتجلى في عدة أسباب منها
- أتعلم القرصنة من أجل التباهي والتفاخر بقوته وبذكائه أمام الناس أو من أجل تحرير فلسطين وتدمير أمريكا من خلال أغلاق بعض المواقع وطبعاً لن ينسى أن يضع اسمه المرمز مثل هذا الاسم الذي صادفته في أحد المرات-|@|\$|<| ومعناها الحرفي كلاش!!!

ب-التأثر بأفلام هوليوود مثل أفلام القرصنة والسرقات وعملية اختراق البنوك ومحاولة تقليد هذه الخرافات !

ج-وهو الشخص الطبيعي الذي تعلم الأساسيات وتعلم البرمجة والشبكات بالإضافة إلى التعامل مع الأنظمة الحرة مثل لينوكس وعائلته المحترمة وأخيراً أنصح جميع الأشخاص الذين يفكرون في هذا المجال أن ينظروا إلى هذه الشهادة من مفهوم أكبر وأن يبدأوا بتطوير أنفسهم من خلال تعلم الأساسيات المطلوبة لهذا المجال وأن يبتعدوا عن فكرة القرصنة والتخريب وأتخذ هذا المقولة الانكليزية كشعار لك Hack to learn not learn to hack ويبقى السؤال موجود في ذهني هل هي مصادفة أم هو واقع نعيش فيه؟؟؟ ودمتم بود

موقع المجلة

www.networkset.net

بريد المجلة

magazine@networkset.net

بريدي الخاص

admin@networkset.net

جميع الحقوق محفوظة لكاتبها

محتويات أيار 2110



- 16 - شهادة جديدة من سيسكو CCNA SP
- 17 - كيفية تفعيل web-J على أجهزة جونيبر
- 18 - كيف تستغل وقتك في تعلم الشبكات
- 18 - كيف تقوم بعمل اختصار لكل أوامر سيسكو
- 19 - مقارنة بين IPv4 و IPv6
- 20 - هجوم Vlan Hopping وطريقة التصدي له
- 21 - مقارنة بين سيرفراي + RADIUS & TACACS
- 22 - قسم عتاد ومعلومات
- 24 - قسم مصطلحات تقنية
- 25 - قسم مشاكل وحلول

- 3 - حصاد الشبكة العنكبوتية لعام 2009
- 4 - تقرير حول محاكي الشبكات الأول GNS3
- 7 - كيف تتم عملية التتبع في الشبكات
- 8 - من أين وكيف أبدا طريق الشبكات
- 12 - كيف تقوم بتأسيس شبكة فويس من الصفر
- 13 - دليلك نحو شهادات جونيبر
- 14 - نتائج الاستفتاء الشهري
- 15 - أنواع كوابل الايثرنت وطريقة اختيار الكبل المناسب

حصاد الشبكة العنكبوتية لعام 2009

بقلم محمد التميمي

رغم الكم الهائل من التغيرات والتطورات التي تحدث في عالم الإنترنت فإن الجانب الإحصائي لهذه التغيرات تكاد تكون متقدمة ولهذا قامت شركة بينجودوم بنشر مقالة عرضت فيها إحصائيات شبكة الإنترنت في عام 2009. مستعينة بمجموعة متنوعة وواسعة من المصادر من مختلف أنحاء الشبكة علاوة على إضافة المزيد من المعلومات التي رصدها الشركة بنفسها. كم من المواقع الإلكترونية تم إضافتها على شبكة الإنترنت؟ كم يريد إلكترونياً تم إرساله؟ كم بلغ عدد مستخدمي الإنترنت في 2009؟ هذا الموضوع سوف يجيب على جميع هذه الأسئلة وغيرها من الأسئلة الكثيرة ذات العلاقة.

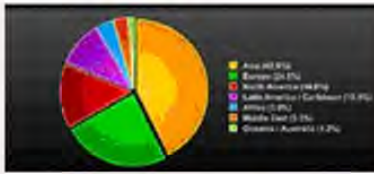
- 234 مليون موقع 126 مليون مدونة...

- 1.73 مليار عدد مستخدميها عالمياً

- 90 تريليون رسالة إلكترونية...

- 4 مليار صورة... ومليار مقطع فيديو يومي

- 179.031.479 عدد مستخدمي الإنترنت في أمريكا اللاتينية ومنطقة البحر الكاريبي
- 67.371.700 عدد مستخدمي الإنترنت في أفريقيا
- 57.425.046 عدد مستخدمي الإنترنت في الشرق الأوسط
- 20.970.490 عدد مستخدمي الإنترنت في أوقيانوسيا/ أستراليا
- 18% نسبة الزيادة في عدد مستخدمي الإنترنت مقارنة بالسنة الماضية



البريد الإلكتروني

• عدد رسائل البريد الإلكتروني المرسلة على شبكة الإنترنت في عام 2009

بلغ 90 تريليون رسالة

• متوسط عدد رسائل البريد الإلكتروني المرسلة يوميا 274 مليار

• عدد مستخدمي البريد الإلكتروني في جميع أنحاء العالم 1.4 مليار

• عدد مستخدمي البريد الإلكتروني الجدد منذ العام قبل الماضي

100 مليون

• 81% نسبة رسائل البريد الإلكتروني "المزعجة" من إجمالي عدد رسائل البريد الإلكتروني المرسلة في عام 2009

• 24% نسبة الزيادة في عدد الرسائل المزعجة مقارنة بالعام السابق

• عدد الرسائل المزعجة "غير المرغوب فيها"

المرسلة يوميا 200 مليار على افتراض أن

81% من الرسائل الإلكترونية المرسلة كانت مزعجة

المواقع الإلكترونية

• 234 مليون عدد المواقع على شبكة الإنترنت حتى ديسمبر 2009

• 47 مليونا عدد المواقع الإلكترونية التي تم إنشاؤها في عام 2009

خوادم الويب

• 13.9% نسبة الزيادة في الخوادم التي تستخدم Apache في عام 2009

• 22.1% نسبة الزيادة في خوادم الإنترنت التي تستخدم IIS

• 35.0% نسبة الزيادة في خوادم الإنترنت التي تستخدم جوجل GFE

• 384.4% نسبة الزيادة في الخوادم التي تستخدم Nginx

• 72.4% نسبة الزيادة في الخوادم التي تستخدم Lighttpd

أسماء النطاقات

• وصل عدد النطاقات التي تستخدم COM 81.8 مليون نطاق مع نهاية 2009

• عدد النطاقات التي تستخدم NET 12.3 مليون

• عدد النطاقات التي تستخدم ORG 7.8 مليون

• عدد نطاقات البلدان مثل CN, UK, DE ect. بلغ 76.3 مليون

• 8% نسبة الزيادة في أسماء النطاقات مقارنة بالعام السابق

مستخدمو الإنترنت

• 1.73 مليار عدد مستخدمي الإنترنت حول العالم حتى سبتمبر 2009

• 738.257.230 عدد مستخدمي الإنترنت في آسيا

• 418.029.796 عدد مستخدمي الإنترنت في أوروبا

• 252.908.000 عدد مستخدمي الإنترنت في أمريكا الشمالية

الشبكات الاجتماعية

• بلغ عدد المدونات على شبكة الإنترنت 126 مليون مدونة

• 27.3 مليون تدوينة قصيرة تضاف يوميا إلى "تويتر" حتى نوفمبر 2009

• 57% من مستخدمي تويتر هم من سكان الولايات المتحدة الأمريكية

• 350 مليون عدد مستخدمي فيس بوك

• 50% من مستخدمي فيس بوك يقومون بالاطلاع على ملفاتهم بشكل يومي

• 500.00 عدد التطبيقات الفاعلة في فيس بوك

الصور

• عدد الصور التي تم حفظها في فليكر 4 مليار صورة أكتوبر 2009

• عدد الصور التي يتم تحميلها شهريا على فيس بوك

2.5 مليار أي 30 مليار صورة يتم حفظها سنويا على فيس بوك

الفيديو

• عدد مقاطع الفيديو التي تتم مشاهدتها يوميا في يوتيوب حول العالم (مليار مقطع)

• عدد مقاطع الفيديو التي تتم مشاهدتها شهريا في يوتيوب في الولايات المتحدة الأمريكية (12.2 مليار مقطع نوفمبر 2009)

• عدد مقاطع الفيديو التي تتم مشاهدتها شهريا في "هولو" في الولايات المتحدة الأمريكية (924 مليار مقطع نوفمبر 2009)

• 182 متوسط عدد مقاطع الفيديو التي يشاهدها مستخدم الإنترنت الواحد في أمريكا

البرمجيات الخبيثة

• 148.000 جهاز كمبيوتر يصاب يوميا بمواد خبيثة

• 2.6 مليون مادة خبيثة تمهد الأجهزة في بداية 2009 (فيروسات وديدان)

• 921.143 عدد توقيعات الشفرات الخبيثة التي أضافتها سيمانتيك Symantic

متصفحات الإنترنت

• 7.26% لمتصفح انترنت اكسبلورر

• 6.42% لمتصفح فايرفوكس

• 6.40% لمتصفح قوقل كروم

• 5.40% لمتصفح سفاري

• 4.20% لمتصفح أوبرا

• 2.10% لمتصفحات أخرى



تقرير كامل حول محاكي الشبكات الأول

بقلم أيمن العجيمي



يعد برنامج الـ GNS3 هو البرنامج الأول في عالم المحاكيات نظرا للتسهيلات الكبيرة التي قدمها لكل دارسي الشبكات في العالم من خلال توفير منصة قوية لمحاكاة أجهزة سيسكو سابقا وأجهزة جونيبر لاحقا التي تم إضافتها إلى الإصدار الأخير منها.

ونظرا لأهمية هذا البرنامج سوف أحاول في هذا الموضوع أن ألقى الضوء على كيفية تنصيب وتشغيل البرنامج بالإضافة إلى ذكر أكثر المشاكل شيوعا في هذا البرنامج كما سوف يكون هناك بعض الإضافات والانسداد الخاصة فيه والتي تساعد في زيادة كفاءة وعمل البرنامج.

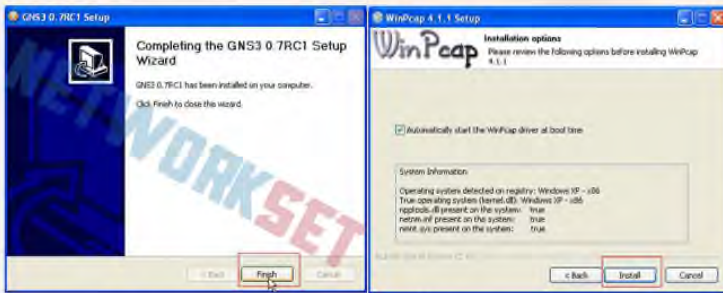
الـ GNS3 ببساطة هو ليس برنامج محاكي للشبكات كما يظن الأغلبية لأنه فقط عبارة عن واجهة رسومية لمحاكي الشبكات الـ Dynamips وهو برنامج مفتوح المصدر يعمل على جميع أنواع الأنظمة من بينها ويندوز ولينوكس وماكنتوش ولكي يعمل يحتاج إلى 3 أشياء مهمة أولا يحتاج طبعاً إلى الـ Dynamips والذي يعد بدوره قلب النظام الذي سوف يقوم بمحاكاة أنظمة سيسكو من خلال محاكاة الـ IOS ثانياً يحتاج إلى الـ Dynagen وهو صلة الوصل بين قلب النظام Dynamips والمستخدم ويتم عبر نقله الأوامر الكتابية من وإلى ثالثاً يحتاج إلى برنامج WinPcap وهو برنامج يقوم بالنقاط ونقل الـ Packet في الشبكة عبر مجموعة من البروتوكولات رابعاً غير مهم لكن إذا في حال أردت أن تقوم بعمل محاكي للجدران النارية الخاصة بـ سيسكو أو جونيبر فانت تحتاج إلى برنامج Qume

طريقة التنصيب (لويندوز فقط)

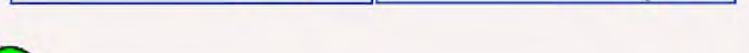
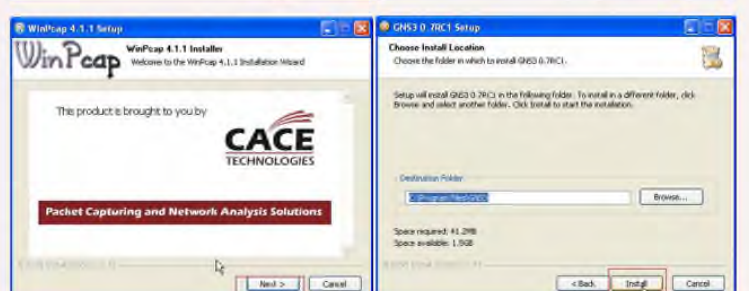
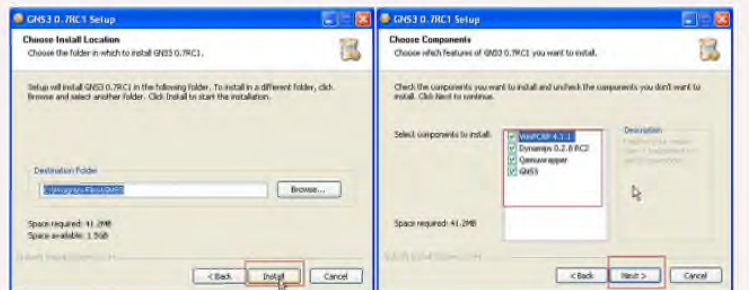
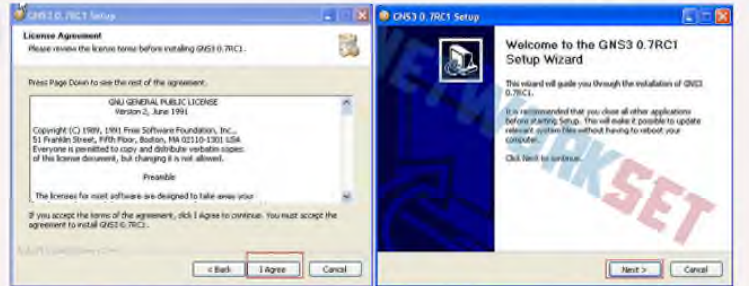
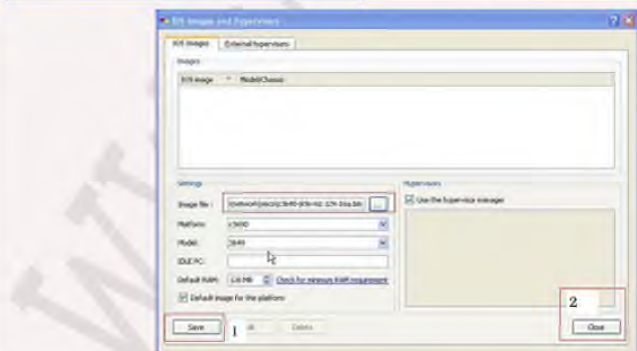
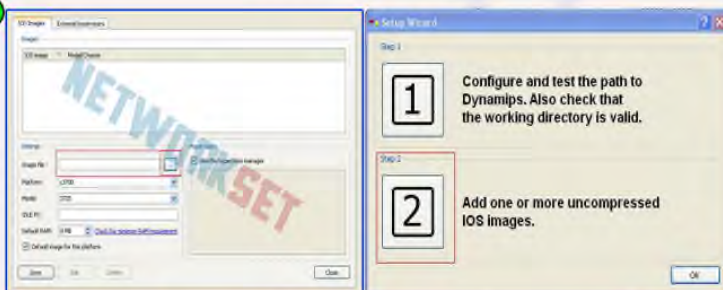
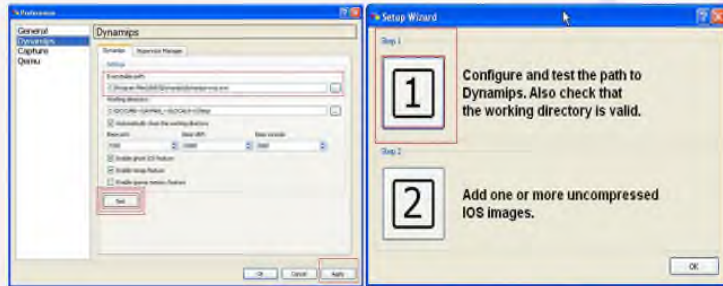
نقوم أولاً بتحميل آخر نسخة من البرنامج ولا نحتاج إلى أي شيء آخر لأن مع البرنامج يأتي الديناميس والداينجين كما سوف نرى في الشرح وللتحميل سوف نتوجه إلى رابط الموقع

<http://www.gns3.net/download>

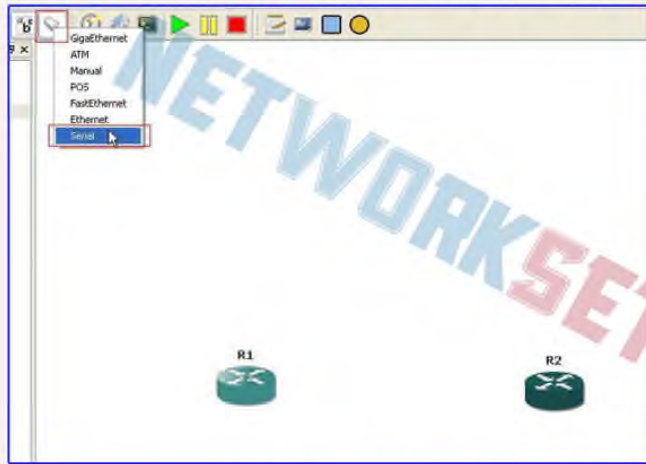
ونختار آخر إصدار ونقوم بتحميله ونبدأ التنصيب بالخطوات



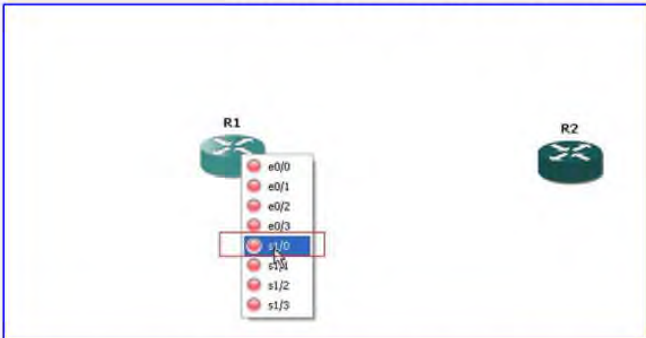
بعد أن انتهينا من التنصيب يلزمنا نسخ الـ IOS لكي نضيفه للبرنامج وهي موجودة في كل مكان على الإنترنت والشرح سوف يكون عن نسخة 3640 بعد تحميل النسخة من الإنترنت نقوم بتشغيل البرنامج لأول مرة لنجد Wizard يطلب منا تنفيذ شيئين مهمين لضمان تشغيل البرنامج بشكل جيد الأول هو التأكد من أن الديناميس منسوب على الجهاز ويعمل مع الـ GNS3 الثاني هو إضافة نسخة سيسكو الـ IOS للبرنامج ولكي نقوم بتنفيذها نقوم بالتالي:



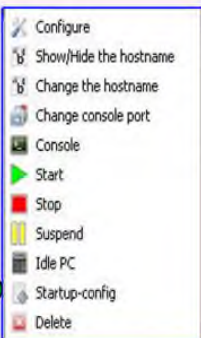
وبعد أن ننتهي من تحديد الـ slots نقوم بتكرار العملية مع روتر آخر وننتقل مباشرة إلى طريقة الوصل بين الروتين والقيام بذلك يتوجب علينا أن نعرف أن اختيار كبل التوصيل يعتمد على نوع الـ Slot الذي قمنا باختياره وهي موضحة بالصورة



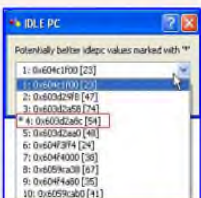
بعد تحديد الكبل نضغط على الروتر الأول ونختار رقم البورت



ونقوم بتوصيله مع الروتر الثاني بنفس الطريقة ولم يبق علينا إلا أن نضغط على زر البدء Start من التول بار لبدء البرنامج عمله ويقوم بتشغيل عملية المحاكاة لكلا الروتين والتي لا تحتاج منك إلا الضغط على زر Console لكي تصل إلى موجه الأوامر الخاص بكل روتر. أما بخصوص الخيارات الموجودة على كل روتر والتي نستطيع أن نراها من خلال الضغط بالزر اليمين على الروتر فهي كالآتي:



Configure لاعداد الروتر وقد تم التطرق لها من قبل
Show/Hide لاختفاء واظهار اسم الروتر من على التبلوجي
Change the hostname لتغيير اسم الروتر
Change console port لتغيير رقم الكونسول بورت
Start لبدء تشغيل الروتر
Stop لإطفاء الروتر
Pause لتوقيف مؤقت
Idle PC وهي من أهم الأشياء وفائدتها تحديد قيمة معينة من المعالج تساعد في تخفيف الضغط عليه ويتم تحديده بان نقوم أولا بتشغيل الروتر وبعدها نضغط Idle PC وننتظر قليلا لنرى عدة أرقام ونختار القيمة التي بجانبها علامة النجمة وكما هو موضح بالصورة



Startup-config لاختيار اسم معين لملف الاعدادات
Delete لحذف الروتر بشكا كامل

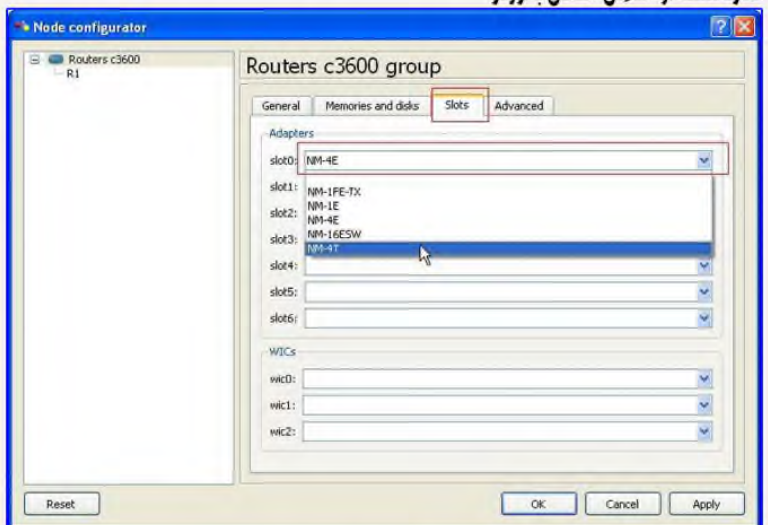
بعد أن انتهينا من اعداد البرنامج نتعرف على الـ ToolBar الخاص بالبرنامج



بعد ان تعرفنا على التول بار لنبدأ الشغل العملي من خلال قيامنا بتطبيق محاكاة لروترين سوف نقوم أولا بسحب روتر 3600 من القائمة اليسرى الى وسط البرنامج



وبعدها نضغط بالزر اليمين على الروتر ونختار configure لنقوم باعداد الـ SLOTS والتي نقوم فيها باختيار عدد ونوع البورتات التي أريد أن استخدمها في الروتر ويمكننا أيضا تحديد كمية الـ رام وحجم الهارد ديسك أو الفلاش الخاص بالروتر



NM-1FE لإضافة بورت واحد من نوع فاست إيثرنت

NM-1E لإضافة بورت واحد من نوع إيثرنت

NM-4E لإضافة أربع بورتات من نوع إيثرنت

NM-16ESW نقوم باختيار هذا الـ Slot في حال أردنا أن نقوم بعمل محاكاة لسويتش لأن الـ

Dynamips غير مجهز لعمل محاكاة للسويتش

NM-4T لإضافة أربع بورتات من نوع سيربال

مشاكل وحلول وأسرار في برنامج الـ GNS3

سؤال تواجهني هذه المشكلة عند تشغيل الروتر ؟

error 209 unable to start vm instance Ro

جواب: هذه المشكلة تحدث عادة عندما تقوم بإضافة ملفات IOS موجودة في مجلدات مكتوبة باللغة العربية أو لغة أخرى عدا الانكليزية ولايتصر الموضوع على المجلد الموجود فيه النسخة بل يشمل كل الملفات التي تدخل في مسار النسخة وهذه بعض الأمثلة للتوضيح



سؤال: قمت باختيار قيمة الـ Idle PC لكن المعالج مازال يعمل بنسبة عالية ؟

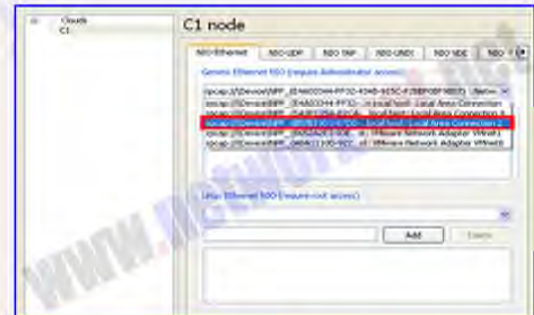
جواب: تحدث هذه المشكلة أحيانا من خلال البرنامج نفسه ويعود هذا الى خطأ في استخراج القيمة المناسبة لذلك قم بالمحاولة أكثر من مرة حتى تجد المعالج قد بدأ يعمل بشكل طبيعي ولاتنسى أن تختار القيمة التي بجانبها علامة نجمة.

سؤال: لماذا ياخذ الروتر وقتا طويلا حتى يعمل وكيف استطع إنقاص هذه المدة ؟

جواب: ياخذ الروتر وقتا طويلا بسبب قيامه بفك ضغط برنامج التشغيل IOS على الذاكرة ولكي نقوم بتشغيل الروتر في سرعة أكبر نقوم بفك ضغط نظام التشغيل على الهارد وبعدها نقوم بإضافته مرة ثانية على البرنامج وطريقة فك الضغط تتم كالتالي اضغط بالزر اليمين على ملف الـ IOS واختر فتح بواسطة أو Open with وقم باختيار برنامج الوينزار وبعدها قم باختيار فك ضغط الملف هنا وأخيرا قم بإضافة النسخة الجديدة إلى البرنامج مرة أخرى

سؤال: كيف أقوم بربط البرنامج مع جهاز كمبيوتر آخر لتخفيف الحمل على الجهاز ؟

جواب: للقيام بهذا الموضوع قم بإضافة غيمة إلى الـ Topology وبعدها بالزر اليمين اختر إعدادات وقم باختيار كرت الشبكة المتصل مع الجهاز الآخر كما هو موضح بالصورة وبعدها اضغط على كلمة ADD



سؤال: كيف أقوم بربط البرنامج مع برنامج الفتي أم وير ؟

جواب: أول شيء يجب عمله هو إضافة لوبوك بالـ انترفيس على جهاز الكمبيوتر وبعدها نقوم بإضافة غيمة كما في السؤال السابق ونربطها مع اللوبوك بالـ انترفيس وبعدها نتوجه إلى برنامج الفتي أم وير وندخل إلى Edit Virtual Network Editor ومن خيار Bridged to نقوم باختيار اللوبوك بالـ انترفيس وآخر شيء نقوم به إعطاء أجهزة الكمبيوتر والانترفيس أيبات تنتمي جميعها لشبكة واحد

سؤال: لماذا لا يحفظ البرنامج الإعدادات التي قمت بعملها على الروتر ؟

جواب: لكي يقوم البرنامج بحفظ الإعدادات يجب عليك أولا وقبل تشغيل الروترات أن تتوجه إلى File New Project وقم باختيار المكان التي سوف يقوم البرنامج بحفظ إعدادات الروتر وبعدها قم بوضع إشارة عند كل خيار موجود في نفس النافذة وهي خياران الأول Save NVRam والثاني Router Export

سؤال: كيف أقوم بربط برنامج الـ GNS3 مع برنامج الـ SecuerCRT ؟

بعد تنصيب كل من برنامج الـ GNS3 و SecuerCRT على الكمبيوتر نقوم أولا بإنشاء ملف تكست جديد ونضع بداخله هذا الكود

```
#Language="VBScript"
#$Interface="1.0"
Sub main
crt.window.caption=crt.arguments(0)
End Sub
```

بعد نسخ الكود داخل الملف نقوم بحفظه باسم securecrt.vbs ونضع السكريبت داخل مجلد الـ GNS3 والموجود على الامتداد التالي

C:\Program Files\GNS3

وأحب أن أؤنبه أن مكان الحفظ هام حتى يعمل السكريبت بشكل جيد وبعدها نقوم بتشغيل برنامج الـ GNS3 ونضغط على Edit وبعدها نختار Preference وفي خانة الـ Terminal command قم بوضع هذا الكود

```
start C:\progra~1\vandyk~1\SecureCRT\SecureCRT.EXE /script C:\progra~1\gns3\securecrt.vbs /arg %d /T /telnet %h %p
```

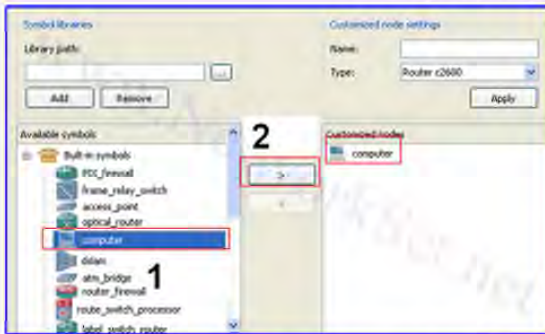
ملاحظة أخيرة لكي يعمل السكريبت يجب مراعاة مكان وجود برنامج الـ SecurCRT وهو على الامتداد التالي

C:\Program Files\VanDyke Software\SecureCRT

سؤال: كيف أقوم بربط البرنامج مع برنامج الـ VPCS ؟

جواب: قبل أن أعرض الطريقة سوف أشرح بشكل سريع ما هو برنامج الـ VPCS ؟ الـ VPCS أحد البرامج المقترحة المصدر التي تهدف إلى عمل محاكاة بسيطة جدا لنظام التشغيل من خلال دعم بروتوكول الـ Ping والـ Trace route وهي الأدوات الوحيدة تقريبا التي نحتاجها في اللابات التطبيقية بالإضافة إلى أنه يدعم الـ IPv4 و IPv6 كما أنه مزود بـ DHCP client لتزويده بالآيبي بشكل أوتوماتيكي ويستطيع أن يوفر لك 9 أجهزة وهمية وهو يعد من أصغر أنظمة التشغيل البسيطة وحجمه 2 ميغا فقط.

بعد تحميل البرنامج وفك الضغط عنه نقوم أولا بتشغيل السيرفر الخاص بالبرنامج وهو VPCS.exe وبعدها نقوم بتشغيل برنامج الـ GNS3 وهي ملاحظة هامة تشغيل السيرفر قبل برنامج الـ GNS3 وبعدها نتوجه مباشرة إلى Edit->Symbol Manager ونبحث في القائمة اليسرى عن صورة لجهاز كمبيوتر ونقوم بإضافتها إلى القائمة اليمنى كما هو موضح بالصورة



وبعدها نقوم باختيار Cloud من خيارات الـ Type المتاحة ونضغط على زر Apply ونختمه بالضغط على OK

بعدها نتوجه إلى برنامج الـ VPCS ونقوم بكتابة الأمر show لتظهر لنا هذه النتائج والتي يهمنها منها آخر اثنان وهما الـ Lport و Rport نقوم بحفظ أحدهم وليكن 30001 و 20001 ونتوجه بعدها للمرة الأخيرة إلى برنامج الـ GNS3

أقوم أولا بإضافة روتر وجهاز كمبيوتر وبعدها اضغط بالزر اليمين على جهاز الكمبيوتر وأختار إعدادات وأتوجه إلى التبويب الثاني وأقوم بكتابة الأرقام السابقة بالإضافة إلى 127.0.0.1 في الصندوق الثاني.



وأرجو منكم أن تلاحظوا معي أن في خيار LocalPort قمت بكتابة رقم Rport الموجود في البرنامج وفي خانة الـ RemotePort قمت بكتابة رقم Lport وإذا قمت بعكس الأرقام لن ينجح الاتصال وبعدها نضغط على زر ADD وبعدها OK ونقوم بالتوصيل بين جهاز الكمبيوتر والروتر من خلال كبل FastEthernet ونقوم بتشغيل الروتر ونعطي المخرج المتصل مع جهاز الكمبيوتر آيبي وليكن 192.168.2.1/24 ونتوجه مرة ثالثة إلى برنامج الـ VPCS ونكتب في موجه الأوامر الرقم 2 وهو يعني النظام التشغيل الثاني ونعطيه آيبي وملسك وغيت واي من خلال الأمر التالي 192.168.2.2 192.168.2.1 24 ip وبهذا نكون قد انتهينا



من أين أبدأ وكيف أبدأ في الشبكات؟؟؟

سؤال لطالما حيرني!!!

بقلم: عادل الحميدي

دعنا نتفق منذ البداية على أننا نريد البداية الصحيحة والتي يتم فيها التأسيس المتين لمستواك العلمي والعملية ثم نتدرج حتى نصل إلى مستوى الاحتراف ثم الخير ، ولا نريد الاستعجال فما بني على باطل فهو باطل ، وليس معنى هذا أننا سننهي عمرك كله ولن تستفيد لا ألف لا ، بل سأضع أنا وأنت خطة زمنية محددة بوقت ننتهي خلالها كل ما نريد وهذا شيء مهم جداً جداً وبعد هذه الفترة نكون وصلنا لمستوى الخبراء وحتى تكون مميزاً يصدق ، ومن سمات هذه الخطة الزمنية أن تقف بعدها مع نفسك وتحاسيها تكافئها إن أنجزت وأحسنت وتعاقبها إن أساءت ، وتقيم تلك المرحلة تتعلم من أخطاءك وتستفيد خبرة والله المستعان ...

دعنا نقول من الآن وإن كان هذا سابق لأوانه (مهندس شبكات محترف في ثلاث سنوات) هذا شعار الخطة الزمنية ومدتها ، ثم التقويم والمراجعة كل شهر ثم كل سنة ، ماذا أنجزت وفيما أخطأت وهل تحتاج الخطة لإعادة هيكلة وهكذا ... دعك من العشوائية ولكن منظماً .



الكورس الأول ::::

دعني أسألك سؤال أيها المبتدئ ما هي وحدة بناء الشبكة (شبكة الحاسب الآلي) ؟ [لا تستعجل أيها المتقدم في المستوى قليلاً فأنا سأتدرج حتى مستوى الخبراء ولكني أراعي المبتدئين فلا تمل وانتظر وسوف تستفيد]
تمام صحيح : الكمبيوتر (الحاسب الآلي) هو وحدة بناء الشبكة
إذن لابد لك أن تتعلم استخدام الحاسب الآلي الويندوز والبرامج الأساسية الأوفيس مثلاً ، وهذا يمكن تغطيته بكورس الـ **ICDL** (International Computer Driving License) الرخصة الدولية لقيادة الحاسب الآلي .



وأنا اعتقد أن أغلبكم يعرف مثل هذه المعلومات وإلا ما كانت وصلت تلك المجلة ولا قرا هذا المقال ...

لكن ما لابد لك أن تتعلمه وهو شيء هام جداً في طريقك هو صيانة الحاسب الآلي ، مثل مكوناته وأنواعها وتركيبه وتحميل نظام التشغيل عليه وأنواع نظم التشغيل مثل الويندوز

وكذلك تركيب البرامج من أول الأوفيس لغاية الجافا وإصلاح المشاكل في الهاردوير أي الصيانة أو السوفت وير أي البرامج و... إلخ

والكورس الذي يغطي هذه الجزئية وبشكل ممتاز هو كورس A+ كورس الصيانة المتقدم .

إذن البداية بكورس A+ وهذا الكورس مقدم من خلال شركة CompTIA !!! كومبتيا

ليس الآن وقت التفاصيل أعرف أن همتك العالية تجعلك الآن تريد أن تعرف معلومات كثيرة عن هذا الكورس مثل مدته والمناهج الخاص به وأين يدرس وتكلفتها واختباراته ومن هي CompTIA هذه ، لكن إتفقنا ألا تستعجل خلينا نتفق على نقطتين الأولى : أننا مازلنا في الحلقة الأولى من السلسلة وهناك حلقات ستكون مخصصة للكلام عن كل كورس سأذكره بالتفصيل وخصوصاً الشركة المقدمة لهذا الكورس ...

الثانية : أننا سننتج أسلوب التأصيل ثم التفصيل بمعنى أننا سنذكر الخطة التي سنسير عليها بالكامل ملخصة ، خطتي خلال الثلاث سنوات القادمة ، ثم نبدأ بشرحها تفصيلياً والله الموفق ، نسألكم الدعاء ...



سؤال لطالما تكرر في الكورسات والمنتديات من الأفاضل الأعضاء وخصوصاً الشباب ، أو ممن قرأ في المجال أو سمع عنه وأعجبه ، أو أراد أن يطور من نفسه للحصول على وظيفة أفضل وخصوصاً في مجال الـ IT تكنولوجيا المعلومات ، والذي أشتهر عنه أنه أعلى المجالات رواتب وأقلها في ساعات العمل فزاد الإقبال عليه .

وهو في الحقيقة سؤال محير فعلاً ، فكلنا في البداية مر به هذا السؤال وتلك الحيرة ، ففي بداية الطريق يكون الشخص متخوف وتائه وحيران لما يسمع من كلام كثير وبعض هذا الكلام يناقض بعضه بعضاً ، وهو لا يدري أين الصواب ؟ ولا أين الإتجاه الصحيح ؟ بل هناك من يزيد هذا الكلام الكثير حيرة على حيرته وخوف على خوفه ، حتى إن بعضهم يحكي لي أنه جلس ثلاث سنوات محتار لا يعرف كيف يبدأ ؟ بل وبعضهم قرر أن هذا المجال محال وهرب بجملده كما يقولون ...

من أين يبدأ وكيف يبدأ ؟ وما هو المفيد حسب الموقع الجغرافي (بلد الإقامة أقصد لأن كل بلد لها ظروفها الخاصة) ؟

قد يقول البعض لعل هذا المقال سيزيدني حيرة فوق حيرتي سأغلقه ***
أنصحك لا تفعل استمر معي للنهية وسترى النور بعينيك ، فوالله الذي لا إله غيره ما كتبت هذا الكلام إلا بعد عناء طويل أخذ من عمري سنين بل أستطيع أن أقول أنني رويت بداية هذا الطريق بدمي ، فبدل أن تضع مثل هذه السنين وهي غالية اسمع مني لدقائق لعلك تستفيد ...
إتفقنا إذن لنبدأ ...



أسئلة كثيرة تدور في خلد المبتدئين ولا يعرفوا لها إجابة وأحببت أن أنزع فتيل هذه الحيرة حتى أفجر تلك الطاقات المكبوتة عند شباب المسلمين حتى يشعلوا نهضة هذه الأمة من جديد .

ولا أعرف إن كان أحد الأفاضل قد سبقني وأدلى بدلوه في مثل هذا الموضوع أم لا ؟؟؟ ولعلي أستفيد ، لكن هو جهد المقل فما كان فيه من خطأ فمن نفسي ومن الشيطان ، والله ورسوله منه براء ، وما كان فيه من توفيق فمن الله وحده لا شريك له .

كما أن هذا يعبر فقط عن وجهة نظر خاصة وشخصية تكونت لدي من خلال سنين الخبرة قد يوافقتني فيها البعض وقد يختلف معي فيها آخرون ، والخلاف لا يقصد للود قضية .
وحتى وإن كان أحد أجاب قبلي على مثل هذه التساؤلات لكن ما رأيته أحداً أفرد لها موضوعاً مستقلاً بل سلسلة من المقالات ، فأردت أن أجعلها سلسلة مستقلة من المقالات تحت نفس هذا العنوان بحيث يحيل إليه الإخوة الأفاضل أي أحد من الشباب الجدد والذين يسألون مثل هذه التساؤلات ؟؟؟

وأرجو من الله العون والتوفيق ، اللهم مدني بمددك أعرف أنني أطلت عليكم في مقدمتي لكن كما يقولون " اللي أوله شرط آخره نور " ، ولنبدأ



وأقول بعد باسم الله فكل عمل لا يبدأ فيه باسم الله فهو منزوع البركة ، ولا نخطط لمستقبل باهر ...



الكورس الثاني ::::

بعد إتقانك لأساسيات الصيانة ، لابد أن تتعلم أساسيات هذا العلم ، علم الشبكات ...
فالشبكات والله العظيم ولا أكون مبالغ علم عظيم من علوم هذا العصر ، علم يحتاج لأعمار
فيه تفنى لكن الله الموفق ، نسأل الله أن يبارك لنا في أعمارنا وأن يعمرها بما ينفعنا في الدنيا
والآخرة

لذلك البداية لابد وأن تكون من شركة أو منظمة حيادية غير منحازة لمنتجاتها على حساب
المنتجات الأخرى من الشركات المنافسة ، وتلك المنظمة هي نفسها CompTIA فهي جهة
غير هادفة للربح وليس لها أي منتج تنحاز له سنوضح ذلك لاحقاً .

فمثلاً Cisco سيسكو كل كورساتها تطبق المفاهيم العلمية للشبكات على أجهزتها فقط ،
ليل نهار تتحدث عن التكنولوجيا الخاصة بها

وأيضاً Microsoft مايكروسوفت كذلك ليل نهار تتحدث عن التكنولوجيا الخاصة بها
يعني بعد كورس A+ بأي كورس أبدأ ؟ إبدأ بـ Network+

شركة CompTIA تقدم كورس في مبادئ وأساسيات الشبكات يسمى Network+
تتكلم فيه عن الشبكات كعلم وليس كشرح آلية عمل منتج معين .

لكن ما تكلفتها ومدتها اتفقنا أننا سنكتب مقالات خاصة عن كل كورس من هذه الكورسات
، لكن عموماً هذه الكورسات غير مكلفة ووقتتها ليس بالطويل .

إلى اللقاء في الحلقة القادمة

تقرأون في هذه الحلقة ::::

مهندس شبكات محترف في ثلاث سنوات

الكورس الأول : A+

الكورس الثاني : Network+

تقرأون في الحلقة القادمة ::::

ما هي الكورسات التالية ؟؟؟

لا تيأس من روح الله ...

لابد وأن تقوي نفسك في اللغة الإنجليزية ...

الآن تستطيع أن تعمل في مجال الـ IT ...

... CCNP, CCNA, Network+

تعرف على تقنية الـ

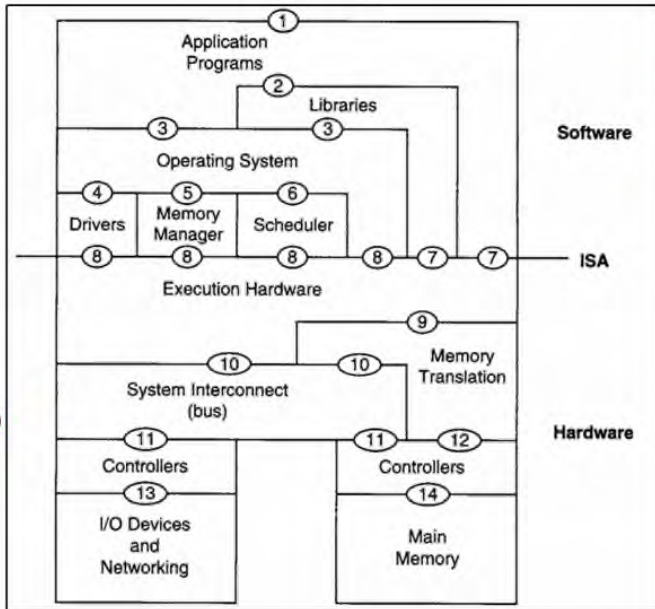
Virtualization

بقلم : أيمن النعيمي

Virtualization أو التمثيل الافتراضي تلك الكلمة التي شدت العالم بأسره إليه وكثيرة هي الأسئلة التي طرحت حولها ولم تجد لها أجابة وهذا ماسوف أقدمه لكم في هذا المقال البسيط الذي سوف أستعرض فيه كيفية وأسباب نشوء هذه التقنية بالإضافة إلى الفوائد التي تحققها هذه التقنية

مقدمة

قد يعتقد البعض أن هذه التقنية هي حديث العهد نتيجة التطور الكبير الذي نراه كل يوم في أجهزة الكمبيوتر أو العتاد المكون لها والحقيقة غير ذلك أبداً لأن بدايات هذه التقنية قديمة جداً وتعود إلى عام 1960 وأول من طورها كانت شركة IBM أو International Business Machines فكما هو معروف أن أجهزة الكمبيوتر في ذلك العصر وأخص بالذكر جهاز (M44) IBM 7044 كانت تقوم بعملية معالجة واحدة كل مرة والذي انعكس سلباً على مقدرة المعالجات للعمل وخصوصاً أن تطوير قوة المعالجات لم يكن بالأمر الصعب والتي كانت سبب في ولادة تقنية التمثيل الافتراضي التي أتاحت استخدام قوة المعالج من قبل عدة أشخاص من خلال تقسيمه إلى عدة أجهزة وهمية يتم التحكم بها من خلال أجهزة مخصصة أو Client وبالتالي أتاح لهم إمكانية تشغيل أكثر من تطبيق في نفس الوقت، وقد واجهت هذه التقنية في حينها مشاكل كثيرة مثل عدم تمكين العملاء من تشغيل البرامج الغير آمنة untrusted لأن أدائها يمكن أن ينعكس سلباً على النواة بشكل عام بالإضافة إلى عدم مقدرة كل عميل القيام بأي عملية تحديث أو ترقية للنظام الخاص به وأخيراً لم يكن هناك إمكانية للتحكم بتقسيم العتاد بشكل منصف بين أجهزة العملاء .



فكما هو واضح أن للكمبيوتر عدة طبقات

الطبقة الأولى خاصة بي البرامج أو Software وهي يحد ذاتها مقسمة لعدة طبقات ونستطيع أن نشاهد أن هناك برامج تعمل من خلال الاتصال بالهاردوير بشكل مباشر وهناك من يتصل بطبقة المكتبات التي تخص نظام التشغيل والخ...

الطبقة الثانية Instruction Set Architecture أو ISA وهي الطبقة التي تفصل طبقة الهاردوير عن السوفت وير وهي النقطة التي بنى فيها المطورون أول أفكار تقنية التمثيل الافتراضي الطبقة الثالثة وهي طبقة الهاردوير وهي توضح المدخلات والمخرجات الخاصة بالكمبيوتر



كيف تعمل هذه التقنية

يحتاج منك لفهم كيف تعمل هذه التقنية الكثير من الوقت والكتب لكن سوف أقدم لحة بسيطة عن مبدأ عملها لذا دعوني أولاً أقدم لك هذا المخطط الذي يوضح الطبقات الموجودة في الكمبيوتر



Xen 3.0: أحد الأنظمة المفتوحة المصدر والتي تحوي على حوالي 50.000 سطر من الاوامر وهي تعمل على كل من معالجات Intel or AMD x86 and 64bit



VMWare: وهي الأشهر في هذا المجال والأكثر تحميلا بين باقي الأنظمة وخصوصا بعدما اتاحة برامجهما للتحميل بشكل مجاني وهي تملك عدة برامج فمنها من يعمل من خلال أنظمة التشغيل نفسها مثل VMWare-Player أو VMWare-Server بالإضافة إلى وجود نظام تشغيل يدعى VMWare ESX Server خاص بأدارة عملية التمثيل الافتراضي أو كما قمنا بتعريفها من قبل بي Hypervisor



Windows Server 2008
Hyper-V™

Microsoft: وهي تعرف بي Hyper-v وهو النظام المطور من خلال مايكروسوفت والذي أصبح جزء من ويندوز سيرفر 2008



Sun VirtualBox: أيضا نظام تشغيل مفتوح المصدر مشابه لي XEN

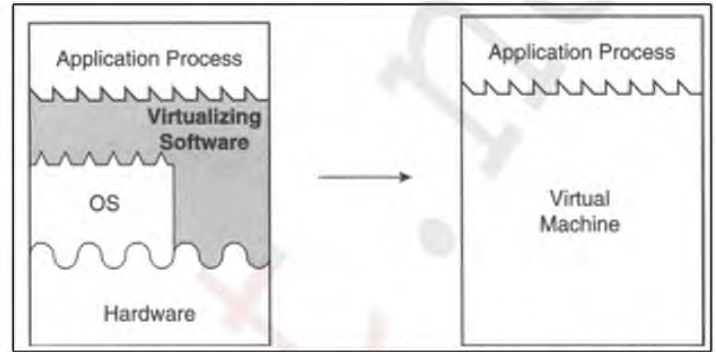
CITRIX®

Citrix XenServer: نظام مبني على Xen Hypervi- sor وهو مجاني أيضا

Virtual Iron
IBM Virtualization Engine Platform
SWSOFT Virtuozzo
OpenVZ
Linux-VServer
QEMU

هذه كانت لحة بسيطة عن هذه التقنية الرائعة وأن كنت لم أغطي كل شيء عنها في هذا المقال فهي أكبر بكثير من أن يتم تغطيتها بمقال واحد والذي سوف أتركه لكم في العدد القادم

فمن خلال طبقة ISA قام المطورون بتطوير تقنية التمثيل الافتراضي لتمثل لنا بهذه التقسيم البسيطة الموضحة بالصورة القادمة والتي تتيح إمكانية التحكم في موارد الهاردوير الموجودة من خلال نظام تشغيل خاص بها يدعى hypervisor أو virtual machine monitor (VMM) والتي بدورها تسمح لنا بتنصيب أكثر من نظام تشغيل ومراقبتها وأعدادها طبعا



وكما ذكرت أن الموضوع يحتاج الكثير من الشروحات والتحليلات ولأنني أردت أن يكون الموضوع مفهوم لجميع الفئات وأنصح أي شخص يريد أن يعرف أكثر عن آلية العمل أن يقرأ كتاب Virtual Machine الذي كتب بواسطة James E. Smith & Ravi Nair

ماهي الفائدة التي نحققها

وهو السؤال الأهم في موضوعنا ما الذي توفره لي هذه التقنية ولستعرضها بالتسلسل التالي:

توفير المال: من أكثر الحقائق غرابة أن أغلب أجهزة الكمبيوتر الموجودة في عصرنا لاتستخدم أكثر من 10% من قدرتها وطاقتها وطبعاً هذه الحقيقة ترجعنا إلى عام 1960 وهي لماذا لا أستفيد من طاقة المعالج بشكل كامل وفي نفس الوقت أوفر على نفسي المال لشراء كمبيوتر آخر يقوم بأعمال أخرى

توفير الوقت: من خلال نظام تحكم واحد سوف تستطيع الوصول إلى كل الأجهزة والسيرفرات الموجودة لديك وبالتالي سرعة في اكتشاف الأخطاء وإصلاحها زد على ذلك سرعة القيام بعمليات الصيانة الدورية والتي تشمل أمور مثل backup, archiving and recovery فمن قبل كان يتطلب منك تنصيب ويندوز سيرفر وأعداده حوالي الثلاث ساعات لكن مع التمثيل الافتراضي لن يستغرق معك الأمر أكثر من اثنتين من خلال القيام بعمل صورة لنظام التشغيل

توفير الطاقة: أن التوفير التي تقدمها لنا تقنية التمثيل الافتراضي في الطاقة كافية لأن تكون هي الفائدة الوحيدة لها فمن خلال تقليل عدد السيرفرات التي تعمل إلى أكثر من النصف سنجد أن الطاقة التي تخصص لها قد نقصت بمعدلات كبيرة والتي أكدها مستخدم برنامج VMWare الذين صرحوا بتوفير حوالي 60% من الطاقة المستخدمة

توفير في الشبكات: فكما هو معروف أن الربط بين السيرفرات الحقيقية يحتاج منك سويتشات وروتات تقوم بهذه العملية لكن مع تقنية التمثيل الافتراضي سوف تقوم بهذه العملية بشكل مجاني وبأداء وسرعة قد تكون أفضل وأمن من الشبكة العادية.

سهولة التحكم: فمن خلال جهاز واحد سوف تستطيع الوصول لجميع الأجهزة أو Desktop الخاص بكل كمبيوتر بالإضافة إلى إمكانية مراقبة أداء وعمل كل الأجهزة من شاشة مراقبة واحدة تعطيك كل التفاصيل المطلوبة

الأمان والحماية: فمن خلال الأجهزة الوهمية الموجودة تستطيع أن تقوم بتجربة بعض البرامج الغير آمنة والتأكد من خلوها من أي فايروسات أو ديدان خبيثة وبالتالي حماية سيرفرك منها

إمكانية تنصيب واستخدام عدة أنظمة تشغيل على جهاز واحد مثل ويندوز لينوكس أبل دوس .

هذه كانت أهم الفوائد التي تحققها لنا تقنية التمثيل الافتراضي وهناك أيضاً المزيد من الفوائد التي تختلف بحسب أنظمة التشغيل التي تقوم باستخدامها وهذه لأثمة بأهم الشركات المطورة لهذه التقنية



كيف تقوم بتأسيس شبكة فويس من الصفر (VOIP)

بقلم أحمد الشحات

سوف أحاول في هذا الموضوع شرح طريقة أعداد شبكة فويس من الصفر لذا سوف يكون الموضوع مقسم لعدة أجزاء وسوف يتم نشر باقي الأجزاء في الأعداد القادمة آن شاء الله وسوف يقتصر هذا الموضوع على مقدمة حول البروتوكول وتوضيح فوائد استخدامه .

مقدمة

Viop هو اختصار لكلمة Voice Over Internet Protocol وهي عبارة عن نقل الصوت عبر الشبكة الى تستخدم البروتوكول IP وهذا يشمل النقل عبر الأنترنت او عبر الشبكات العادية ويعود تاريخ هذه الفكرة الى عام 1995 بواسطة بعض المستخدمين العاديين للأنترنت والتي تطورت لتشمل نقل الصوت والصورة ولتمكين هذه الخدمة نحتاج الى أجهزة تلفون خاصة تدعى بي IP Telephony والتي سوف يتم التطرق إليها في الأجزاء القادمة .

طريقة النقل

في نقل الصوت عبر الشبكة يتم تحويل الصوت من analog الى رقمي ويتم تقسيم الإشارة الى حزم صغيرة يسهل نقلها ويتم النقل في عدة مسارات لضمان سرعة الوصول وعند وصولها الى جهة الوصول يتم تجميعها مرة أخرى بعكس الاشارات ال analog القديمة حيث أنها تأخذ مساراً واحداً فقط للوصول الى المستمع وإذا كان المستمع في جهة الوصل من النوع analog فيتم تحويلها مرة أخرى الى analog لكي يستطيع الجهاز فهمها

فوائد استخدام VOIP

عندما بدأ موضوع نقل الصوت عبر الشبكة VOIP المعظم قالو ما الفائدة لو ارسلنا الصوت عبر الشبكة والفائدة الوحيدة ستكون هي توفير ثمن الكابلات فقط ولكن عند البحث في فوائد نقل الصوت عبر الشبكة سوف نجد فوائد كثيرة سوف نستعرضها الآن

تقليل ثمن المكالمات

حيث أن المستخدمين للشبكة يستطيعون عمل أي عدد من المكالمات فيما بينهم مجاناً ليس هذا فقط بل أن هناك ستكون Dial Plan دائمة يستطيع فيها المستخدمون الاتصال فيما بينهم مجاناً ومن خلال تحويلة مكونة من أربعة أرقام مثلاً وفي جميع أنحاء العالم لنفس الشبكة فمثلاً لو كان لديك شركة في السعودية واحد فروعها في مصر والفرع الآخر في سوريا وهكذا فإن الموظفين سيتصلون مجاناً فيما بينهم وبتحويلة داخلية فقط ولا داعي للاتصال بالأرقام الدولية ومفاتيح الخطوط الدولية

تقليل تكلفة تمديد الكابلات بطريقة رهيبة

حيث أنه النقل يتم عبر كابلات الداتا فلن نستخدم كابلات الفويس وتخيل لو مشروعك يقع بين عدة مدن وطبعاً تستطيع أن تتخيل التوفير الذي تم من عدم استخدام كابلات الفويس

سلاسة وانسيابية الشبكة

كما قلنا ان النقل يتم عبر شبكة الداتا التي هي اصلاً قد قامت بتوصيل المكاتب والمستخدمين من قبل فأن شبكة الصوت تلقائياً تراث تلك الخصائص عن شبكة الداتا وتصل لنفس المدى الذي تصله شبكة الداتا بدون برمجة اضافية او تكلفة اضافية ليس هذا فقط بل أن هناك تحكم مركزي بكل الاجهزة المتصلة بالشبكة

التنقل بالتليفون بسهولة

الآن أي موظف يستطيع حمل تليفونه الى المكتب المقابل او الطابق الآخر وبمجرد توصيله بالشبكة سيأخذ نفس الاعدادات القديمة وبدون برمجة اضافية كما انه لو كان هناك اتصال VPN فإن الموظف يستطيع مل تليفونه معه الى المنزل ويأخذ نفس الاعدادات

Ip Soft Phones

يعتبر برنامج سوفت فون مثال رائع عن طريقة اندماج شبكة الداتا مع الفويس فالآن بمجرد وصل سماعة صغير وميكروفون بالكمبيوتر الخاص بك تستطيع ان تعامل مع الشبكة كأن لديك تليفون حقيقي كمان ان برنامج سوفت فون الآن يتكامل مع التطبيقات الأخرى مثل الماسينجر وجهات الاتصال والايمل

توحيد الرسائل

الآن تستطيع استقبال جميع الرسائل في صندوق بريد واحد سواء كانت فاكس او رسالة صوتية او ايمل

زيادة الإنتاجية

توجد ميزة في VOIP وهي انك تستطيع ان تجعل أكثر من تليفون يرن قبل ذهاب الرسالة الى الفويس ميل ولذلك في حالة عدم وجود الموظف سيرد موظف آخر بدلاً عنه ويقوم بإنهاء المهمة بدلاً من الموظف الهارب

تكامل أنواع مختلفة من الأجهزة

الآن تستطيع العمل مع أجهزة مختلفة في الشبكة الواحدة ممكن يمكنك من اختيار الأفضل لشبكتك بدون التعقيد بمصنع وحيد وفي العدد القادم سنتكلم عن شكل وتركيب شبكة الفويس ان شاء الله .

JNCIA JNCIS

Juniper Networks Technical Certification Program (JNTCP)
Firewall/VPN Track

JNCIA JNCIS → JNCIE

Juniper Networks Technical Certification Program (JNTCP)
Enterprise Routing Track

JNCIA JNCIS → JNCIP → JNCIE

Juniper Networks Technical Certification Program (JNTCP)
M/T-series Routers Track

E Series Track

هذه الشهادة خاصة بالتعامل مع أجهزة جونيبر من الـ Series E وفيها 3 مستويات

JNCIA JNCIS → JNCIP

Juniper Networks Technical Certification Program (JNTCP)
E-Series Routers Track

وهي تتحدث عن المواضيع التالية & virtual routers, BRAS, routed & bridged 1483, PPP over ATM, PPP over Ethernet, dynamic configuration mode, L2TP, policy management
وهذه لائحة بأرقام الامتحانات ومتطلباتها

الشهادات المطلوبة	رقم الامتحان	E Series
لا يوجد	JNO-120	JNCIA-E
لا يوجد	JNO-130	JNCIS-E
JNCIS-E	CERT-JNCIP-E	JNCIP-E

Firewall/VPN Track

لهذه الشهادة مستويان فقط المبتدئ Associate والمختص Specialist وكما هو موضح بالصورة التالية

JNCIA JNCIS

Juniper Networks Technical Certification Program (JNTCP)
Firewall/VPN Track

وهي تتحدث عن المواضيع التالية: VPNs, Network Management, Troubleshooting with Debug & Snoop, Traffic Management, Virtual Systems, NSRP, Dynamic Routing/Routing over VPNs, Attack Prevention, Multicast ومتطلباتها

الشهادات المطلوبة	رقم الامتحان	Firewall/VPN
لا يوجد	JNO-522	JNCIA-FWV
لا يوجد	JNO-532	JNCIS-FWV

هذه كانت اهم الشهادات برشي الشخصي وليس كلها لان في جونيبر هناك المزيد من الامتحانات وهذه لائحة بباقي الامتحانات

Intrusion Detection & Prevention (IDP) Track

SSL Track

DX Track

WX Track

Unified Access Control (UAC) Track

وعلى هذا الرابط تستطيع إيجاد تفاصيل أكثر عن الشهادات

www.juniper.net/us/en/training/certification

دليلك نحو شهادات جونيبر

أعداد: أيمن النعيمي

تملك جونيبر عدد كبير من الشهادات العلمية المختلفة والتي تغطي كل منتجاتها في الشبكات وأن كان البعض منها تجاري بسبب تكرار المواضيع فيها لذا سوف احاول في هذا الموضوع القاء الضوء على اهم الشهادة الموجودة وأرقام الامتحانات الخاصة بها قبل أن نبدأ أريد أن ألفت انتباهك إلى شيء مهم وهو فهمك لمنتجات جونيبر يساعدك في اختيار الشهادة الافضل للدراسة وقد تم شرح منتجات جونيبر في العدد السابق ولنبدأ

Enterprise Routing Track

شهادة الراوتينغ وهي تتألف من 3 مستويات المبتدئ Associate والمختص Specialist والخبير Expert

JNCIA JNCIS → JNCIE

Juniper Networks Technical Certification Program (JNTCP)
Enterprise Routing Track

وهي تتحدث عن كيفية إدارة الراوتر والبروتوكولات الخاصة بالروتينغ مثل OSPF, BGP, RIP, NAT, VPN وأرقام الامتحان على الشكل التالي

الشهادات المطلوبة	رقم الامتحان	M&T Series
لا يوجد	JNO-201	JNCIA-M
لا يوجد	JNO-303	JNCIS-M
JNCIS-M	CERT-JNCIP-M	JNCIP-M
JNCIP-M	CERT-JNCIE-M	JNCIE-M

Enterprise Switching Track

للسويتش هناك شهادة واحدة فقط وهي JNO-400 وهي بمرتبة مبتدئ Associate

Junos Security Track

لهذه الشهادة امتحان واحد وهو JNO-331 هو بمرتبة Specialist ولكي تستطيع أن تتقدم لهذا الامتحان يتوجب عليك ان تحصل على أحد هذه الشهادات: JNCIA-JUNOS or JNCIA-ER or JNCIA-M

وهي تتحدث عن المواضيع التالية: Introduction to SRX-series, Zones, SCREEN Options, Security Policies, NAT, IPSec VPNs, HA Clustering, Intro to IDP, Firewall User Authentication

M Series & T Series Track

هذه الشهادة خاصة بالتعامل مع أجهزة جونيبر من الـ Series M&T ولها أربع مستويات كما هو واضح من الصورة

JNCIA JNCIS → JNCIP → JNCIE

Juniper Networks Technical Certification Program (JNTCP)
M/T-series Routers Track

وفيها مواضيع مكررة مع امتحانات الراوتينغ (ER) وهي بشكل عام تتحدث عن BGP, OSPF, IS-IS, and RIP, routing policy, firewall filters, CoS, MPLS, VPNs, IPv6, and multicast

وهذه لائحة بأرقام الامتحانات ومتطلباتها

الشهادات المطلوبة	رقم الامتحان	M&T Series
لا يوجد	JNO-201	JNCIA-M
لا يوجد	JNO-303	JNCIS-M
JNCIS-M	CERT-JNCIP-M	JNCIP-M
JNCIP-M	CERT-JNCIE-M	JNCIE-M

نتائج الأستفتاء الشهري

نتائج الأستفتاء

ماهو أفضل منتدى عربي للشبكات ؟

- منتديات عرب هاردوير

87%

- منتديات أخرى

4%

- منتدى بوابة العرب التعليمية

4%

- منتديات برامج نت

2.5%

- منتدى المهندسين العرب

1.5%

- منتديات الفريق العربي

1%



مع 135 مصوت تم اغلاق الاستفتاء الأخير على المدونة وطبعا العنوان ما هو أفضل منتدى عربي للشبكات وصراحة نتائج التصويت كانت مخالفة بعض الشيء لتوقعاتي. فقد توقعت أن يكون عرب هاردوير

هو الرابح الأكبر لكن ليس بهذه النسبة العالية وهذا يدل على الثقة الكبيرة التي نالها هذا المنتدى في عالم الشبكات وسبب نجاح منتديات عرب هاردوير في عالم الشبكات برائي يعود إلى سببين -السبب الأول وهو سبب نجاح أي منتدى في العالم هو الانضمام أنفسهم فيوجود نخبة كبيرة من الأعضاء تقوم بتقديم المساعدة وإرشاد باقي الأعضاء إلى أمور الشبكات وكورساتها وطريقة حل مشاكلها كان من أقوى الأسباب التي أدت إلى نجاح المنتدى ب-الانسانة والمشرفين الموجودين في المنتدى والذي لهم دور فعال في نشر العلم وأخص منهم الأستاذ محمد سمير والأستاذ لومارك وأحمد سرحان وأحمد جودة وطبعا الأستاذ ياسر رمزي بالإضافة إلى باقة كبيرة من الانسانة .

والكلمة الأخيرة التي احب أن أضيفها هي أن منتديات عرب هاردوير قد حولت عالم الشبكات إلى تاريخان تاريخ الشبكات قبل عرب هاردوير وتاريخ الشبكات بعد عرب هاردوير ونيابة عني أشكر جميع القائمين على المنتدى من إداريين مشرفين مؤسسين والشكر الأكبر للأعضاء التي تساهم فيه دائما وبشكل إيجابي

شجع هذا النوع من المجالات بوضع أعلانك هنا

أنواع كوابل الإيثرنت وكيفية اختيار الكبل المناسب

بقلم أيمن النعيمي



لنتفق أولاً على أن كوابل الإيثرنت ليست متشابهة وهي تختلف بحسب قدرة الكبل على نقل البيانات فيها ونستطيع أن نفرق بينها من خلال أما النظر أو من خلال قراءة ماكتب عليها لكننا سوف نقع في حيرة من أمرنا لأن هذا النوع من الكوابل له الكثير من الأنواع ولفهمها يجب أن نعلم أن للكوابل تصنيفات عالمية أو مايعرف بي Categories وقد صدر منها حتى الآن 7 تصنيفات وفهمك لهذه التصنيفات يعطيك القدرة على اختيار الكبل المناسب للعمل والذي يتناسب مع متطلبات العمل لديك وطبعا هذه التصنيفات ليست كلها لتقنية الإيثرنت بل يوجد استخدامات أخرى لذا لن اكتفي بعرض تصنيفات الإيثرنت فقط بل سوف أقوم بعرض كل التصنيفات للفائدة العامة مع الإشارة إلى استخدام كل نوع منها

CAT 1

وهي اختصار لكلمة Categories وهو أول وأقدم تصنيف وغير متعلق بتقنية الإيثرنت وهو يستخدم عادة في كوابل الهاتف وخطوط الـ ISDN

CAT 2

التصنيف الثاني هو أيضا غير متعلق بتقنية الإيثرنت واستخدامه محصور في ميغا بت في الثانية 4 وتصل سرعته القصوى إلى Token Ring شبكات الـ 1 MHz وبتردد

CAT 3

وهو أول كوابل الإيثرنت وسرعته تصل إلى 10 ميغا بت وبدأ استخدامه في بداية التسعينات ولكن توقف استخدامه في الشبكات بعد ظهور CAT 5 ولينحصر استخدامه الآن في الاتصالات أو عبر مايعرف بي VoIP telephone وبتردد وصل إلى 16 MHz وهذه صورة توضيحية للكابل



CAT 4

هذا التصنيف أيضا يتبع شبكات الـ Token Ring وهو عبارة عن أربع أزواج من الأسلاك وتصل سرعة النقل إلى 16 ميغا بت وبتردد 20 MHz

CAT 5

قام هذه النوع من الكوابل بأحداث نقله نوعية في الشبكات بتوفيره سرعة كبيرة مقارنة بأقرانه السابقين والتي وصلت إلى 100 ميغا بت وهو يعمل مع تقنية الإيثرنت ويصلح لكي يعمل مع تقنية نقل الصوت والـ Token Ring والـ ATM

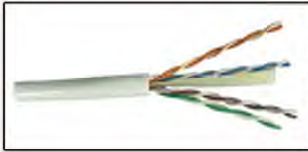


CAT 5E

كما واضح من الاسم يعد هذا التصنيف شكل متقدم عن الـ CAT 5 ومايميزه هو دعمه لي Ethernet Gigabyte وتصل سرعته إلى 125 ميغا بت كحد أقصى

CAT 6

هو التصنيف الرسمي لي Gigabyte Eth- ernet وسرعته تصل إلى ضعف سرعة CAT 5e أي حوالي 250 ميغا بت وهذه صورة توضيحية



CAT 6A

أيضا تصنيف مطور من السابق وبسعة نقل وصلت إلى الضعف لدعم الـ 10Gigabyte Ethernet أي حوالي 500 ميغا بت

CAT 7

وهو التصنيف الرسمي لي 10Gigabyte Ethernet وبسرعة تجاوزت التصنيف السابق لتصل إلى 600 ميغا بت وقد تم عزل كل زوج من الأسلاك عن الآخر بشكل كامل كما هو موضح بالصورة



CAT 7A

تصنيف مطور عن السابق لدعم السرعات التي تصل إلى 100Gigabyte Ethernet وبسرعة وصلت إلى 1000 ميغا في الثانية



شهادة جديدة من سيسكو CCNA SP

أعلنت سيسكو بتاريخ 5-أيار/مايو عن طرح شهادة جديدة خاصة بي Service Provider بمستوى مبتدأ Associate وليكتمل الهرم الخاص بهذه الشهادة وتحمل هذه الشهادة الرقم 640-760 وتحمل الاسم التالي Supporting Cisco Service Provider IP NGN Operations (SSPO) وهي تتحدث بشكل عام عن المبادئ الرئيسية في أعداد مخدمات الأنترنت بالإضافة إلى مقدمة عن IP NGN أو IP Next-Generation Network وهي طبعا الجيل الجديد من أجهزة سيسكو CRS وهذه لائحة بمحتويات هذه الشهادة

CCNA Service Provider



Perform the network incident management process

Describe how a trouble ticket processes through the network operations center(NOC)
Identify key network incident metrics in a NOC incident report
Apply an incident management process
Perform incident management using basic tools and documentation
Close an incident ticket
Prioritize incident tickets according to standards
Escalate an incident ticket according to typical criteria
Create an RFC to implement a fix or workaround for an incident

Apply the problem management process

Apply the Information Technology Infrastructure Library (ITIL) problem management process to the task of managing networks
Distinguish between incident management and problem management, and determine the interactions that occur between them

Perform first-level network monitoring and troubleshooting

Use network management tools to monitor network status
Interpret device specific alarms and determine the severity of the alarm
Initiate troubleshooting procedures based on received alarms and/or log messages
Use network management tools to troubleshoot first-level network incidents
Use syslog functions, severity levels, syslog traps, and buffering
Use knowledge of IP fundamentals to determine the most likely cause of a network problem
Determine the most probable cause of a problem from standard output and SNMP traps
Utilize common structured troubleshooting approaches

Perform network configuration management

Backup configurations across standard NOC architectures
Interpret basic standard scripting commands used in automating network maintenance
Interpret basic UNIX cron job commands used in automating network maintenance
Use a network inventory management process

Implement network changes and change management

Accurately document a network
Utilize a network change implementation rollback
Implement a network change based on change documentation
Perform a network upgrade
Identify upgrade or downgrade issues and recommend corrective actions
Verify the usability and effectiveness of a network change

Apply the fundamental concepts of service level agreements (SLAs)

Identify the unique characteristics of different SLAs
Inform customers about SLA issues
Monitor service levels against the requirements of an SLA

Describe basic IP technology in the Service Provider NOC

Describe the purpose and components of an IPv4 address
Describe the purpose of and components of IOS XR
Use IOS XR to perform basic router functions
Compare and contrast IPv4 to IPv6 addresses



كيفية تفعيل J-Web والحصول على كل مميزاته

عودة مره أخرى مع جونيبر وهذا المرة لكي نقوم بتفعيل J-web والتي من خلالها تستطيع أن تتحكم بالروتير أو السويتش من خلال واجهة رسومية تتيح لك أن تقوم بجميع الإعدادات اللازمة بالإضافة الى الكثير من أقسام المراقبة الخاصة بالأداء وهي طبعا مشابهة لعمل الSDM الموجودة في أجهزة سيسكو. ولكي تتم عملية التشغيل يلزمنا J-web Package الخاصة بكل إصدار من JUNOS ويتم تحميلها أولا على الروتر وبعدها نقوم بتسويتها على نظام التشغيل JUNOS والشرح سوف يكون على النسخة الخاصة بالإصدار 9.0 وسوف يكون بمساعدة Olive + VMware من خلال عدة مراحل

المرحلة الأولى

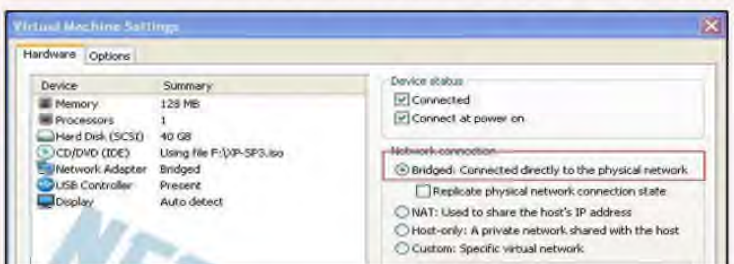
هي تثبيت سيرفر FTP على ويندوز أكس بي مثبت على VMWare والهدف منه تكوين سيرفر نستطيع من خلاله أن نسحب الباكيج الى داخل الروتر وطريقة تثبيته بسيطة جداً تتبع الترتيب التالي -> Start -> Add/remove --> add/remove windows components --> Internet Information Services IIS بأختيار FTP Service كما هو موضح بالصورة



بعد الانتهاء من التنصيب سوف يظهر مجلد جديد على السي اسميه Inetpub وبداخله ملف ftproot هذا الملف قم بوضع الباكيج الخاصة بالJ-web وبعدها سوف أعطي كرت الشبكة الإعدادات التالية

IP 192.168.1.2
Mask 255.255.255.0
Gateway 192.168.1.1

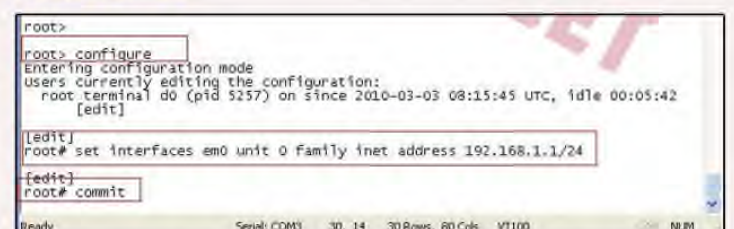
ولاننسى أن نضع إعدادات الشبكة الخاصة بي الVMware كما هو موضح بالصورة حتى يكون هناك جسر بين الويندوز والروتير أي على الروتر وعلى الويندوز يجب أن نضع نفس الإعدادات



المرحلة الثانية

نتوجه الى روتر جونيبر ونقوم بأعطاء الانترفيس أيبى بالدخول على الconfigure mode وتطبيق الأوامر التالية

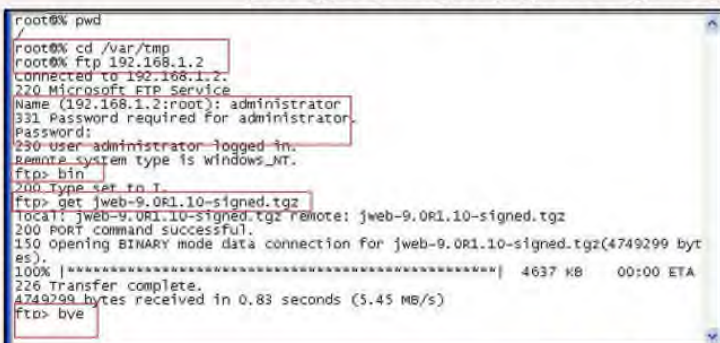
root# set interfaces em0 unit 0 family inet address 192.168.1.1/24
root# commit



وبعدها نقوم بالتأكد من وجود اتصال بين الويندوز والروتير من خلال الأمر Ping

المرحلة الثالثة

هي الاتصال مع سيرفر ال FTP وسحب الباكيج الى داخل الروتر وذلك من خلال الأوامر الموضحة بالصورة التالية



المرحلة الرابعة

تثبيت الباكيج على الروتر من خلال الأوامر التالية

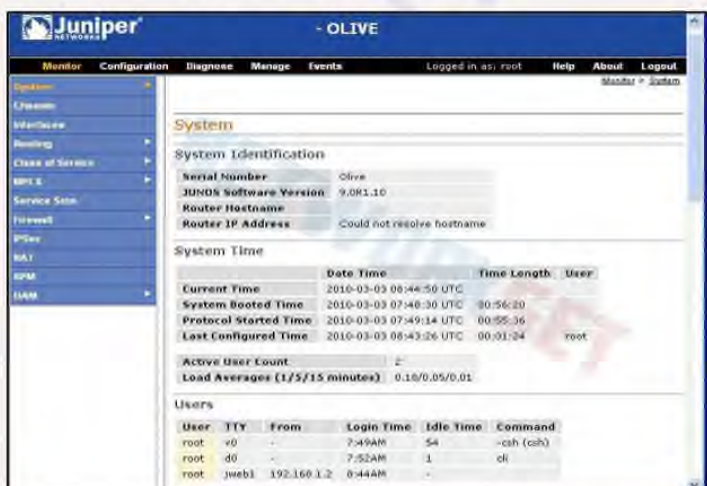


بقي علينا أمر واحد وننتهي من الإعدادات وهي تفعيل ال Http على البورت الذي سوف نقوم بالاتصال عليه من الويندوز وذلك من خلال الأمر التالي:

root# set system services web-management http interface em0

root# commit

نذهب الآن الى الويندوز ونقوم بفتح صفحة أنترنت ونكتب فيها الأيبى الخاص بالروتير والنتيجة سوف تكون "أهلا وسهلا بك في عالم جونيبر"



كيف تقوم بعمل اختصار لجميع أوامر سيسكو

أحد الأشياء التي أجدها في سيسكو مميزة وتساعد كثيرا في كتابة الأوامر وتسريع العمل هو الأمر **Alias** يقدم هذا الأمر الكثير من المساعدة في اختصار الوقت في كتابة بعض الأوامر التي تحتاجها بشكل مستمر من خلال عمل اختصار له على شكل حرف أو حرفين وهو يقسم إلى ثلاثة أقسام رئيسية

القسم الأول خاص بالأوامر التي تكتب في **Privileged Mode** وصيغة الأمر تكون على الشكل التالي

Alias exec

القسم الثاني خاص بالأوامر التي تكتب في **Global Configuration Mode** وصيغة الأمر تكون على الشكل التالي

Alias configure

القسم الثالث خاص بالأوامر التي تكتب في **Interface Configuration Mode** وصيغة الأمر تكون على الشكل التالي

Alias interface

وهذه بعض الأمثلة لتوضيح طريقة كتابة الأوامر في كل قسم

Router(config)#alias exec a show ip int br | exclu unass

Router(config)#alias exec sr show ip route

Router(config)#alias exec acl show access-lists

Router(config)#alias exec srnt show running-config interface

وكما تشاهدون بعد كتابة الأمر **alias exec** أقوم بكتابة الحرف الذي أريده لكي يكون اختصارا للأمر **show ip int br | exclu unass** وطبعا قمت باختيار الحرف **a** لتنفيذ الأمر ونفس الشيء مع باقي الأوامر

Router(config)#alias configure in interface fastethernet 0/0

Router(config)#alias configure eigrp router eigrp 10

Router(config)# alias interface x1 switchport mode access

Router(config)# alias interface x2 switchport port security

Router(config)# alias interface ns no shutdown

هذه كانت بعض الأمثلة التوضيحية وتستطيع أن تقوم بتجهيز اختصارات لأي أمر تحتاجه بشكل مستمر أضف على ذلك أن سيسكو قد قامت بإضافة بعض الاختصارات الجاهزة والتي تستطيع استخدامه مباشرة وهذه أمثلة عليها

p stands for ping

h stands for help

lo stands for logout

u and **un** stand for undebug

wr stand for copy start run

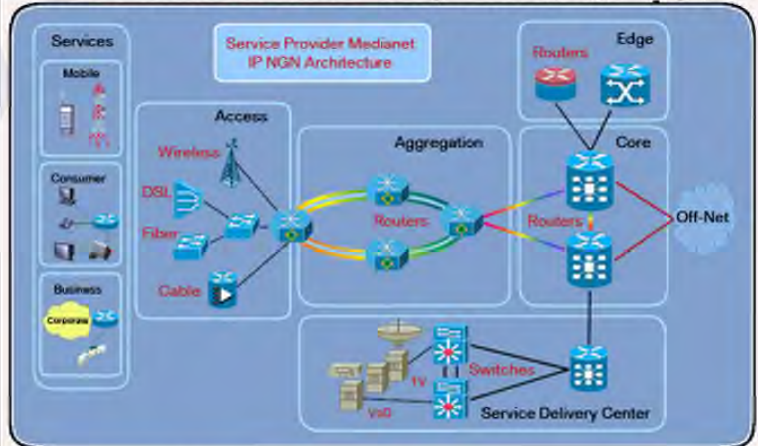
w stands for where

كلمة أخيرة لهذا الأمر الكثير من الأقسام والتي ذكرت هنا تعتبر هي الأساسية وأكثر استفادة يحققها لك هذا الأمر برائي هو الجزء المتعلق بأوامر الـ **Show** لأنها من أكثر الأوامر التي نقوم باستخدامها كما يعد استخدام أمر **Alias** من النصائح التي توجه للأشخاص الذين يريدون الدخول إلى امتحان العملي الخاص بي شهادة **CCIE** من أجل تسريع العمل

كيف تستغل وقتك في تعلم الشبكات



قد يمر على بعض الأشخاص أوقات يريد فيها أن يرفه عن نفسه ويبتعد قليلا عن الدراسة والقراءة على الكمبيوتر كما يحدث معي أحيانا لذا ألجأ دائما إلى أن ألعب لعبة الـ **Solitaire** أو أتجه إلى موقع ياهو ولعب الشطرنج وقد تركت هذه الألعاب منذ تعرفت على ألعاب سيسكو وخصوصا لعبة الشبكات الاستراتيجية **myPlanNet** فكرة اللعبة تبدأ مع عام 1990 من مدينة صغيرة لا يوجد فيها أي نوع من الاتصالات لا تلفونات ولا كابلات تلفزيونية وطبعا لا يوجد إنترنت وهي المهمات التي يجب عليك القيام فيها ففي بداية اللعبة يتاح لك أن تختار أما البدء في تمديد المدينة بالهواتف أو الوايرليس أو الأيثرنت وطبعا هناك مراحل كثيرة تدخل في اللعبة والهدف منها هو أن تصل إلى المرحلة النهائية وهي تشغيل تقنية **IPNGN** أو **IP Next Generation Network**



وعندما تبدأ اللعب سوف تكتشف أهميتها فهي تعلمك كيفية بناء استراتيجية شبكات من الصفر وأن كنت لم أتعلم اللعبة بشكل كامل فلي فيها 3 أيام فقط ولكن أستطعت أن أفهم فيها أشياء كثيرة وأهم شيء التسلسل الذي يجب أتباعه في بناء الشبكة والكثير من الأشياء لذا إذا كان لديك أحيانا وقت فارغ فأنصحك بتجربة هذه اللعبة بغض النظر عن المقولة بأن الألعاب للصغار فقط لتحميل اللعبة توجه إلى موقع سيسكو

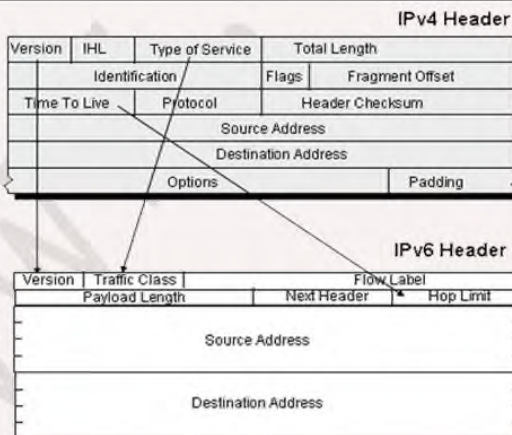
<http://www.cisco.com/web/solutions/sp/myplannet/index.html>

ولزيد حول اللعبة توجه إلى صفحت اللعبة على الـ Facebook
<http://www.facebook.com/pages/Cisco-myPlanNet/153538644090>

مقارنة بين IPv4 و IPv6

لفت انتباهي البارحة وأثناء البحث في غوغل عدم وجود أي موضوع باللغة العربية تطرق إلى مقارنة الـ IPv4 مع الـ IPv6 لذا دعوني أكون أول واحد يقدم هذه الخدمة لآخواننا العرب كون الموضوع مهم ومعقد بعض الشيء للبعض. وقبل أن أبدا المقارنة أحب أن أقول أن هذا الموضوع ليس مقارنة بالمعنى الحرفي لأن أغلبنا يعلم جيدا الـ IPv4 ويعلم محتوياته ومميزاته وسوف يكون الموضوع بشكل عام هو توضيح لمميزات الـ IPv6 لكن على شكل مقارنة مع الـ IPv4

IPv4	IPv6
يستخدم الايبي 32 بت أي حوالي 4 بايت	يستخدم الايبي 128 بت أي حوالي 16 بايت
يوفر 4,294,967,296 ايبي وعدد كبير منها يستخدم لاهداف معينة مثل Privet IP و Multicast الخ.	يوفر (شذ حيلك قبل ماتقرأ الرقم) 340,282,366,920,938,463,374,607,431,768,211,456 وهذا يعني لكل شخص فيني سوف يحصل على 5×1028 ايبي فقط
يستخدم Broadcast لعمل Flood على كل الأجهزة الموجودة على الشبكة.	لا يوجد شيء اسمه Broadcast على الإطلاق وتم استبداله بي IP Multicast لعمل Flood على كل الأجهزة الموجودة على الشبكة وهو FF02::1
يحتوي الـ Header على قسم خاص بي الـ Checksum	تم إزالة قسم الـ Checksum من الـ Header وسوف يتم الاعتماد على الـ Checksum الموجود على الـ Link Layer او الموجودة في الطبقات الاعلى أي على TCP, UDP الخ
أعداده يتم بشكل يدوي أو من خلال DHCP سيرفر	لا يتطلب لأعداده كتابة أي شيء فهو يستطيع أن يولد لنفسه ايبي بشكل أوتوماتيكي ويمكنه العمل مع وبدون DHCP سيرفر
غير مدعومة بمثل هذه التقنية	يوفر تقنية نقل جديدة تعرف بي Anycast والتي توفر سرعة أكبر في النقل وتوفير في الباندويث
يحتوي الـ Header قسم خاص بي الـ Option	تم إزالة قسم الـ Option من الـ Header مع توفير extension headers يوفر لك حيز في حال وجود بعض الخيارات التي يجب إضافتها
يستخدم Arp Protocol للحصول على ماك أدريس معين لاايبي أو العكس	تم توقيف Arp Protocol عن العمل وحل محله Multicast Neighbor Solicitation
خاصية الـ IPsec موجودة ضمن الـ Option الموجودة على الـ Header ويتطلب أن يكون الطرفين معدان للعمل من خلالها	خاصية الـ IPsec مبنية ضمن الـ Header
يحتوي الـ Header على قسم خاص بي الـ Fragmentation وهي تتم إما من خلال المرسل أو من خلال الـ روتر	تم إزالة قسم الـ Fragmentation من الـ Header وتم ضمه إلى extension headers وهو يدار من خلال المرسل فقط
لا يوجد قسم لي Flow Label وتتم عملية QoS من خلال الـ روتر	تم إضافة قسم جديد إلى الـ Header تدعى Flow Label وهي خاصة بي الـ QoS



وهذه صورة توضح Header كل بروتوكول على حدى ومهامي التعديلات التي تم القيام بها



قسم أمن وهماية الشبكات

هذا القسم سوف يتم عرض فيه كل الامور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التي تحدث على الشبكة وارجو منك ان تدقق على كلمة تخفيف لان النظرية العامة تقول لا يوجد جهاز امني خالي من الثغرات مهم كانت قوته!

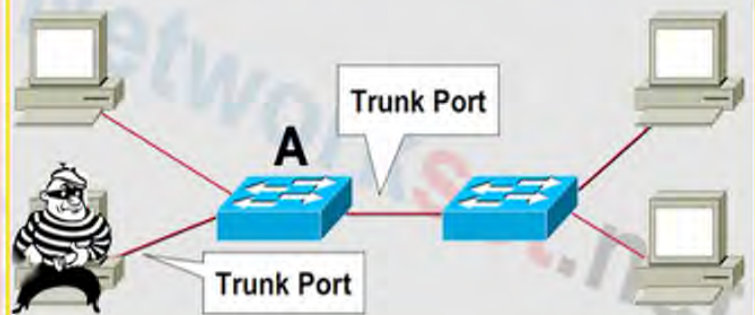


هجوم الـ Vlan Hopping وطريقة التصدي له

ما هو الهجوم الـ Vlan Hopping ؟

الهجوم الثاني الذي اريد ان اتحدث عنه ايضا يستهدف الـ Layer 2 Devices ويدعى بي Vlan Hopping وتقوم فكرة هذا الهجوم باختراق قواعد الـ Vlan على الشبكة وذلك بالسماح لشخص معين موجود على Vlan2 مثلا بالدخول على Vlan3 والاتصال بكل الاجهزة الموجودة هناك لاننا كما نعلم ان احد مميزات الـ Vlan هي عزل الاجهزة عن بعضها البعض وينقسم هذا النوع من الهجمات الى نوعين
Switch Spoofing
Double Tagging
تتعرف على كل واحد منهم

VLAN HOPPING - ATTACK



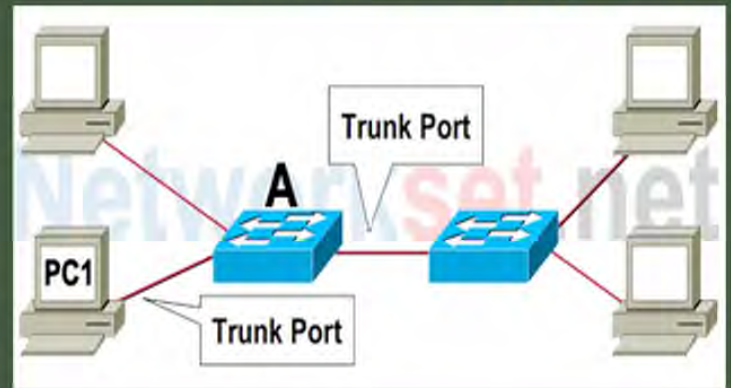
```
SwitchA#conf t
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#switchport mode access
```

بهذا الأمر نكون قد أوقفنا نصف الهجوم لان السويتش يحوي ثغرة أخرى تتم عن طريق بروتوكول الـ DTP أو Dynamic Trunk Protocol وظيفة هذا البروتوكول باختصار هي تحديد نوع الـ Trunk الذي يجب استخدامه بشكل أوتوماتيكي أي تحديد هل يجب استخدام الـ 802.1Q أو ISL وهو يعمل Be default على كل البورترات الموجودة على السويتش وهذا ما يستغله العايب بشكل جيد فهو يقوم بإرسال الـ DTP Packet إلى السويتش مخبرا إياه بأنه يستخدم بروتوكول الـ 802.1Q مثلا ليتحول الـ Port إلى Trunk Port بشكل أوتوماتيكي حتى لو كنا قد طبقنا الأمر السابق ولأيقاف هذه البروتوكول عن العمل نقوم بتنفيذ الأمر التالي

```
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)# switchport mode trunk
SwitchA(config-if)# switchport nonegotiate
```

وفيه أخبر البورت بأن لايقوم بالتفاوض مع الطرف الآخر حول نوع البروتوكول الذي يجب استخدامه وبالتالي قُمت بتوقيف عمل البروتوكول المسؤول عن عملية التفاوض مع الطرف الآخر وهو طبعا الـ DTP Protocol ن خلال كتابتي للأمر الثالث switch port nonegotiate

الطريقة الاولى Switch Spoofing



كما نعلم جميعا ان وظيفة الـ Trunk Port هي السماح بالاتصال بين جميع الـ Vlans الموجودة في السويتش مع نفس الـ Vlans الموجودة على سويتش آخر وذلك بوسم كل Traffic ذاهب الى السويتش الآخر برقم الـ Vlan التي أرسلت منه وهذا بدوره يعطي الـ Trunk Port القدرة على الاتصال بكل الـ Vlans الموجودة على الشبكة لتسهيل اول حالات هذه الهجوم

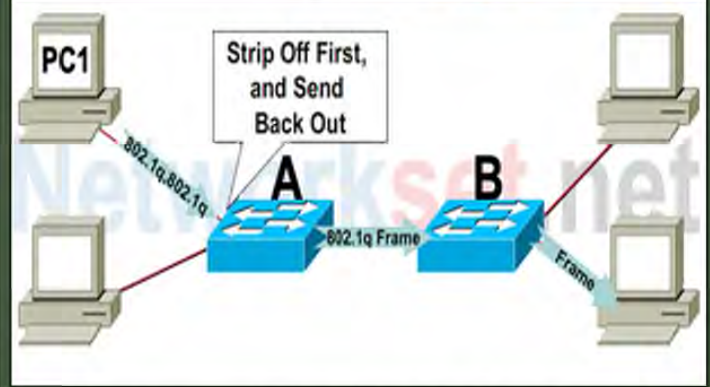
يقوم العايب الموجود على PC1 بعمل سويتش وهمي أو يقوم بوصل سويتش حقيقي على الجهاز مخبر السويتش A بأنه Trunk Port وهذا بدوره يعطي العايب الصلاحيات في الوصول إلى كل الأجهزة الموجودة على الشبكة بالإضافة إلى إمكانية التنصت على كل الباكيث المرسلة بين الـ Vlans والسبب طبعا لان البورترات الموجودة في السويتش A تكون في حالة auto مع الطرف الآخر فهو يستجيب لك اذا أخبرته أنك سويتش وأنك Trunk Port وللتصدي لهذا النوع تقوم بكتابة أمر واحد على كل Interface موصول مع Host

تصل وهي تحمل ال Tag الداخلي الذي تم أعداده من قبل وليقوم السويتش بعدها بإرسال البايت إلى المكان المطلوب يمكن التصدي لهذا النوع من الهجوم بأرسال كل بايت Untagged إلى Vlan تم أعداده مسبقا وغير مستخدمه لأي شيء ويتم ذلك من خلال الأمر التالي:

```
SwitchA(config)#vlan 210
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)# switchport trunk native vlan 210
```

في الأمر الثالث أخبر البورت بأن يرسل أي بايت تعد Untagged إلى ال Vlan 210 كلمة أخيرة أحب أن أضيفها وهي أن جميع هذه الأوامر مترابطة مع بعضها البعض ويجب تنفيذها جميعا حتى نستطيع أن نوقف هذا النوع من الهجوم الخبيث .

الطريقة الثانية: Double Tagging



فكرة الطريقة الثانية أجمل من الأولى لأنها تسمح للعابث للوصول إلى Vlan أخرى حتى لو قمنا بعمل كل الخطوات السابقة وهي ببساطة تقوم على مبدأ إرسال بايت تم وسمها مرتان بي 802.1Q tags وعندما تصل البايت إلى السويتش A يقوم السويتش بإزالة ال Tag الخارجي فقط ويقوم بإرسالها إلى السويتش B كـ untagged packet وعندما تصل إلى السويتش B

مقارنة بين سيرفرا التصاريح RADIUS & TACACS+

بقلم: أيمن النعيمي

وطبعاً بعد قراءتك لكل هذا الفروقات سوف تستنتج أن سيرفر TACACS+ هو الأفضل بلا منازع إلا أنا الواقع العملي يقول أن استخدام ال RADIUS أكثر من استخدام ال TACACS+ والسبب على ما أعتقد هو أن الأول هو مفتوح المصدر والذي يتيح للمستخدمين خيارات أكثر عند الاستخدام.

متى أختار RADIUS ؟

نختار RADIUS إذا كنا من مراهضي البرامج المفتوحة المصدر والذي تعطي أيضا سبب كبير لاستخدام هذا النوع من السيرفرات والسبب إمكانية التعديل على الكود المصدري

نختار RADIUS في حال كنا نتعامل مع أجهزة مختلفة المنشأ وهذا يشمل كل الأنواع ومن بينها سيسكو وجونيبر

نختار RADIUS في حال كان يهتما الأداء أو ال Performance الخاص بالروتات لان ال RADIUS يعمل بشكل أخف من TACACS+.

متى أختار TACACS+ ؟

نختار TACACS+ عندما يكون موضوع الأمن مهم عندنا على الشبكة لان ال T+ ACACS يقوم بتشفير عملية التبادل بشكل كامل بالإضافة إلى إمكانية التحكم بمستوى التصاريح المعطاة للمستخدمين

نختار TACACS+ عندما تكون الشبكة عندنا تعمل مع بروتوكولات مختلفة مثل AppleTalk, Novel, NetBios, X.25

نختار TACACS+ عندما تكون المرونة شيء مطلوب على الشبكة والسبب طبعاً هو استخدامنا لـ ال TCP والذي يعطي مرونة أكبر للشبكة من خلال استخدامه خاصية three-way handshake

تعتبر هذه السيرفرات من الأشياء المهمة في الشبكة والتي توفر لك حيز جيد من الأمان والحماية لشبكته وللمستخدمين الموجودين عليها وهي تعتمد على خاصية تعرف بي AAA وتعني authentication, authorization, and accountability وهي خاصية موجودة في جميع أنواع الروتات وبعض الأنواع من السويتشات ووظيفتها الرئيسية إعطاء التصاريح للدخول إلى الشبكة بالإضافة إلى تحديد الصلاحيات لكل شخص يدخل على الروتر.

لنتعرف الآن على أهم الفروقات بين السيرفران

TACACS+ server	RADIUS server
سيرفر خاص بأجهزة سيسكو فقط	سيرفر مفتوح المصدر ويمكن استخدامه مع كل الأجهزة ومن بينها أجهزة سيسكو
يستخدم بروتوكول ال UDP والذي بدوره يجعل توصيل التصاريح بشكل أسرع من ال TCP بالإضافة إلى وجود برمجة خاصة على السيرفر تتيح إعادة إرسال التصاريح في حال انقضاء الوقت المسموح به	يستخدم بروتوكول ال TCP والذي بدوره يجعل توصيل التصاريح بشكل أسرع من ال UDP بالإضافة إلى وجود برمجة خاصة على السيرفر تتيح إعادة إرسال التصاريح في حال انقضاء الوقت المسموح به
يقوم بتشفير عملية الأرسال بشكل كامل وهذا يشمل كل المعلومات المرسل من وإلى السيرفر ومن بينها اسم الدخول وكلمة السر والتصاريح المرسله	يقوم بتشفير كلمة السر فقط
لا يستهلك كثيراً من حجم الذاكرة الموجودة على الروتر ولا من قوة الروتر	استهلاك أكبر للذاكرة وللمعالج الموجود على الروتر
يتعامل مع كل خاصية بشكل مستقل وهذا يشمل الخواص الثلاث	يقوم بدمج ال authentication, authorization بخطوة واحدة
يدعم كل التصاريح الموجودة على الروتر أي أنه يتيح 15 تصريح مختلف	التصاريح فيه محدودة وتتمثل بتصريح واحد وهو ال privilege mode والسبب طبعاً هو دمج ال authentication, authorization مع بعضهم البعض
يدعم كل أنواع البروتوكولات	لا يدعم البروتوكولات التالية - AppleTalk, Novel, NetBios, X.25

مساحة إعلانية

أدعم هذا النوع من المجلات بأعلانك معنا

عتاک و معلومات

أعداد عثمان إسماعيل

CISCO SYSTEMS



RAM	256 MB (installed) / 1 GB (max)
Flash memory	64 MB (installed) / 256 MB (max)
Type	Router
Connection Type	Ethernet, Fast Ethernet, Gigabit Ethernet
Encryption Algorithm	DES, Triple DES, AES
Supplied OS	Cisco IOS SP services
Voice Codecs	G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726
IP Telephony Features	Echo cancellation (G.168)
Protocol Remot	SNMP 3
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x management - console 1 x network - auxiliary
Firewall protection, 128-bit encryption, hardware encryption, VPN support, MPLS support, URL filtering, 256-bit encryption	



**Cisco 2800 Series
Voice Bundles
(CISCO2851-CCME/K9)**

RAM	128 MB
Flash memory	16 MB Flash
Type	stackable -Switch
Mac-Address Table	12000 Entries
Interfaces	48 x Ethernet 10Base-T, Ethernet 100Base-TX
Connection Type	Ethernet, Fast Ethernet
Data Rate	100 Mbps
Authentication method	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Protocol Remote	SNMP 1, RMON 1, RMON 2, SNMP, Telnet, SNMP 3, SNMP 2c
Routing Protocol	OSPF, IGRP, BGP-4, RIP-1, RIP-2, EIGRP, HSRP, IGMP, DVMRP, PIM-SM, static IP
Flow control routing, auto-sensing per device DHCP support, auto-negotiation, ARP support, trunking, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, manageable , IPv6 support	



**Catalyst 3750 Series 10/100
Workgroup Switches
WS-C3750-48TS-E**

RAM	512 MB
Flash memory	64 MB Flash
Type	Security appliance
Connection Type	Ethernet, Fast Ethernet, Gigabit Ethernet
Interfaces	1 x network - Ethernet 10Base-T/100Base-TX - RJ-45 1 x management - console - RJ-45 2 x Hi-Speed USB - 4 PIN USB Type A 1 x serial - auxiliary - RJ-45 4 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45
Encryption	DES, Triple DES, AES
Performance	Firewall throughput : 450 Mbps VPN throughput : 225 Mbps Connection rate : 12000 connections per second
Features	Firewall protection, VPN support, load balancing, VLAN support, High Availability
Concurrent sessions : 280000 IPSec VPN peers : 750 SSL VPN peers : 2 Virtual interfaces (VLANs) : 100	



**Cisco ASA 5520 Firewall Edition
ASA5520-BUN-K9
security appliance**



Juniper®

NETWORKS

Aggregate Half-Duplex Throughput

- * 10 Gbps

FPC Slots and Full Duplex Throughput per Slot

- * 1 built-in, 4 Gbps additional 1 Gbps for FIC

PICs per Chassis

- * 4, plus 2 additional fixed FE, or 1

fixed GE ports

Chassis per Rack

- * 24

Redundancy

- * No

Dimensions

- * 3.5 x 17.5 x 18 in
- * 8.9 x 44.5 x 45.7 cm

Mounting

- * Front or center

Maximum Weight

- * 38.2 lbs / 17.3 Kg

Power Options

- * DC Input Power (Fully Loaded): 10 A at -48 VDC; 378 watts
- * No. of power supplies required (non-redundant/redundant): 1/2
- * AC System Input Power (Fully Loaded): 4 to 2 A; 100 to 240 VAC; 47 to 63 Hz; 400 watts

Router M7i



Number of Interfaces*

8 mini-GBIC (SX, LX or TX), or 2 XFP 10 Gig (SR or LR)

Maximum Number of IP Addresses in Trusted Interfaces

Unrestricted

Maximum Throughput

- * 10 Gbps FW
- * 5 Gbps 3DES VPN

Maximum Number of Sessions

1,000,000

Maximum Number of VPN Tunnels

25,000

Maximum Number of Policies

40,000

Maximum Number of Virtual Systems

0 default, upgradeable to 500

Maximum Number of Virtual LANs

4094

Maximum Number of Security Zones

16 default, upgradeable to 1,016

Maximum Number of Virtual Routers

3 default, upgradeable to 503

Routing Protocols Supported

OSPF, BGP, RIPv1/v2

High-Availability Modes Supported

- * Active/Passive
- * Active/Active
- * Active/Active Full Mesh

IPS (Deep Inspection FW)

Yes
Integrated / Redirect Web Filtering
Yes

NetScreen-5200



Maximum Performance and Capacity

- * Junos Software Version Support: Junos Software 9.1
- * Firewall Performance (Large Packets): 600 Mbps
- * Firewall Performance (IMIX): 400M
- * Firewall and Routing PPS (64 Byte): 175,000 pps
- * 3DES and SHA-1 VPN Performance: 140 Mbps
- * Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512
- * Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K
- * New Sessions/Second: 5,000

Network Connectivity

- * Fixed I/O: 4 x 10/100/1000
- * Maximum PIM Slots: 3
- * Maximum EPIM Slots: 0

Routing, Virtualization, Encapsulations

- * BGP, OSPF, RIP, Static, ECMP: Yes
- * Multicast, PIM SM, SSM, IGMP: Yes
- * Maximum Number of Security Zones: 40
- * Maximum Number of Virtual Routers: Yes
- * Maximum Number of VLANs: 256
- * PPP, FR, MLPP, MLFR, HDLC: Yes

Router J2320



Data Rate

- * 480 Gbps

Throughput

- * 357 Mpps (wire speed)

10/100/1000BASE-T Port

Densities

24 (dual-mode 1/10GbE network ports)

10GBASE-X Port Densities

24

100BASE-FX / 1000BASE-X (SFP) Port Densities

N/A

Resiliency

Dual load-sharing internal autosensing AC power supplies

Power Options

Autosensing; 110/220 VAC; 60/50 Hz

Operating System

JUNOS

QoS Queues / Port

8

Traffic Monitoring

N/A

MAC Addresses

16,000

Jumbo Frames

9216 Bytes

IPv4 Unicast / Multicast Routes

N/A

Number of VLANs

1,024

Switch EX2500





مصالحات تقنية

TCP : وتعني Transmission Transfer Protocol وهو أحد البروتوكولات التي تنتمي إلى الطبقة الرابعة Transport Layer ويستخدم مع بروتوكول الـ IP ووظيفته الرئيسية هي نقل البيانات في الشبكة العنكبوتية وأكثر ما يميزه هو مراقبة نقل البيانات بين المستقبل والمرسل والتأكد من وصول جميع البيانات بشكل صحيح من خلال القيام بعملية الـ Three-Way Handshake

UDP : وتعني User Datagram Protocol وهو البروتوكول الثاني الذي أيضا يستخدم في نقل البيانات وطبعا ينتمي إلى الطبقة الرابعة ويميزه سرعة النقل بين الأجهزة ويعيبه أنه لا يقوم بالتأكد من وصول البيانات بشكل صحيح لذا نجد استخدامه ينحصر في نقل الصوت والفيديو

DNS : وتعني Domain Name System وهي خدمة تقوم بترجمة أرقام أسماء المواقع إلى أيبات تستطيع من خلالها أجهزة الكمبيوتر التواصل مع السيرفرات التي تحوي هذه المواقع والسبب لان الأنترنت بشكل عام يتعامل مع الأرقام أي صفر وواحد كما أنها أيضا تتيح التعرف على الاسم من خلال رقم الأيبي ويمكن اختصارها إلى أنها مركز الاستعلام الذي يوفر لك معلومات عن كل اسم أو أيبي

DHCP : وتعني Dynamic Host Configuration Protocol وهو بروتوكول يعمل في الشبكة ويقوم بتزويد الأجهزة بكل المعلومات اللازمة للاتصال مع الشبكة وهذا يشمل ايبي وماسك وحيت واي بالإضافة إلى DNS ويشترط على الأجهزة وجود DHCP Client يقوم بالاتصال مع السيرفر ويحصل على كل المعلومات اللازمة

FTP : وتعني File Transfer Protocol ويمكن ترجمتها إلى العربية إلى بروتوكول نقل الملفات وهو بروتوكول يسهل عملية نقل الملفات بين الأجهزة من خلال سيرفر خاص فيه ويستخدم البورت 21 للنقل كما يتطلب من الأجهزة التي تريد أن تقوم بنقل الملفات من السيرفر إلى أجهزتها وجود FTP Client

Telnet : وتعني Terminal Network وهو أحد بروتوكولات الشبكة المعروفة ويستخدم للاتصال والتحكم بأجهزة السيرفر والكمبيوتر على الشبكة العنكبوتية ويعمل من خلال بروتوكول الـ TCP ويستخدم البورت 21 ويعيبه أنه يقوم بأرسال الأوامر من دون أي نوع من التشفير إلى الجهاز المستقبل

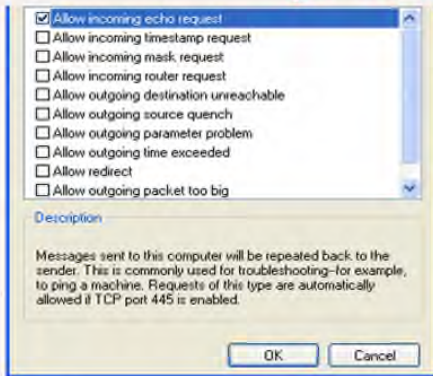
ARP : وتعني Address Resolution Protocol وهو يعد Computer Networking Protocol ويعمل في الطبقة الثانية Link Layer ووظيفته الرئيسية الحصول على عنوان الماك أدريس لأيبى معروف وذلك لأتمام عملية الاتصال معه أو القيام بعكس العملية أي الحصول على ايبي لماك أدريس معلوم من خلال بروتوكول رديف له يدعى Inverce ARP

HTTP : وتعني Hyper Text Transfer Protocol وهو أحد البروتوكولات التي تعمل في الطبقة الأولى Application Layer ويستخدم لنقل البيانات في الشبكة العنكبوتية WWW ويتطلب وجود برنامج وسيط يقوم بهذه العملية ومثال عليه برامج التصفح مثل فايرفوكس وأنترنيت أكسبلورير ويعيبه أن يقوم بأرسال البيانات من دون أي تشفير بعكس بروتوكول HTTPS الذي يقوم بتشفير جميع البيانات بين المرسل والمستقبل

مشاكل وحلول

سوف يتم تخصيص هذا القسم لعرض المشاكل التي قد تواجهك في الشبكة بالإضافة إلى طريقة حل المشكلة كما أرحب أيضا بارسال مشاكلكم على بريد المجلة magazine@networkset.net للنظر فيها وتقديم أفضل الحلول لها .

مشكلة : لماذا الـ PING لا يعمل في شبكة مؤلفة من جهازين كمبيوتر وقد تم التأكد من طريقة التوصيل وأرقام الأيبي؟



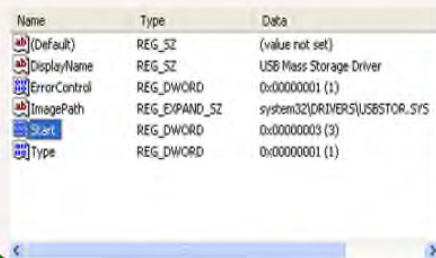
الحل : هذا النوع من المشاكل يحدث غالبا بسبب وجود الجدار الناري الموجود مع ويندوز والذي يقوم بشكل أوتوماتيكي بمنع كل رسائل الـ ICMP من الدخول إلى الجهاز ولحل هذه المشكلة لدينا طريقتان الأولى وهي إيقاف عمل الجدار الناري بشكل كامل ويتم ذلك من خلال الدخول إلى لوحة التحكم وبعدها إلى إعدادات الجدار الناري ووضع المؤشر على خيار إيقاف أو OFF الطريقة الثانية تتم بأضافة Exceptions أو استثناء للجدار الناري لكي يسمح بعبور رسائل الـ ICMP ويتم الأمر من خلال التوجه أيضا إلى لوحة التحكم وبعدها إعدادات الجدار الناري وبعدها نضغط على خيارات متقدمة أو Advanced وبعدها نختار ICMP ونضع المؤشر كما هو موضح بالصورة على خيار Allow incoming echo request

مشكلة : السيرفر عندي لا يفتح أغلب مواقع الحماية ومضادات الفايروس مثل Kaspersky, Norton ؟



الحل : تحدث هذه المشكلة بفعل فايروس أوكراني الصنع ويدعى كونفكير أو Conficker يقوم هذا الفايروس بإغلاق أغلب مواقع الأنتي فايروس بالإضافة إلى موقع مايكروسوفت والكثير من المواقع الهامة أيضا للقضاء عليه يجب عليك أن تقوم بتحميل أداة خاصة تقوم بحذف الفايروس وتدعى Conficker Removal Tool 1.0.0.16 وهي أداة مجانية تستطيع أن تجدها من خلال استخدام البحث في غوغل

مشكلة : كيف أقوم بإغلاق كل فتحات الـ USB على جهاز الكمبيوتر ؟



الحل : قم بالتوجه إلى إبدأ أو Start وبعدها قم بالضغط على تشغيل وقم بكتابة regedit للوصول إلى مسجلات الكمبيوتر وبعدها توجه إلى العنوان التالي HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR وابحث عن هذا التسجيل Start وقم بتغيير قيمته من 3 إلى 4 وهي تشير إلى تعطيل كل الخارج ولو في حال أردت أن تقوم بنفس الموضوع على مستوى الشبكة تستطيع أن تنفذ هذا الأمر من خلال عمل بوليسي على مستوى الشبكة

مشكلة : كيف أقوم بمنع النسخ واللصق على جهاز الكمبيوتر وعلى الشبكة أيضا ؟



الحل : لكي تقوم بإيقاف كل أشكال النسخ واللصق على جهاز الكمبيوتر لدين طريقتان الأولى الدخول على الريجستري والقيام بالتعديل على بعض المسجلات الخاصة بكل أمر والطريقة الثانية وهي أيضا تعتمد على المسجلات لكن تتم من خلال برنامج صغير جدا يدعى Prevent 1.0 يقوم بإيقاف كل أشكال النسخ واللصق بالإضافة إلى اختصارات لوحة المفاتيح تستطيع أن تجدها على محرك البحث غوغل .

بالنسبة لمنع النسخ على الشبكة فهي تتم من خلال سيرفر مخصص يثبت على ويندوز سيرفر و يدعى Rights Management Services وهو يقوم بأضافة صلاحيات لكل ملف من بينها صلاحيات النسخ واللصق والطباعة ويعييبها أنه لا يدعم كل أنواع الملفات الموجودة فهو يدعم ملفات الأوفيس والأدوب أكروبات وسوف يكون له موضوع كامل في المستقبل