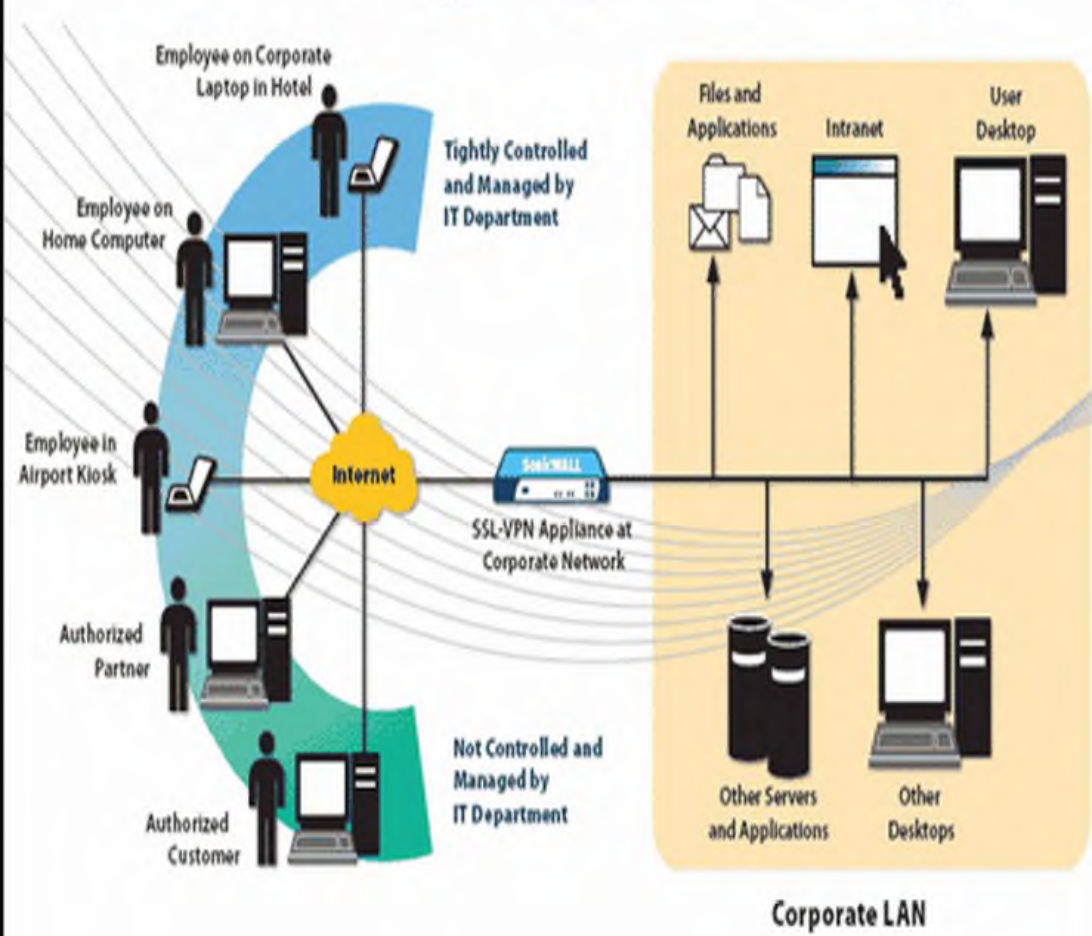


# الشبكات الافتراضية VPN



## نتائج الاستفتاء

كيف تحدد مستواك في الشبكات ؟

مبتدئ

77%

محترف

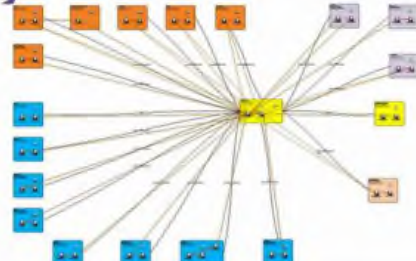
18%

خبير

5%

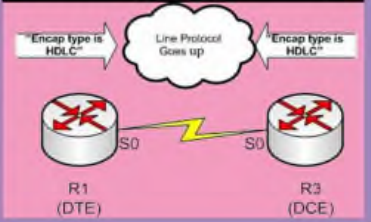
- كيف تعمل الشبكات الافتراضية
- كيف يتم حماية الشبكات الافتراضية
- مكونات الشبكات الافتراضية

## كيف تقوم برسم وتوثيق الـ Active Directory



تقرأون في هذا العدد

تعرف معنا على بروتوكول الـ HDLC



20 شخصية غيرت مجرى

الصناعات التقنية

كيف تقوم بمشاركة أقمية

التلفاز عبر الشبكة

أنواع الضغط المدعومة من

بروتوكول الـ PPP

مقارنة بين GNS3 و

Packet Tracer

والعديد من المواضيع الجديدة  
والقيمة

شاهدوا أيضا أقسام

مصطلحات تقنية



عتاد ومعلومات



مشاكل وحلول



9



# أفتتاحية العدد

## التشاؤم

هل فكرت يوما ان تكون في هذا الموقف ,كيف سيكون شعورك عندما تصل لمرحلة تكره فيها كل ما حولك وكل من حولك ؟ كيف سيكون شعورك عندما تتمنى ان تنام لساعات طوال او لشهور عديدة حتى تتخلص من مرحلة عابرة تكره فيها حتى النفس الذي تتنفسه.....

هو تهايم واحد سيتهمني الناس به وموقف واحد سيضعني فيه كل من حولي التشاؤم

كلمة لاظن ان كل من حولي سيقبل حتى بمجرد النقاش بها ومع ذلك سابقى ابتسم ابتسامة مخفية

وساقول للجميع غنكم لازلتهم وستبقون سجناء حياة مفروضة عليكم ستموتون كلكم وانتم تعلمون جيدا انها حسبت عليكم حياة

ويا لها من حياة

نعم ...

قد تكونون اديتم صلاة وصيام وحج و .... لكن هل هذا يكفي ؟

لا اظن ان الها عظيما كرب العزة خلقنا لهذا السبب فقط فلو كان هذا الهدف لاكتفى بملائكة لايعصون له امرا يجب ان نعرف المعنى الحقيقي للحياة ونجس بمدى حلاوة نعيمها وكنف رضى الله حتى نشتاقي لنعيم اكبر ونعمل بلهفة لنعيم اطول عمرا لن تكون الحياة نافعة مالم توضع على المحك ومحكها هو الموت ....

نعم هو الموت يجب ان تكون لهدف واحد هدف مرتبط بالآخرة والدنيا هدف تستطيع بكل جرأة ان تقول

اذا لم يتحقق قلن استحق الحياة .... كفانا تقاليد بالية ومبادئ نظرية لا اظن ان حياة كجد السيف اسطورة خرافية او ضرب من ضروب الخيال .... يجب ان نعرف ما نريد وبصراحة .... نحدد ثم نسير باتجاهه مهما ادمينا على الطريق وحتى لو كان الثمن ذكرى يتناقلها من حولنا باننا كنا نريد كذا وسينا اليه وسعينا اليه ولكن الثمن كان .. نحن .....

عندها فقط سنتوقف عن وضع رؤوسنا على مخداتنا قبل انا ننام لنحس عندها باننا قضينا حياتنا كارانب وسنموت كارانب ..... الموت ..... ليكون كلمة او حدثا او فكرة او موقف او او او او

مهما كان فليبق بالنتيجة موقف مميز نواجهه فقط بنفس عميق وابتسامة خفيفة وغمضة عين تطول لثواني ثم تتبعها نظرة تخيف الموت نفسه عندها فقط نموت ونحن نبتم بثقة ونحن نعلم جيدا انه حتى لو لم ننجز مانطمح اليه في حياتنا فالموت اخذ نصيبه من نار حارقة توقدت في قلوبنا وغذتها انفسنا.

أنس الأحمد

## المحررون الدائمون

- المهندس أيمن النعيمي

www.networkset.net

- المهندس عادل الحميدي

adel\_husni2000@hotmail.com

- المهندس أحمد الشحات

warior10@hotmail.com

- المهندس عمر السويدي

om18899@gmail.com

- المهندس أحمد مصطفى

www.amnetwork.blogspot.com

- المهندس أحمد الجلولي

ahm\_ijal@hotmail.com

موقع المجلة

www.networkset.net

بريد المجلة

magazine@networkset.net

بريدي الخاص

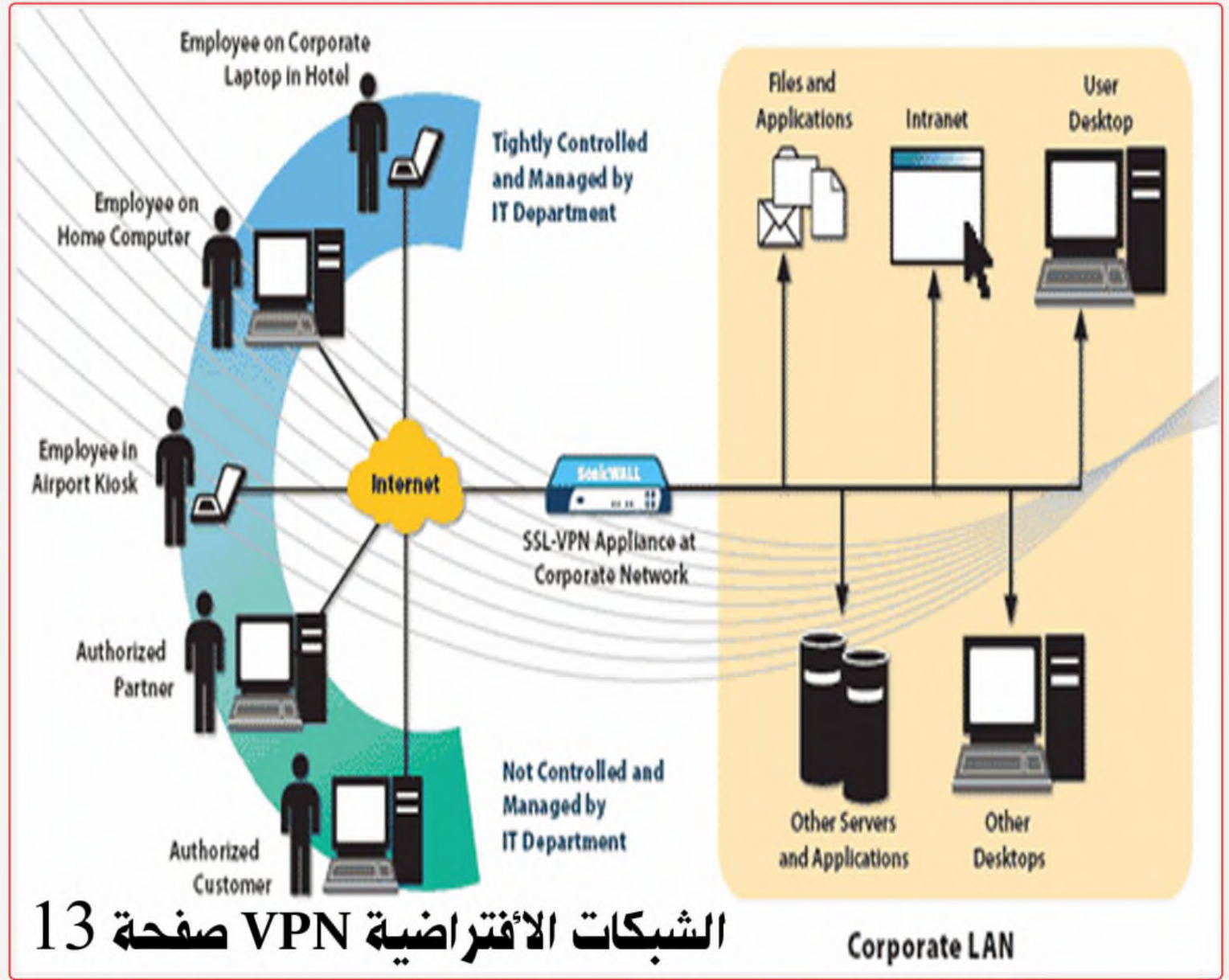
admin@networkset.net

جميع الحقوق محفوظة لكاتبها





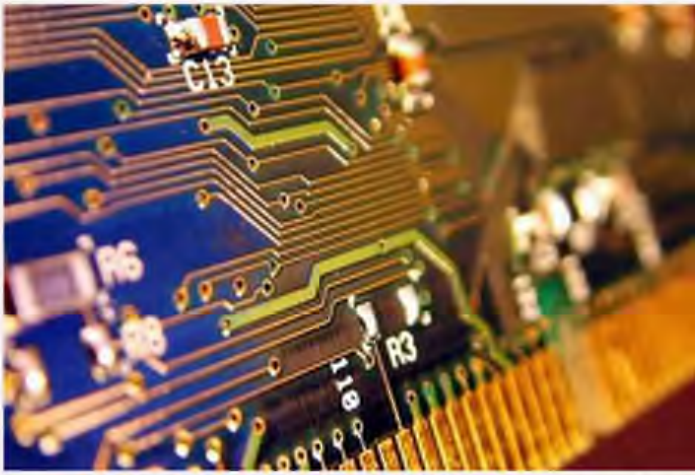
# محتويات ديسمبر 2010



- 3 - كيف يغلب Static على Dynamic route
- 5 - Mac Address Access-List
- 7 - Network Device Vulnerabilities
- 8 - قسم الأمن والحماية
- 10 - كيف أعداد الـ Authentication في EIGRP
- 11 - كيف أعداد الـ Authentication في OSPF
- 12 - قسم عتاد ومعلومات
- 13 - قسم مصطلحات تقنية
- 15 - قسم مشاكل وحلول
- 17 - قسم مشاكل وحلول

- 20 - شخصية غيرت مجرى الصناعات التقنية
- DUAL FINITE STATE MACHINE - الفرق بين GNS3 & Packet Tracer
- كيفية مشاركة أفضية التلفاز على الشبكة
- تعرف معنا على بروتوكول الـ HDLC
- كيف تقوم برسم وتوثيق الاكثيف دايركتوري بثواني
- نتائج الاستفتاء الشهري
- الشبكات الافتراضية VPN
- جونوس من جونيبر ونظرة عن قرب
- أنواع الضغط المدعومة في بروتوكول PPP





# 20 شخصية غيرت مجرى الصناعات التقنية اعرفهم هنا

إن في النظر إلى عقدين من الزمن مدعاة للتعجب في الفهرسة التاريخية لصناع التقنية الذين كان لهم الدور الرائد في إحداث تأثير كبير في تغيير مسارات هذه الصناعة، بعضها أسماء لعبت، وبعضها تالألات لكن جميعها أسماء أعادت كتابة تاريخ الثورة التقنية بعدما أحدثت فرقاً خلال عشرين عاماً.

## الشبكات (Networking)

لين بوزاك (Len Bosack) و ساندني ليرنر (Sandy Lerner)

للسرعات في نقل البيانات ومدى التقدم الذي أحرزته بطاقات الربط الشبكي إيثرنت على مستوى السرعة حتى أصبحت خياراً أوحد للربط سواء على مستوى الشبكات المحلية أو المنزلية أو على مستوى الشبكات واسعة النطاق. أسس ميتكالف شركة (3Com) عام 1979م وبرز كأحد الرواد المتميزين في هذا المجال.

## راي نوردا (Ray Noorda)

عرف نوردا في عالم صناعة الشبكات بلقب رجل الشبكات المحلية، ففي العام 1982م استلم دفة القيادة في شركة نوفل (Novell) التي كانت في حالة من الكفاح العام للبقاء في السوق آنذاك، وخلال مرحلة إعادة تقديم الشركة إلى السوق بشكل جديد، أسس سوفاً جديداً لبيئات التشغيل الخاصة بالشبكات. لقد كان إصراره يتمحور حول دفع المهندسين لابتكار وسائل تجعل من بيئات التشغيل المتباينة لمجموعة من الأجهزة تعمل ضمن نطاق بيئة تشغيل موحدة، وهو ما وضع شركة نوفل على خط الريادة في تقديم البرامج لعالم الشبكات المحلية (LAN) لسنوات عديدة.

## راديا بيرلمان (Radia Perlman)

تقف بيرلمان في صف المخترعين الذين أحدثوا ثورة كبيرة في عالم الصناعة التقنية لإسهاماتها الكبيرة في مجال تطوير الموزعات خلال عقد الثمانينات، وقد كان إسهامها مؤثراً في تضخيم أحجام الشبكات وجعل مفهوم الشبكات المشجرة ذات التعددية في وسائل الربط واقعاً ممكناً. وتحظى بيرلمان باحترام كبير في مجال صناعة الشبكات كما أنها تحتل منصباً متميزاً في شركة صن (Sun).

## ياكوف رايختر (Yakov Rekhter)

يعتبر رايختر الأب الروحي لمفهوم (MPLS) وهي الآلية المستخدمة لنقل البيانات في الشبكات التي باتت تستخدمها معظم الشركات الكبيرة اليوم. لقد أسهم رايختر في تقديم نمط جديد في نقل البيانات بين الشبكات التي تتشابه في خصائصها، كما يحسب له أيضاً إسهاماته في ابتكار وتطوير بعض المعايير (Protocols) كمعيار (Border Gateway Protocol) وهو معيار توزيع أساسي على شبكة الإنترنت.

يربط بعضهم اعتقاداً خاطئاً بين كل من بوزاك وليرنر وبين اختراع الموزع Router. وعلى الرغم من أن كليهما ليس له علاقة باختراع هذا الجهاز إلا أنهما يرتبطان به ارتباطاً وثيقاً من خلال الشركة التي أسسها لتؤدي دوراً رائداً في استغلال إمكانيات ذلك الجهاز.

لقد فهم الاثنان الامكانات التجارية للموزع متعدد البروتوكولات (Multi Protocol Router) فأسسوا شركة سيسكو (Cisco) في العام 1984م حيث بدأت هذه الشركة بأربعة موظفين فقط ثم ما لبثت أن دمت ضمن محيط من الاستقرار في الجو العام فأصبحت تضم 250 موظفاً، حيث بلغت قيمتها الفعلية في السوق فيما بعد أكثر من 224 مليون دولار أميركي. وتترجم اليوم شركة سيسكو سوق الموزعات وتقنياتها بالإضافة إلى قيامها بدور أساسي في أسواق أخرى مرتبطة كالشغلات (Switches)، واتصالات الإنترنت الهاتفية (VoIP)، ولها سلطة واسعة في أسواق الاتصالات اللاسلكية. وتقدر قيمة سيسكو السوقية اليوم بأكثر من 120 مليار دولار أميركي.

## دش دشباندني (Desh Deshpande)

أطلق دشباندني ثورة خدمات المعلومات في العام 1991م عندما أسس شركة (Cascade Communications) التي كان لها دور كبير في تقديم مفهوم مغاير لنقل البيانات بشكل رقمي بأقصى سرعة ممكنة، وبأقل التكاليف (Frame Relay). تحولت الشركة في فترة وجيزة إلى قوة مهيمنة على سوق الشبكات، فبعد أن كانت موظفاً واحداً أصبحت تمتلك 900 موظف بقيمة إجمالية تقدر بـ 500 مليون دولار أميركي، وسرعان ما ثبتت الشركة نفسها في الأسواق العالمية لترتفع قيمتها إلى 4 مليارات دولار.

لقد أثبتت جهود دشباندني في إمكانية تحسين وتطوير أداء شبكات المعلومات وعزز ذلك بنجاح شركته في الأسواق العالمية، لكنه قرر بيعها، والمشاركة في تأسيس شركة (Sycamore Networks) عام 1998م.

## بوب ميتكالف (Bob Metcalfe)

عندما كان مهندساً شاباً يعمل لدى شركة زيروكس (Xerox) عام 1973م، قام ميتكالف باختراع إيثرنت (Ethernet)، التي يستخدمها الكثيرون اليوم لربط أجهزة الكمبيوتر بعضها البعض لتصبح الإيثرنت مرتبطة ارتباطاً وثيقاً ذا صلة قوية بعالم الشبكات والتشبيك على وجه العموم.

لقد حولت الإيثرنت مفهوم الربط بين الأجهزة إلى واقع سهل وبسيط ولا يقف مستوى التطوير فيها عند حد معين، إذ يلاحظ المهتمون بالتناقل المتتابع



#### لينس تورفالدس (Linus Torvalds)

يطلق على تورفالدس لقب بطل المصادر المفتوحة (Open sources)، فعندما كان طالباً جامعياً في هلسنكي قام بنشر المصادر الخاصة ببيئة تشغيل عرفت باسم لينكس (Linux)، وذلك عام 1991م، وقد حرر تورفالدس هذه المصادر من سلطة الحماية الفكرية بحيث يستطيع الآخرون الإضافة أو التعديل عليها بهدف تطويرها. ويعمل تورفالدس حالياً في معامل تطوير المصادر المفتوحة بهدف الإبقاء على حرية اللينكس وتفعيل دور استخدامه في المؤسسات الكبيرة وفي قطاع الأعمال.

#### سكوت ماكنيلي (Scott McNealy)

لقد كان لماكنيلي تصور بأن الشبكة ليس سوى مجرد كمبيوتر، وقد فتح ذلك التصور العقول لفهم كيان البيانات المرتبطة بالأجهزة في نهاية الثمانينات وبداية التسعينات، وقد كانت الأفكار التي يقدمها ماكنيلي تؤسس لتقديم نمط جديد في اشتراك الشبكات المختلفة ضمن سياق تخاطب محدد تعتمد عليه جميع الشبكات لتحكي بذلك بعضها البعض. وفي العام 1995م خطى ماكنيلي بقطار الصناعة التقنية إلى اتجاه جديد عرفه الجميع باسم جافا (Java).

#### الاتصالات اللاسلكية (Telecom)

##### فيل إيفانز (Phil Evans)

إيفانز هو رئيس مجلس إدارة المنظمة الدولية للاتصالات، وهو أحد الذي أسهموا في تطوير عالم الاتصالات اللاسلكية، وساعد في تشكيل مجال الاتصالات في الحقبة الجديدة. ويعتبر أحد الأعلام في مجال الشبكات، وقد كان تأثيره واضحاً في مجال الاتصالات اللاسلكية وخصوصاً تطبيقات التعامل مع نقل البيانات باستخدام وسائل الاتصالات، فقد قاد جهود المنظمة الدولية للاتصالات في عصر خدمات الاتصالات اللاسلكية، كما وضع الاستراتيجيات الخاصة بالاتصالات اللاسلكية لأكثر من خمسمئة شركة حول العالم، وله مؤلفات منها كتاب مدير الشبكة (Handbook s' Network Manager).

#### ماريا خورساند (Maria Khorsand)

ولدت ماريا في إيران وتلقت تعليمها في الولايات الأمريكية المتحدة قبل أن تنتقل للعيش في السويد لتلتحق بالعمل في كبرى شركات إنتاج الهواتف وأجهزة الاتصالات أريكسون (Ericsson)، وفي منتصف التسعينات رأت خورساند فريقاً من الباحثين قادتهم إلى ابتكار تقنية اتصالات كان لها الفضل في تحرر مفهوم الاتصالات اللاسلكية. ففي العام 1998م قام فريق الباحثين الذي ترأسه خورساند بابتكار تقنية البلوتوث (Bluetooth) التي أحدثت نقلة كبيرة في عالم الاتصالات اللاسلكية.

#### الأمن (Security)

##### شلومو كرامر (Shlomo Kramer)

أينما توجد شبكة كبيرة لابد أن يكون هناك جدار ناري (Fire wall)، وهو التطبيق المتبع لحماية الشبكات أو أجهزة الكمبيوتر من عمليات الاختراق أو استخدام الملفات التي قد تؤثر سلباً في دور الشبكة، علاوة على منح إمكانية أكبر للدرء الشبكات في عملية التحكم وفرض السيطرة على مسارات الشبكة. وقد كان لابتكار الجدران النارية الفضل في تدعيم أطر الحماية والأمنية للشبكات في العقد الأخير من القرن الماضي، ويرجع في ذلك الفضل إلى كرامر الذي غير النظرة الأمنية للشبكات.

#### طاهر الجمل (Taher Algamal)

كلما فكرت درجات الحماية التي تحصل عليها في عملية حفظ البيانات وتبادلها، فتذكر أن طاهر الجمل يقف خلف مبدأ التشفير الذي تستخدمه الشبكات وأجهزة الكمبيوتر اليوم لنقل البيانات بسرية تامة للحفاظ على أمنها. فعندما كان يرأس فريق العلماء في شركة نتسكيب (Netscape) في نهاية التسعينات، قام الجمل بابتكار بروتوكول التشفير الشهير (SSL) الذي يعتبر معياراً أساسياً في نقل البيانات السرية بين الشبكات وعلى الويب.

نقلاً عن جريدة أسواق العرب ولكتيبها عارف الرويعي

بينما كان طالباً يدرس في جامعة إلينوي عام 1993م، وخلال فترة عمله الموقت في المركز الوطني لتطبيقات الكمبيوتر، قام اندريسن بالتعاون مع صديقه أريك بينا (Eric Bina) بابتكار متصفح (rowserB) ذي واجهة تطبيق رسومية سهلة الاستخدام. وقد كانت النسخة الأولى من المتصفح موزاييك (Mosaic) نقلة نوعية في الوصول إلى المعلومات على شبكة الإنترنت، فسرعان ما شاع استخدامه بين المستخدمين الذين كانوا يستخدمون متصفحات تتعامل مع النصوص فقط. ثم عمل اندريسن على تطوير نسخة تجارية للمتصفح لكنه لم ينجح في ذلك لكنه قام بتأسيس شركة (Loudcloud) عام 1999م.

#### تيم بيرنرز لي (Tim Berners-Lee)

طالما حلم بيرنرز لي بنظام متكامل لتبادل وعرض المعلومات على نطاق واسع بين مجموعة هائلة من المستخدمين بأسلوب مغاير عما كان متعارفاً عليه آنذاك. وقد كان نتاج بحثه المتواصل في الخروج بثورة جديدة في عالم الإنترنت كانت بمثابة الانطلاقة الحقيقية لهذه الشبكة، فقد ابتكر بيرنرز لي شبكة الويب (World Wide Web)، ثم تابع عملية التطوير في مجال وضع المعايير الأساسية لاستخدام هذه الخدمة خاصة وأنه يرأس المنظمة العالمية (W3C).

#### فينت سيرف (Vint Cerf)

عندما تتصل بشبكة الإنترنت وتطلب معلومة معينة فإنها تنتقل عبر خطوط الشبكة على هيئة حزم يمكن للجهة الأخرى استقبالها، وعندما تستقبل تلك المعلومة فذلك يعني أن الحزم التي أرسلتها عادت بالمعلومات المطلوبة، والفضل في ذلك يعود إلى فينت سيرف الذي ابتكر بروتوكول الإنترنت (IP) الذي أسهم في تطوير وسائل الاتصال والتخاطب بين الشبكات المختلفة، ويعمل سيرف اليوم في شركة غوغل.

#### جون بوستل (Jon Postel)

يصفه بعض الخبراء بأنه مايسترو شبكة الإنترنت الذي عمل على تطوير العديد من المعايير التي أسهمت في تطوير عمليات الاتصال بين الشبكات وتأسيس شبكة الإنترنت، ويقول عنه الكثيرون إنه صاحب الفضل في تطوير عدد من المعايير المفتوحة التي تستخدمها الشبكة اليوم والتي من دونها لم تكن الإنترنت ولا الويب بهذه السرعة من النمو والتطوير. توفي بوستل عام 1998م في الخامسة والخمسين.

#### الحواسيب (Computers)

##### لاري برايد (Laurie Bride)

أثناء فترة عمله لدى شركة بوينغ (Boeing) في الثمانينات وبداية التسعينات، كان لديه الحس التقني في فهم الاحتياجات والمتطلبات التي تحتاجها أجهزة الكمبيوتر المختلفة للتخاطب في ما بينها، لذلك فقد كان له الفضل في التحول إلى ما عرف بالأنظمة المفتوحة (Open Systems)، فقد دعمت الأفكار والبحوث التي قدمها برايد إلى إعادة هيكلة المعايير والبروتوكولات التي يستعان بها لتسهيل عملية التخاطب بين الأجهزة المختلفة.

#### بيل غيتس (Bill Gates)

لقد كانت الشراكة التي عقدها غيتس مع شركة (IBM) بمثابة الأساس الذي دعم لظهور بيئات تشغيل واسعة الانتشار سهلت على المستخدم التعامل مع الأجهزة سواء الشخصية أو المرتبطة ببعضها البعض في المؤسسات الصغيرة والكبيرة. ثم كان لظهور بيئة التشغيل ويندوز أثر واضح في تغيير الأساليب في الاستخدام والتعامل مع البيانات وعملية تبادلها. لقد أسهمت شركة مايكروسوفت (Microsoft) التي أسسها بيل غيتس في إضافة إسهامات كبيرة إلى الصناعة البرمجية وإثراء عالم الصناعة الحاسوبية.

#### لو جيرستنر (Lou Gerstner)

على الرغم من أن جيرستنر لم يكن تقنياً بالدراسة أو الممارسة إلا أنه أحدث تغييراً كبيراً في عالم الصناعة التقنية من خلال فهمه الواضح لأهمية الخدمات الإلكترونية، والمعايير المفتوحة، وشبكة الإنترنت، والأعمال الإلكترونية، وقد أسهم في مساعدة المستخدم من خلال بحوثه في مجال الاستخدام المرن للكمبيوتر، وتطوير مجال تصميم الخدمات الإلكترونية.



# DUAL FINITE STATE MACHINE

بقلم: أحمد مصطفى

(RD) Feasibility condition - استمراراً في الحديث عن الإصلاحات التي أدخلها جيل الإصلاحيين علي عائلة بروتوكولات Distance Vector، نأتي إلي أهم هذه الإصلاحات، وإن شئت فقل قلب هذه الإصلاحات.

(ES) EIGRP successor - فقل قلب هذه الإصلاحات. وهذه الإصلاح ينفرد به EIGRP في هذه العائلة العريقة، ألا وهو DUAL Algorithm.

(FS) Feasible successor - اعتمدت عائلة Distance Vector في حساب Cost على نموذج Algorithm.

(FSM) Finite State Machine -

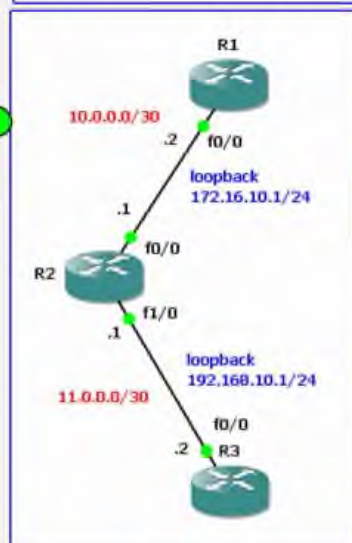
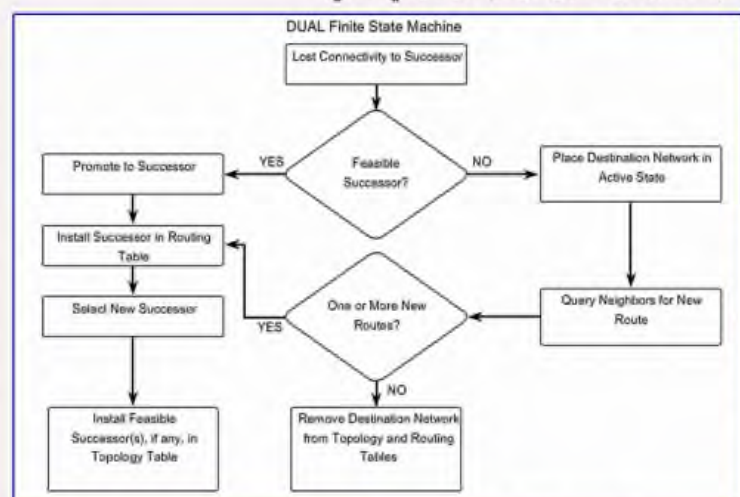
هذا المفهوم هو مفهوم عام، وله تطبيقات عديدة في مجالات عدة، فهو يوضح الاحتمالات التي من الممكن أن يمر بها شئ معين، و الأسباب التي تؤدي إلي ذلك، وأيضا النتائج المترتبة علي هذه الأسباب.

(2) تم تطوير هذا النموذج في بداية التسعينات علي يد الدكتور J.J. Garcia-Luna-Aceves

(3) راجع مجلة الشبكات عدد نوفمبر 2010 مقال بعنوان Eigrp Cost Calculations.

ويستخدم هذا المفهوم مع DUAL Algorithm ليوضح كيف يتصرف ال EIGRP في حالة حدوث Fail لـ (ES).

ويمكن تلخيص الحالات التي يمر بها DUAL Algorithm من خلال نموذج ال (FSM) من خلال الرسم التوضيحي التالي:



R3#debug eigrp fsm

EIGRP FSM Events/Actions debugging is on

وبفرض أن ال LINK بين R2، R3 حدث له Fail نجد أن ال FSM علي R3 بدأ في العمل كالتالي:

استمراراً في الحديث عن الإصلاحات التي أدخلها جيل الإصلاحيين علي عائلة بروتوكولات Distance Vector، نأتي إلي أهم هذه الإصلاحات، وإن شئت فقل قلب هذه الإصلاحات.

وهذه الإصلاح ينفرد به EIGRP في هذه العائلة العريقة، ألا وهو DUAL Algorithm.

اعتمدت عائلة Distance Vector في حساب Cost على نموذج Algorithm.

(1) Bellman-Ford algorithm وهذا النموذج كان هو المسيطر على

عائلة بروتوكولات Routing لفترة طويلة في وقت كانت فيه الشبكات صغيرة، وكان حجم البيانات التي تمر من خلال الشبكة Traffic بسيط، وبالتالي لم يكن عامل الوقت Convergence Time يمثل مشكلة كبيرة في ذلك الوقت.

ولكن مع توسع الشبكات وزيادة حجمها بدأت تظهر عدة مشاكل واجهها هذا النموذج، على سبيل المثال:

- مشكلة ال counting to infinity، فمثلاً هذا الشكل، إذا حدثت مشكلة في link بين A و B، هنا يقوم B بسؤال الراوترات بجانبه عن طريق A، فيجيب C أنه يعرف طريقاً إلي A، ولكن عن طريق 2 hops، فيحاول B الإرسال عن طريق C الذي هو نفسه يعرف الطريق إلي A عن طريق B، وهكذا إلى ما لا نهاية.

- مشكلة أخرى هي مشكلة ال Long Convergence Time، فالوقت الطويل الذي يأخذه هذا النموذج ليتعرف كل راوتر على الطريق المتاحة إلي شبكة معينة يؤدي إلي حدوث Routing Loop في الشبكة.

- مشكلة ال Big Overhead نتيجة لزيادة حجم ال Traffic في الشبكة الذي بدوره نتيجة لطريقة عمل ال Bellman-Ford algorithm، الذي يقوم بعمل broadcast لـ Routing Table كل 30 ثانية، أضف إلي ذلك كبر حجم ال Routing Table نفسه.

كل هذه المشاكل وغيرها استدعت، البحث عن طرق لمعالجة هذه المشاكل، من هنا بدأنا نسمع عن ال Split Horizon mechanism، وال Split Horizon، أي شبكة قادنا في النهاية وفي بداية التسعينات إلي ال Dual Update Algorithm (2).

وقد تم تلافي المشاكل والعيوب المتعددة لنموذج ال Bellman-Ford algorithm، في هذا النموذج الجديد، بل وأثبت هذا النموذج مع بروتوكول ال EIGRP أنه الأفضل بلا منازع في عائلة ال Distance Vector.

وقد تحدثنا في مقال سابق عن طريقة عمل هذا النموذج والمعادلات الرياضية المستخدمة في حساب ال Cost في هذا النموذج (3).

حديثنا اليوم إن شاء الله عن الكوارث!!!

نعم، ماذا يفعل ال EIGRP إذا حدثت كارثة في الشبكة، مثلاً لا يستطيع الوصول لشبكة معينة، كيف يفاضل بين ال Routes المختلفة الموجودة عنده، وكيف يختار الأفضل في النهاية.

قبل أن نشرع في هذا المبحث، هناك عدة مفاهيم يجب أن تكون واضحة في ذهن القارئ قبل أن نبدأ.

(FD) Feasible distance - هي أقل metric إلي جهة معينة.

(RD) Reported distance - هي ال metric التي يستطيع neigh-

bor router الوصول إلي جهة معينة.

(نسبة إلي Richard Bellman and Lester Ford)

NetworkSet أول مجلة عربية خاصة بالشبكات

5



```

*Mar 1 00:19:26.115: %DUAL-5-NBRCHANGE: IP-
EIGRP(0) 100: Neighbor 12.0.0.2
(FastEthernet1/0) is down: holding time
expired
*Mar 1 00:19:26.119: DUAL: linkdown: start -
12.0.0.2 via FastEthernet1/0
**Output Omitted**
*Mar 1 00:19:27.083: DUAL: Removing dest 192.
168.10.0/24, nexthop 12.0.0.2
*Mar 1 00:19:27.091: DUAL: RT installed 192.
168.10.0/24 via 10.0.0.1
*Mar 1 00:19:27.091: DUAL: Send update about
192.168.10.0/24. Reason: metric chg
*Mar 1 00:19:27.095: DUAL: Send update about
192.168.10.0/24. Reason: new if

```

هنا نلاحظ أن R1 حذف Route إلى شبكة 192.168.10.0/24 عن طريق R3 واستخدم بدلاً منه 10.0.0.1 والذي هو R2، ثم بدأ بإرسال التحديثات لهذه الشبكة 192.168.10.0/24 لنتيجة لتغير الـ Metric وتغير الـ Next Hop. وهنا نقطة هامة هل إذا عاد f1/0 على R3 هل يقوم الـ DUAL بالعمل من جديد؟

الحقيقة نعم، كما يتضح من التالي:

```

R1#show ip eigrp to
**Output Omitted**
P 12.0.0.0/8, 1 successors, FD is 28160
via Summary (28160/0), Null0
P 12.0.0.0/30, 1 successors, FD is 28160
via Connected, FastEthernet1/0
P 192.168.10.0/24, 1 successors, FD is 156160
via 12.0.0.2 (156160/128256), FastEthernet1/0

```

وهذا عكس بروتوكول الـ OSPF، فحتى لو عاد الـ DR بعد حدوث أي انقطاع له من الشبكة، لا يتم انتخابه DR مجدداً في نفس الوقت، بل ينتظر الـ OSPF حدوث انقطاع للـ DR الحالي، ويدخل الـ DR القديم في عملية الـ Elections من جديد، وهذه نقطة هامة للـ OSPF لأنه يستخدم في شبكات أكبر وأوسع من الشبكات التي يستخدم فيها الـ EIGRP.

هذا والله أعلى وأعلم

وصلي الله وسلم وبارك على المصطفى وآله وصحبه وإخوانه أجمعين

محرم، 1432

(4) وهي الجداول التي يعتمد عليها الـ EIGRP في عمل العلاقات Relationships مع الراوترات المجاورة.

```

*Mar 1 00:11:37.339: DUAL: rcvquery: 192.168.10.0/24 via 10.0.
0.1 metric 4294967295/4294967295, RD is 158720
*Mar 1 00:11:37.343: DUAL: Find FS for dest 192.168.10.0/24.
FD is 158720, RD is 158720
*Mar 1 00:11:37.347: DUAL: 10.0.0.1 metric
4294967295/4294967295 not found Dmin is 4294967295
*Mar 1 00:11:37.351: DUAL: Peer total/stub I/O template/full-
stub I/O
*Mar 1 00:11:37.355: DUAL: Dest 192.168.10.0/24 (Split
Horizon) not entering active state.
*Mar 1 00:11:37.355: DUAL: send REPLY(rl/nl) about 192.168.
10.0/24 to 10.0.0.1
*Mar 1 00:11:38.135: DUAL: Removing dest 192.168.10.0/24,
nexthop 10.0.0.1
*Mar 1 00:11:38.139: DUAL: No routes. Flushing dest 192.168.
10.0/24

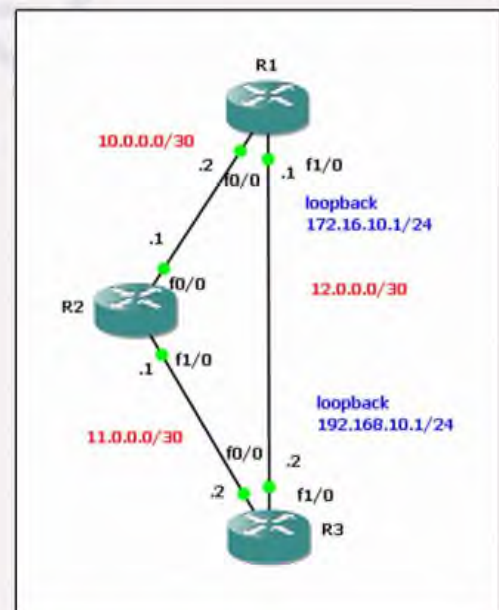
```

هنا وفي هذه الحالة لما لم يكن هناك أي طريق آخر بالنسبة لـ R1 للوصول إلى شبكة 192.168.10.0/24 قام R1 بحذف هذه الشبكة من الـ Routing table والـ topology table (4).

وهذا واضح من السطرين الأخيرين في الـ OutPut.

وهذا يوضح الجزء الأول من نموذج الـ FSM، الذي ذكرناه أعلى.

أما إذا كان عندنا أكثر من Route إلى شبكة 192.168.10.0/24 كما في الشكل التالي، تعالوا لنرى كيف يتعامل معها الـ DUAL: أولاً لنرى ما هي الـ Routes الممكنة بالنسبة لـ R1 للوصول إلى شبكة 192.168.10.0/24:



```

R1#show ip eigrp topology all-links
**Output Omitted**
P 12.0.0.0/8, 1 successors, FD is 28160, serno 6
via Summary (28160/0), Null0
P 12.0.0.0/30, 1 successors, FD is 28160, serno 4
via Connected, FastEthernet1/0
P 192.168.10.0/24, 1 successors, FD is 156160, serno 7
via 12.0.0.2 (156160/128256), FastEthernet1/0
via 10.0.0.1 (158720/156160), FastEthernet0/0

```

هنا نلاحظ أن R1 لديه طريقين للوصول إلى شبكة 192.168.10.0/24 كما هو موضح في الـ OutPut ولكن المستخدم حالياً للوصول إلى شبكة 192.168.10.0/24

via 12.0.0.2 (156160/128256), FastEthernet1/0

عن طريق R3، وبفرض أن الـ LINK بين R1 و R3 حدث له Fail، نلاحظ أن الـ DUAL بدأ بالعمل طبقاً للـ FSM كالتالي:



## Dynamips

برنامج يقوم بعمل Emulation للهاردوير وهو برنامج رائع من تصميم طالب فرنسي اسمه كريستوف فيلوت عام 2005 ويستخدم في المراحل الاعلى من كورس CCNA حيث يستخدم نسخة IOS حقيقية وكل ما عليك اختيار النسخة المناسبة للراوتر ويكون عندك روتر حقيقي بنسبة خطأ صغيرة جداً .

وانا شخصيا افضل هذا البرنامج عن الجميع لان الواجهة الرسومية تساعدك على التعرف على المشكلة ولكن بدون واجهة رسومية ستفكر انت في مكان المشكلة وهذا جزء مهم لجميع الشركات وهو Troubleshooting حيث ان في الشبكات الواقعية قد يكون كل راوتر في مكان مختلف وهناك مشكلة معينة فتخيلك للمشكلة وفقاً للمعطيات هو ما تحتاجه .

وايضا من المزايا انه يمكن ربط الديناميس او GNS3 مع برنامج SDM أو برنامج VMware وبرامج اخرى قد لا تكون متصلة بشكل مباشر منها WireShark الذي يراقب الـ Packets ونلاحظ ان الديناميس يقوم باستهلاك جزء كبير من البروسيسور والرامات لذلك نستخدم قيمة idle-pc التي تقلل استهلاك البروسيسور ويمكن استخدام خاصية mmap = true لجعل الـ rوترات تأخذ الـ رام من الـ هاردديسك وليس من الـ رامات

```

C:\Program Files\Dynamips>
Cisco Router Simulation Platform (version 0.2.8-RC2-x86)
Copyright (c) 2005-2007 Christophe Fillet.
Build date: Nov 9 2007 09:54:39

ILI: loaded table "mips64j" from cache.
ILI: loaded table "mips64e" from cache.
ILI: loaded table "ppc32j" from cache.
ILI: loaded table "ppc32e" from cache.
Hypervisor TCP control server started (port 7200).
Shutdown in progress...
Shutdown completed.

C:\Program Files\Dynamips>
Reading configuration file...
Network successfully loaded

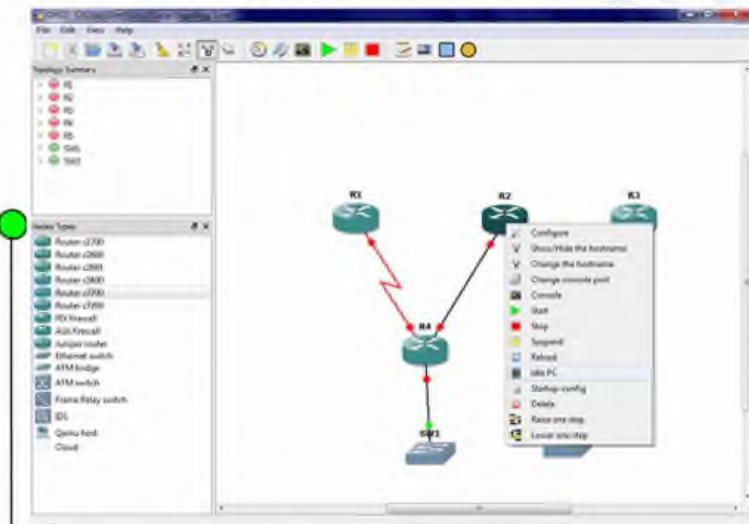
Dynamips management console for Dynamips and Penetration 0.11.0
Copyright (c) 2005-2007 Greg Anuzelli, contributions Pavel Skovajsa

=> list
Name      Type      State      Server      Console
R1        3640     stopped   AnR-PC:7200 2000
S1        3640     stopped   AnR-PC:7200 2001
=>

```

## GNS3 (Graphical Network Simulator)

برنامج يوفر الواجهة الرسومية لبرنامج الديناميس ويعمل بنفس مزايا برنامج الديناميس وايضا يجب تحديد قيمة idle-pc ويمكن اختيار mmap = true لتقليل استهلاك الـ رامات وقام بتطويره Xavier Alt و Jeremy Grossmann وهو برنامج رائع يستخدم في المراحل الاعلى من كورس CCNA .



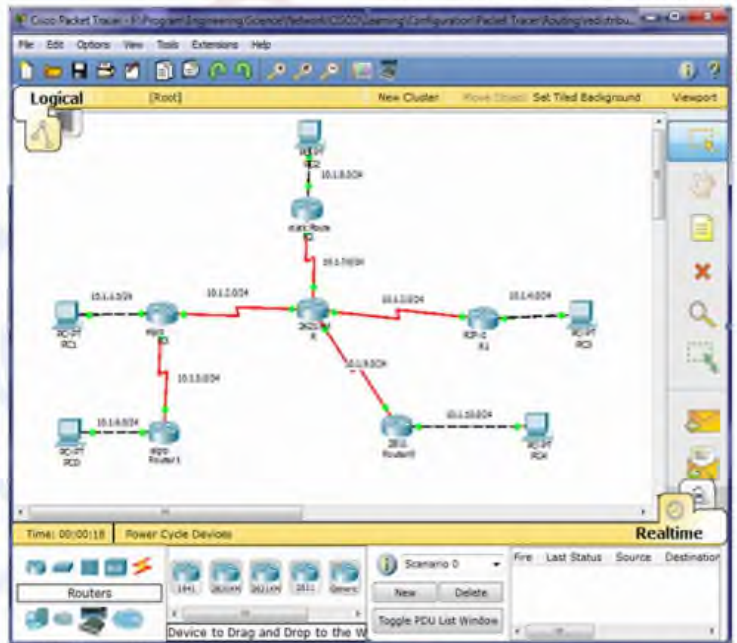
واتمنى ان يكون المقال نال اعجابكم ولكن كنصيحة يجب ان تمر على الثلاث برامج بالترتيب حيث تبدأ مع الباكايت ترايسر في شهادة CCNA وبعدها برنامج الديناميس مع الشهادات الاعلى وبعدها الواجهة الرسومية الـ GNS3

عمرو يحيى

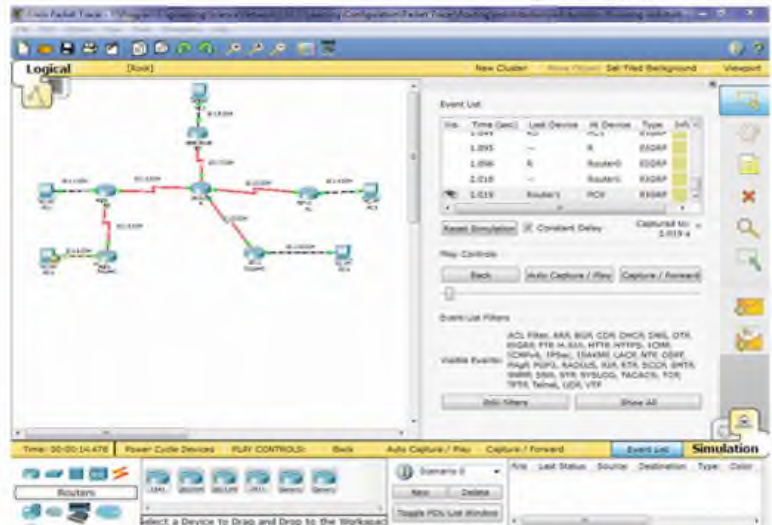
## الفرق بين Dynamips Packet Tracer GNS3

### Packet Tracer

برنامج مقدم من شركة CISCO تم تطويره بواسطة CISCO Networking Academy وهو برنامج محاكاة Simulation حيث يوفر المحاكاة والتصور والتقييم ويسهل على الدارسين تطبيق اللابات وربط النظرى بالتطبيق العملى ويفضل الباكايت ترايسر في المراحل الاولى لتعلم سيسكو لانه يتميز بسهولة استخدامة وسرعة حيث لا يؤثر على اداء الكمبيوتر ويشمل الاوامر الخاصة بكورس CCNA ولكنه في المراحل الاعلى تظهر به بعض المشاكل ويفضل حينها استخدام الديناميس او الواجهة الرسومية للديناميس ويقوم البرنامج بعمل محاكاة لكل من Routers, Switches, Hubs, Wireless Devices, WAN Emulation End Devices, WAN Emulation



ويستخدم الباكايت ترايسر للتعليم ويتميز بعدم تأثيره على الكمبيوتر من حيث استهلاك البروسيسور والرامات ويوجد بالبرنامج خاصية Simulation حيث يقوم بتمثيل انتقال الباكايت من مكان لآخر ونوع البروتوكول والوقت وهذا الخاصية تمكن الدارس لمناهج سيسكو لتخيل ما يحدث أثناء تنفيذ اى امر والملاحظة الفعلية للتعامل بين الاجهزة



لا تكسب المال وتخسر الناس فإن كسب الناس طريقة لكسب المال



# TV Broadcast



الخطوة الثالثة سوف تكون من أجل تحديد معيار الفيديو الذي سوف تبثه PAL or SECAN or NTSC وذلك يتم من خلال التوجه إلى VIDEO PROPERTIES وبعدنا نختار بحسب المعيار المستخدم في القناة وهذه صورة للتوضيح



في الخطوة الرابعة سوف نحدد كيفية وصول البث إلى التلفاز وهو أما من خلال انتين أو من خلال كابل وهذه صورة للتوضيح

## كيف تقوم بمشاركة

## أقنية التلفاز عبر الشبكة

بقلم : أيمن النعيمي

امتدادا للسلسلة التي بدأتها حول طريقة مشاركة الميديا على الشبكة وهي الصوت والصورة والتي سوف تمتد لتشمل الكثير من المواضيع الهامة والتي سوف تنتهي بموضوع سوف يكون الأول عربيا ان شاء الله والذي أفضل أن يبقى سرا حتى نضوجه لذلك تدوينتي لهذا اليوم سوف تكون حول طريقة مشاركة التلفاز وأقنيته على الشبكة

### متطلبات التشغيل

كرت تلفزيون

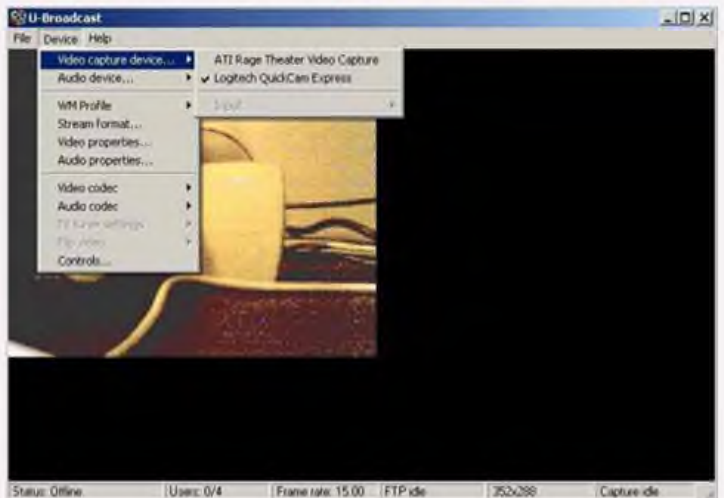
برنامج U-Broadcast تستطيع تحميله من الرابط التالي  
<http://www.softpedia.com/progDownload/U-Broadcast-Download-22775.html>

### طريقة الأعداد

بداية وقبل كل شيء نتأكد من تركيب كرت التلفزيون على الكمبيوتر وبعدنا نقوم بتسليط البرنامج على الجهاز وهو لا يحتاج أي خبرة عملية وبعد ان ننتهي تظهر لنا هذه النافذة ونقوم باختيار التالي



وكما يتضح لكم قمت بوضع الإشارة على video Tuner كما يمكنك من خلال هذا البرنامج مشاركة الكاميرا الخاصة بالجهاز الذي لديك كما في الصورة القادمة



في الخطوات القادمة نستطيع ان نتجاهلها لانها سوف تكون معه ولا تحتاج إلى أي تغيير لكن أفضل أن أذكرها حتى يكون الجميع بصورة كاملة حول طريقة الأعداد بعد ان نحدد كرت التلفزيون نقوم بتحديد مركز الصوت وهو سوف يكون كما هو موضح في الصورة لذلك لو أردت ان تشارك الكاميرا على الشبكة فيجب عليك اختيار المايكروفون الخاص بالجهاز



وقبل أن أنهى أحب أن أونود إلى نقطة مهمة وهي تحديد دقة العرض من خلال معرفة سرعة كبل الشبكة وهو يتم من خلال Device>WMV واختيار الدقة المناسبة وأنا أفضل دائما اختيار 384 Kbps أو 768 Kbps



وبهذا نكون قد أنهينا من أعداد السيرفر وبدأت عملية البث نتوجه الآن إلى أحد الاجهزة الموجودة على الشبكة ونفتح أحد برامج الفيديو مثل ويندوز ميديا بلير ونتوجه إلى خيار ونقوم بكتابة أيبي السيرفر متبوعا برقم البورت على الشكل التالي

mms://192.168.1.1:7474

والنتيجة سوف تكون على الشكل التالي



وأخيرا أحب أن أشير إلى إمكانية بث أحد محطات الستلايت من خلال ربط جهاز الستلايت بكرت التلفاز من خلال كبل التلفاز العادي وتوليف الكرت على المحطة الخاصة بقناة الستلايت وبث القناة على الشبكة وهي الطريقة التي وعدت أن أقدمها لأحد الأشخاص الذي أرسل لي على الخاص يسألني عن طريقة بث بعض المباريات على الشبكة .

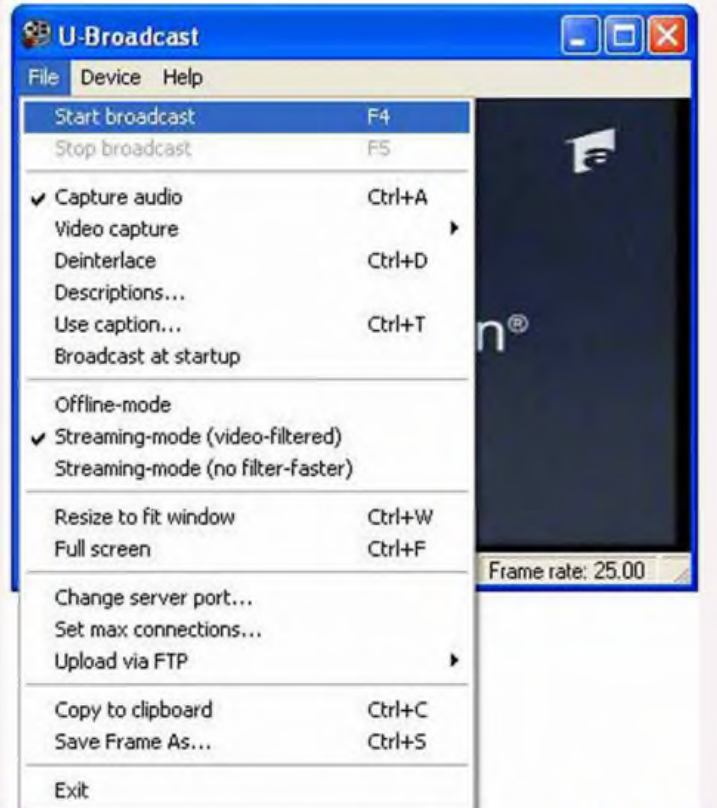
في الخطوة الخامسة نقوم بالضغط على F6 أو نتوجه إلى TV > Device Set channe > Tuner setting من اجل تحديد المحطة التي نريد بثها إلى الشبكة وهذه صورة للتوضيح



وأخيرا لتغيير المنفذ الذي سوف يتم من خلاله البث والذي عادة يكون 8080 نتوجه إلى File>Change Server Port ونقوم بكتابة منفذ جديد وهذه صورة للتوضيح



وأخر خطوة نضغط على F4 لبدا البث أو نتجه إلى File> Start Broadcast وهذه صورة للتوضيح أيضا

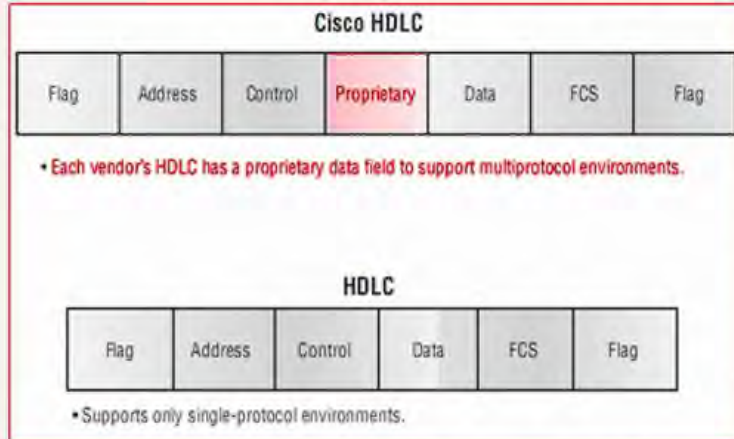




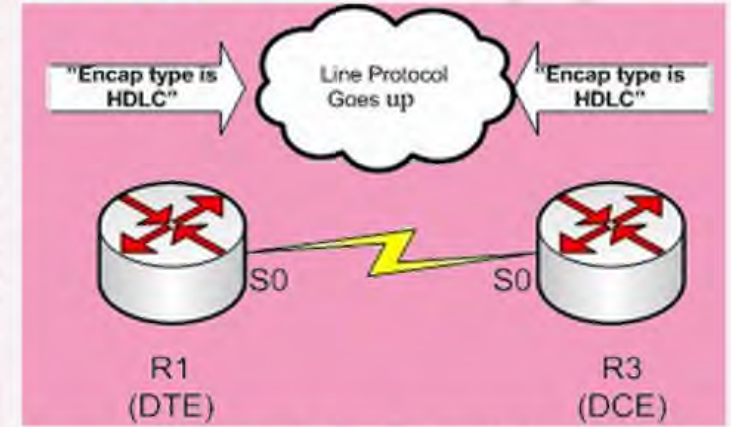
# تعرف معنا على بروتوكول الـ HDLC

بقلم: أيمن النعيمي

وبكلام آخر لكي يتم الاتصال بين الروتين من خلال الـ HDLC يجب عليهم أن يعملوا من خلال أحد بروتوكولات الطبقة الثالثة أي أما IP أو IPX أو AppleTalk وليس استخدام أثنان منهم أو ثلاثة في نفس الوقت وهذا ما قامت به سيسكو بتطويره فقد دعمت استخدام جميع البروتوكولات في نفس الوقت من خلال إضافة قسم جديد للـ Header وهو الـ Type وطبعا هذا لا يمنع باقي الشركات المصنعة من الاستفادة من هذه الخاصية أي إتاحة استخدام أكثر من layer Protocol 3 في نفس الوقت لكن بشرط إضافة نفس القسم للـ Header وخاص بي الشركة المطورة ويمكن أن نطلق عليها Priority وأن لم تكن لهذه الشركة Priority خاص بها إذا سوف يتوجب عليها استخدام البروتوكول الأساسي وطبعا سوف تطرأ لإستخدام بروتوكول واحد من بروتوكولات الطبقة الثالثة فقط والتي لم تعد مشكلة في وقتنا الحالي بسبب اعتماد أغلب الشركات على بروتوكول الـ IP وهذه صورة توضيحية لتقريب المعلومة بشكل أكبر



وكون البروتوكول يعمل على الطبقة الثانية فهذا يعطيه ميزة الـ Error Detection أما السلبية الثانية في استخدام هذا البروتوكول هو عدم وجود أي نوع من أنواع الـ Authentications بين الروتين بغض النظر عن كون البروتوكول هو الخاص بسيسكو أو العادي ويعتمد على آلية واحدة في الضغط والمعروفة باسم Stacker وأخيرا لا يسعني إلا أن أذكر الميزة الوحيدة لهذا البروتوكول وهي الأعدادات ففي سيسكو لن تحتاج لكتابة أي شيء لتشغيل البروتوكول كون هذا البروتوكول هو الـ Default على أجهزتها وعلى غير أجهزتها لن تحتاج أكثر من تحديد نوع الـ Encapsulation في HDLC



وتعني High Level Data-Link Control وهو IBM عام 1974 تحت اسم Synchronous Data Link Control أو SDLC وبعدها أحيل إلى المنظمة العالمية للمعايير ISO والتي قامت هي أيضا بتطويره وإعادة تسميته إلى الاسم المعروف في وقتنا الحالي HDLC وقبل أن ندخل أكثر في التفاصيل أحب أن أوضح أن جميع البروتوكولات المستخدمة في شبكات الـ WAN تعمل على الطبقة الثانية Data Link لذا يعد هذا البروتوكول أحد بروتوكولات الطبقة الثانية وكما ذكرنا أن منظمة الـ ISO هي أول من قام بتطويره ويعد استخدامه ينحصر على اتصال نقطتان بشكل مباشر أو كما يعرف بي الـ PPP (Point-to-point) ومن أكثر الأخطاء الشائعة التي يقع فيها بعض المهندسين هو الاعتقاد أن بروتوكول الـ HDLC هو بروتوكول ليسيسكو فقط لأن الـ HDLC والـ Cisco-HDLC هما بروتوكولان أثنان يعد الثاني منها خاص بسيسكو ولا يعمل إلا على أجهزتها لذلك عندما تقوم بربط روتر سيسكو مع روتر لشركة أخرى فإن الاتصال بينهم لن يعمل وسوف تطرأ إلى تغيير البروتوكول إلى بروتوكول آخر لكي نتمكن من الاتصال بينهم والسبب لأن سيسكو لا تدعم البروتوكول الأساسي على أجهزتها وهي تدعم بروتوكول الـ Cisco-HDLC فقط لذا فأول سؤال سوف يخطر على بالك ماذا فعلت أو ماذا طورت سيسكو في هذا البروتوكول؟ للإجابة على هذا السؤال يجب علينا أن نعلم حقيقة هامة في بروتوكول الـ HDLC وهي سلبية هذا البروتوكول وهي عدم دعم أكثر من بروتوكول Layer 3 في نفس الوقت

للدومين وبكل ما يحويه من سيرفرات ومستخدمين و Site بالإضافة إلى Exchange Server والـ Policy المطبقة على كل وحده والكثير من الأشياء وكل هذا يتم بضغطة زر واحدة .

المتطلبات

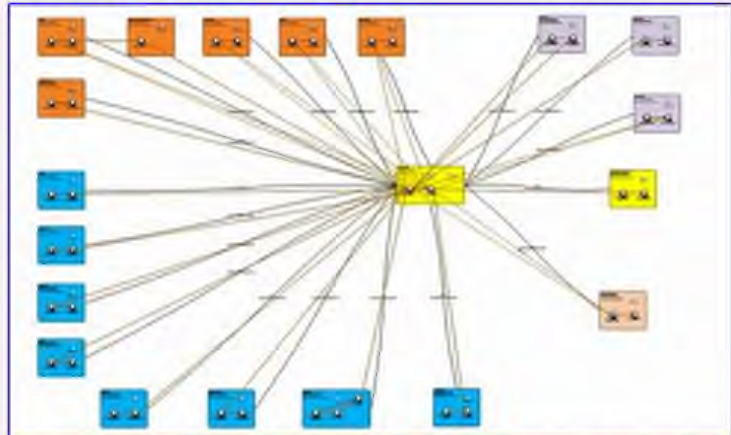
Microsoft Office Visio 2003 or 2007  
Microsoft .NET Framework Version 2.0  
Active Directory Topology Diagrammer



بعد تحميل كل المتطلبات وتنصيبها على النظام وهي لا تحتاج إلى أي خبرة مجرد - Next - Next-Finish نتجه إلى قائمة الـ Start ونقوم بتشغيل الأداة كما هو موضح بالشكل القادم

## كيف تقوم برسم وتوثيق الـ Active Directory

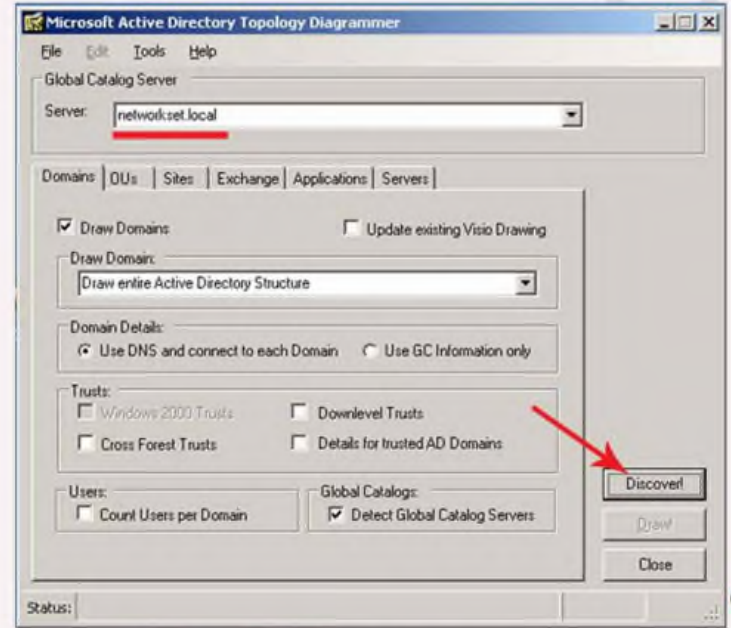
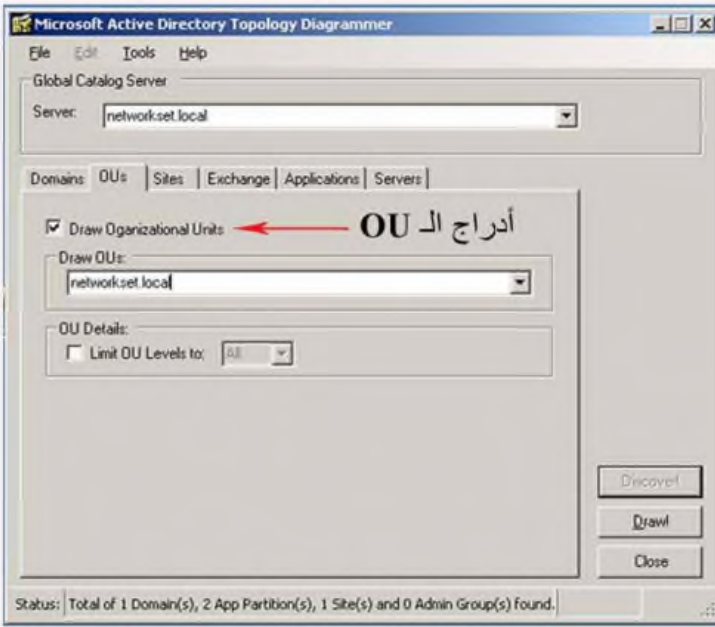
بقلم: أيمن النعيمي



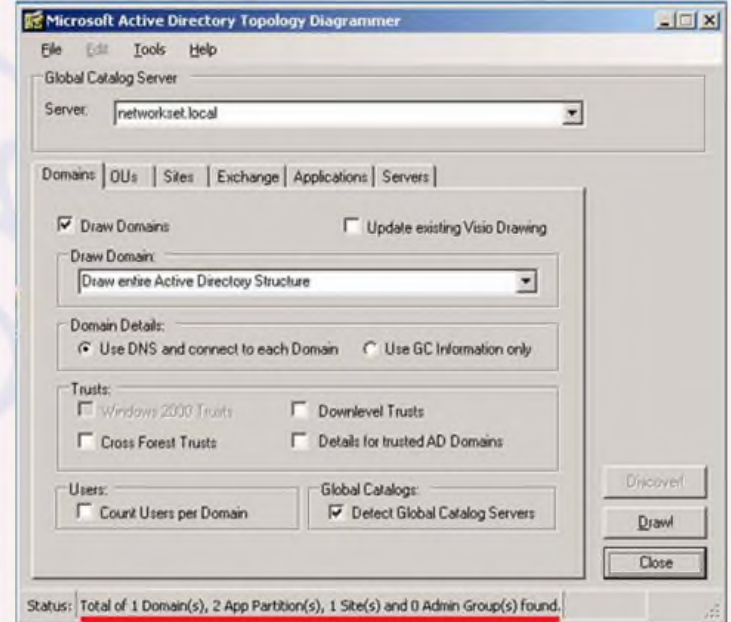
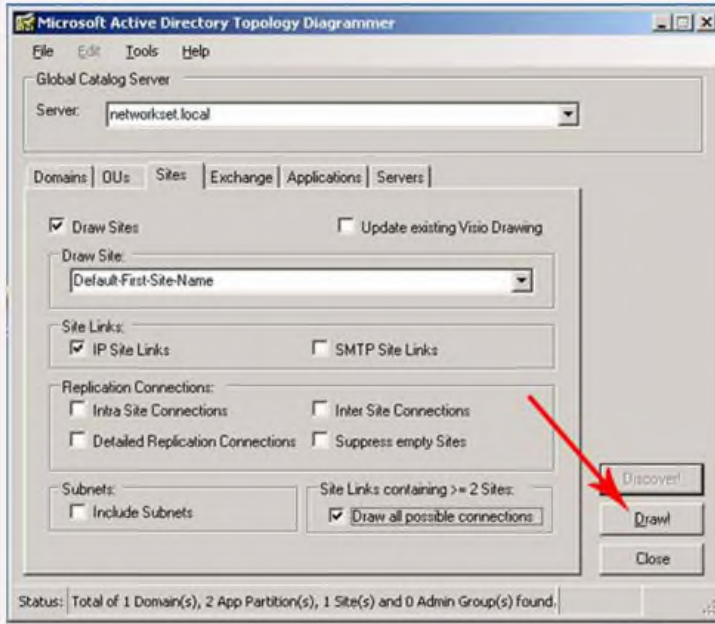
ثناء تصفحي لأحد المواقع وجدت أداة صغيرة بحجمها وكبيره بمفعولها يطلق عليها Active Directory Topology Diagrammer وهذه الأداة هي عمل خريطة كاملة للدومين وتوضيح المجموعات والمستخدمين الموجودون بكل مجموعة وبكل OU وبشكل أوتوماتيكي تعتمد الأداة على برنامج الـ Visio المعروف وهي تقوم بعمل Diagram كامل



لتظهر بعدها لنا نافذة الأداة نقوم بكتابة أسم الدومين بشكل كامل في الصندوق العلوي

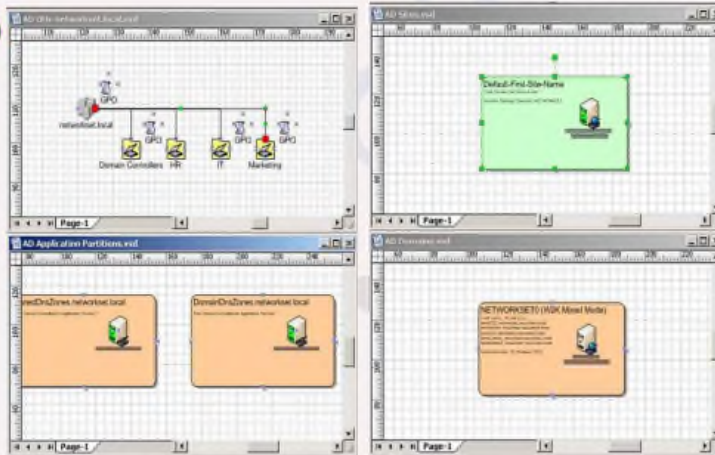


وبعدنا نضغط على كلمة Discover ليبدأ بجمع المعلومات المطلوبة

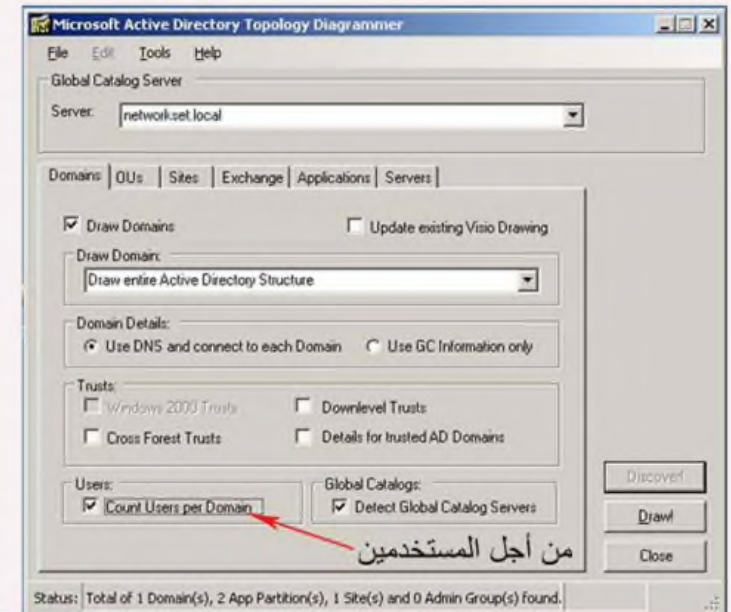


تابع بنفسك باقي النوافذ وحدد كل الأمور التي تريد وضعها في الـ Diagram وأضغط بعدها على Draw ليبدأ الرسم على برنامج الـ Visio والنتيجة سوف تكون على الشكل التالي (الدومين الذي قمنا بالتطبيق عليه بسيط جدا لذا لن تجد الكثير من الأمور)

بعد أن ينتهي نبدأ بتحديد المعلومات المراد وضعها على الـ Diagram من خلال التنقل بين النوافذ الموجودة



تستطيع أن تشاهد معي من خلال الصور أن الأداة ترسم وتوثق كل ماتطلبه منك وطبعاً هذا الشيء مهم جداً بالنسبة لكل مدير شبكة أو مسؤول عن الدومين في الشركة كما تتيح الأداة عمل تحديث للـ Diagram لو في حال أردت ذلك وكل هذا واضح من الأداة ولا يحتاج إلى أي خبرة كبيرة.

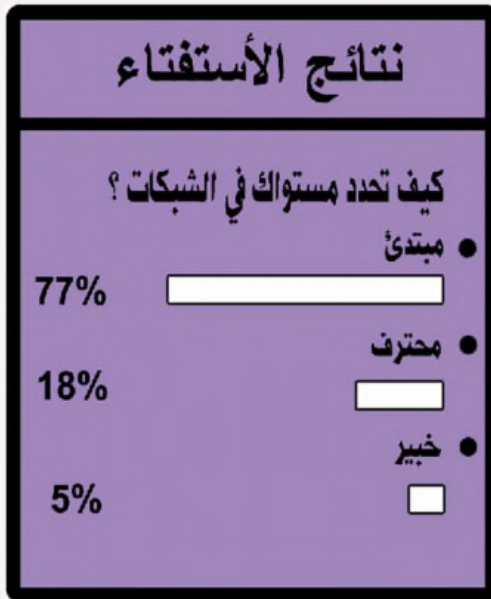


من أجل المستخدمين



# نتائج الاستفتاء الشهري

لا يوجد مداخله هذا الشهر على نتائج التصويت فقط معرفة مستوى ونوعية زوار المدونة .





## الشبكة الهدف أو ( Target Network ) :

تغطي هذه الشبكة صلاحيات مرور محددة ( Limited Access ) لعبور الشبكة والوصول الى البيانات او المعلومات فكما يعرف الجميع انه بعد انتقال هذه البيانات من بوابة الاتصال فان البيانات تكون في فضاء الانترنت سهلة المنال لكل من اراد ان لم يكن هناك من يضبط حركة الوصول الى هذه البيانات وهنا تبدأ أهمية هذه الشبكة ..

كما انها تعطي ايضا صلاحيات محددة لمن اراد الدخول الى الشبكة عن بعد ( Remote Access ) وذلك بضبط شروط معينة واعطاء صلاحيات والسماح لأشخاص معينين بالوصول الى معلومات معينة ... وتحديد مثل هذه الصلاحيات الى الوصول الى معلومات معينة أمر غاية في الأهمية اذا اخذنا بعين الاعتبار إمكانية وصول أطراف غير معنية الى هذه المعلومات فيترشيد البيانات والصلاحيات المعطاة الى الشبكات او الاتصال البعيد تقل الخسائر الممكنة والمتوقعة اذا ما حصل واستطاع احد الوصول الى هذه الشبكة بطريقة غير شرعية ...

أحب هنا ان اوضح نقطة غاية في الأهمية فيما يتعلق بالحزم المعلوماتية بعد خروجها من بوابة الاتصال فهذه البيانات غير قابلة للتشفير ( Unencrypted ) بعد خروجها من بوابة الاتصال لذا فان نظام حماية عالية الكفاءة أمر لا غنى عنه .

## من يستخدم نظام الشبكات الافتراضية ؟

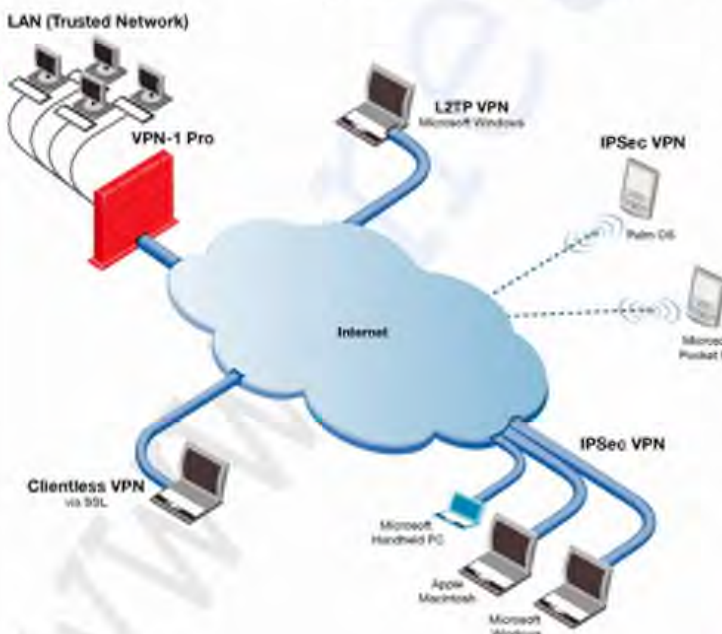
تقوم هذه الشبكات على أي شبكة داخلية ( LAN ) .... وتستطيع أي شركة استخدام مثل هذه الشبكات الافتراضية للاتصال ببعضها البعض اينما كانت فروعا وذلك لانها رخيصة التكاليف ان لم تكن معنومة ايضا ويلزمك لاستخدام مثل هذه الشبكة وجود نظام تشغيل داعم للشبكات مثل نظام التشغيل ( Windows Server 2000 ) او أي نظام مشابه تتم عملية تنصيبه على جهاز يعتبر السيرفر ...

تساعد ايضا هذه الشبكات رؤساء الشركات على الدخول الى الشبكة الداخلية ( Intranet ) والخاصة بالشركة ومن ثم القيام بأعمالهم وهم في منازلهم كما ولو أنهم في مكاتبهم .. كما انها تساعد الموظفين التنفيذيين على الاتصال بالشبكة من أي مكان في العالم فكل ماعليه فعله هو فقط شبك جهازه النقال بأي شبكة انترنت ومن ثم العبور عبر بوابة الاتصال بعد اثبات الهوية والدخول الى المعلومات التي يريد كما لو انه في الشركة نفسها

الى هنا تنتهي هذه المقدمة البسيطة عن نظام الشبكات الافتراضية ... واسمها مقدمة لان هذه الشبكات علم قائم في ذاته لايمكن حصره في موضوع او اثنين او عشرة ولم ارد التعمق اكثر في آلية عمل الشبكة لتوسيعها ...

أحببت فقط ان اوجز باختصار هذه التكنولوجيا العملاقة بسطور بسيطة وسهلة

أسأل الله ان يوفقني وإياكم لما يحب ويرضى



قد لا يخفى على الكثير منكم بأن البيانات المرسله عن طريق الانترنت ولنقل على سبيل المثال الرسالة التي يرسلها الشخص منا الى صديقه في الطرف الآخر من العالم عن طريق البريد الالكتروني تتحول الى طرود صغيرة تحتوي على معلومات مترابطة يتم تجميعها عند الطرف الآخر وهو المستقبل .. يتم تقسيم هذه الرسالة الى اقسام صغيرة بحيث تسهل عملية نقلها وتساعد في عملية اسراع النقل ايضا ... لكن هذه الطرود او الحزم المعلوماتية غير آمنة مطلقا وقابلة للخسارة اذا ما عرفنا ان الحزمة لا بد وان تصل الى محطتها الأخيرة في 15 قفزة متتالية تتم بين اجهزة من الدرجة الثانية من مستويات الكفاء تسمى بالراوترز ( Routers ) حيث يقوم هذا الجهاز بتقسيم هذه العينات والتحكم بمسارها معتمدا بذلك على معلومات توفرها له الاجهزة المماثلة والقريبة منه بحيث تقفز كل حزمة اقل من او 15 قفزة فقط حتى تصل الى محطتها الأخيرة وهي عند المستقبل والا فان هذه الحزمة تصعب ... بالنسبة للشبكة العنكبوتية بشكل عام لا تحدث عمليات الخسارة المعلوماتية دائما ولكنها متوقعة اذا ماتعتل احد هذه الاجهزة ...

• لكن ما الفرق بين الشبكة العنكبوتية العادية والشبكة الافتراضية ؟ هنا يبدأ مفهوم الامن والحماية والحرص على الخصوصية في نقل المعلومات والبيانات

## كيف تتم حماية البيانات في الشبكة الافتراضية ؟

تتم حماية البيانات بشكل عام عادة بتشفيرها بحيث يصعب فهمها اذا ما تمت سرقتها ... لكن ايضا حتى تشفير المعلومات لا يكفي احيانا اذا وضعنا بعين الاعتبار وجود انواع كثيرة من آليات التشفير والتي يمكن كسرها بطريقة او باخرى وما اكثر الامثلة هنا ابتداءا بسرقة ارقام البطاقات الائتمانية وانتهاءا بسرقة البرامج القيد البرمجة من اصحابها وغيرها الكثير من الامثلة ... لذلك كان لا بد دائما من اتباع لوائح قوية ومؤكدة من شركات كبيرة وذات اسم لامع في عالم التشفير كنقطة مبدئية للعمل على هذه الشبكات الافتراضية ...

هنا تظهر مشكلة اخرى وهي ان المعلومات التي يتم ارسالها بين الشبكتين كما عرفنا مسبقا يتم تقسيمها الى حزم صغيرة يتم ارسالها باستخدام بروتوكولات متعددة تعتمد على طبيعة الشبكة والمعلومة مما قد يسبب ضياع هذه المعلومات وعدم الاستفادة منها اذا وضعنا في عين الاعتبار عجز الشبكة المستقبلية لهذه الحزم على فهمها نتيجة لعدم تعرفها على طبيعتها لذا كان من الواجب ايجاد حل وسطي وسلمي وأمن في نفس الوقت وهذه ماقدمته شركة ( Tunneling ) حيث اقترحت هذه الشركة ان يقوم بارسال الحزم المعلوماتية في طرود عادية في داخل طرود اخرى تكون مشفرة بحيث ان الطرود الحاوية على الطرود المعلوماتية تكون مفهومة لدى الشبكة المستقبلية .. وبهذا تحل مشكلة قرانة هذه الحزم المعلوماتية ..

## • مكونات الشبكة الافتراضية ..

تتكون الشبكات الافتراضية من العميل ( Client ) وبوابة الاتصال ( GateWay )

## • وظائف بوابة الاتصال ( GateWay )

تنقسم الى قسمين ( HardWare & SoftWare ) موجودة في مقر الشركة . في معظم الشركات تتوفر الشبكات المحلية والتي تربط اجهزة الشركة الواحدة ببعضها البعض ( LAN ) ولكل شبكة محلية شبكة افتراضية خاصة بها تعتبر نقطة البداية والنهاية لهذه الشبكة تتحكم بها بوابة الاتصال والتي بإمكانها الاتصال بأكثر من عميل ( Client ) في الوقت الواحد باستخدام قنوات متعددة والتي تعتمد في عددها على مكونات الكمبيوتر الصلبة ( HardWare ) وسرعة الاتصال ..

تقوم بوابة الاتصال بالعديد من المهام كبدأ واعطاء الصلاحيات وادارة القنوات بعد بدأ الاتصال بعد ذلك تقوم بوابة الاتصال بإيصال المعلومات الى الجهة الصحيحة على الشبكة .. كما ان بوابة الاتصال تقوم بعملية مهمة لغاية وهي عملية تشفير البيانات ( Encryption ) قبل ارسالها وتقوم بفك تشفيرها ( Decryption ) عند استلامها ..

## • وظائف العميل ( Client ) :

يقوم الجهاز العميل ( Client ) تقريبا بنفس مهام بوابة الاتصال اضافة الى ذلك انه يقوم باعطاء تصاريح الدخول الى الشبكة على مستوى الأفراد المستخدمين .. لا بد من توفر بعض النقاط الضرورية اذا ما اخذنا بعين الاعتبار ان العميل هو حلقة الوصل بين طرفين فمن هذا المنطق وجب اخذ الحذر من احتمالات اصابة بعض الملفات المرسله بفايروسات او حتى حملها لملفات تجسس مما قد يخل بأمان الشبكة لذا كان من الضروري التأكد من وجود مكافح فايروسات قوي ومحدث بأخر التحديثات من الشركة الام وايضا لا يمكن الاستغناء عن جدار ناري للتأكد بأنه بالفعل حتى ( لو ) وجدت ثغرة بسيطة في هذه الشبكة فان هناك من يرصدها ويحميها ... وعندما نتكلم عن الحماية فان الشبكة الافتراضية تتم حمايتها في ثلاث نقاط عبور وهي :

1- بوابة الاتصال ( GateWay )

2- الشبكة الهدف ( Target Network )

3- العملاء ( Clients )



ممالك على الشركات التي تتناول فيما بين فروعها معلومات عن مشاريع قادمة ووصفا دقيقا لمكونات وطريقة عمل هذه المشاريع ... سرقة معلومة واحدة قد تكلف الكثير وأعني بذلك الكثير ... من هذا المنطلق بدأ مايسمى ببرامج الحماية وبدأت كلمة الحماية تطفوا على السطح وتثبت أقدامها في مجال واسع وعالم مفتوح هو عالم الانترنت ...

لكن السؤال الذي يطرح نفسه هنا : هل أنا بالفعل إذا قمت باتخاذ جميع سبل الحماية فأنتي وبياناتي في أمان ؟

لن اجيب على هذا السؤال بأفضل ما اجاب خبير امن الشبكات Peter Norton حيث قرأت له في احدي كتبه انه قال ( الجهاز الوحيد المؤمن والمحمي بنسبة 100% من أي مخاطر للسرقة والاختراق هو جهاز يوضع في زاوية الغرفة ولكنه لايشبك نهائيا على الانترنت ) .....

وكما قيل ( الحاجة أم الاختراع ) من هذا المنطلق بدأت الشركات الكبيرة وحتى الصغيرة النامية بالبحث عن سبل أخرى لحلحلة هذه المشكلة وحتى لو بالالتفاف عليها ...

وكان لهم مبتغاهم ولو الى 95% حيث تم اكتشاف مايسمى ب VPN ( Virtual Private Networking ) او بالعربية ( الشبكات الافتراضية الخاصة ) واعذروني على الترجمة فهي اجتهدات شخصية ...

## ماهي ال VPN :

الاسم يدل على كونية هذه الشبكات فهي شبكات افتراضية لوجود لها في الواقع ولكنها مع ذلك تؤدي واجبها على اكمل وجه كأكثر انواع الشبكات أمانا وأكثرها شيوعا وحتى استخداما بين الشركات الكبيرة .. طبعاً كونها شبكات افتراضية فلا بد من وجود داعم حقيقي يحمل هذه الافتراضية الى ارض الواقع .. لا بد لهذا الداعم ان يكون مستقيظا كل الوقت جاهزا ومستعدا في أي لحظة وهنا كانت الشبكة العنكبوتية لتثبت انها دائما الارض الخصبة لكل من اراد الثمر بقليل من الجهد في الغرس والسقاية .. هذه الشبكات الافتراضية هي نفسها الشبكة العنكبوتية لكن تم توظيف خصائصها لتلائم سرية نقل البيانات والحفاظ على امن المعلومات

## كيف تعمل الشبكات الافتراضية ؟

حتى نستطيع فهم آلية عمل الشبكات الافتراضية لابد من التوقف قليلا عند آلية عمل الشبكة العنكبوتية او غيرها من الشبكات في البداية .. لن اتعمق كثيرا في وصف آلية العمل لكن سأطرق الى ما يهمنا منها ..

في عصر اقل ما يقال عنه انه عصر التكنولوجيا وسرعة المعلومات .. عصر أصبحت فيه المعلومات هي العنصر الرئيس في جميع تحركاتنا وتنقلاتنا وتحديد مرابحنا وحتى خسائرنا .. ومع ازدهار وتطور اساليب التقنية الحديثة وحتى تواكب الركب في توسع وانتشار الشركات العالمية كان لابد من احداث ثورة في مجال الاتصالات الشبكية السلكية منها واللاسلكية بين فروع هذه الشركات .. فعلى سبيل المثال يعتبر تواصل الفرع الرئيسي لشركة مايكروسوفت العملاقة مع احد فروعها في دولة ماليزيا والتناقص حول قضية وجود ثغرة أمنية اكتشفها خبراء مايكروسوفت في معامل روسيا أمراً بالغ السرية وبالغ الخطورة أيضا وبالمقابل فإن اجراء مكالمات هاتفية مطولة كهذه قد تسبب في انهالك ميزانية اكبر الشركات اذا ماوضعنا في عين الاعتبار اجراء مكالمات على مدار الساعة واتمام العمليات هاتفيا .. لذا كان الحل موجودا وسهلا وممكنا للجميع وهنا تبدأ احد فوائد الانترنت الجملة في اتمام عمليات التواصل بين الاطراف المعنية بأقل التكاليف .. وشكرا للانترنت الذي أزال عن ظهور الشركات عباً فواتير الاتصالات في آخر كل شهر لكن الانترنت أفضل مافيه انه باب مفتوح للجميع وأسوأ مافيه انه ايضا باب مفتوح للجميع .

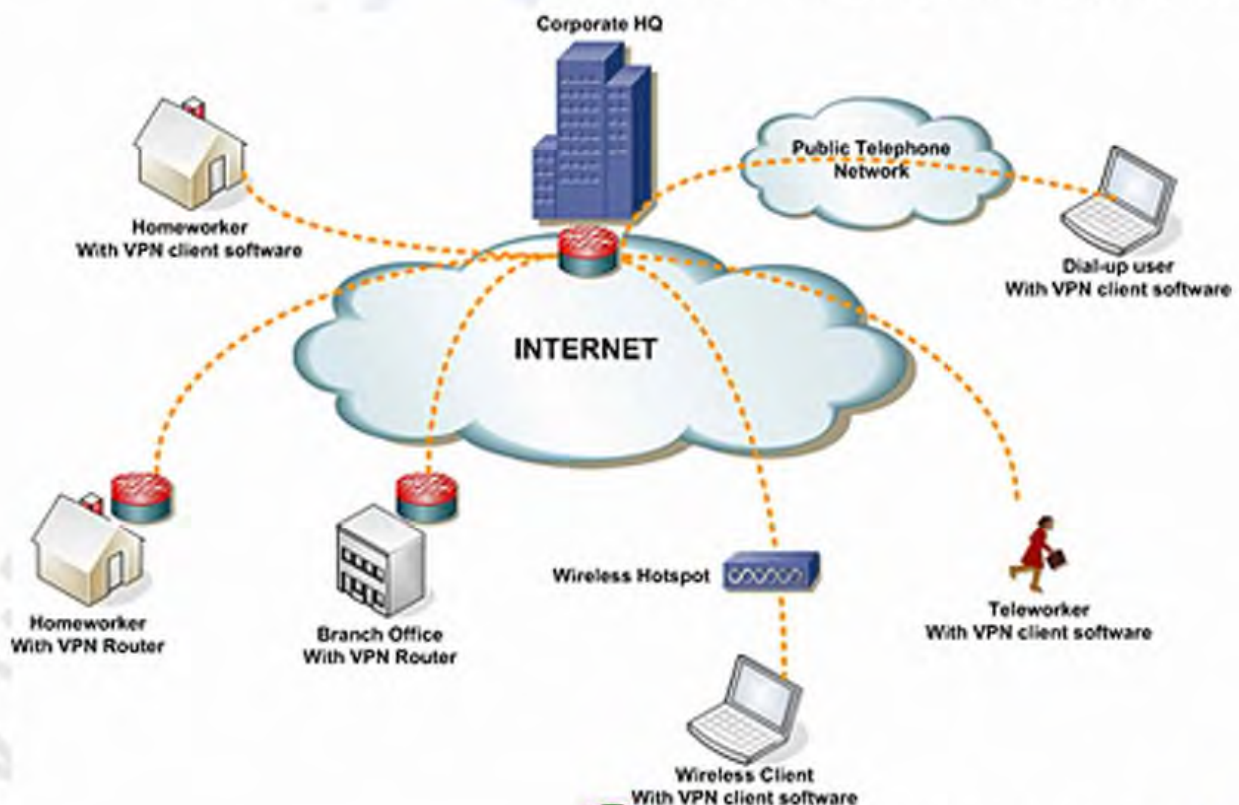
وهنا يبدأ القلق ... اسئلة تطرح على مدار الساعة .. هل أنا مراقب ؟؟؟ هل اخترق أحد جهازي ؟؟ هل تمت سرقة هذه البيانات ؟؟؟ والكثير الكثير منها !!! أسئلة قد لا تلج الى عقول المستخدمين العاديين للانترنت .. فجل ما تحتويه اجهزتنا هي بعض من الملفات والتي حتى وان فقدت فمصدرها الرئيسي الانترنت مرة أخرى .. او ان نخسر اشتراكا تبقى منه لحظات قليلة لن يستمتع من سرقة بها .. قد تكون خسارة البريد الالكتروني من اكبرها وقعا في النفوس لأنها شيء من الخصوصية والتي يكره الانسان بطبيعة حاله ان يفقدها او يعرضها على الغير .. كل هذه الخسائر لا تعني شيئا في الحقيقة اذا ماقارناها بخسارة بحث امضى صاحبه الشهور الكثيرة وسهر الليالي الطويلة ليفقده في ليلة مظلمة ...

لكن ماذا عن المستخدمين الحقيقيين للشبكة العنكبوتية ؟ ماذا عن اصحاب رؤوس الاموال والذين تتم معاملاتهم من بيع وشراء عن طريق هذه الشبكة ؟ هل سبق لك ان قمت بعملية شرائية من الانترنت ؟

في الحقيقة اتوقع ان معظم من سيقرا مقالتي هذا لم يسبق له ان فعل ذلك وبنيت كلامي على نتيجة بحث اجرته مجلة PC Magazine في عددها العاشر من تشرين الأول من عام 2003 والتي شارك فيها حوالي 136 شخصا 86% منهم لا يشتركون من الانترنت .. أنا شخصيا لا أفعل ذلك حاليا مع انني قمت بذلك مرتين حتى الآن والحمد لله انني لم اتفاجأ حتى الآن برصيدي في البنك وقد وصل الى الصفر .. مع ذلك الشعور بالخوف من المجهول دائما يروادني بانني قد واجه يوما اغبر مثل هذا لا سمح الله ..

لماذا كان هذا التخوف من الشراء عبر الانترنت !!! هنا تأتي مسألة خطيرة جدا وهي مسألة الحماية .. حماية البيانات الشخصية ...

هذا على مستوى الفرد العادي والتي تمثل خسارة 10 ريالات قد تكون محزنة له





# جونوس من جونيبر نظرة عن قرب

بقلم: أيمن النعيمي

والذي يسمح لنا بالتعديل وتغيير وإضافة بعض الأعدادات لكن ليس بالصورة التي تتصورها ولكي أقرب لك الفكرة بشكل أكبر سوف أعرض عليك نتيجة كتابة إشارة الأسطفا

## Juniper's JUNOS

root# ?	
Possible completions:	
<[Enter]>	Execute this command
activate	Remove the inactive tag from a statement
annotate	Annotate the statement with a comment
commit	Commit current set of changes
copy	Copy a statement
deactivate	Add the inactive tag to a statement
delete	Delete a data element
edit	Edit a sub-element
exit	Exit from this level
extension	Extension operation
help	Provide help information
insert	Insert a new ordered data element
load	Load configuration from ASCII file
quit	Quit from this level
rename	Rename a statement
replace	Replace character string in configuration
rollback	Roll back to previous committed configuration
run	Run an operational-mode command
save	Save configuration to ASCII file
set	Set a parameter
show	Show a parameter
status	Show users currently editing configuration
top	Exit to top level of configuration
up	Exit one level of configuration
[[edit	

أول ماسيلفت تظرك أن الأوامر هي أوامر تنفيذ فقط ولا يوجد أي أمر يساعدني لكي أقرر ما أفعل وهذا يعود إلى طريقة التعامل مع جونوس وحقيقتنا أن أحب دائما تشبيه فكرة التعامل مع جونوس مثل التعامل مع لغة برمجة فانت ترى كل شيء يتم من خلال اكواد تقوم أنت بكتابتها ويقوم هو بتنفيذها ولو نظرنا إلى أمر عرض الأعدادات لوجدناه مثل هذا الشكل

```
root> show configuration
## Last commit: 2010-05-24 13:34:23 UTC by root
version 9.0R1.10;
system {
  root-authentication {
    encrypted-password "$1$srYh6cKn$B.706Hk9hvmieudr029Ih1"; ## SECRET-DATA
  }
  syslog {
    user * {
      any emergency;
    }
    file messages {
      any notice;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
  }
}
```

فلو في حال أردت أن تضيف شيء يجب عليك أولا أن تتجه إلى المكان المخصص لهذا الكود وتقوم بكتابتها هناك وهذا مانفعله عندما نريد تنفيذ معين فأننا أملك طريقان

الطريق الأول أن أتوجه إلى ذلك المكان وأقوم بكتابة الشيء الذي أريده ويتم التوجه من خلال استخدام الأمر edit والذي ينقلني من مستوى آخر فأننا عندما ادخل إلى الـ Top level أكون في الـ Configuration Mode وعندما أستخدم الأمر edit أتتحرك إلى مستوى أقل وهذا مثال يوضح كيف أنتقل من مرحلة إلى مرحلة من خلال الأمر edit

مقالتي لهذا العدد حول جونوبر سوف أخصصها لكي أجيب على أحد الطلبات التي وصلتني على الأيميل بخصوص JUNOS وتحديد الترتيب الشجري للأوامر المستخدمة وكيفية التحرك والتنقل بينها بالإضافة إلى كيفية تنفيذ الأوامر والتعديل على الأعدادات الموجودة

فعندما ينتقل أي طالب دارس لمنتجات سيسكو إلى دراسة منتجات جونوبر أول مايقابله هو نظام التشغيل الفريد من نوعه والذي يختلف تماما عن سيسكو فنحن هناك تعودنا أن نكتب الأمر مباشرة وبعدها نقوم بكتابة exit وينتهي الأمر لكن مع جونوس الأمر مختلفا قليلا فكما تحدثنا من قبل أن جونوس مبني على نظام تشغيل يونكس UNIX لذا الولوج إلى الروتر أو السويتش لن يكون مباشرة مع سطر الأوامر الخاص بالأعدادات بل إلى الـ Shell الخاص بيونكس لذا يتوجب عليك كتابة الأمر cli للتعامل مع الجهاز المقصود مباشرة وهذه صورة للتوضيح

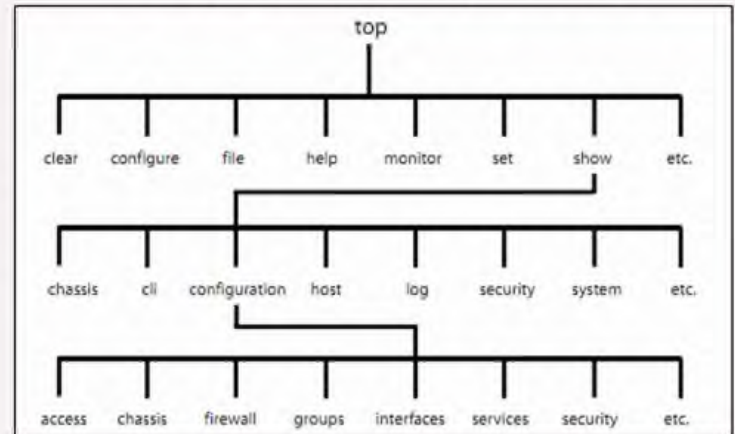
```
host {ttyd0}

login: root
Password:

== JUNOS 8.3R2.8 built 2007-07-07 00:21:56 UTC
root@host% cli
root@host>
```

Shell Prompt  
CLI Prompt

بعد أن ندخل على موجه الأوامر نصل إلى الـ Operational Mode وهي الوضعية التي تسمح لنا عادة بالمراقبة ومراقبة الأعدادات وال Troubleshoot والتي تناظرها في سيسكو الـ Privileged Mode وقبل أن نتحدث عن الأوامر وأنواعها لننتحدث عن أمر مهم فكما هو معروف عند الأشخاص الذي يتعاملون مع أجهزة يونكس وعائلته أن ترتيب الملفات هناك يكون على شكل شجري والتي عادة مايكون "/" هو قمة الشجرة وبعدها تأتي باقي الملفات والمجلدات وفي جونوبر الأمر ذاته فلو في حال أردت أن تكتب أمر ما فانت الآن في أعلى قمة لكن في الـ Operational Mode ولأيضاح سوف أستعين بمثال صغير مصور



طبعاً قد يخطر على بالك أن الأمر مشابه لنظام التشغيل في سيسكو فأننا أقوم بكتابة الأمر Show وأجد بعده نفس الترتيب المتبع وسوف أقول لك أصبر حتى نصل إلى الوضعية الثانية وعندها سوف يتضح الموضوع لك بشكل أفضل وقد أحببت أن أوضح لك الأمر من البداية قد تدرك أن الأمر هو نفسه هنا وهناك لذا لندخل إلى الوضعية الثانية وهي وضعية الـ Configuration Mode من خلال كتابة الأمر configure

## Juniper's JUNOS

```
root> configure
Entering configuration mode
[edit]
#root
```



وينفس هذا الأسلوب وهذه الطريقة أقوم بأعداد الروتر وذلك من خلال اضافة أكواد إلى صفحة الأعدادات لكن إذا طلبت منك أن تحذف شيء من هذه الصفحة ماذا تفعل ؟ الأمر بسيط نقوم بكتاب الأمر delete

#### Juniper's JUNOS

```
root# delete interfaces em0 unit 0 family inet address 192.168.10.1
```

أو استطيع الاكتفاء بأمر delete interface em0 طيب لنفرض أنني أريد تغيير الأبي الموجود فماذا يجب علي أن أفعل ؟ سوف تقول لي توجه إلى ذلك المكان وقم بحذف الرقم وبعدها قم بكتابة رقم جديد من خلال أمر set ؟ لكن ماراتيك بأمر جميل جدا وهو replace أو استبدال سوف أكتب فيه ضع هذا الرقم 192.168.10.2 مكان هذا الرقم 192.168.10.1 ينتهي الأمر

#### Juniper's JUNOS

```
root# replace with 192.168.10.2 pattern 192.168.10.1
```

أعتقد أنك قد بدأت تحب جونيير وتحب نظام التشغيل الخاص بها لنشاهد هذا المثال أيضا

#### Juniper's JUNOS

```
root# rename interfaces em0 to ge-0/0/0
```

ببساطة قمت بتغيير المسمى الخاص المتبع في عملية المحاكاة من em0 إلى ge-0/0/0 طيب سوف معي آخر مثال

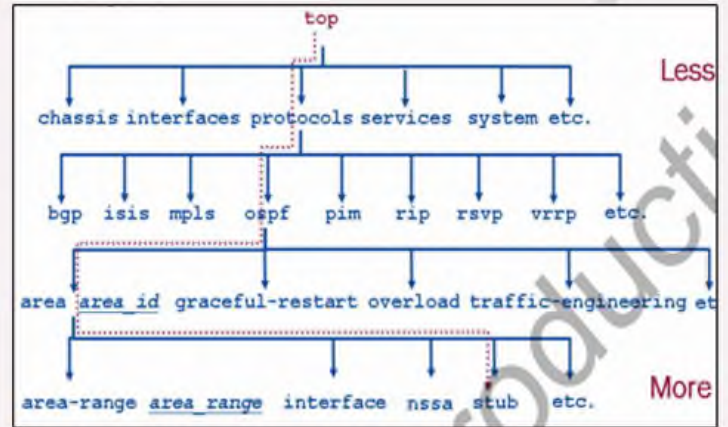
#### Juniper's JUNOS

```
root# copy interfaces em0 to em1
```

يعني أنسخي الأعدادات الموجودة في em0 إلى em1 وطبعا كل هذه الامور يستطيع ان يقدرها من يتعامل بشكل دائم مع الروترات والتي تعطيك سرعة كبيرة في تنفيذ كل المتطلبات وبمرونة رائعة لنعرض لكم الأمر الأخير وهو أظهار كل الأعدادات التي قمت بها على صفحة الأكواد وذلك من خلال أمر ال show

```
root# show
## Last changed: 2010-10-04 02:43:11 UTC
version 9.0R1.10;
system {
  root-authentication {
    encrypted-password "$1$sRYh6cKn$B.706HK9hvmreudr029IH1";
  }
  syslog {
    user * {
      any emergency;
    }
    file messages {
      any notice;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
  }
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.10.2/24;
      }
    }
  }
  em0 {
    unit 0 {
      family inet {
        address 192.168.10.2/24;
      }
    }
  }
}
[edit]
root#
```

وأخيرا ملاحظة هامة كل ماكتبناه لم يفعل ولم يدخل حيز التنفيذ لا لم نكتب أمر commit والذي يستخدم لتأكيد الأوامر وتوثيقها .



طيب لو أردت الصعود مرة أخرى ؟ الموضوع بسيط أما أن تستخدم الأمر up وهو سوف ينقلك خطوة خطوة للأعلى أو استخدم الأمر top والذي سوف يأخذك إلى أعلى القمة

الطريق الثاني ان أقوم بتنفيذ الأمر من المكان الذي أنا موجود عليه وطبعا مع مراعاة ال Level الذي أنا فيها بحيث أنني لن أقوم بتنفيذ شيء معين على أحد المنافذ وأنا موجود على Level الخاص بالروتوكولات لتوضح الصورة بالمثال التالي

#### Juniper's JUNOS

```
root# set interfaces em0 unit 0 family inet address 192.168.10.1/24
```

لاحظ معي أنني استخدمت الأمر Set لكي أغير شيء في صفحة الكود التي أتقنا عليها وكتبنا بعدها ترتيبها الشجري وهو interface حددت ماهو المنفذ وأخترت بعدها نوع الأبي IPv4 وبعدها كتبت الأبي ولو حاولت أن أقوم بتطبيق الطريق الأول لأعطاء المنفذ أربي سوف أقوم باستبدال الكلمة الأولى بي Edit ولن أضع الأبي

#### Juniper's JUNOS

```
root# edit interfaces em0 unit 0 family inet
[[edit interfaces em0 unit 0 family inet
root# set address 192.168.10.1/24
#root
```

أعتقد أن الصورة بدأت تتضح لأقم الآن بكتابة الأمر Show وأنا موجود على هذا المستوى وأشاهد ماذا يجب ان يظهر لي

#### Juniper's JUNOS

```
root# show
address 192.168.10.1/24;
[[edit interfaces em0 unit 0 family inet
#root
```

لأتوجه الآن إلى أعلى الهرم وأقوم بكتابة الأمر Show

```
[edit interfaces em0 unit 0 family inet]
root# top

[edit]
root# show interfaces
em0 {
  unit 0 {
    family inet {
      address 192.168.10.1/24;
    }
  }
}

[edit]
root#
```



# أنواع الضغط المدعومة من بروتوكول ال PPP

بقلم: أيمن النعيمي

## PPP Protocol

### Stacker - Predictor - MPPC Compression

وهي النقطة الإيجابية لهذا النوع من الضغط أما النقطة السلبية لهذا النوع هو ال overhead الذي يحدث على المعالج بسبب عملية التشفير وفك التشفير المستمرة وينحصر استخدام هذا النوع من التشفير في بروتوكول ال PPP عندما يكون الترافيك بين النقطتين مختلف يعني فيديو، تصفح، تحميل الخ.....

**Predictor** : معناها باللغة العربية التنبؤ أو التخمين وسوف نعلم لماذا أطلق عليه هذا الاسم فيما بعد، والتي يعود تطويرها إلى شركة Novell عام 1993 وتعد هذه الطريقة من الضغط حصرية على بروتوكول ال PPP فقط وهي أسرع بكثير من ال Stacker ولا تحتاج إلى أي ترخيص لاستخدامها ولا تستهلك كثيرا من المعالج وهي كطريقة ضغط تعد ضعيفة جدا إلا في حالة واحدة وهي أن يكون الترافيك أو البيانات من نوع واحد يعني أما صوت أو فيديو أو تصفح مواقع http ويعود سبب ضعفها إلى الخوارزمية المستخدمة فهي لا تقوم بأي عملية ضغط للبيانات وكل ماتقوم به هو التنبؤ بالبيانات القادمة وخصوصا البيانات المتكررة والتي تم إرسالها من قبل معتمدا على فهرسة للبيانات السابقة والتي يتم الاستعاضة عنها بإكواد خاصة طبعا الموضوع يطول جدا لو تحدثنا بشكل معمق في الآليات وسوف أتركها لك لكي تبحث فيها للمزيد حول هذا الموضوع أدخل على الرابط التالي ونفهم من كل ماسبق أن هذا النوع من الضغط يعتمد على تكرار البيانات بشكل مستمر لذا فهي طريقة ناعمة لو في حال كانت البيانات من نوع واحد كما ذكرنا سابقا .

**Microsoft Point-to-Point** وتختصر عادة إلى MPPC وهي كما واضح أنها خاصة بمايكروسوفت وتستخدم بين الروترات وأنظمة مايكروسوفت فقط أو بين أنظمة مايكروسوفت وهي تستخدم نفس الخوارزمية المتبعة في ال Stacker أي خوارزمية LZS وتتمتع بنفس الخواص السابقة أي القدرة على ضغط أنواع مختلفة من البيانات

Feature	Stacker	MPPC	Predictor
Uses LZ algorithm	Yes	Yes	No
Uses Predictor algorithm	No	No	Yes
Supported on HDLC	Yes	No	No
Supported on PPP	Yes	Yes	Yes
Supported on Frame Relay	Yes	No	No
Supports ATM and ATM-to-Frame Relay Service Interworking (using MLP)	Yes	Yes	Yes

**Stacker** : أول طريقة من طرق الضغط وهي مدعومة في ال PPP وال HDLC وال Frame Relay والأكثر استخداما وهي بشكل عام تعتمد على خوارزمية معروفة جدا تدعى Lempel-Ziv والتي طورها كل من Abraham Lempel, Jacob Ziv عام 1978 وقام بعدها Terry Welch بتطويرها عام 1984 (ZWL) أما الصيغة التي نستخدمها في ال PPP فقد تطورت من قبل شركة تقنيات تدعى Stac Electronics كتقنية ضغط خاصة بالهارد ديسك والتي تم اعتماده فيما بعد مع بروتوكولات ال Wan جميعها لكن تبقى LZW هي الأكثر استخداما في الواقع العام ويتطلب استخدامها وجود License أو ترخيص من مطوريها .

تعتمد هذه الخوارزمية بشكل عام على بناء جدول أو قاموس من الرموز والأرقام يتم استبدالها بالأشياء المتكررة في الداتا نفسها وسوف لن أدخل كثيرا في هذه الخوارزمية وكيفية التشفير وفك التشفير حتى لا تتحول هذه التدوينة إلى درس رياضيات مع انصح الجميع بالتعرف عليها لأهميتها من خلال هذا الرابط لذا لنعد إلى موضوعنا بعد تشكيل الجدول يتم إرسال نسخة من هذه الجداول إلى الطرف الثاني لكي يتمكن من فهمها وفك تشفيرها وبالتالي يتم ضغط كل أنواع البيانات المارة ومن دون استثناء

## كيف يغلب ال Dynamic Protocol على ال Static Route ؟

بقلم: أيمن النعيمي



سبب إستبعادي لهذا الخيار كون رقم 255 في ال AD تعني Unknown Router والتي يشك فيها الروتر ويعتبرها خاطئة ولا يقوم بإضافتها للـ Routing Table

أما الإجابة الثانية فهي تقول أن الروتر دائما يقوم باستثناء ال Default Route ويعتبره الخيار الأخير وبغض النظر عن قاعدة ال AD والتي تقربنا إلى القاعدة التي درسناها وبالنسبة لي إستبعدها ولم أقتنع منها أيضا

أما الإجابة الثالثة والتي أعتبرتها الأكثر منطقية فهي تقول أن ال Default Route يأخذ نفس رقم ال AD الخاص بي ال Dynamic Route فلو كان ال Default Route موجود مع OSPF فهو سوف يملك AD=110 أيضا مثله مثل ال OSPF وهو الجواب الذي أعتمدته للسؤال المطروح فما هو رأيك أنت بالحل؟

سؤال صغير سألته لنفسه ولم أجده حلا في بادئ الأمر وبعد البحث والتقصي وجدت حلا منطقيا وأردت اليوم أن أشارككم هذا السؤال فكما نعلم أن لكل Routing Protocol و لا Static Route هناك Administrative Distance تحدد من هو الأحق لكي يعتمد عليه الروتر لتمرير البيانات والسؤال الذي يطرح نفسه :

لماذا عندما نقوم بأعداد أحد بروتوكولات ال Routing على الروتر ولكن OSPF ونقوم أيضا بإضافة ال Default Route من خلال استخدام ال Static Route والذي يكون عادة على الصيغة المعروفة ip route 0.0.0.0 0.0.0.0 0 يكون ال Default Route هو آخر احتمال سوف يلجأ له الروتر عندما لا يجد في ال Routing Table والتي سوف تكون مخصصة للمسارات التي قام ال OSPF بجمعها ؟ (أعد قراءة السؤال لو في حال لم تفهم الفكرة ) طبعا قد لا تجد سؤال يمكن طرحه لأن هذا الشيء درسناه على أساس قانون ثابت يقوم الروتر باتباعه وهو الاعتماد على ال Default Route كآخر خيار لذا لنعيد صياغة السؤال الذي أتمنى أن يكون قد أنتبه إليه أحدا منكم.

لماذا يعتمد الروتر على معلومات ال Dynamic Protocol قبل أن يعتمد على ال Default Route مع العلم أن ال Administrative Distance الخاص بي ال default Route أقل من أي بروتوكول كونه يندرج تحت ال Static Route وهذا يعني أن ال AD=1 ؟

بعد البحث والتقصي وجدت إجابات لكن لم أقتنع من الأولى وهي تقول أن ال Default Route عندما يكون موجود مع أحد بروتوكولات ال Dynamic Protocol فهو يحصل على AD=255 وهذا يجعله آخر احتمال للروتر وطبعاً



## Mac Address Access-list

# MAC Access-List

وأخيرا أحب أن أشير إلى بعض النقاط الهامة

- 1- تلك الأديس يجب أن يكتب على الشكل التالي 0000.0000.0000
- 2- نكتب مكان ال Mac of blocked pc سورس ماك أديس وفي المكان الثاني ال Destination mac address
- 3- على المنفذ نقوم باختيار متى نريد تطبيق الأكسس ليست IN or OUT
- 4- نستطيع أن نضيف بعد الأكسس ليست رقم الذي لان نريد تطبيق عليها كخيار اضافي
- 5- لعرض حالة الأكسس ليست على المنفذ نقوم بتنفيذ الأمر التالي show mac access-group
- 6- لعرض اعدادات الأكسس ليست نقوم بتنفيذ الأمر التالي show mac access group
- 7- لاختيار اسم للأكسس ليست تستطيع أن تكتب بأحرف كبيرة وصغيرة وأرقام والأشعار التالية .. وكحد أقصى 31

### متى نحتاج لـ Mac access-list

كحال أغلب الشبكات الكبيرة والصغيرة أحيانا تعتمد أغلب الأجهزة على سيرفر ال DHCP في توزيع الأيبيات وهي عادة ماتكون عشوائية في التوزيع ففي كل مرة يطلب الجهاز ايبي يحصل على عنوان جديد فكيف سوف نتصرف لو في حال أردنا منع بعض الأجهزة من الوصول الى سيرفرات او حتى الوصول الى الأنترنت ؟ الجواب هو ال Mac access-list طبقا ليس الحل الجذري لهذه المشكلة لكن يساعدنا قليلا في هذا الأمر

وقد نحتاجه أحيانا لمنع بروتوكولات ال CDP او ال VTP من الوصول الى الروتر لسبب ما ( هناك حلول موجودة لمثل هذه الأشياء لكن ما أريد أن اوصل لكم فكرة جديدة فقط )

لذا لنأخذ المثال الأول ونقوم بتطبيق الفكرة على أجهزة سيسكو وسوف أقوم أولا بكتابة الأكسس ليست وأقوم بتطبيقها على المنفذ المطلوب

```
Cisco's IOS
mac access-list extended BLOCK_MAC
deny host <MAC of blocked PC> host <MAC of Gateway>
permit any
```

وبعدنا نتوجه الى المنفذ الذي نريد تطبيق الأكسس ليست عليه ونقوم بكتابة الأمر التالي

```
Cisco's IOS
interface fastethernet 0/1
mac access-group BLOCK_MAC in/out
```

# Network Device Vulnerabilities

بقلم: صفا الرمضاني

\*عدم تغيير كلمة المرور إلا عند الضرورة وبالتالي يتمكن المهاجم الذي يتمكن من الدخول للجهاز سيبقى يدخل له في المستقبل لأن كلمة المرور لم تتغير .

\*استخدام كلمة مرور قصيرة (ABCD) كلمات السر القصيرة اسهل واسرع للكسر من الطويلة

\*استخدام معلومات شخصية في كلمة السر ( مثل اسم الأب .. الخ )

\*استخدام نفس كلمة المرور لجميع الحسابات ، فالمهاجم الذي يتمكن من معرفة كلمة مرور جهاز يتمكن من الدخول لعدة أجهزة ..

\*تدوين كلمة المرور ، وتدوين كلمة المرور يعتبر دعوة مفتوحة للدخول الى الحساب او الجهاز .

### 2- الحساب الافتراضي

عبارة عن حساب يتم انشاؤه آليا من قبل الجهاز عوضا عن المدير اثناء عملية تثبيت واعداد الجهاز وعادة يمتلك صلاحيات ادارية كاملة على الجهاز وذلك لمنع إعاقة عملية اعداد الجهاز . ويعتبر الهدف الأول الذي يفكر المهاجم في الوصول إليه ، لأن الحساب الافتراضي عادة يحمى بكلمة مرور افتراضية وسهلة وشائعة ، وهذا يمكن المهاجم من الولوج للنظام بسهولة مثلا بعض الراوترات Default user: admin

Default password: 1234

وللحماية من هذه المشكلة يجب حذف هذا الحساب تماما بعد استكمال عملية اعداد وتثبيت الجهاز

### البوابات الخلفية

ال back door هو حساب يتم انشاؤه في احد أجهزة الشبكة بشكل سري دون علم مدير الشبكة ومن دون تصريحه بذلك ، ولا يمكن كشفه بسهولة ويمكن من الاتصال والوصول للجهاز عن بعد . يمكن انشاء ال back door بطريقتين :

1- حقن الجهاز من قبل المهاجم باستخدام فايروس او worm او Trojan horse ثم اقحام حساب ال back door .

2- انشاء حساب ال back door من قبل مبرمج البرنامج الذي يعمل على الجهاز .

3- توسيع الصلاحيات Privilege Escalation

من الممكن استغلال الثغرات في البرامج المستخدمة في أجهزة الشبكة للتمكن من الوصول الى المصادر المحصورة عن المستخدم العادي .

نقاط الضعف في الأجهزة المستخدمة في الشبكة غالبا ما تكون هدفا للمهاجمين . وتشمل ضعف كلمة المرور weak password ، الحساب الافتراضي default account ، الأبواب الخلفية back doors وتوسيع الصلاحيات privilege escalation .

### 1- ضعف كلمة المرور

أجهزة الشبكة عادة تكون محمية بكلمة مرور لمنع المستخدمين غير الشرعيين من الولوج للأجهزة وتغيير اعداداتها والعبث بها .

وبالرغم من أن كلمة المرور تعتبر خط الدفاع الأول الا انها في الوقت نفسه تعتبر نقطة ضعف تهدد امن الشبكة .

ولضمان بقاء سرية كلمة المرور ، ومنع المهاجمين من التوصل لها ، يجب أن لا يتم تدوين كلمة المرور في أي مكان ، لكن يتم حفظها في ذاكرة الشخص فقط ! كذلك يجب أن تكون بطول وتعقيد مناسبين ، بالتالي لن يسهل على المهاجم معرفتها . لكن هنا تظهر مشكلة تسمى بـ Paradox password .

فبالرغم من طول وتعقيد كلمة المرور وعدم كتابتها في أي مكان ، فإنه من الصعب جدا تذكر هذا النوع من كلمات المرور .

بالإضافة لذلك فإن أغلب مديري الشبكات لديهم عدة أجهزة تحت مسؤوليتهم كل جهاز لديه كلمة مرور خاصة ، وكلمات المرور يتم وضعها ثم تنتهي صلاحياتها بعد فترة معينة من الزمن ، بعد شهر مثلا ، وبعدها يجب انشاء كلمة مرور جديدة . وبعض الأجهزة تمنع استخدام كلمة المرور السابقة أي انها تجبر المستخدم على تغيير كلمة المرور في كل مرة يتم الدخول للجهاز ، وبالتالي فإن المستخدم مجبر على تذكر كلمة المرور الجديدة باستمرار لعدة أجهزة ، مما يجعل استخدام وتذكر كلمات المرور صعب جدا .

كل العوامل السابقة كانت سبب في جعل أغلب مديري الشبكات يقومون باستخدام كلمات مرور ضعيفة وبالتالي يكون أمن الشبكة تحت التهديد .

-صفات كلمات المرور الضعيفة :

\*استخدام كلمات عامة مثل اسم الأيام او الشهر . ( يقوم المهاجم باستخدام قواميس الكترونية للكلمات العامة تساعد على كشف كلمة المرور ) .





# قسم أمن وهماية الشبكات

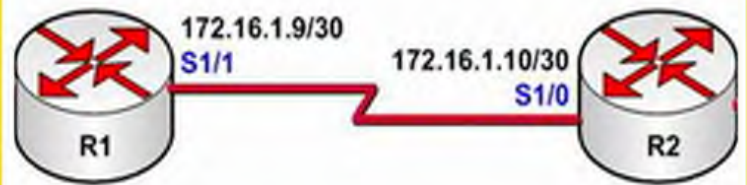
هذا القسم سوف يتم عرض فيه كل الامور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التي تحدث على الشبكة وارجو منك ان تدقق على كلمة تخفيف لان النظرية العامة تقول لا يوجد جهاز امني خالي من الثغرات مهم كانت قوته!



## كيفية إعداد الـ Authentication في بروتوكول الـ EIGRP & OSPF

بقلم: أيمن النعيمي

في مقالتي الأمنية لهذا الشهر سوف أتحدث عن طريقة إعداد الـ Authentication في بروتوكول الـ EIGRP والـ OSPF وقد حرصت على تقديم هذا الموضوع لأن هناك الكثير منا لا يعير انتباها كبيرا وكون الموضوع قد يسبب خراب الشبكة بالكامل لو أستخدمها أحد المخربين وقام بأرسال معلومات مزورة إلى الروتر وقام بتزوير المسارات إلى جهازه

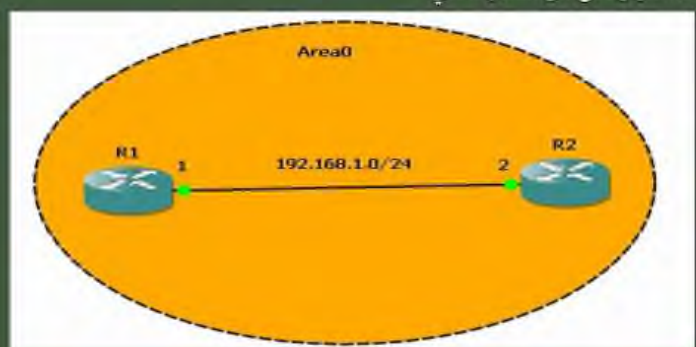


### IOS

```
Router#configure terminal
Router(config)#interface serial 0/0
Router(config-subif)#ip authentication mode eigrp 10 md5
Router(config-subif)#ip authentication key-chain eigrp 10 networkset
Router(config-subif)#end
```

في الأمر الثالث قمنا باختيار وضعية الـ MD5 وبعدها قمنا بربط البروتوكول مع المفتاح المستخدم والذي يحمل الاسم networkset وبهذه الخطوة نكون قد انتهينا من إعداد بروتوكول الـ EIGRP وأحب أن أشير إلى أن الإعدادات هي نفسها على الروتر الآخر.

أما بالنسبة لبروتوكول الـ OSPF فكما أشرنا في بداية المقال أن البروتوكول يدعم طريقتان من الـ Authentication الـ Simple Password و الـ Auth وفيه يتم إرسال كلمة السر على شكل Clear Text والطريقة الثانية الـ Message Digest Authentication أو الـ MD5 وهي ترسل مشفرة وسوف نلقى الضوء على الطريقتان ولناخذ هذا اللاب الصغير ونبدأ بالروتر الأول ونقوم بتطبيق طريقة الـ Simple Password وهي تنفع عندما يكون الروتران متصلان ببعضهما البعض بشكل مباشر Point-to-Point كما هو واضح من الشكل التالي :



قبل أن نتكلم عن الإعدادات لنذكر أولا أنواع الـ Authentication الموجودة في بروتوكولات التوجيه وهي نوعان

الأول: Simple Password authentication وهي بشكل عام ترسل بدون تشفير أو Clear-Text وتستخدمها البروتوكولات التالية: IS-IS, OSPF, RIPv2.

الثاني: Message Digest Authentication أو الـ MD5 وهي ترسل مشفرة وتستخدمها البروتوكولات التالية: RIPv2, OSPF, EIGRP, BGP. وكما نلاحظ أن هناك بروتوكولات تدعم الاثنان كما في الـ OSPF, RIPv2 وهناك بروتوكولات تدعم نوع واحد فقط كما في الـ EIGRP, BGP, IS-IS.

لنعد الآن إلى موضوعنا الأساسي وهو طريقة الإعداد الخاصة بي الـ EIGRP وكما اتفقنا من قبل أن الـ EIGRP لا يدعم الـ Simple Password لذا يتوجب علينا أولا أن نقوم بإعداد مفتاح خاص للتشفير يدعى Key-Chain ومن خلاله سوف نحدد كلمة السر الخاصة بالبروتوكول وبعدها سوف نعود لربطها بالبروتوكول لذا لنبدأ أولا بعمل المفتاح

### IOS

```
Router#configure terminal
Router(config)#key chain networkset
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string networksetpassword
Router(config-keychain-key)#end
```

بعد الدخول إلى الـ Configuration Mode نقوم في أول أمرين باختيار اسم ورقم للمفتاح ويفضل أن يكون متطابقين بين الروتران أما في الأمر الثالث فهو من أجل اختيار كلمة السر والتي يجب أن تكون متطابقة بين الروتران أما الخطوة الثانية فهي تتم على المنفذ الذي يتصل مع الروتر وهي من أجل ربط المفتاح الذي قمنا بإعداده مع الـ EIGRP وهي كالآتي :



لننتقل الآن إلى الطريقة الثانية والتي ترسل فيها كلمة السر مشفرة وسوف نستخدم نفس الالاب السابق والأعدادات نفسها تطبيق على كلا الروتران

#### Cisco's IOS

```
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip ospf message-digest-key 1 md5 NetworkSet
Router1(config-if)#exit
Router1(config)#router ospf 1
Router1(config-router)#area 0 authentication message-digest
Router1(config-router)#exit
```

وأخير نستخدم نفس الأمر السابق للتأكد من أن ال Authentication قد تفعل بشكل صحيح

#### Cisco's IOS

```
Router#show ip ospf interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/30, Area 0
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost:
1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.1.2, Interface address 192.168.1.2
Backup Designated router (ID) 192.168.1.1, Interface address
192.168.1.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:04
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.1.2 (Designated Router)
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
```

وسوف نبدأ بالأعدادات الخاصة بي ال Simple Password

#### Cisco's IOS

```
Router1>enable
Router1#conf t
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#ip ospf authentication-key NetworkS
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#router ospf 1
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router1(config-router)#area 0 authentication
Router1(config-router)#exit
```

نتجه الآن إلى الروتر الثاني ونقوم بنفس الشيء مع ملاحظة تغيير الأبي

#### Cisco's IOS

```
Router2>enable
Router2#conf t
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ip address 192.168.1.2 255.255.255.0
Router2(config-if)#ip ospf authentication-key NetworkS
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#router ospf 1
Router2(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router2(config-router)#area 0 authentication
Router2(config-router)#exit
```

وتستطيع ملاحظة كلمة NetworkS والتي تمثل كلمة السر بين الروتران وللتأكد من أن ال Authentication مفعل على المنفذ قم بكتابة الأمر التالي ولاحظ معي السطر الأخير

#### Cisco's IOS

```
Router1#sh ip ospf interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost:
1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.1.2, Interface address 192.168.1.2
Backup Designated router (ID) 192.168.1.1, Interface address
192.168.1.1
Flush timer for old DR LSA due in 00:01:09
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.1.2 (Designated Router)
Suppress hello for 0 neighbor(s)
Simple password authentication enabled
```



# عتاك و معلومات

أعداد: أيمن النعيمي

## CISCO SYSTEMS



RAM	512 MB (installed) / 1 GB (max) - DDR SDRAM
Flash memory	128 MB (installed) / 512 MB (max)
Type	Router
MAX Transfer Rate	1 Gbps
Encryption Algorithm	DES, Triple DES, SSL, 128-bit AES, 192-bit AES, 256-bit AES
Supplied OS	Cisco IOS Advanced IP services
Digital Signaling Protocol	Wired
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocol Remot	SNMP 3, SSH-2
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, hardware compression, hardware encryption, VPN support, MPLS support, content filtering, URL filtering, QoS, Dynamic Multipoint VPN	



CISCO 3845-HSEC/K9

RAM	128 MB
Flash memory	16 MB
Ramer Table of MAC Addr	12K entries
Authentication method	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Interfaces	management-console RJ-45/2 x network stack device
Connection Type	Half-duplex, full-duplex
Data Rate	100 Mbps
DCP	Ethernet, Fast Ethernet 10Base-T/100Base-TX
Protocol Remote	SNMP1, RMON1, RMON2, SNMP, Telnet, SNMP3
Number of Ports	48 x Ethernet 10Base-T, Ethernet 100Base-TX
Flow control, full duplex, routing, IP-routing, DHCP support, auto-negotiation, ARP support, trunking, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, manageable, IPv6 support	



Catalyst 3750 48TS-E

RAM	256 MB (installed) / 1 GB (max)
Flash memory	64 MB (installed) / 256 MB (max)
Protocol Remote	SNMP 3
Type	Voice / fax module
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45   2 x USB   1 x management - console   1 x network - auxiliary
Encryption	DES, Triple DES, AES
Supplied OS	Cisco IOS SP services
OS Required	Microsoft Windows 98 Second Edition
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Voice Codecs	G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726



CISCO 2821-V/K9





# Juniper®

## NETWORKS

### JUNOS Software version tested

JUNOS 10.0

### Firewall performance (max)

650 Mbps

### IPS performance (NSS 4.2.1)

60 Mbps

### AES256+SHA-1 / 3DES+SHA-1 VPN performance

65 Mbps

**SRX 100**

### Maximum concurrent sessions

16 K (512 MB DRAM) / 32 K (1 GB DRAM)

### New sessions/second (sustained, TCP, 3-way)

2,000

### Maximum security policies

384

### Maximum users supported

Unrestricted

### Fixed I/O ports

8 x 10/100

### CX111 3G Bridge support

Yes

### Firewall

- \* Network attack detection: Yes
- \* DoS and DDos protection: Yes
- \* TCP reassembly for fragmented packet protection: Yes
- \* Brute force attack mitigation: Yes
- \* SYN cookie protection: Yes
- \* Zone-based IP spoofing: Yes
- \* Malformed packet protection: Yes

### Intrusion Prevention System

- \* Stateful protocol signatures: Yes
- \* Attack detection mechanisms: Stateful signatures, protocol anomaly detection (zero-day coverage), application identification
- \* Attack response mechanisms: Drop connection, close connection, session packet log, session summary, email, custom session
- \* Attack notification mechanisms: Structured
- \* Worm protection: Yes
- \* Simplified installation through recommended policies: Yes
- \* Trojan protection: Yes



### ScreenOS version tested

ScreenOS 6.2

### Firewall Perf (Large Packets)

160 Mbps

### Firewall Performance (IMIX)

90 Mbps

### Firewall Packets Per Second

30,000 PPS

### 3DES+SHA-1 VPN Perf

40 Mbps

### Concurrent VPN Tunnels

25/40\*

### Max Concurrent Sessions

8,000/16,000\*

### New Sessions/Second

2,800

### Max Security Policies

200

### Max Security Zones

8

### Max Virtual Routers

3/4\*

### Max Virtual LANs

10/50\*

### Fixed I/O

5x10/100

### Mini-Physical Interface Module (Mini-PIM) Expansion Slots

2

### Physical Interface Module (PIM) Expansion Slots

0

### Enhanced PIM (EPIM) Expansion Slots

0

### 802.11 a/b/g

Optional

### Convertible to JUNOS

No

**Switch SSG-550M**



### Maximum Performance and Capacity

- \* Junos Software Version Support: Junos Software 9.1
- \* Firewall Performance (Large Packets): 1.6G
- \* Firewall Performance (IMIX): 600 Mbps
- \* Firewall and Routing PPS (64 Byte): 225,000 pps
- \* 3DES and SHA-1 VPN Performance: 600M
- \* 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: 10,000
- \* Maximum Security Policies: 5192 (1 GB DRAM)

### Network Connectivity

- \* Fixed I/O: 4 x 10/100/1000
- \* Maximum PIM Slots: 6
- \* Maximum EPIM Slots: 2

**Router J4350**



### Routing, Virtualization, Encapsulations

- \* BGP, OSPF, RIP, Static, ECMP: Yes
- \* Multicast, PIM SM, SSM, IGMP: Yes
- \* Maximum Number of Security Zones: 50
- \* Maximum Number of Virtual Routers: Yes
- \* Maximum Number of VLANs: 512
- \* PPP, FR, MLPP, MLFR, HDLC: Yes

### Data Rate

- \* EX3200-24P/24T: 88 Gbps
- \* EX3200-48P/48T: 136 Gbps

### Throughput

- \* EX3200-24P/24T: 65 Mpps (wire speed)
- \* EX3200-48P/48T: 101 Mpps (wire speed)

### 10/100/1000BASE-T Port

24 / 48 per platform

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

4 per switch (via optional four-port GbE uplink module)

### 10GBASE-X Port Densities

2 per switch (via optional two-port 10GbE uplink module)

### Resiliency

External redundant power supply; internal field-replaceable power supply; field-replaceable fan

### Power Options

- \* AC: 320W, 600W and 930W autosensing; 100-120V / 200-240V
- \* DC: 190W; input voltage range 36V-72V; dual input feed

### Operating System

JUNOS

### QoS Queues / Port

8

### Traffic Monitoring

sFlow

### MAC Addresses

24,000

### Jumbo Frames

9216 Bytes

### IPv4 Unicast / Multicast Routes

16,000 / 8,000

### Number of VLANs

4,096

**Switch EX3200**







# مصالحات تقنية

**RIP** : وتعني Routing Information Protocol أحد البروتوكولات المعروفة جدا عند مهندسي الشبكات ووظيفته توجيه البايت القادم إلى أجهزة الطبقة الثالثة إلى مكانه المناسب ويعود تاريخ تطوير هذا البروتوكول إلى عام 1988 من قبل منظمة الـ ARPANET ويعد هذا البروتوكول Distance Vector وهو يعتمد على عملية حسابية تدعى Bellman-Ford Algorithm والتي تعتمد في مقامها الأول في اختيار أفضل مسار على عدد الهوب المتاح للوصول إلى الهدف وهو يملك إصداران مختلفان V1, V2.

**EIGRP** : وتعني Enhanced Interior Gateway Routing Protocol وهو أيضا أحد البروتوكولات المسؤولة عن عملية التوجيه وهو أحد البروتوكولات التي قامت شركة سيسكو بتطويره لصالح أجهزته فقط وهو يعد advanced distance-vector ويعتمد على عملية حسابية تدعى Diffusing Update Algorithm والتي تعتمد على عدة قيم وحسابات معقدة من أجل حساب أفضل مسار وهي ستة Bandwidth, Delay, Load, Reliability, MTU, Hop Count.

**OSPF** : وتعني Open Shortest Path First بروتوكول آخر من بروتوكولات التوجيه المعروفة ويعد الأكثر استخداما في الشبكات كونه متاح لكل مصنعي أجهزة الطبقة الثالثة وهو يعد Link State ويعتمد على عملية حسابية تدعى Dijkstra's algorithm وأكثر ما يميزه إمكانية تقسيم الأجهزة لعدة أقسام أو مناطق Area والتي تساعد في دورها في رفع أداء الشبكة والأجهزة

**IS-IS** : وتعني Intermediate system to intermediate system وهو أيضا أحد بروتوكولات التوجيه ويندرج تحت الـ Link state مثله مثل الـ OSPF حتى أنه يشبه كثيرا في بعض الأمور وهو بروتوكول قديم لم يعد مستخدم كثيرا ولا يعتمد على بروتوكول الـ IP الذي نعرفه بل يعتمد على بروتوكول يدعى CLNP وهناك نموذج مطور منه يدعى Integrated IS-IS يدعم بروتوكول الـ IP

**BGP** : وتعني Border Gateway Protocol يعد هذا البروتوكول أيضا أحد بروتوكولات التوجيه لكن ليس للاستخدام الداخلي كما هو حال جميع البروتوكولات التي ذكرناها من قبل لأنه استخدامه ينحصر فقط في الأنترنت وأحب أن أطلق عليه لقب قلب الأنترنت فبدونه سوف تتوقف حركة الأنترنت بشكل كامل فهو مسؤول عن ربط جميع الـ autonomous System ببعضها البعض وبالتالي يقوم بتوجيه كل الطلبات التي تحدث في عالم الأنترنت مثل تصفح المواقع أو الاتصال عن بعد وهو يعد path-vector ويعتمد على عدة أشياء تدعى Attribute تساعد في اختيار أفضل مسار للبايت .

**EBGP** : وتعني Exterior Gateway Protocol وهو بروتوكول آخر من بروتوكولات التوجيه ويستخدم في الأنترنت وفي الشبكات العالمية وهو بروتوكول قديم وبطل بعض الشيء ظهر عام 1982 وأحيل للتقاعد بعد ظهور بروتوكول الـ BGP .



# مشاكل وحلول

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

**سؤال:** كيف أقوم بأعداد وتنصيب سيرفر خاص بي ال **TFTP** ؟  
**جواب :** تنصيب مثل هذا النوع من السيرفرات لا يحتاج إلا شيء كل ماعليك تنصيب هذا البرنامج على جهازك وتحديد المنفذ الذي سوف يعمل عليه وانتهى الأمر .

[http://tftpd32.jounin.net/tftpd32\\_download.html](http://tftpd32.jounin.net/tftpd32_download.html)

**مشكلة:** عندي روتر DSL ( 2640u -D-link ) وفيه أربعة منافذ وكل منفذ يتم وصله بكومبيوتر و بالتالي تبدأ هذه الكومبيوترات بتصفح النت، لذلك أردت سؤالك هل هناك برنامج أو طريقة أستطيع من خلالها أن أعرف مصروف أو الترافيك الذي يصرفه كل كومبيوتر عن طريق منافذ الروتر ؟  
**الحل:** بعد الاطلاع على مواصفات وأماكنيات المودم لم أجد هذه الخاصية متاحة أي تحديد كمية الترافيك الذي يعبر على كل منفذ لكن لو مكانك وكنت مطر إلى مراقبة الترافيك لكنت أشرت سويتش بسيط وكرت شبكة لجهاز الكمبيوتر وربط الأجهزة الموجودة على الشبكة مع السويتش والسويتش وصلته مع كرت الشبكة الجديد ونصبت برنامج CCProxy وحددت الترافيك لكل مستخدم أو قمت بتثبيت سيرفر مايكروتيك الذي يعطي مميزات رهيبه لمثل هذه المواضع .

**سؤال:** أنا حاصل على mcp,ccna وسوف استمر في شهادات سيسكو ومايكروسفت الى اعلى مستويات الشهادة ولكني غير حاصل على شهادة جامعية هل تغني شهادات الشبكات عن الشهادة الجامعية للعمل كمهندس شبكات ؟  
**جواب:** شوف السؤال هذا صعب أجيبك عليه لان هذا الموضوع هو موضوع أرزاق لكن حصولك على شهادة مثل CCIE يساعدك على حل هذه المشكلة وطبعا هناك شركات تشترط وجود شهادة جامعية .

**سؤال:** أنا حاصل على بكالوريوس نظم ومعلومات إدارية أريد الدخول في مجال الشبكات فباي شيء أبدأ وأي كورسات وفي أي مكان ؟  
**جواب:** أطلع على المجلة هناك سلسلة من المقالات حول هذا الموضوع للأستاذ عادل الحميدي

**سؤال:** أريد دراسة شهادة ال Troubleshoot لكن مختار في أي كتاب أدرس إما  
CCNP TSHOOT 642-832 Official Certification Guide

أو  
Troubleshooting and Maintaining cisco ip networks (Student guide v1&v2)

فأيهم أشمل، بمعنى مستوعب معلومات أكثر مع أنني متحيرة نوعا ما للأول ؟

**جواب :** الكتاب الثاني وبلا منازع فهو أقوى بكثير من الأول لكن أفضل ان تقرأ السيناريو الموجود في آخر كل جابتر من الكتاب الأول .