NO. 28 July 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

SWITCH PORT ANALYZER - SPAN

شهادات شركة Vmware

إعداد أجهزة الشّبكة لتطبيقات الملتيميديا والألعاب

أنواع فيروسات الحاسب

بروتوكولات نقل الصّوت Protocols Voip

الأسباب العشر الأكثر إغفالاً في عملية Troubleshooting

نظام الفاكس المركزي

مقدمه فى الاسكريبتات introduction to scripts

أفضل عشر شهادات فى مجال الآي تي لعام 2012

www.networkset.net

أريد أن أكون منصفاً

من تابع معنا الحلقة الحية والمباشرة التى تحدثت فيها منذ أسبوعان تقريبا على راديو مهندسي الشبكات «سيسكاوي» فهو يذكر معي أن أهم نقطة ركزت عليها في تلك الحلقة كانت « أسس نفسك أولا ببعض الشهادات ولاتلتفت إلى متطلبات السوق,أصنع مستقبلك بنفسك وعود نفسك على التفكير» هذه الجملة التى كتبتها بعد أنتهاء الحلقة وعلق أحد الأصدقاء عليها بأن الأغلبية مهما تحدثنا ومهما فعلنا تعتبر العلم هو أداة للوظيفة وليس أداة المعرفة التى يمكن أن نتطور بها نحو الأفضل, جلست قليلا أفكر في هذا الرد ووجدت أن النقض بحق هؤلاء (طالبي العلم للوظيفة) هو شيئ سلبي وغير منصف, فأنا تحدثت في مقالات كثيرة عن أهمية العلم وضرورة أن نكون منتجين وفاعلين اكثر في الحياة وحاولت أن أتجاهل مسألة عدم إيجاد فرصة العمل المناسبة. والحقيقة شعرت بأن غير منصف ابدا فأنا أطلب من الجميع بأن يتابعوا طريق علمهم وأن لايلتفتوا لسوق العمل وبل جعلت مسألة إيجاد الوظيفة والعمل شيئ ثانوي في الحياة وهذا كان إجحاف كبير مني بحق أساس من أساسيات الحياة والعيش الكريمة واليوم مقالي هذا لأعترف بهذا الخطأ لكم.

حتى نصل إلى أهمية العلم على العمل أعتقد أولا ان الأمر يحتاج شجاعة وصبر وثقة باللّه, بدون وجود هذه الأمور سوف تصل الفكرة ناقصة إلى الجميع وسوف يظهر الكلام على أساس أنه تسخيف للعقول والتحدث في اللأمنطقيات الواقعية وأنا مع هذا الكلام, فالشعوب العربية تعاني من هاوية البطالة وإنخفاض عدد الوظائف مقارنة بأعداد الخريجين الجامعيين, وخصوصا أن الخريج الجديد يعتقد أن الوظيفة والمنصب والأمور التى كان يحلم بها طيلة خمس سنوات سوف تبدأ تتحقق فور حصوله على هذه الشهادة الورقية ليجد بعدها صدمة الخبرة وصدمة قلة الوظائف المتاحة فيجلس في البيت بدون عمل مصابا بحالة من الأكتئاب والضيق الشديد ليجد بعدها من يقول له أدرس وأقرا وتعلم ولاتنظر إلى العمل وسوف تتيسر قريبا. الحقيقة أنا بالغت في كلامي عدة مرات لكن ليس باليد حيلة فأفضل ما استطيع أن أقدمه لك هو الأمل والعزيمة وحتى لو تناقضت مع الواقع الموجود فمجرد كونك عربي هذه الأيام يعني أنك تعيش وتأكل وتشرب وتنعم بكل الخيرات من جيب حاكمك الخاص مباشرة وكأن الامر صدقة. ربما قررت الأنصاف اليوم لأن مررت بأكثر من تجربة فلقد مررت بتجربة الجلوس بدون عمل وكنت أدرس فيها أفضل من أيام الدراسة بالجامعة والمحصلة كانت مقال كتبته ونشرته على المجلة تحت عنوان «الهدف» والثانية تجارب كثيرة لأناس أعرفهم جيدا وأعرف حالهم وأعرف مدى أحباطهم فهمها حدثتهم فأنا لا انكر أن الموضوع صعب وبل صعب جدا, وشعرت بعدها أن من اللأزم أن أنصف الجميع وعلنا وأعترف بأن كلام الشباب حول ضرورة وجود فرصة عمل مناسبة شيئ مهم حتى يتجدد النشاط فلقد يكون الكلام جميلا ولطيفا لفترة معينة من الزمان لكن عندما اسمع أن هناك شاب جلس سنتان بدون أن يجد فرصة مناسبة وأقول له أدرس وتابع مشوارك فأنا هنا أجحف كثيرا في حقه والأفضل لي أن اساعده في إيجاد وظيفة خيرا من أقول له إقرا مقال الهدف فلعله ينفعك.

الحقيقة شبابنا مقهور وحيله قليلة نوعا ما والأمر في النهاية لن يمر بدون شجاعة وصبر وإيمان وثقة باللّه فلو تحليت بها فأكيد أنك سوف تمر بهذا الضيق كما مررت أنا وغيري, لا اعلم كيف لي أن أخرجك من هذا المقال بشعور إيجابي غير أن أنصفك أولا والأنصاف هنا يعني الحديث بواقعية أكثر من حديث الهمم والتحفيز الذاتي لذلك اتمنى أن يكون أنصافي لك في هذا المقال هو صورة إيجابية وأعتراف صريح أن حقوقك في فرصة عمل جيدة هو من أعلى وأهم الأولويات في الحياة لكن أريدك أيضا أن لاتيأس فواللّه إن ربنا هو اعدل من هو موجود وسوف ينصرك مهما اشتدت عليك ودمتم بود.

أيمن النعيمي - سوريا

مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

أسـرة المجلـة

المؤسس و رئيس التحرير

م.أيمن النعيمي

المحـررون

م.نادر المنسي	م. حسام الدين حشيش	م.عبد الرقيب عبده صالح الفقيه
م.خالد عوض	م.أحمد هيكل	م.فادي الطه
م.أنس المبروكي	م. أحمد سلطان	---
م.شيماء جابر	م.خالد الدسوقي	---

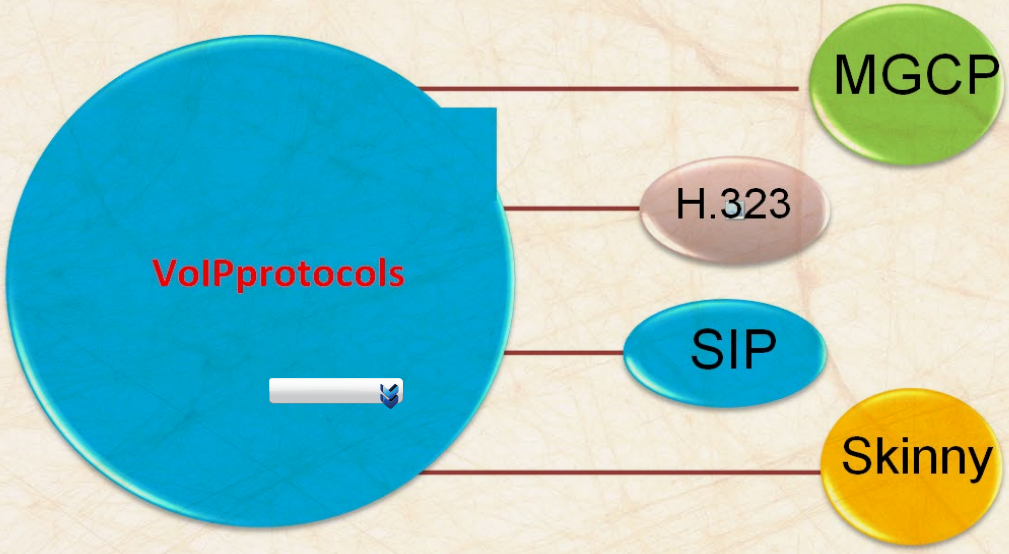
التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : أسـامـة كـامـل

www.networkset.net

بروتوكولات نقل الصّوت PROTOCOLS VOIP

هناك بعض البروتوكولات التي تستخدم في نقل الصّوت بين المصدر والهدف أحببت في مقالنا لهذا العدد أن أوضح قدر الأمكان من المعلومات عن هذه البرتوكولات للتّعرّف عليها ولتعم الفائدة للجميع وسوف نوضح في هذا المقال بشكلٍ مختصر بروتوكول MGCP .



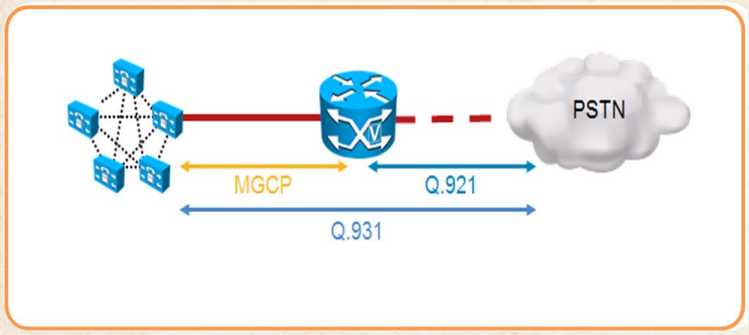
ما هو بروتوكول MGCP

بروتوكول MGCP هو اختصار (Gateway Control protocol Media):

يعتبر بروتوكول MGCP بروتوكول التّحكّم في المكالمات والإشارات والقدرة على التّحكّم عن بعد وإدارة الصّوت (Voice) و أجهزة نقل البيانات ويقدم العديد من الخدمات المتعلّقة بحزم الشبكات. وهذا البروتوكول MGCP يعرف بـ RFC 3435.

فوائد بروتوكول MGCP
Advantages of MGCP gateways

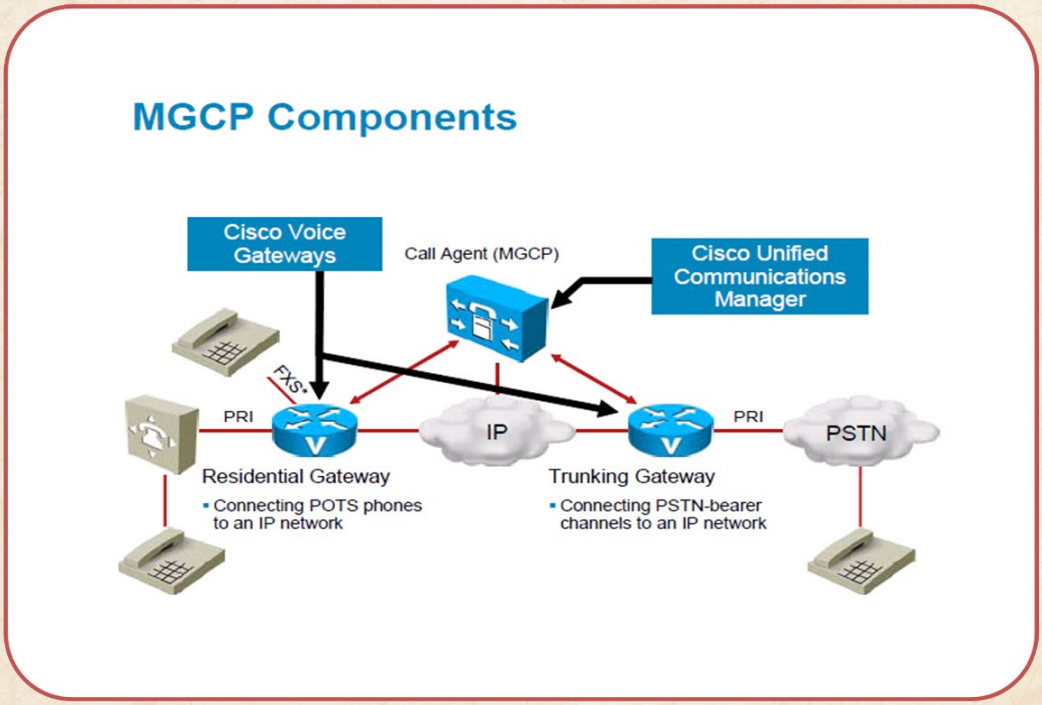
- يبسط إعدادات نظام تشغيل Cisco.
- ستعمل بروتوكول MGCP بورت الUDP كما هو الحال فيSGCP لإنشاء المكالمات الصوتية في شبكة الـIP وكما تستعمل أيضًا طريقة تسمى Hair Pinning لإرجاع المكالمات إلى شبكة الPSTN في حالة عدم توفر الشبكة الـWAN.
- يستخدم بروتوكول MGCP مع نظام توزيعVOIP .
- كما أن هذا البروتوكول يسمح لمكونات التحكم المركزي أو مكالمات العميل بالتحكم عن بعد بالعديد من الأجهزة .



- يعتبر بروتوكول محفز .
- العنونة بواسطة E.164 لأرقام التلفون
- يستخدم IETF SDP.
- الهندسة المعمارية والمتطلبات تحدد في RFC2805.

المكونات الأساسية MGCP

بروتوكولMGCP:
يعرف العديد من المكونات والمفاهيم التي يجب فهم العلاقة بين هذه المكونات وكيفية تطبيق عمله في بيئة بروتوكول GMCP .



- **نقطة النهاية Endpoints :**

تمثل النقطة التّوصيلية بين حزمة الشّبكة وشبكة الهاتف التقليدية القديمة .

- **بوابة اتصال Gateways :**

تعالج ترجمة الصّوت بين Switched Circuit Network و Packet Network وال GATEWAY يستعمل بروتوكول MGCP لتسجيل الأحداث وإرسالها إلى Call Agent مثل (في حالة رفع سماعة الهاتف).

- **وكيل (عميل) اتصال Call Agent :**

وظيفته السيطرة والتحكم على عمليات الـ GATEWAY وإخبارها بالعمل القادم الذي يجب أن تقوم به، ويستعمل الـ CALL AGENT بروتوكول MGCP لإخبار الـ GATEWAY بالمعلومات الآتية:

- أي حدث يجب أن يخبر به الـ CALL AGENT.
- كيفيّة ربط نقاط التّوصيل مع بعضها.
- أي إشارات يجب أن تطبّق على نقاط التّوصيل .

آليـــة الـعـمـل

في حالة رفع سماعة الهاتف مباشرة بعد رفعها يذهب الـ GATEWAY إلى الـ CALL AGENT

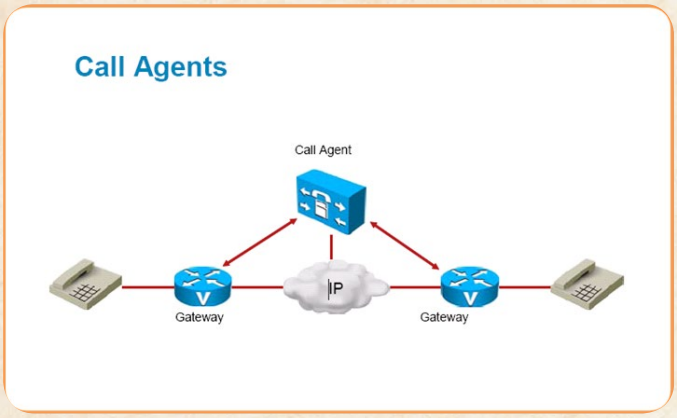
ويرسل له رسالة مبينًا له على وجود حدث Event ليسأله ماذا يفعل فيعطي أو يأمر الـ GATEWAY بتزويد الهاتف بنغمة الهاتف وهي نغمة الطلب

وعلى سبيل المثال وبعد رفع سماعة الهاتف في حالة طلب أي رقم ولو رقم واحد فقط يذهب الـ GATEWAY مجددًا إلى الـ CALL AGENT ويرسل له Event مره أخرى للسؤال عن ما المطلوب عمله، فيجيبه الـ CALL AGENT

حتى في حالة جعل الهاتف الآخر يرن عند نهاية طلب الرّقم كاملاً وهذه صورة مبسّطة لطريقة العمل .

أنواع الأحداث (Events)

منها حالة رفع السماعة وغلقها ونغمات الفاكس والمودم وأرقام التليفون من نوع DTMF وهو نوع يشّكل عمليّة مزج نوعين من الترددات عند طلب رقم واحد وكل رقم يدمج نوعين مختلفين من التردّدات.



أنواع الإشارات Signal

نغمة الهاتف عندما يكون مشغولا.
نغمة انتظار المكالمات.
نغمة الطّلب.
نغمة إعادة المكالمة.
نغمة رنين الهاتف .

ولنا معكم لقاءً في العدد القادم مع بروتوكول H.323 إن شاء اللّه

إعداد أجهزة الشبكة لتطبيقات الملتيميديا والألعاب

معظم المستخدمين العاديّين يقومون بإعداد راوتر الوايرلس الشّخصي ليقوم بعمله الأساسي فقط،ألا وهو الـ Routing بين الشّبكة الدّاخلية والإنترنت، وقد يسْتخْدم لِمشاركة الملفات والطّابعة. ولكن ماذا تعمل إذا أردت بثْ فيديو عالي الدقّة من جهاز الألعاب أو سيرفر ملفات أو مشغّل Blu-Ray إلى باقي أجهزة الشّبكة؟ أو استعمال خدمة VOIP أو ألعاب Multiplayer على الشّبكة.

هل ستكتفي بالإعدادات الأساسية فقط؟

يمكنك أن تكتفي بالإعدادات الأساسية في بعض الرّاوترات المخصّصة لذلك، ولكن بعضها يتطلّب إعدادات إضافية لكي تستخدم هذه الخدمات بدون مشاكل. لهذا، سأتناول في مقالي هذا بعض الطّرق التي من شأنها المساعدة في تحسين أداء الرّاوتر وتقليل التأخير في الـ streaming، وهو موجه للمستخدمين العاديين بالأساس.

Dual-Band

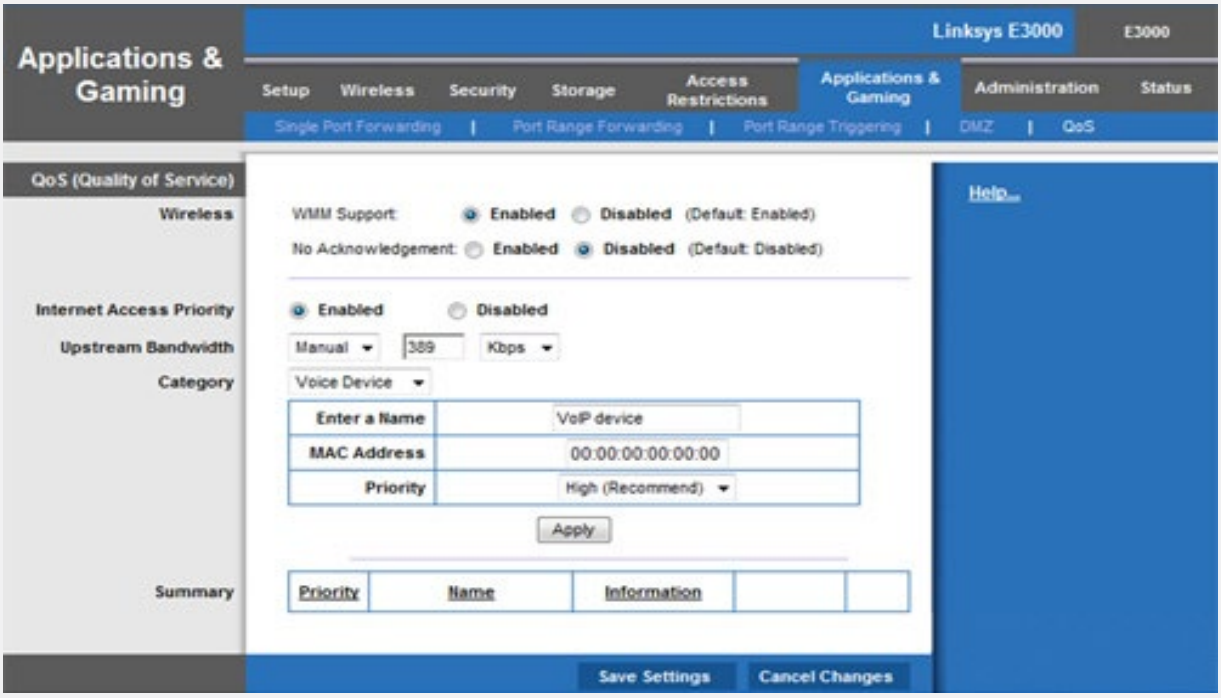
هذه الميّزة بسيطة ومعروفة لَدى الكثيرين، وهي استعمال حزمة 5GHz لغرض تحسين البث بصورة عامّة بدلا من حزمة 2.4 GHz. فبما أن معظم الأجهزة التي تستخدم الـ WiFi تستعمل حزمة 2.4 GHz، فهي تعتبر أكثر عرضةً للـ noise والتّداخل مع باقي الإشارات.

البث بأكثر من SSID

هذه الخاصية توجد في بعض أنواع الرّاوترات التي تدعم البث بترددين، حيث نقوم بإنشاء شبكتين تبثان بـ SSID مختلف، ونربط الأجهزة التي تبث الفيديو على الشبكة ذات التردد 5 GHz والأجهزة التي تستعمل للاتّصال بالإنترنت على الشّبكة ذات التردد 2.4 GHz.

Wireless Multimedia

بعض الرّاوترات الحديثة وأجهزة الوايرلس تدعم هذه الخاصية (WMM)، وهي وضع أولوية قصوى لبيانات معينة (مثل الفيديو) وهي تتشابه مع QoS ولكنها مخصّصة للمستخدمين العاديّين لكي تعمل بأقل إعدادات لازمة.

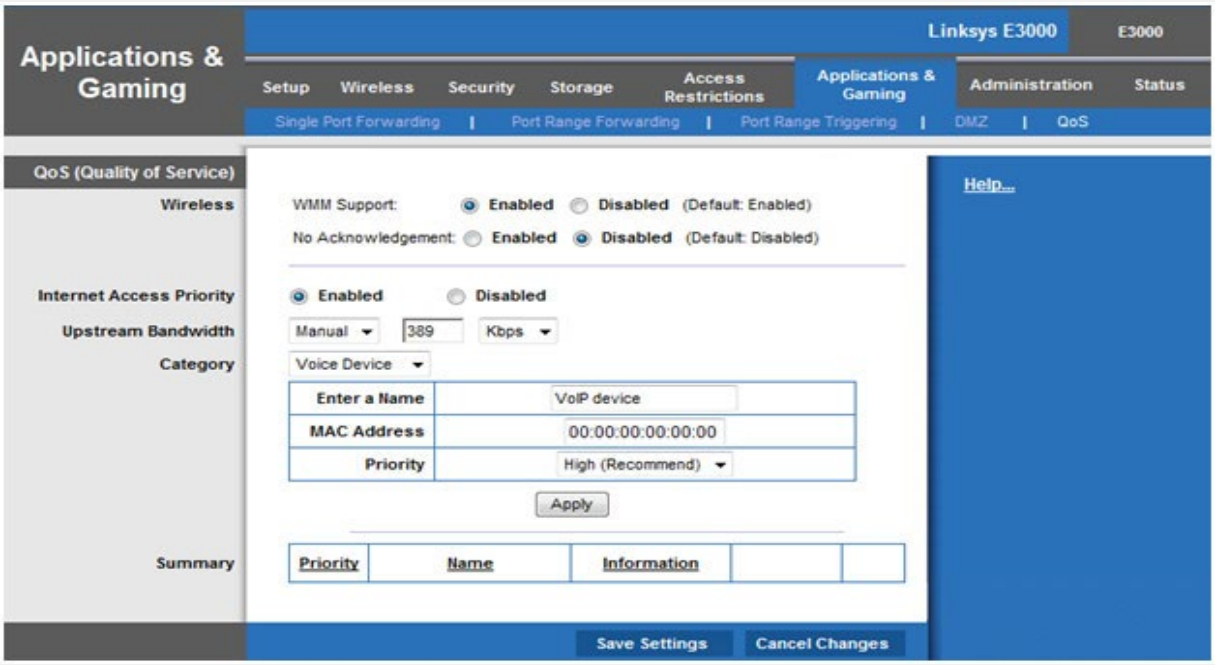


نكمل طريقنا الى باقي الملتيميديا وهو نقل الصوت VOIP. فاستعمال هذه الخدمة في الشّبكة تتطلب إعداد الرّاوترات لتقليل التّأخير في النّقل أو التّقطيع.

Quality of Service

وهذه أهم ميزة تستعمل لتحسين نقل الصوت في الراوترات QoS. حيث أن أقصى سرعة الـ Upload لتطبيقات الصّوت تكون محددة كـ auto بشكل افتراضي. ولكن تحديد السّرعة بشكل رقم معين من قبل المستخدم تساعد في تحسين السّرعة وهي عادةً تتراوح من 80 الى 90 بالمئة من سرعة الـ Upload.

فمثلا إذا فحصنا سرعة الـ Upload على موقع speedtest.net وكانت Kbps480 فان سرعة 80٪ تساوي Kbps384. لذلك يفضّل ضبط هذه القيمة كسرعة محدّدة لنقل بيانات الصوت. أو نقوم بتغييرها ما بين 80 و90 ٪ حتى نحصل على أفضل أداء. وممكن في بعض أنواع الرّاوترات أن تكون عملية الإعداد عن طريق وضع اسم جهاز VOIP والـ MAC له والأولويّة التي نخصّصها للبيانات التّابعة له. وهذا ينطبق بالتّأكيد على جميع أنواع الملتيميديا

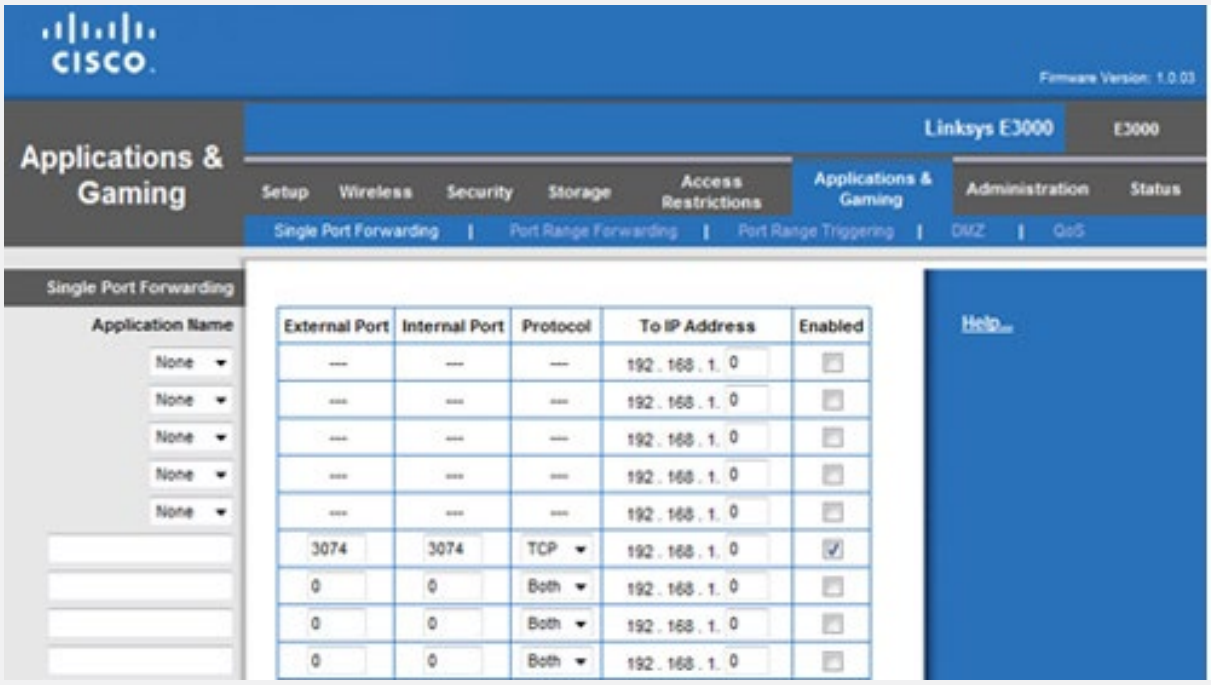


أما بخصوص اللّعب Multiplayer على الشّبكة فأكثرنا يصادفه التّقطيعات والتّأخير في اللّعبة أو حتى عدم القدرة على اللّعب وخصوصًا في الألعاب الحديثة التي تتطلب نقل كميّات كبيرة من الدّاتا، وخصوصًا عند استعمال المحادثات الصوتية أثناء اللّعبة.

لذا من الأفضل الأخذ بنظر الاعتبار الأمور اللاحقة عند إعداد الرّاوتر لكي تساعد ولو بالقليل في تحسين الأداء.

Port Forwarding

بعض أنواع الراوترات تكون معدّة افتراضيًا بحيث تغلق عددًا من الـ Ports وبالتحديد تلك الخاصّة بالألعاب بحيث لا تستطيع اللّعب نهائيا. لذلك يتوجب البحث عن هذه الـ Ports التي تستعملها اجهزة الألعاب او ألعاب الكمبيوتر لتمرير الداتا الخاصة بذلك وفتحها في الرّاوتر عن طريق Port Forwarding. فمثلا أحد الـ Ports اللازم فتحها عند استعمال أجهزة الألعاب لمايكروسوفت هو بورت 3074 في بروتوكول TCP.



استعمال اكثر من NAT

إذا كانت الشبكة تعاني من بطئ أثناء اللّعب فمن الممكن أن يكون إحدى أسبابها هو استعمال الـ NAT في أكثر من راوتر (double-NAT)، فعلى سبيل المثال قد يكون المودم المستخدم في استقبال الانترنت يقوم بعمل NAT إضافة إلى راوتر الوايرلس أيضا يقوم بعمل NAT، وهذا يقتل أداء الشبكة.

Universal Plug and Play

تستعمل هذه الخاصّية (UPnP) لحل مشاكل الاتصال والفصل مع باقي المستخدمين. وهو بالأساس مجموعة من البروتوكولات تسمح لأجهزة الشبكة المختلفة باكتشاف بعضها البعض والاتّصال بكل سهولة وبشكل ذاتي.

لذلك يفضل تفعيل هذه الميزة في الرّاوتر وباقي الأجهزة الأخرى.

إضافةً إلى كل ما سبق يمكن أن نضيف أن قوة إشارة راوتر الوايرلس تلعب دور أساسي في سرعة النقل وخصوصًا في نقل الملتيميديا والألعاب. كذلك فمقالي هذا لم يتطرق الى تأثير سرعة خط الإنترنت وأنا أتكلم هنا على الشّبكة الدّاخلية وعلى الأمور التي بمقدورنا ضبطها لتحسين عملها.

أخيرًا فإن هذه الطّرق ليست الوحيدة وغير ملزمة لكل نوع من أنواع النّقل أي يمكن التنويع بينها لأفضل أداء وماهي إلا مجرّد وسيلة تساعد في زيادة السرعة بطريقةٍ ما.

NetWork Set

معنى جديد لعالم الشبكات
في سماء اللغة العربية

الموسوعة

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

GO زيارة الصفحة

المجلة

أول مجلة عربية متخصصة
في مجال الشبكات

GO زيارة الصفحة

المدونة

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

GO زيارة الصفحة

(س) و (ج)

قسم خاص
بالأسئلة والاجوبة

GO زيارة الصفحة

القناة

YouTube

قناة المدونة
على موقع يو تيوب

GO زيارة الصفحة

ترجم

أول مشروع عربي لترجمة
المواد العلمية و التقنية

GO زيارة الصفحة

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

الأسبابِ العشر الأكثر إغفالاً في عملية Troubleshooting

تعتبر تقنيّات استكشاف الأخطاء وإصلاحها (Troubleshooting) عمليّة بالغة الأهمّيّة و حسّاسة بالنّسبة لشبكات اليوم، إذْ يجب على مهندسي الشبكات التعرف على المشاكل وإصلاحها في أسرع وقتٍ ممكن. فهناك مجموعة متنوعة من البيانات تعتبر شبكات اليوم، وهي مختلفة تمامًا عمّا كانت عليه قبل بضع سنوات، مع إضافة تطبيقات الصّوت والفيديو فإنّ فهمْ الأسباب الأكثر إغفالاً في عملية الـ Troubleshooting سوف يساعدك في حل معظم المشكلات بسرعة وسهولة. يمثل هذا الموضوع دليلاً للأسباب العشرْ التي تزيد المشاكل في الشبكة وكيفيّة معالجتها، لكنْ لا يمكنْ اعتباره دليلاً لعملية Troubleshooting.

1. عدم معرفة من أين سأبدأ :

الحصول على المعلومات من المستخدمين أمر بالغ الأهمية في فهم من أين ستبدأ حل أي مشكلة في الشبكة، فطرح الأسئلة التي من شأنها أن تساعدك في تحديد المشكلة هو شيء لا يَقلّ أهميةً عن حل هذه المشكلة.

سؤال المستخدمين عن الشيء المعطل هل كان يعمل من قبل؟ ،هو واحدٌ من أكبر المشاكل التي تواجه مسؤولي الشّبكة . إذ يقوم المستخدمين بالإبلاغ عن مشاكل الشبكة عن طريق فتح Ticket في تطبيق مخصّص للدّعم وذلك عندما يتم استنفاذ كل الحلول الخاصة بهم، والأمر متروك لمدير الشّبكة لجمع المعلومات عند أول اتصال مع المستخدم. إذا ما قام مسؤولي الشّبكة بعدم طرح الأسئلة المناسبة، يمكن أن يؤدي هذا إلى إهدار الوقت أثناء عملية الـ Troubleshooting .

فيمكن لمسؤولي الشّبكة أن يسبّبوا مشاكلَ أخرى في الشبكة للمستخدمين الآخرين. وهذا ناجم عن تنفيذ خطوات قد تكون غير ضرورية ولا تؤدي إلى كشف سبب المشكلة.

2. Documentation غير محدثة:

عندما يتم استكمال المشاريع لا بد أن نخصّص بعض الوقت

لاستكمال الوثائق(Documentation) المخصصة للمشروع، ومع ذلك، هناك بعض الحالات حيث لا نتوفر على الوقت لتكملة هذه الوثائق . أثناء عملية الـTroubleshooting ، فمن الأهمّيّة الحصول على وثائق صحيحة و محدثة. توفير هذه الأخيرة يساعدك على ضمان اجتناب خطوات Troubleshooting التي لا لزوم لها. وجود وثائق مضبوطة يساعد مديري الشبكة في التركيز على مكان وجود المشكلة .

3. سوء فهم للعمليات :

من أجل فهم الأسباب المحتملة للمشكلة، مسؤول الشبكة يحتاج إلى فهم العمليّات التي ينطوي عليها إرسال واستقبال البيانات. هناك ساعات طويلة من الوقت تنفَق أثناء عملية الـTroubleshooting بسبب عدم وجود معرفة قوية للعملية (Process) . إذا كنت لا تعرف كيفية عمل العملية يمكن أن يؤدي هذا إلىTroubleshooting غير فعال. على سبيل المثال مشكلة في الـ Application عندما تكون المشكلة الحقيقية هي أن عنوانIP خاطئ مخصص للجهاز الذي يضم هذه الـApplication . كل شيءٍ تقريبًا في مجال الشّبكات هو عملية (Process) ومسؤول الشّبكات الذي ليس على بيّنة من تلك العمليات يلزمه عمل إضافي لا لزوم له. ترتبط العمليات التي يجب على مسؤول الشبكة معرفتها بـOSI Model، إذ يجب إدراك هذا الأخير جيدًا.

4. تصاميم الشبكة معقدة :

في الشّبكات الكبيرة يمكن للتصميم (Design) أن يكون معقدًا جدًا، عندما تكون في هذا النّوع من البيئات فإنه من السهل جدًا أن ترتكب أخطاءً خلال عملية Troubleshooting. ففي بعض الظروف، نجد أساليب مختلفة لتحقيق نفس الهدف.
عندما تكون الطّرق ليست موحّدة ،يتم استخدام أكثر من أسلوب واحد فيمكن للـTroubleshooting أن يصبح أكثر تعقيدًا.

5. تكرار Troubleshooting :

تكرار Troubleshooting لها علاقة إما بوجود أكثر من مسؤول للشبكة يؤدي المهمة نفسها أو مسؤول واحد يؤدي نفس المهمة مرارًا وتكرارًا. على الرغم من أن تكرارTroubleshooting لا يسبب مشكلة في الشبكة، بل يمدد مدة المشكلة. فإنّ مهارات الاتّصالات الجيّدة ضروريّة بين مسؤولي الشبكة من أجل تجنب تكرار Tshoot .
إذ يمكن لاثنين من مسؤولي الشبكة عمل Tshoot لمشكلتين مختلفتين في جهاز مشترك. على سبيل المثال، اثنين من المستخدمين بلّغا عن وجود مشاكل في الاتصال مع الخادم نفسه. وينبغي أن يؤدي هذا الوضع بمسؤولي الشبكة إلى أن ينظرا إلى قاسم مشترك، والذي قد يكون المسار بين المستخدمين والخادم، فمن خلال استخدام مهارات التواصل الجيدة، يمكن للمسؤولين الاثنين عن الشبكة تخفيض وقت العثور على الحل .

6. نقص في التواصل :

بعض المشاكل في الشبكة يجب أن تنتقل إلى مسؤولين آخرين يمكنهم من أن يستمروا فيTshoot . ربما في بعض هذه الحالات يمكن تكرار بعض الخطوات بسبب عدم وجود اتصال بين المسؤولين. غياب التواصل يمكن أن يؤدي إلى هدر الوقت و الجهود وهذا لا يقود الى حل المشكلة. من المهم جدًا وجود طريقة لنقل

وتحويل المشاكل بين مسؤولي الشبكة الذين يعملون في شبكات تحتاج إلى دعم 7/24. وهذا turnoverينبغي أن يكون مفصلاً لضمان عدم تكرار تلك الجهود، ويمكن التركيز على حل المشكلة.

7. الإعدادات المعقدة :

تتطلب التّصاميم المعقّدة أحيانًا إعدادات معقّدة في أجهزة الشّبكة. فهم التصميم يساعد مديري الشبكة على فهم وتفسير نتائج show وdebug . فمسؤولي الشّبكة في حاجةٍ إلى فهم العمليات اللازمة لتنفيذ ودعم هذا النوع من الإعدادات، فعندما يفهم المسؤولين الأسباب التي جعلت الأمور على ما هي يمكنهم تقديم الدعم بنجاح.

8. سوء فهم Device Outputs :

عندما تكون الإعدادات المعقدة مطلوبة، يمكن أن تكون نتائج أوامر التحقق مخيفة ومُرْبكة. وينبغي لمسؤولي الشبكة أن يكونَ لديْهم الأدَوات التي تساعد في فهم معنى نتائج أوامرshow و

debug .

9. عدم توثيق الحلول :

توثيق ما أدى إلى حل المشكلة يؤدي إلى وجود وثائق دقيقة. عندما يتم التعرف على سبب المشكلة فقم بتوثيق ذلك. فعندما يحدث مشكلة مشابهة ، يمكن لمسؤولي الشبكة التعرف عليه بسرعة أو استبعاده كسبب .

10. KISS (Keep it Simple, Sir):

KISSلا تزال واحدة من الطرق الأكثر أهمية عندما يتعلق الأمر بتصميم الشّبكة، وكما ذكرنا سابقًا، التصميم الأكثر تعقيدً يُنتجُ أوتوماتيكيًا إعدادات أكثر تعقيدًا. فالتّصاميم المعقّدة تضيف طبقة فوق طبقة من التعقيد إلى الإعدادات التي بدورها تزيد من صداع Tshoot . إبقائها بسيطة يساعد المسؤولين من تضييق مجال تحديد سبب المشكلة. لكن مع وجود تطبيقات متنوعة تعمل في شبكات اليوم، يعد احترام هذه القاعدة صعبًا للغاية.

تعد مشاكل شبكات اليوم معقدة لأنها تدعم تطبيقات متنوعة وهذا يتطلب من مسؤولي الشّبكة أن تكون لديهم مهارات التواصل الجيد مع زملائهم وعملائهم على حدٍّ سواء. هذه المهارات تساعد في الوصول إلى المعلومات المطلوبة لعزل الأسباب المحتملة وفهم العمليات من أجل حل أي مشكلة.

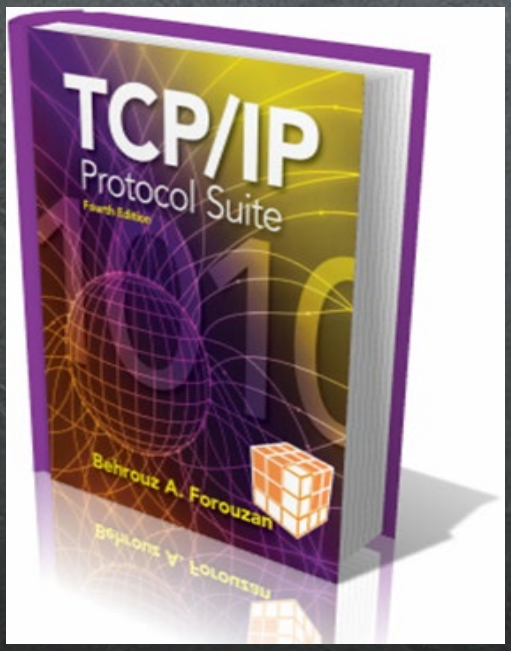
تساعد الوثائق الدقيقة على تخفيض أي فترة توقّف بسبب حل المشاكل التي لا لزوم لها في الأجهزة التي ليست من مسار البيانات، وبالتالي، ليست جزءًا من المشكلة. توثيق الحل هو أيضا في غاية الأهمية عندما يتم توثيق الحلول فهي تساعد المسؤول المقْبِل في حل نفس المشكلة .

كتاب أعجبني

إسم الكتاب :

TCP/IP Protocol Suit

تأليف : Behrouz A. Forouzan
اللغة : الانجليزية
عدد الصفحات : 1029 صفحة



يتحدث هذا الكتاب عن مواضيع كثيرة جدا وليس فقط البروتوكولات .

ففي البداية يبدأ المؤلف بتقديم نبذة عن تقنيات الشبكات وتاريخها والمعايير المنظمات التابعة لها . ثم يدخل في اهم المواضيع وهو OSI ويشرح عملية إنتقال البيانات ويعطي شرح لكل طبقة وكيف تتعامل هذه الطبقات مع البيانات .

ثم يدخل في أنواع الإتصالات مثل LAN و WLAN وغيرها ويعطي نبذة عنها .

كذلك يقدم فصل كامل حول Network Layer ويوضح عملية إنتقال البيانات بمخططات جميلة وواضحة ويذكر فيها بعض تقنيات الإتصال مثل Circuit Switching . وفصل أخر مختص بـ IPv4 وكل المعلومات الأساسية حول عنونة الشبكات يذكرها بشكل رائع ومفصل. وهنالك فصل حول كيفية إرسال وتحويل البيانات وكيفية وصولها طريقة تعامل الراوتر مع الـ Packets . ثم يعود مرة

أخرى ليتحدث عن IPv4 ولكن يسلط الضوء على Datagrams والـ Checksum و IP over ATM وايضا يذكر النقاط التي تتعلق بحماية IPv4 . ومن المواضيع التي فصلت في هذا الكتاب أيضا ، موضوع ARP خصص له فصل كامل وكذلك فصل يتكلم عن ICMP ومبدأ عمله . يناقش أيضا الكاتب هنا قضية Mobile IP ومشكلة العنونة عندما تنتقل الأجهزة فرع إلى فرع أخر في الشبكة . وهنالك موضوع مهم تألق فيه المؤلف بعلومات رائعة هو Routing ال1ي يذكر فيه أنواع Routing Protocols وكيف تعمل على تحديد المسارات فقد وضع الكاتب في هذا الفصل العديد من المخططات الجميلة توضح عمل هذه الروتوكولات . ثم الفصل الذي يليه يتكلم بأكلمه حول Multicasting .

كذلك يتكلم المؤلف عن أهم البروتوكولات مثل DNS و DHCP و SCTP و SSH و Telnet ....الخ ويتطرق لها بشكل مفصل . وهنالك فصول أخرى حول IPv6 و Multimedia وأمن الشبكات وتشفيرها.

الخاتمة :

بذل مؤلف في هذا الكتاب جهدا عظيما لم أراه في أي كتاب أخر . وفصل كثيرا في المعلومات حول البروتوكولات والية عمل تقنيات الشبكات . والأجمل من ذلك أن هذا الكتاب مليء بالرسومات التوضيحية . فأنصح من يتبحث حول عمل البروتوكولات وإنتقال البيانات أن لا يفوت الإطلاع على هذا الكتاب الثمين .

نظام الفاكس المركزي
Fax Software Solution

يسرّني أن أقدّم لكم أولى مقالاتي لكي أتحدّث عن الخدمة التي تعتبر من الخدمات القليلة التي أثّرت بشكلٍ كبيرٍ في عالم توفير الوقت والجهد لتسهيلِ سيرِ العملِ في الشّركات والمؤسّسات الكبيرة.

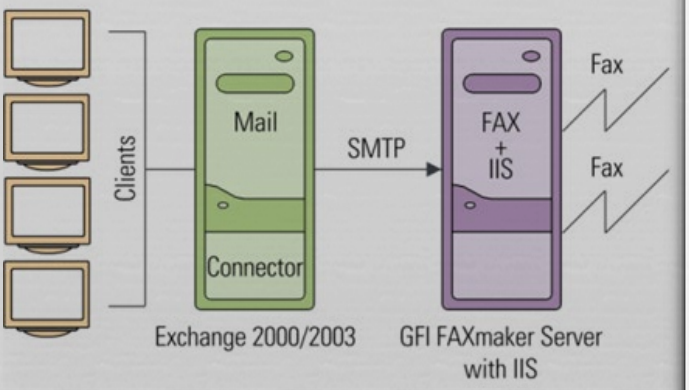
في الحالات الطّبيعية جميع الشركات تتبع الروتين المعروف بطريقة استلام واستقبالِ الفاكسات وهو شراء تجهيزات مركزية وعادةً مايكون عن طريق قسم السكرتارية الذي يعمل على استقبال الفاكسات ومسحها عن طريق الماسح الضوئي (السكانر) من أجل أرشفتها أو إرسالها إلى الموظفين المعنيين عن طريق البريد الإلكتروني، أما عملية إرسال الفاكس تتم بالطّريقة العكسيّة، وهي استلام قسم السّكرتارية الملف المطلوب وإرساله عن طريق جهاز الفاكس الموجود عادةً في قسم السّكرتارية.

وفي بعض الشّركات وعند الضّغط الكبير يتم شراء عدّة أجهزة فاكس من أجل السرعة وتخفيف الضغط لدى الأقسام المسؤولة عن هذه العمليات.

وجميعنا نعلم بوجود البرامج التي يتم تنصيبها على أجهزة الكمبيوتر بعد تركيب مودم ووصل خط هاتف عليه تتم عمليه إرسال واستقبال الفاكسات ولكن نواجه مشاكل ومنها عند تعطل الجهاز أو عندما يكون متوقف عن العمل بهذه الحالة لن نستطيع استقبال وإرسال الفاكسات.

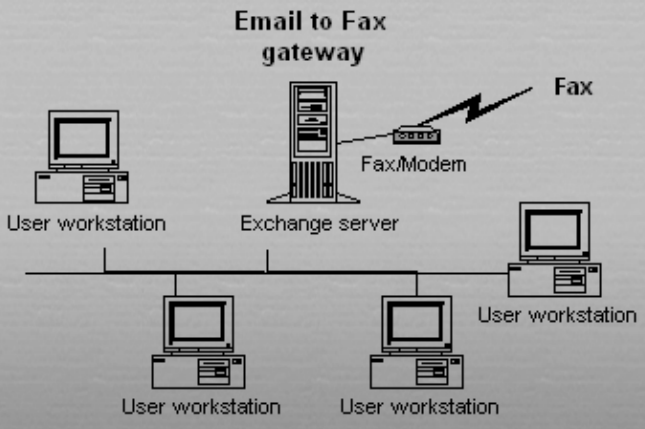
بعد بحثي المتواصل عن حلول لجميع المشاكل التي تواجهها الشركات تم العثور على GFI FaxMaker Software.

إن شركة GFI من الشّركات المعروفة عالمياً بتقديم حلول لبعض الخدمات الشّبكية وهذا البرنامج يتيح لنا وبآلية مركزية إرسال واستقبال الفاكسات، مع توفير ألوف الليرات لكلفة ثمن التجهيزات والطّابعات ورالمحابر والأوراق ،إلخ.



ميزات نظام الفاكس GFI FaxMaker

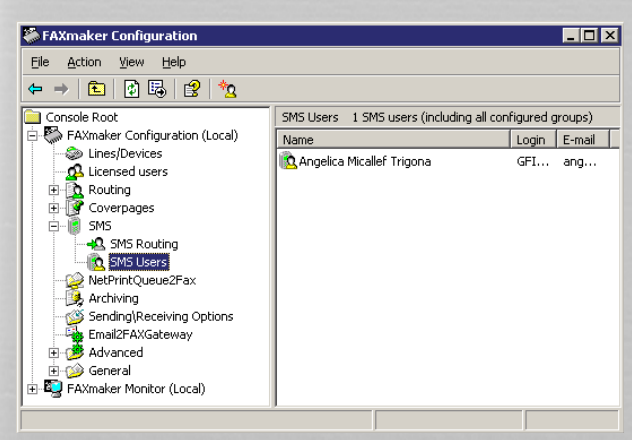
1. إرسال الفاكسات عن طريق البريد الإلكتروني Exchange الخاص بالشركة ومن رقم الهاتف المخصص، أي أنه يتم تركيب مودم و تنصيب برنامج FaxMaker على السيرفر وربطه مع نظام البريد الإلكتروني Exchange Server بـ Exchange Connector ليتم استقبال الفاكسات بعلبة الوارد بشكل تلقائي مع إمكانية تحويل الفاكسات الواردة لمجموعة من الأشخاص أي وضع صلاحيات بالأشخاص التي يسمح لها باستقبال أو ارسال الفاكسات عن طريق حسابهم على الـ Domain .



2. أرشفة الفاكسات مع إمكانية طباعتها مباشرة على أي طابعة.

3. إمكانية تركيب أكثر من جهاز مودم على السيرفر وفرز الصلاحيات عن طريق النظام.

4. عملية Monitoring لعملية إرسال واستقبال الفاكسات ويتم ارسال بريد إلكتروني للشخص المرسِل بوصول الفاكس بنجاح، أو رسائل بفشل عملية الإرسال؛ لأسباب منها مثلاً عدم استجابة الجهة الأخرى على الفاكس.



أفضل عشر شهادات فى مجال الآي تي لعام 2012

تختلف وتتنوع الشّهادات بشكل كبير من فترة إلى أخرى ويعتمد ذلك بشكلٍ أساسي على التكنولوجيا المدعمة فى الوقتً الحالي وتقوم هذه المقالة بالتركيز على أهم عشر شهادات فى هذه الفترة وفى نفس الوقت هامّة لأى شخص يعمل بـ الآي تي.

MCITP: Enterprise Administrator on Windows Server 2008

1

Microsoft CERTIFIED IT Professional

هذه الشهادة تؤهلك لكي تعمل أدمن لويندوز سيرفر 2008 وتتعامل باحترافية مع الآكتف دايركتوري وإضافة للعديد من التطبيقات الجديدة للنيتوورك وليس فقط على نطاق النيتوورك الواحدة أو الصّغيرة بل على نطاق واسع فى حالة ربط أكثر من نيتوورك ببعضهًا البعضً وأيضا احترافية فى التّعامل مع نظام تشغيل الويندوز كـ Client ويفضل لو كان ويندوز سفن.

وهي عبارة عن مجموعة قوية بشكل لا يعقل من المهارات والتى تحتاجها المؤسّسات ابتداءً من النّطاق الصّغير وصولاً بالمؤسّسات الكبرى.

إضافتك لهذ السطر: «حاصل على MCITP» إلى سيرتك الذّاتية يعطيك فرصةًعاليةً للحصول على فرصةٍ أعلى في مكانٍ أفضل .

MCTS (Microsoft Certified (Technology Specialist

2

Microsoft CERTIFIED Technology Specialist

تعبر واحدة من أهم الشّهادات التى يمكن لأي مهندس الحصول عليها حيث أنّها لا تتطلب الكثير من الامتحانات كما هو الحال فىMCITP.

وحيث أنّ معظم ما يحيط بنا من تكنولوجيا تعتبر فى الأساس ويندوز،و يمكن أن نعتبر مجازًا أننا نعيش فى عالم الويندوز وهذه الشّهادة تعزز بشكل كبير من خبراتك فى استخدام كل ما يخص ميكروسوفت من Exchange Server, Sharepoint,Virtualization, Windows Client,

or Windows Server
وبالتّالى يقوى بشكل كبير من سيرتك الذّاتية.

لا مجال للإخفاق أو الفشل فى مثل هذين النّوعين من العمل فى حالة حصولك على أيٍّ من الشّهادتين والبدءْ بالعمل بهم لأن كل منهم ببساطة يؤهلك لكي تعمل باحترافية فى تكنولوجيا معينة، هذه التكنولوجيا تحتاج إلى مؤسسة كبيرة لكي تقوم بتصميمها وبناءها ومتابعة سير العمل بها ولكن بشكل فعال.

VCP (VMware Certified Professional) 3

كم هى عظيمة هذه التّكنولوجيا فهى تعتبر بمثابة اختراع. المصنّعون شغلْهم الشّاغل هو تصنيع سيرفرات أسرع وأسرع، يمكنها تخزين الكثير من الداتا ومع ذلك نجد الكثير والكثير من هذه السيرفرات يوجد فى الداتا سنترز ومع ذلك لا تحمل سوى كسور بسيطة من سعتها التخزينية.

الافتراضية التى تتيح استخدام أكثر من سيرفر افتراضى على نفس السيرفر الحقيقى، سوف تستمر فى التّطور والزيادة فى الأهمّية ما دامت المؤسّسات مهتمة بتحسين استثمار السّعات التّخزينيّة للسيرفرات الحقيقية.

VMWARE تعتبر من أهم أنواع السوفت وير المستخدمة فى تكنولوجيا الـ Virtualization إن لم تكن هي الرائدة فى ذلك.

حصولك على هذه الشهادة يعطى صاحب العمل الثّقة الكبيرة فى قدرتك الحالية والمستقبلية فى تصميم وبناء وتشغيل بيئة متكاملة من السيرفرات الافتراضية باستخدام ال vmware أيضًا إذا تحدثت مع أي شخص مسؤول عن.

أي داتا سنتر سوف تكتشف مدى أفضلية ال vmware على Microsoft's Hyper-V ولكن هذا لا يمنع من وجود بعض المحترفين فى هذا المجال والذين يفضلون حلول ميكروسوفت على أساس أنها تحسن من الأداء وتساعد فى سد الفجوات .

CCNA 4

من المفترض أن تكون الشّهادة التّالية على قائمة سيسكو هي:

(CCIE (Cisco Certified Internetwork Expert ولكي تحصل عليها عليك أولاً اجتياز اختبار هائل وفي الحقيقة القليل جدًا من محترفي الشّبكات وجدوا الفرصة لأداء هذا الاختبار. وفى الوقت الذي تجد فيه أجهزة سيسكو تمثل العمود الفقري لأي نيتوورك وتدار بواسطتها العديد من المؤسّسات التى تتراوح من الصغيرة إلى الكبيرة نجد أنّ الكثير منها لا يحتاج لهذه الشّهادة أو حتى يمتلك تكاليف هذه الشّهادة أو القدرة الفنّية على اجتيازها.

لهذا السبب تأتي أهمية CCNA (Cisco Certified Network Associate).

فهى تساعد كثيرًا في التّعرف على أساسيّات النيتوورك ونظم تشغيلها وبدون حاجتك للمساعدة، وفى نفس الوقت فهي تعزز من السّيرة الذّاتية لك.وحيث أنّ النيتوورك سكيورتي أصبح المطلب الرئيسي لأي مؤسّسة فإنه من المفضّل أن تتابع لكي تحصل على CCNA Security certification.

CSSA (Certified SonicWALL Security Administrator)

5

منذ بداية العام 2012 أعلنت شركة ديل عن بدايتها فى الاستحواذ على شركة سونيك وول والسبب؛ هو رغبة ديل المستمرة فى شراء المصنعين وخصوصًا ما حدث مع سونيك وول وهو تطور سونيك وول فى الفترة الأخيرة فيما يخص توحيد إدارة الهجمات أو ما يعرف بـ

«UTM»Unified Threat Management

شخص ما يجب أن تتوافر لديه القدرة على إعداد وصيانة وحل المشاكل المتعلقة بهذا النوع من الأجهزة وهذه الشّهادة لا تكتفى بتقديم إثبات الإحترافية على الورق فقط ولكن تجعلك قادر على التعامل بشكل جيد مع أي جهاز من أجهزة سونيك وول .

دائما ما تسعى جهات العمل لطلب أجهزة نيتوورك تقوم بأغراض الفايروول والرّاوتنج وخدمات إدارة أو صد الهجمات.

استطاعت سونيك وول فى الفترة الأخيرة أن تستحوذ على جزء من الماركت وتخلق مجال للمنافسة والفضل الأكبر يرجع بالطبع إلى شركة ديل ويتوقع أن تزداد المنافسة أكثر وأكثر مستقبلاً.

من المهم أن تعرف كيف تقوم بإعداد هذه الأجهزة ليتوفر لك العديد من فرص العمل وخصوصًا فى البيزنس المحدود.

PMP (Project Management Professional)

6

عند الحديث عن رؤساء العمل فالمشكلة ليست مشكلة تقنية أو فنيّة بقدر ماهى نقص فى الخبرة المتعلّقة بإدارة المشروعات حيث عدم وجود القدرة فى تحديد متطلّبات المشروع وتحديد المصادر اللازمة للبدء فيه واعتماد كل منها على الآخر والمشكلة الأكبر هى العجز عن عمل جدول زمني واقعي يحدد بداية ونهاية المشروع.

معهد إدارة المشروعات هو جهة غير ربحية تتولّى مسؤولية هذا النّوع من الشّهادات والاختبار ليس الهدف منه الربح فهو خصّيصًا لتأهيل المتقدمين على تخطيط وعمل الميزانية وإنهاء المشروع بطريقة فعّالة فى الوقت المحدد وبدون تكلفة اضافيّة.

CISSP (Certified Information Systems Security Professional)

7

إذا كانت لديك رغبةً فى التخصّص والتعمّق فى عالم السكيورتي فإن

The (ISC) (International Information Systems Security Certification Consortium, Inc.)

سوف يفيدك بدرجة كبيرة فهو مسؤول بشكل أساسي عن هذه الشّهادة، والجدير بالذّكر أنّ

هذه الشّهادة محايدة لا تعتمد على نوع محدّد من أجهزة السّكيورتى ولها شهرة عالية بين هذا النوع من الشّهادات المحايدة فى مجال أمن السّكيورتى بشكلٍ عام.

البيانات الخاصة بأي شركة أو نيتوورك أو نظام، تقع تحت خطر مستمر من الهجمات الإلكترونية لأسباب متعددة منها أهمية هذه البيانات وحساسيّتها لذلك الشخص المسؤول عن تصميم وإدارة نيتوورك متوافر لها الحماية بشكلٍ كافٍ يحتاج لمثل هذا النّوع من الشّهادات لما تقدّمه من خبرات كثيرة كونها لا تتعلق بنظام أو جهاز محدد وإنما هى تهتم بطريقة التّفكير نفسها فى توقع الهجمات وكيفية التعامل معها.

8 ACSP (Apple Certified Support Professional)

Certified
Support Professional 10.5

الهدف منها هو إعدادك لاكتساب خبرة فى تقديم الدعم لنظم التّشغيل الخاصّة بآبل ماكنتوش .المهندسون وباللأخص المسؤولون منهم عن تقديم الدعم لنظام الويندوز يتعرضون لكثير من نظم ماك ومع هذه الشهادة يسهل التعامل مع آبل بدرجة كبيرة.ولا تقتصر الفائدة على مجرد الحصول على الشّهادة فحسب بل تمتد لتشمل الدراية الكافية بكيفية تسطيب وصيانة وحل كل المشكلات المتعلقة بأي نظام تشغيل ماك ولكن فقط الـ
.Mac OS X clients

9 A+ / Network+

Network+
CompTIA Certified

على الرغم من كونهم شهادتين منفصلتين تمامًا من النّاحية التقنية إلا أنهم يمثلوا الأساسيّات الضّرورية الواجب توافرها وفهمها بصورة جيدة جدًا لشخص يعمل فى الآي تى.
فى الحقيقة هناك جدل حول ما إن كان من الضرورى توافر هاتين الشّهادتين فى السيرة الذاتية لأى شخص متقدم للعمل فى الآي تي. كومباتيا معتمدة بشكل أكبر حيث أنها من الشهادات المحايدة التى لا تتوقف على نوع محدد .فى هذا الإختبار يتم التّركيز على الهاردوير و السوفت وير فى النيتوورك والتي لابد أن يحترفها كل من يرتاد مجال الآي تي. مثلاً تسطيب نظام تشغيل أو وضع ميزانية أو متابعة وملاحظة السكيورتى أو إدارة النيتوورك والسيرفرات.

10 CompTIA Healthcare IT Technician

CompTIA
HEALTHCARE IT
TECHNICIAN

مع ظهور الكثير من المنشآت منها ماهو طبّى أو ترفيهي أو تجاري أو غيره ولكن كلّهم يجتمعون في حاجاتهم للدعم الفنى مثلا هناك حاجة لوجود ممثلين الدعم الفني وأدمنز للنيتورك ومهندسين ومديرين .

كل ما تريده لتحسين الأداء وزيادة الخبرات سوف تجده فى هذا النّوع من الشّهادات حيث تمدك بصفة مستمرة بالمتطلبات الدورية لأي شركة والأداء المنشود لأي مؤسسة والعمليّة التقنية ومتطلبات السكيورتى و.....إلخ.

مدونة عربية مختصة بأمور التصميم الغرافيكي و تصميم
الويب و التصوير الضوئي و كل مايهم المصمم العربي ،
نعمل على تحسين المستوى العام للتصميم العربي و ذلك
بنشر العلم المشترك بين أعضاء و زوار المدونة الكرام .

- دروس تصميم
- قوالب مساعدة
- مفاهيم عامة
- مصادر مفتوحة
- إضافات برامج التصميم

CREATIVE MINDS

Give Your Design A Soul

ISSUE 02

www.creativesminds.wordpress.com

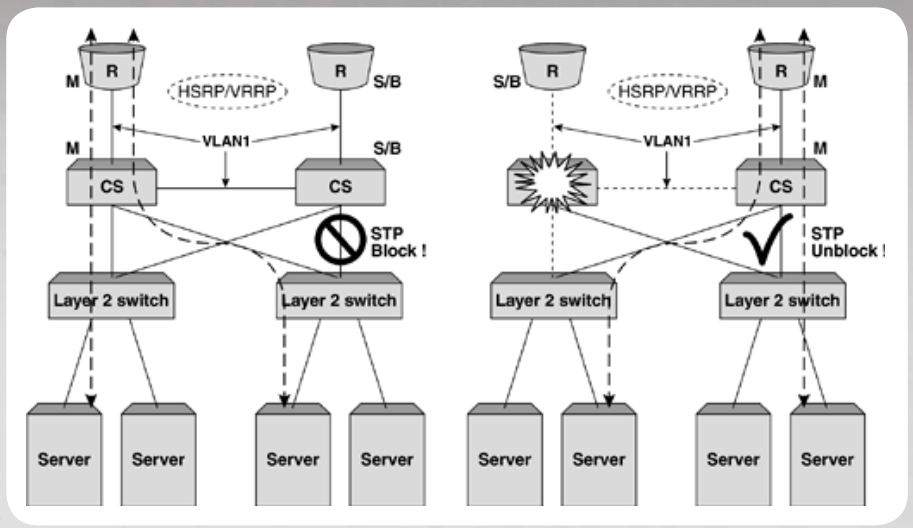
100% FREE

تصدر عنها مجلة خاصة تجد فيها كل جديد بأمور التصميم

http://www.facebook.com/creativesminds

https://twitter.com/creativesminds

شبكات الـ Content Switching



عندما نتكلّم عن تصميم الشّبكات ، نجد أنّ ساحتنا العربيّة دائمًا ما تتمركز مواضيعها حول R&S و WiFi ونتجاهل المجالات الأخرى المتقدمة والتي تساهم في إثراء معلوماتنا . وقد رأيت أنّ أثناء تنفيذ المشاريع المتعلّقة بالشّبكات للمؤسّسات يتطلّب منك دراية في كل المجالات كونك تكلّف لحلّ مشكلة معينة، في حينها تواجه أجهزة وسيرفرات لم تتعامل معها من قبل. ولن أقول أنك ستحترف كل شي ولكن أقول لك : «ركّزْ في شيءٍ ما وأتقنه وخذ من كل شيءٍ ثمرة» .

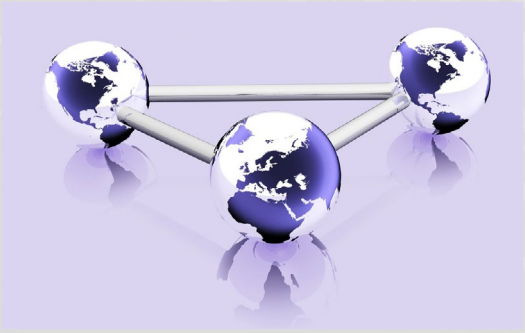
فإذا كنت تهوى الشّبكات اللاسلكية فأأكد لك أنك لن تصبح خبيرًا في هذا المجال إذا لم تكن لديك معلومات جيّدة عن R&S . ومن هذا الباب نسعى لكتابة مقالات بعيدًا عن تلك الشائعة والتّي أصبحت الأغلبية لديها فكرة عنها . ونسعى أن نرتقي نحن كمهندسين عرب لنستغني عن المنصب الوظيفي الذي يحتله الوافد . ومن هنا ، نضع بين أيديكم مقالاً لم يذكر أبداً في الساحة العربية من قبل وهو بعنوان :

شبكات الـ Content Switching والذي سأتكلم عن أهم مفاهيمه الرئيسية بأسلوب مبسّط ومفهوم .

نبذة عن شبكات الـContent Switching :

إنّ مصطلح Content Switching يبدو للأغلبية مصطلح جديد ولم يسمعوا به من قبل . المقصود بهذا المصطلح هو تصميم شبكات عالية الأداء وذات حلول متعددة تساهم في زيادة أداء الشّبكة وعمل نسخ إحتياطة وتسريع تلبية الطّلبات وإيجاد عدّة مسارات وتوصيلات تتبادل في نقل البيانات . وتندرج مواضيع كثيرة متفرّعة تحت هذه التقنية والتي من أمثلتها :

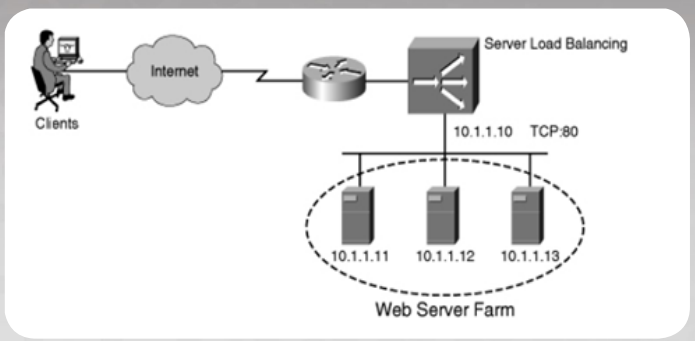
Caching و disaster recovery
و load balancing .



كيف تعمل شبكات الـ Content Switching :

إنّ عمل شبكات من هذا النّوع يختلف حسب بنيتها . ولعلّ أبسط مثال سنوضّحه لك هو Load Balancing كون معظم التّقنيات في هذا النوع من الشّبكات تتمحور حول هذا الموضوع .

يستخدم load balancing لتوزيع الطلبات بين عدة أجهزة أو عدة مسارات بهدف زيادة أداء الشّبكة وإيجاد مسار أخر تلقائيًا في حال تعطل أحد المسارات . ولتوضيح ذلك أكثر ، أضع بين يديك هذا المخطّط وسأشرحه لك :



من خلال المثال السّابق لاحظ وجود عدّة web server تؤدي نفس الغرض .
ووضعتْ بشكلٍ متعدّد لجعل الخدمة متاحة في حال تعطّل فيَعمل أحدهما كبديل. فليس من المعقول سيرفر استضافة يحتوي على 9999 موقع ويب يتم إزالته للصيانة وتتوقف كل تلك المواقع . وعودةً للمخطط فإننا نلاحظ وجود آي بي 10.1.1.10 وهذا الآيبي يمثّل كل السيرفرات ويسمى VIP او Virtual IP . فعندما يقوم الـ Client بعمل طلب فإن SLB أو Server Load Balancing يقوم بعمل ترجمة لأحد عناوين السيرفر عن طريق DNS كما تعلم . ثم يتم اختيار أحد السيرفرات لتلبية الطّلب وذلك وفقًا للإعدادات المبرمجة على SLB .

الأجهزة المستخدمة شبكات الـ Content Switching :
لتصميم هذا النّوع من الشّبكات ستحتاج إلى أجهزة مختلفة حسب تصميم الشّبكة الخاص بك ، ولكن نحن سنذكر لك بعض الأجهزة الأساسيّة والتي تصنعها شركة سيسكو والتي تندرج تحت سلسلة Content Service Switch أو CSS :

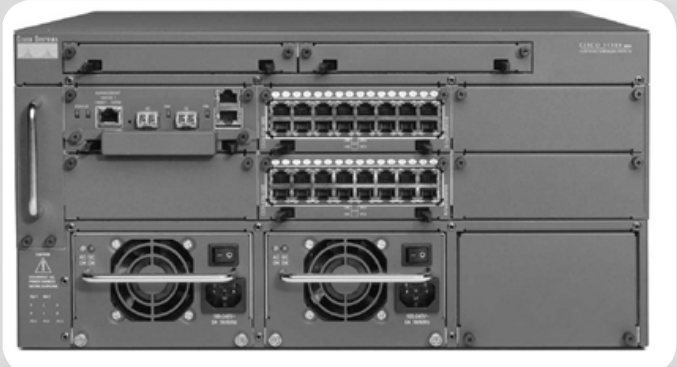
جهاز CSS 11501

هذا الجهاز يستطيع أن ينقل البيانات بين أربع طبقات من Layer 4 وحتى layer 7 . وقد صمّمته شركة سيسكو ليتعامل خصيصًا مع التطبيقات التي تتعامل مع المعاملات الإلكترونية . وهذا الجهاز يعد مناسبًا لعمل load balancing لسيرفرات الويب الصّغيرة. ويستطيع النّقل بسرعة إجمالية تصل إلى 6Gbps .

جهاز CSS 11503 :

هذا الجهاز مكوّن من 3 slots ويحتوي على قطعة واحدة SMC وبها منفذين Gigabyte Ethernet . ويستطيع النّقل بسرعة إجماليّة تصل إلى 20Gpbs .

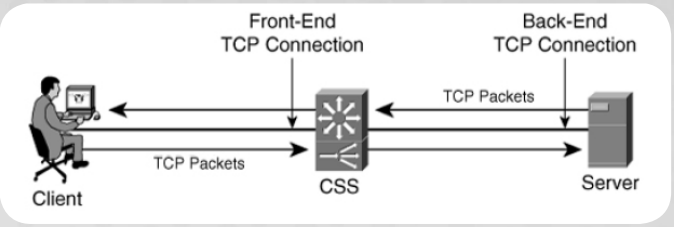
جهاز CSS 11506:



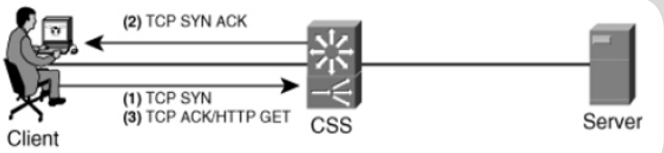
هذا هو أقوى الأجهزة في سلسلة CSS التي تقدمها سيسكو . حيث يستطيع النّقل بسرعة إجمالية تصل إلى 40Gpbs كما يحتوي على slots فارغة لإضافة modules . ويمكن تشغيل 12 منفذ GE فيه.

آلية عمل أجهزة Content Service Switch :

أجهزة CSS لم تصمّم لتعمل كأجهزة عادية مثل Routers ولكنّها صمّمت خصّيصًا للعمل في شبكات Content Switching وأنّ آلية عملها تختلف عن بقيّة الأجهزة ، فلنشاهد الأمثلة :



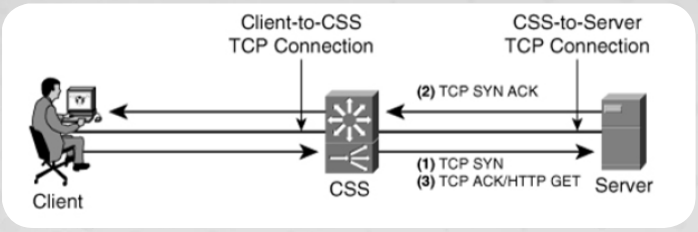
عندما يقوم الـ Client بطلب الخدمة ، تعبُر البيانات عبر جهاز CSS قبل وصول الطّلب إلى السيرفر . ونحن هنا ننقل الاتصال إلى Layer 5 . والذي يحتاج لقراءة header الخاص بطبقة application أو presentation قبل تقديم الخدمة . وهذه الحالة شائعة عند إعداد CSS ليعمل Load balancing لـ HTTP URL . ففي هذه الأثناء يقوم CSS بتأسيس الإتصال بينه وبين الـ Client قبل تحويل الطلب إلى السيرفر وذلك عن طريق TCP three-way handshake كما يظهر في المخطط التالي :



حيث أن CSS هنا يعمل حاله حال Proxy لصالح السيرفر فيقوم بالرّد على SYN packets المرسلة من الـ Client بـ SYN/ACK بدل من أن يجعل السيرفر يرد مباشرةً وتسمى هذه العملية Binding Delay . والفائدة منها أنها تسمح للـ CSS أن يقوم بجمع المعلومات التي يحتاجها من الـ Client لتحديد إلى أي سيرفر سيذهب الطلب ويتم تحديد ذلك وفقًا لعدّة قوانين منها :

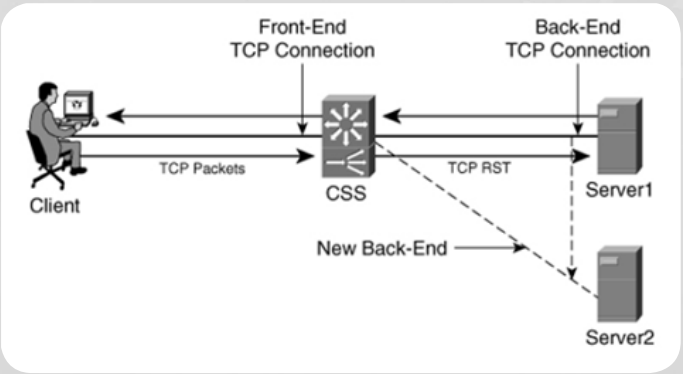
- Content rule match
- Service availability
- Service load
- Cookies
- Source IP address

وبعد أن قام الـ CSS بتحديد السيرفر الذي سينفذ الخدمة ، يقوم بتأسيس الاتصال مع السيرفر ومزاوجته مع اتصال الـ Client أيضًا باستخدام TCP three-way handshake and كما يتّضح من المخطط التالي :



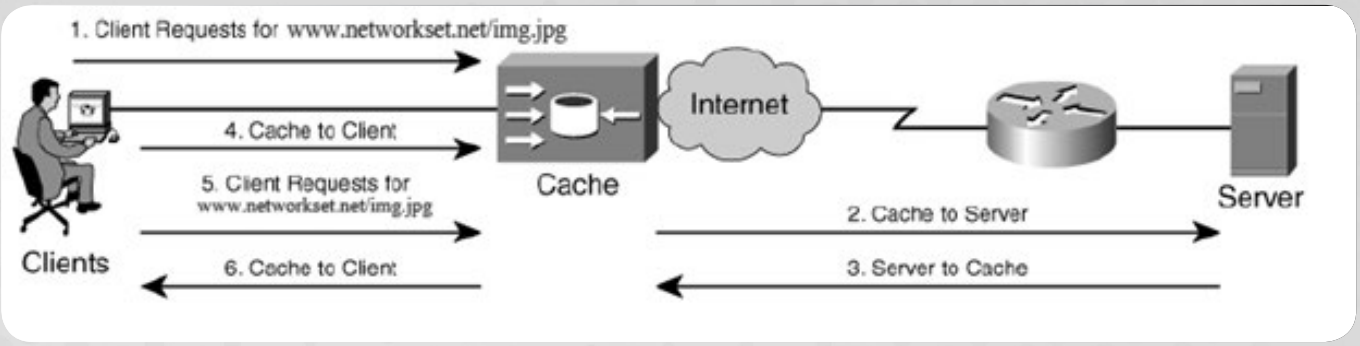
وفي حال قام الـ Client بعمل عدد طلبات متتالية بنفس نوع البروتوكول ، فإن الـ CSS هنا مباشرةً يقوم بتأسيس اتصال مع السيرفر المقدّم لتلك الخدمة، وهذه الحالة تسمّى persistence .

لكن أيضا ما زال الـ CSS يحتاج إلى أن يتوخّى الحذر لأنه أحيانًا قد يكون بحاجةٍ لنقل الطّلب لسيرفر آخر في حال ذلك السيرفر تعطّل، أو في حال قام الـ Client بشكل مفاجئ بطلب خدمة أخرى كما يظهر في المخطّط التّالي حينما قام الـ CSS بتحويل الطلب لسيرفر أخر وعمل مزاوجة مع اتصال الـ Client :



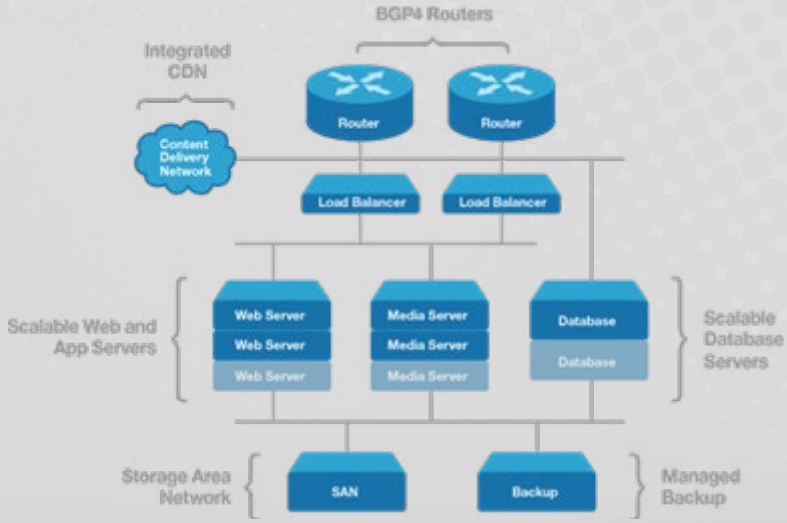
Cache Load Balancing

وبعد أن تكلمنا عن أحد أنواع الـ Content Switching ، سنتطرق لنوع آخر وهو Caching . وهو أحد المصطلحات الشائعة في مجال الشّبكات والذي يقصد به حفظ الطّلبات التي تتكرّر بحيث عند طلبها في المرّات القادمة لا يحتاج السيرفر أن يقوم بطلبها من جهة أخرى أو من سيرفر أخر وإنما تكون مخزّنة لديه ويرسلها مباشرة للجهة التي طلبت البيانات . وإليك المخطّط التّالي للتّوضيح :



هنا يقوم الـCleint بطلب صفحة وهي www.networkset.net/img.jpg . يذهب الطّلب إلى cache ويقوم بالبحث عن هذه الصفحة في ذاكرة الكاش ولا يجدها، بما أنها تُطلب لأول مرة في الشبكة وبالتالي يطلبها الـ cache من سيرفر أخر ويُحْضِرها ويُخزّنها معه ويُرسلها بعد ذلك للـ Client . ولاحظ في الخطوة 5 يقوم العميل بطلب نفس الصّفحة أو المحتوى وانظر في الخطوة 6 الكاش قام بالاستجابة وإرسال الصّفحة دون الحاجة لطلبها من سيرفر أخر كونها مخزنة معه .

Load Balancing Streaming Video Servers

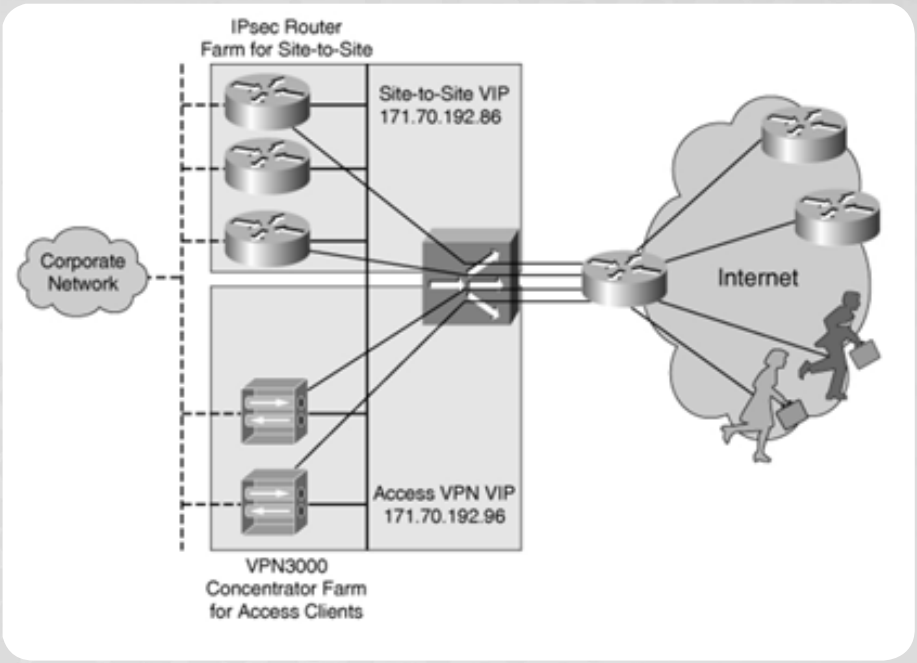


شبكات نقل الفيديو هي إحدى الشبكات المبنية على الـ content switching design وهي تعتبر شبكات ضخمة جدًا تحتاج إلى أداء خارق لتوفير نقل فيديو بجودةٍ عاليةٍ . كما أنها تحتاج لسيرفرات كثيرة جدًا ووحدات نسخ احتياطي . وأبسط مثال لهذا النوع من الشّبكات، موقع يوتيوب الشهير الذي يتلقى مليارات الطّلبات لمشاهدة الفيديو لذا هنا يستخدم load balancing بشكل رئيسي لتوفير live content أو محتوى مباشر، وكذلك VOD أو Video On Demand وهو البث الغير مباشر .

وذلك بالإعتماد على بروتوكولات Streaming والتي من أمثلتها RSTP و MMS . ويوجد عدّة أنواع من السيرفرات المستخدمة لنقل الفيديو وأشهر Apple QuickTime و RealMedia الذي يستخدم بروتوكول RSTP .

Virtual Private Network Load Balancing أو VPNLB

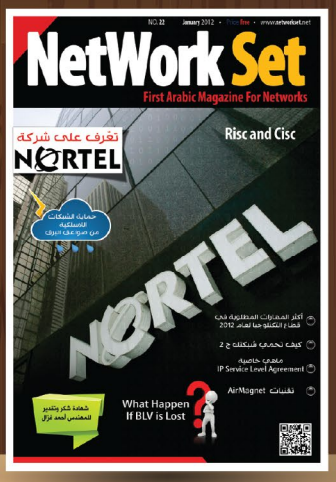
إنّ فكرة Load Balancing واستخدامها مع VPN هي توزيع VPN sessions وتقسيمها بين السيرفرات أو الأجهزة التي تعمل على حماية الإتصال بـ IPsec . وللتّوضيح أكثر ، إن طلبات الاتصال بـ VPN يتم تجميعها على شكل Frames وكل واحد من هذه الفريمات يمثل جهاز.
وهذا المخطط سيوضح أكثر :

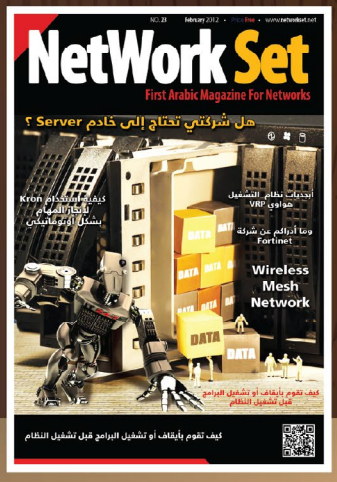


من خلال المخطط نلاحظ وجود طلبان VPN . فعند عمل هذا الطلب فإن كل جهاز سيكون لديه VIP موجود في Content Switch Module أو CSM . وإنّ الجهازان اللّذان عمِلا VPN session تكون هي الأجهزة الوحيدة التي تعلم بـ VIP وIP device Real . ومن هنا يقوم Load Balancer بتحديد الأجهزة التي ستقوم بحجز اتصال في شبكة VPN وذلك بالإعتماد على خوارزمية معينة يُستخدم معها VIP's الخاص بالأجهزة . كذلك يقوم هنا Load balancer بمراقبة الـ traffic المرسلة والمستقبلة بين الجهازان ويتأكد أنها ترسل بين جهازان متزامنان بالاتصال وأي جهاز يفشل في تلقي البيانات يتم حذفه من IPsec Frames حتى يتمكن load balancer مرة أخرى من توزيع sessions بطريقة فعّالة . ولعلّك تفهم من هنا أنّ استخدام VPNLB يزيد من سرعة اتصال VPN كذلك بزيادة عدد الطّلبات للوصول إلى VPN ولا يقل من أداء الشبكة .

هنالك الكثير والكثير حول هذا الموضوع لم أرغب بذكرهِ حتى لا يطول المقال وحتى لا نُكثرْ من تفاصيل كثيرة لا يجد فيها بعض القراء نصيبهم من المعلومة ولكنني لخّصت لكم الأساس بصورة واضحةً . وأشكر اللّه تعالى الذي وفقني في كتابة هذا المقال وأسأله الزّيادة من العلم .

Network Set Magazine Gallery





مقدمه فى الاسكريبتات
introduction to scripts

فى بيئة يونكس أو لينكس يكون جلّ اعتمادنا على الأوامر Commands التى نقوم بتنفيذها على نظام التشغيل حتى نصل إلى النتيجة المرجوةِ منها، ولكن فى بعض الأحيان للقيام بمهمه معينه task فإنها تحتاج إلى أوامر كثيرة نقوم بكتابتها حتى يتم ما نريده، لذلك لتسهيل هذه العمليّة فنقوم بوضع كل هذه الأوامر فى ملف وراء بعضها البعض، وعند تشغيل هذا الملف فإن هذه الأوامر كلها تنفّذ وراء بعضها البعض بالترتيب دون أي تدخل منا كمديرين administrator على نظام التّشغيل وهذا هو ما يعرف بالاسكريبت script .

أي أنه scrip وباختصار هو عبارة عن ملف به أوامر يستعملها نظام التّشغيل لكن بدلا من كتابتها على نظام التشغيل كل مره ، نضعها فى ملف ونقوم بتشغيل هذا الملف فتنفّذ كل الأوامر بترتيب وضعها فى script دون أي تدخل منّا .

```
$ if test "$LOGNAME" = root
> then echo Hello System Administrator
> else
> echo Hello "$LOGNAME"
> fi
```

شكل (١) مثال لسكريبت

لكتابة script هناك شروط وقواعد يجب اتباعها عند كتابة script، وإلا ستصل إلى نتيجة غير مرغوبة وهذه الشروط كالتالي :

1 - أن يبدأ الـ script بالسّطر التالي :

#! [Shell type]

ومثال على ذلك :

#! /usr/bin/bash أي أنك ستقوم باستخدام bash shell.

#! /usr/bin/ksh أي أنك ستقوم باستخدام Korn shell.

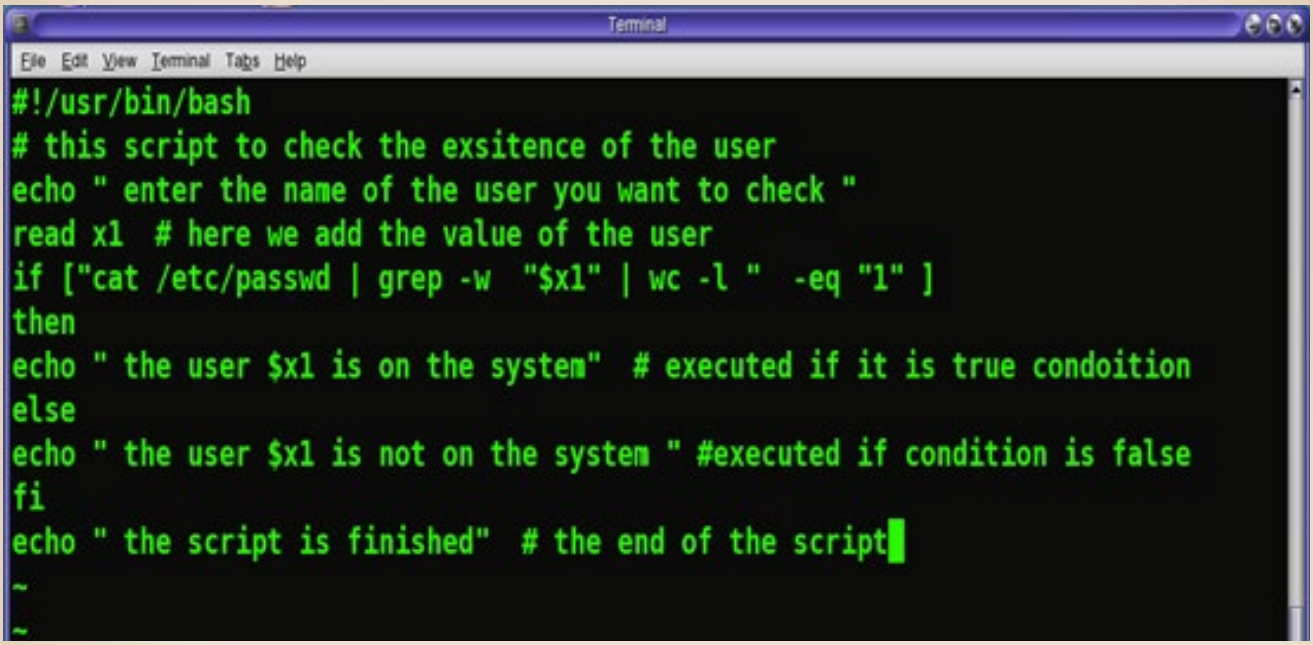
2 - أن يكون اسم script معبرًا عنه بجانب توضيح نوع الشل المستخدمه فى كتابة الاسكريبت وليكن مثلا كالتالي : dns.bash , useradd.ksh.

هنا يجب توضيح نوع الشل المستخدمة لسبب معين؛ وهو أنه فى بعض الشل يوجد أوامر معينه لا تنفّذ إلا فى هذه الشل، وبالتالى نحتاج إلى معرفة نوع هذه الشل حتى نستطيع معرفة الخصائص features الخاصة بها، لذلك نحن قمنا بكتابة اسم الشل التي سنقوم باستخدامها فى كتابة الاسكريبت فى أول سطر فى الاسكريبت .

3 - أن تقوم بوضع بعض الملاحظات comments داخل script والتى توضح ماذا تريد من commands التى تقوم بكتابتها داخل script وذلك يكون بوضع # قبل السطر ، ففي هذه الحالة يعتبرها نظام التشغيل comment ولا يقرأها وبالتالي لا ينفّذ ما بها.

مثال على ذلك:

This script is for adding user #
Useradd Ahmed # this command to add user called Ahmed



شكل اسكريبت لتوضيح كيفية كتابة ملاحظات في الاسكريبت

الآن تعالوا بنا لنتعرف على كيفيّة تشغيل script :
لعمل ذلك يجب علينا أولاً التأكد من أنه هناك permission تسمح لنا بتشغيل script ; والأفضل أن تعطي المستخدم الذي يقوم بتشغيل script سماحية كاملة full permission على الملف كالتالي:
Chmod u=rwx shell-script-name

ثم بعد ذلك نقوم باستخدام أحد الطرق الثلاثة التالية لتشغيل script :

1 - Useradd.ksh :ex Scriptname
2 - Useradd.ksh :ex ksh script Shell-name
3 - ./Useradd.ksh/. :ex script-name

فى هذه الطرق يجب علينا ملاحظة الآتي: وهي أنه عند القيام باستخدام أي طريقة من هولاء فإن نظام التشغيل يقوم بفتح شل جديدة لتنفيذ هذا الاسكريبت، أما إذا أردت أن تقوم بتشغيل الاسكريبت فى الشل التى تعمل منها تقوم بالعمل الآتي :

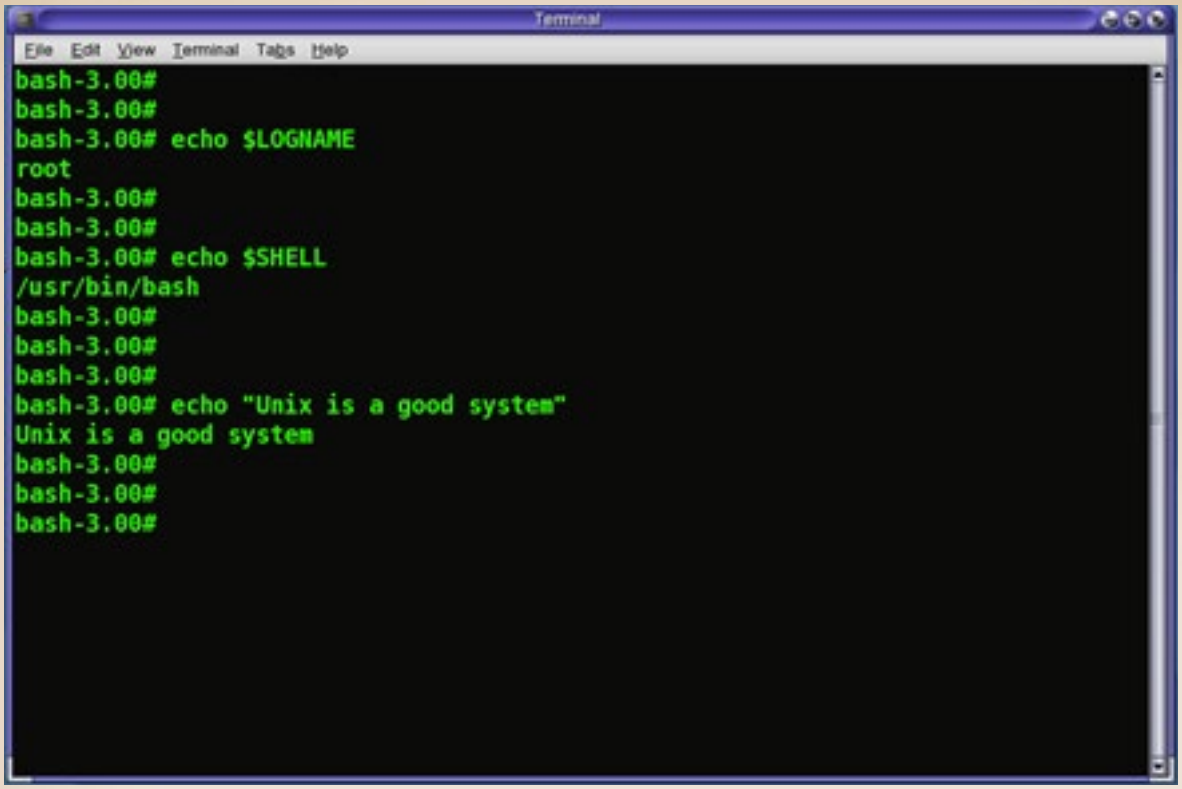
. ./script-name

الآن فتعالوا بنا لنتعرف على بعض الأوامر التى تفيدينا فى كتابة الاسكريبت ، فالسكريبت عبارة عن ملف به أوامر وتأكيدًا كلّما زاد عدد الأوامر التّى تعرفها زادت مقدرتك على كتابة سكريبت بشكل صحيح، وهناك بعض الأوامر التى لا غنى عنها فى أي سكريبت سنتعرف على أهم ثلاثة منهم.

1 - Echo command

Echo هنا معناها صدى، أي أنها تقوم بارجاع قيمة معينة لك تكون أنت قد كتبتها أو يكون النّظام محتفظ بها وأنت أردت أن يظهرها لك النظام. مثلا لمعرفة قيمة متغير variable معين فى النظام فإننا نقوم باستخدام echo command لمعرفة هذه القيمة كالتالي :

Echo $LOGNAME يقوم بعرض اسم المستخدم
Echo $SHELL يقوم بعرض الشل المستخدمة



شكل(٣) توضيح لأمر echo

2 - Read command

فى أغلب الأوقات يكون input command من خلال لوحة المفاتيح «keyboard» أي أنه يأخذ input فى خلال كتابتك للأمر نفسه.

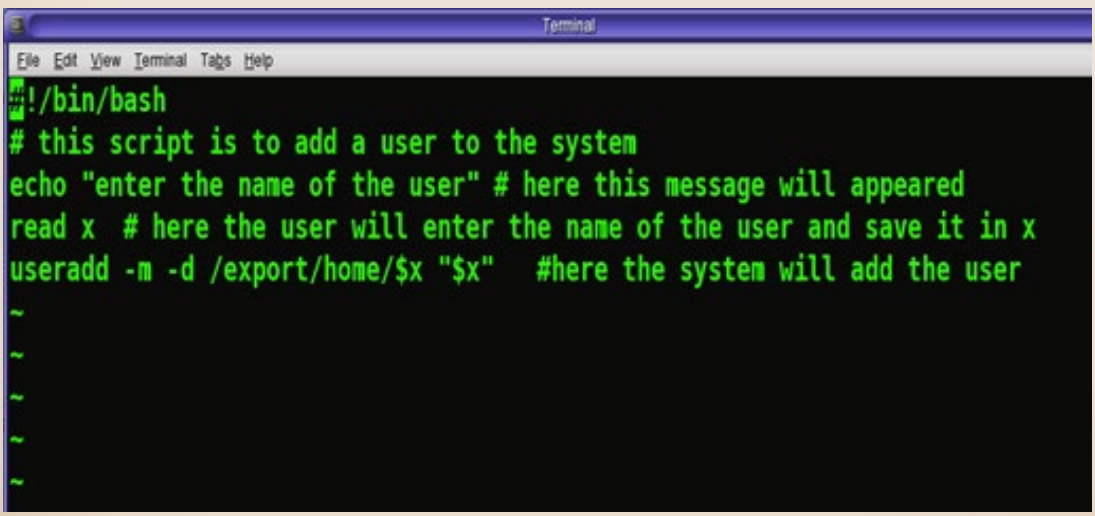
مثال على ذلك:

Ls /export/home

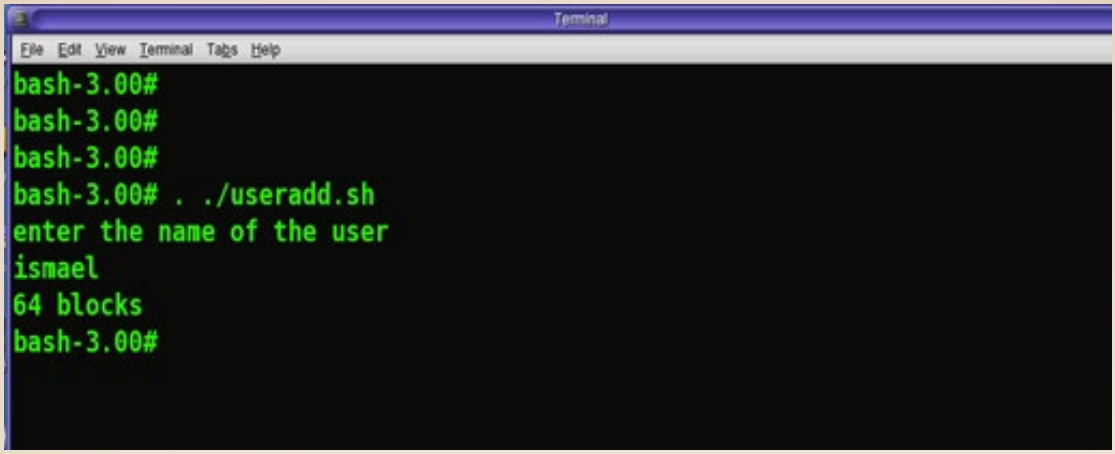
فى هذا الأمر أنت تقول للنظام list المحتويات الخاصة بالمجلد /export/home فهي هنا تعمل بمثابة input للأمر ls .

لكن فى بعض الأوقات عند كتابة script أنت لاتعرف القيمة التى سيقوم المستخدم «user» باستخدامها لذلك فلا نستطيع وضعها فى script فمثلا عندما تقوم بعمل اسكريبت لإضافة مستخدم جديد «new user» إلى النّظام فأنت لا تعرف اسم المستخدم الذي سيضاف إلى النّظام لذلك فأنت لا تستطيع وضعه؟ فما الحل إذن؟

الحل: يكمن الحل فى استخدام read command فى هذه الحالة، فأنت تقول للاسكريبت أنك ستقوم بإضافة مستخدم جديد للنّظام ولكن ليس من خلالي بل من خلال الشخص الذي سيقوم بتشغيل الاسكريبت.



عند وضع permission المناسبة على هذا الاسكريبت وتنفيذه تكون النتيجة كالتّالي :



3 - Test command

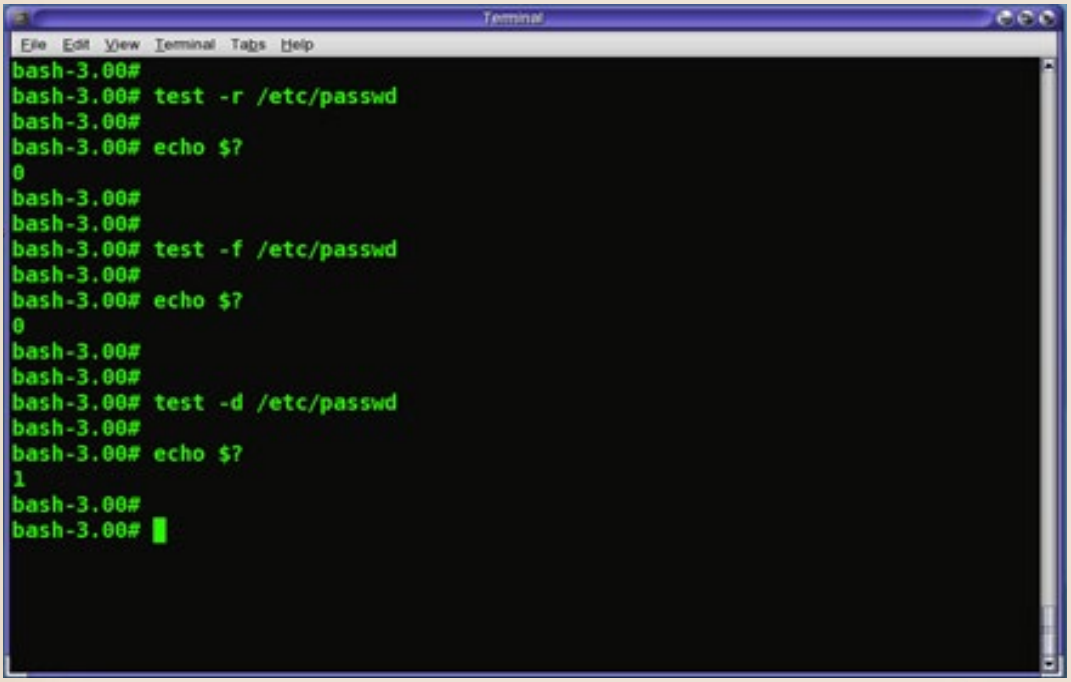
من اسم الأمر واضح أنه من خلاله نستطيع اختبار شيء معين سواء كان موجودًا أو غير موجود، فمثلاً أنت تستطيع test إذا كان الملف لديه read permission أو لا، أو مثلا تسطيع اختبار إذا كان xyz عبارة عن file or directory فإنك باستخدام هذا الأمر تستطيع عمل check إذا ما كان الشيء الذى تريده موجودًا أم لا.

ملحوظة: test command لا يعطي نتيجة معيّنة ولكن نعرفها من خلال echo $? أو ما يعرف exit status أي حالة الخروج من تنفيذ آخر أمر، وهنا تتراوح القيم مابين 0:255 والقيمة فى حالة أن test command صحيح هى 0 أي أنها صفر من الأخطاء، أما باقي القيم فإنها دليل على وجود خطأ أو أكثر فى تشغيل command .

مثال على ذلك:

1 - Test -r /etc/passwd هل /etc/passwd يمتلك read permission أم لا؟

2 - Test -f /etc/passwd هل /etc/passwd هو عبارة عن ملف «f=file and d=directory» أم لا؟



شكل (٥) يوضح امثله على test command

ملحوظة: test command مستخدم بكثرة مع if statement وفى حالة وجود loop فأنت تقوم بعمل test على شيءٍ ما لترى قيمته وهل سيتم استكمال loop أم لا؟.

مثال لاسكريبت عملي على نظام التّشغيل :

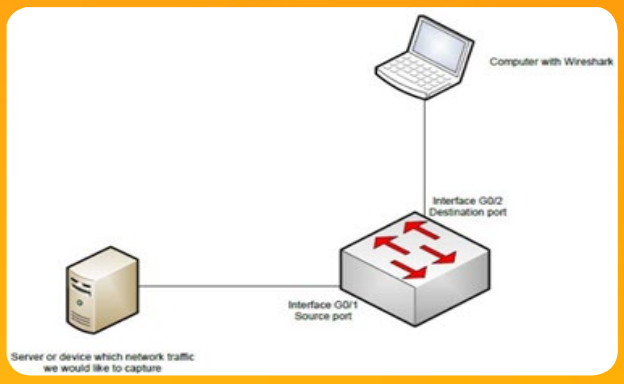
فى معظم المؤسسات الكبيرة فإنك تقوم بعملية monitoring أو مراقبة لكل file systems الموجودة لديك حتى إذا وصل أحدهم إلى 100٪ من مساحته فإنك تقوم بمسح بعض البيانات منه حتى تتيح مساحه أكبر للبيانات الجديدة وهذا يتم يوميًا تقريبًا ولتوفير الوقت من الممكن عمل هذا من خلال كتابته فى اسكريت ثم عمل scheduling له حتى ينفّذ كل يوم على نظام التّشغيل والآن اترككم مع الاسكريبت :

```
This is script is to list the file systems that exceed 90% of its size and # reach #
.100% of its size
This script is made by Eng. Ahmed Hikal #
Mail : Eng.hikal13@yahoo.com #
«echo « this script will let you know the file systems near 100%
touch /filexyzfile1file2
df -h > /filexyzfile1file2
` x1=`cat /filexyzfile1file2 | grep -w [9][012345] | wc -l
«echo «you have $x1 file systems use 90% to 95% of thier space
«echo « these file system are the following
[cat /filexyzfile1file2  | grep -w [9][012345

`x2=`cat /filexyzfile1fie2 | grep -w 100% | wc -l
«echo «you have $x2 file system that reach 100% of their space
cat /filexyzfile1file2 | grep -w 100%
rm /filexyzfile1file2
```

وإلى لقاءٍ آخر فى مقال آخر إن شاء اللّه عن بعض الأوامر المتقدمة فى عمل الاسكريبتات.

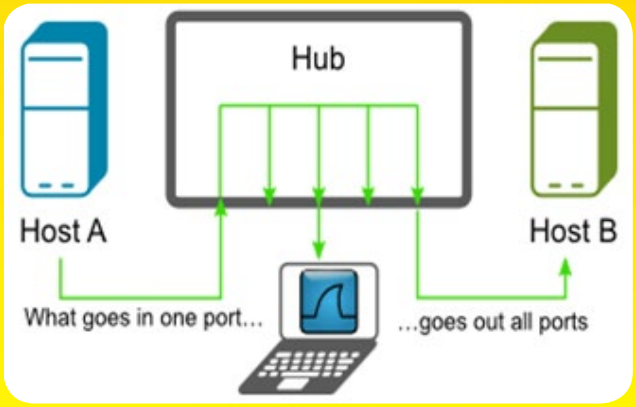
Switch Port Analyzer SPAN



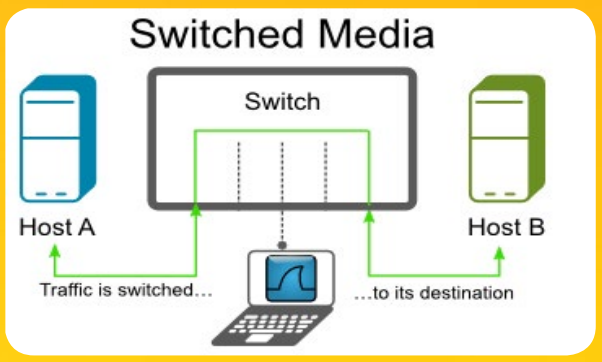
قد تحتاج أحيانًا إلى مراقبة تدفّقات البيانات في السويتش و ذلك لأسباب أمنية لمعرفة نوع البروتوكولات المارة و حجمها و هنا ستحتاج إلى طريقة لنسخ و توجيه البيانات من بورت ما أو VLAN إلى بورت في السويتش متصل بأجهزة بها برنامج مثل Wireshark أو جهاز لتحليل التّدفقات مثل جهاز Cisco SwitchProbe

و هذه الطريقة تسمى في سيسكو Switch Port Analyzer أو SPAN و تسمى أحيانًا هذه الخاصية بـ Port Monitoring أو Port Mirroring

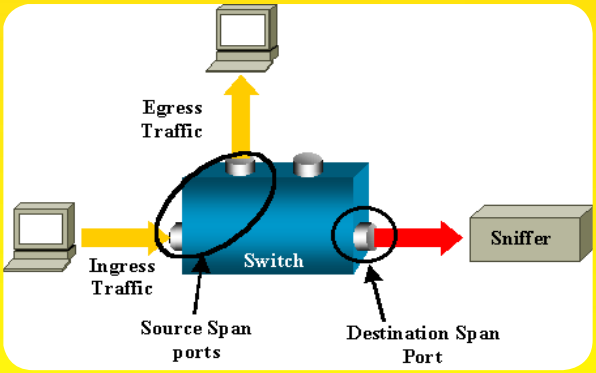
و قديمًا و قبل استخدام السويتش لم نكن نحتاج هذه الطريقة لأن جهاز Hub كان من السهل مراقبة بياناته بوضع جهاز أو برنامج تحليل التدفقات عبر أي بورت لأنه ببساطة يقوم باستلام الفريم من بورت ثم يَنشرها في جميع البورتات عدا التي جاءَ منها الفريم و بهذا فمن السّهل جدًا مراقبة البيانات عبر أي بورت كما ترى.



أما في السويتش فبمجرد أن يتعرّف السويتش على عنوان المرسِل Source MAC و عنوان المستقبل Destination MAC و يخزن عناوينهم الفيزيائية MAC في جدول العناوين لديه فإن أي تدفقات للبيانات يتم استلامها عبر بورت ما يتم إرسالها عبر البورت المخصص و ليس كل البورتات مثل الهب، وبهذا سيمنعك من مراقبة البيانات لعدم توفر البيانات إلّا عبر البورت أو البورتات المحدّدة .



و لمراقبة البيانات المارّة في السويتش فإنه لابد أن يتم إعداد أحد البورتات Destination (SPAN) Port لمراقبة دخول البيانات Ingress Traffic أو خروجها Egress Traffic من بورت Source (SPAN) Port أو من خلال شبكة ظاهريّة Source (SPAN) VLAN و إرسال نسخة من هذه التّدفقات إلى برنامج أو جهاز المراقبة و تحليل التدفقات عبر Sniffer Destination (SPAN) Port .



Source Port

يسمى أيضًا Monitored Port و هو البورت الذي يستقبل الفريم في السويتش Received (Rx)) أو يرسله (Transmitted (Tx و قد يكون بورت واحد أو عدة بورتات أو جميع بورتات السويتش , و تستطيع أن تجعل نفس البورت خاضع لأكثر من عملية مراقبة في نفس الوقت أو ما يسمى بـــ Multiple SPAN Sessions في نفس VLAN أو غيرها.

قد يكون SPAN Source Port في كثير من السويتشات و ليس كلها عبارة عن Routed Port أو Physical Port أو Physical Switch Port أو Access Port أو Trunk Port أو Etherchannel Port .

VLAN Filtering

عندما تقوم بعمل Monitoring لـ Trunk Port فإنه افتراضيًا ستتم مراقبة كل VLAN الموجودة على السويتش و لهذا فإننا نستخدم VLAN Filtering لتحديد التدفقات التي نريد أن نراقبها في Trunk Port , و يتم استخدام VLAN Filter فقط في Trunk Ports أو Voice VLAN Ports.

Source VLAN

يعتبر VSPAN هو مراقبة تدفق البيانات في الشبكة عبر VLAN و يكون Source Interface هنا هو VLAN ID يتم اختيار بورت واحد فقط و نعتبره Destination Port و الباقي سيكون Source VLAN.

Destination Port

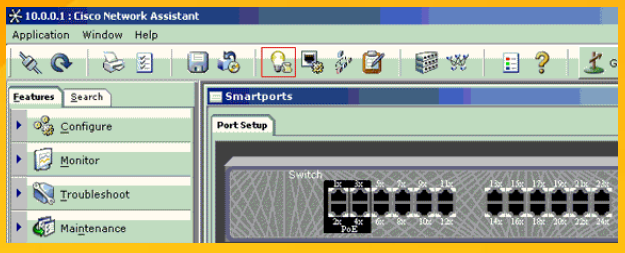
و هو البورت المراقب للبيانات الذي سيستقبل نسخة من التدفقات المرسلة و المستقبلة المراد تحليلها و مراقبتها و يكون على نفس السويتش الذي به Source Port و ينتمي فقط SPAN Session واحدة و لايستطيع أن يلعب دور Source Port و لا يقوم بأي عمل أو استجابة لبروتوكولات الطّبقة الثّانية Layer 2 protocols مثل STP, VTP, CDP, DTP, PagP هذا البورت هو الذي ستقوم بتوصيله على الكمبيوتر الذي يحتوي على برنامج تحليل البيانات Sniffer أو سيقوم بنفس المهمة.

Reflector Port

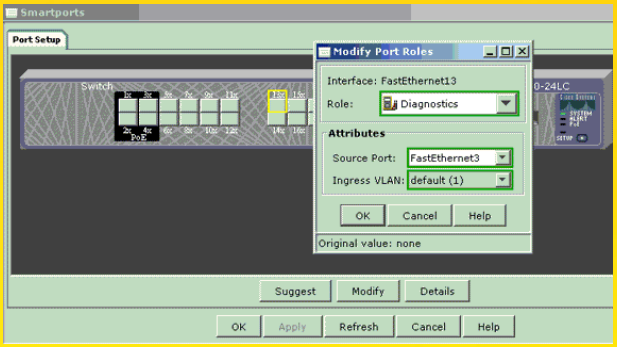
هو بورت وهمي Loop Back أو فعلي يقوم بنسخ كل التّدفقات المرسلة و المستقبلة لكل Monitored Source Ports و لا يَصْلح أن يكون Trunk و هو غير مرئي لكل VLANs و يتم تعطيل Spanning tree عليه أوتوماتيكيًا.

تطبيق SPAN بواسطة برنامج Cisco Network Assistant

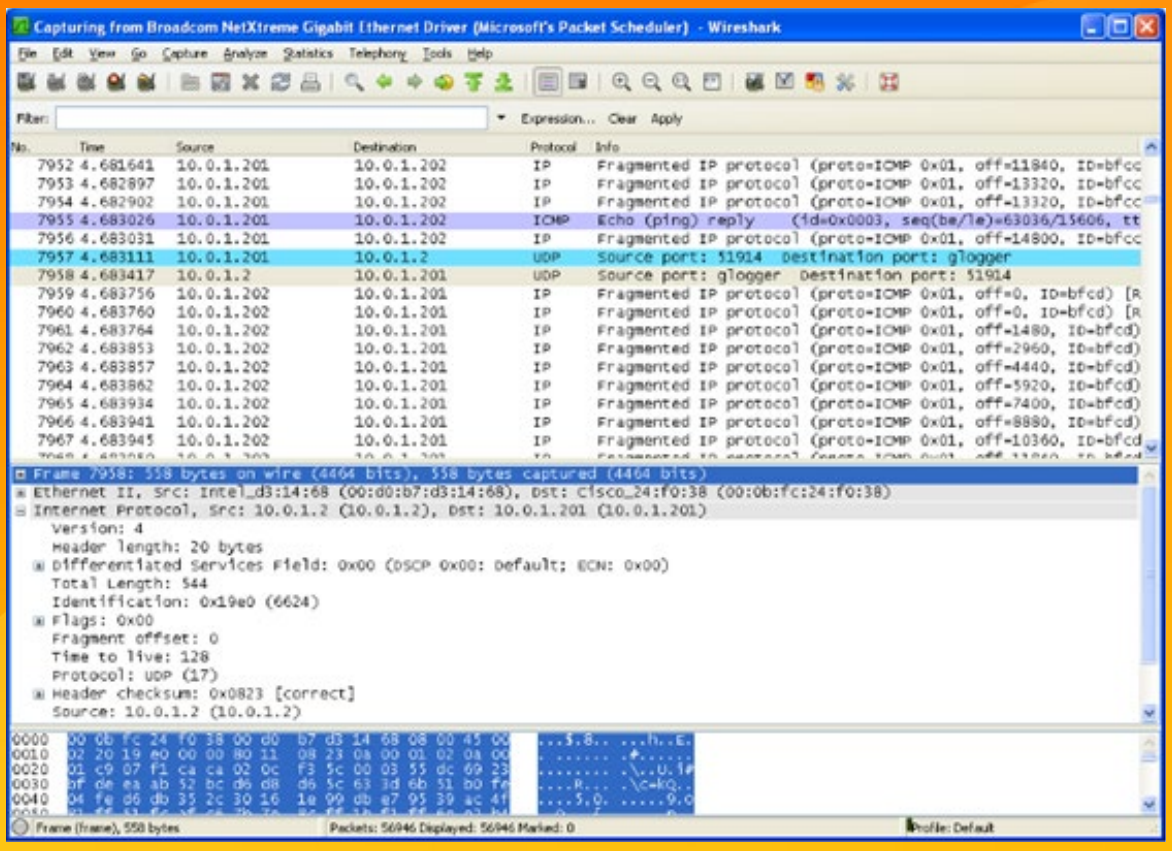
بعض السويتشات تستطيع إعداد SPAN فيهم بواسطة برنامج Cisco Network Assistant (CNA)) قم بالضغط على Smartport



ثم قم باختيار البورت الذي تريد اتصال الكمبيوتر الذي يحمل برنامج المراقبه sniffer به ،و اضغط على modify لتظهر لك صفحة المهام Roles ثم اختر Diagnostics ثم اختر Source Port المراد مراقبته و كذلك VLAN التي ستراقب تدفق البيانات عبرها، فإن لم تخترها سيقوم فقط بمراقبة Source Port كما ترى:



قم بعد ذلك بإعداد برنامج مراقبة على جهازك مثل الوايرشارك لتَظهر لك البيانات كهذه:



إعداد SPAN مبسط علي سويتشات 3560

و تعتبر سويتشات 3560 هي المعتمدة في امتحان CCIE R & S و هذا المثال صالح أيضا للتطبيق علي سويتشات Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 and 3750-E Series Switches.

هنا سيتم مراقبة التدفقات المرسلة و المستقبلة من و إلى 12/fa0 و ذلك بإرسال نسخة من كل البيانات المرسلة و المستقبلة إلى 24/fa0 و المتصل بدوره على برنامج المراقبة مثل وايرشارك.

```
S3560#configure terminal
S3560(config)#monitor session 11 source interface fastethernet 0 / 12
S3560(config)#monitor session 11 destination interface fastethernet 0 / 24
```

و للتأكد مما فعلناه نقوم باستخدام الأمر show monitor متبوعًا برقم الجلسة

```
S3560#show monitor session 11
Session 1
---------
Source Ports:
        RX Only:        None
        TX Only:        None
        Both:           Fa012
Destination Ports: Fa024/
S3560#
```

إعداد SPAN مركب علي سويتشات 2960

و في المثال التالي سيتم إعداد السويتش لمراقبة التدفقات المستقبلة على fa0/18 و المرسلة على fa0/9 و المرسلة و المستقبلة على fa0/19 مع عدم التقاط التدفقات القادمة من الشبكات الظاهرية VLAN برقم 1 و 2 و 3 و 229 , و سيتم إرسال نسخ هذه التدفقات لبورت المراقبة الذي هو برقم fa0/24

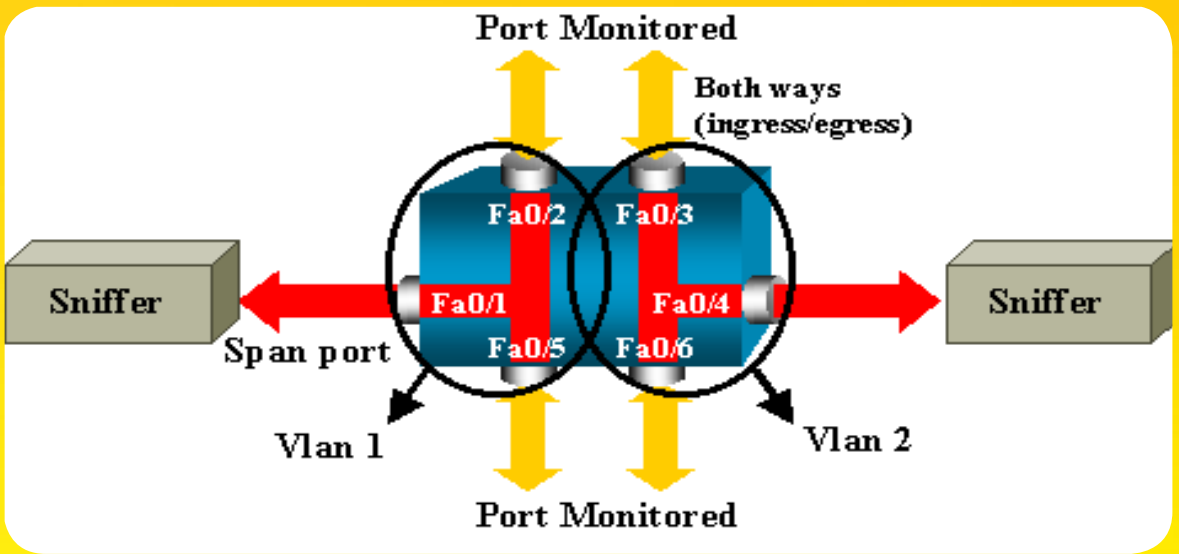
```
S2960#configure terminal
S2960(config)#monitor session 11 source interface fa018/ rx
S2960(config)#monitor session 11 source interface fa09/ tx

S2960(config)#monitor session 11 source interface fa019/

S3560(config)#monitor session 11 filter vlan 1 - 3 , 229
S2960(config)#monitor session 11 destination int fa024/ encapsulation
replicate
```

إعداد جلستين SNAP علي سويتشات 2900XL/3500XL

كما ترى في الشّكل التّالي فهذا مثال على عمل جلستين SPAN و سيتم التطبيق هنا على سويتشات Catalyst 2900XL/3500XL و هي مختلفة في إعدادها عن السويتشات السابقة 3560



أحدهما يقوم فيه البورت 0 1/Fast Ethernet (1/Fa0) بمراقبة التدفقات بين 2/Fa0 و 5/Fa0 كذلك مراقبة التدفقات خلال 1 Management Interface VLAN

الجلسة الثانية يقوم فيها البورت 4/Fa0 بمراقبة التدفقات بين 3/Fa0 و 6/Fa0و تم وضعهم جميعا في VLAN 2 .
و هذه هي طريقة إعداد الجلستين على السويتشين Catalyst 2900XL/3500XL و في هذه السويتشات لابد أن تكون جميع البورتات Source أو Destination في نفس VLAN و غير موجودة في EtherChannel أو تم إعداد Port Security عليها أو كان Monitor Port في وضع Trunk.
لإعداد البورت 1/Fa0 ليكون Destination Port و يكون البورتين 2/Fa0 و5/Fa0 و الشّبكة الظّاهرية VLAN 1 (Management Interface)كـ Source Ports فإننا سنقوم بالعمل أولا على البورت 1/Fa0 و بوضع الأمر Port Monitor متبوعًا بالبورتين 2/Fa0 و 5/Fa0 و VLAN1 و ذلك لنسخ البيانات المرسلة و المستقبلة إلى 1/Fa0 و لبيان administrative interface للسويتش و هو VLAN 1.

```
Switch(config)#interface fastethernet 0 / 1
Switch(config-if)#port monitor fastethernet 0 / 2
Switch(config-if)#port monitor fastethernet 0 / 5
Switch(config-if)#port monitor vlan 1
```

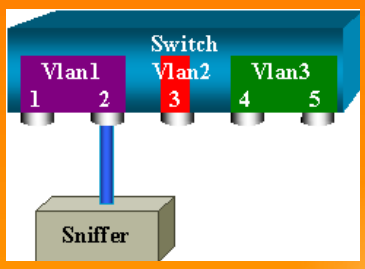
و بنفس الطّريقة لإعداد البورت 4/Fa0 ليكون Destination Port و يكون البورتين 3/Fa0 و 3/Fa0 كـ Source Ports فإننا سنقوم بالعمل أولاً على البورت 4/Fa0 و بوضع الأمر Port Monitor متبوعًا بالبورتين 3/Fa0 و 6/Fa0 و ذلك لنسخ البيانات المرسَلة و المستقبَلة إلى 4/Fa0 .

```
Switch(config-if)#interface fastethernet 0 / 4
Switch(config-if)#port monitor fastethernet 0 / 3
Switch(config-if)#port monitor fastethernet 0 / 6
Switch(config-if)#^Z
```

و للتأكد ممّا صنعناه نقوم بكتابة الأمر show running أو show port monitor .

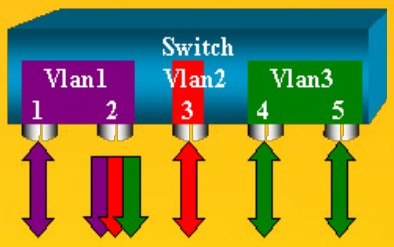
إعداد SPAN علي سويتشات 6000 /4000/5000

في هذه السويتشات الخارقة القابلة لإضافة موديولات إيثرنت أو ما يسمى Line Card لزيادة عدد البورتات و لهذا فلا تتفاجأ عندما تجد أرقام بورتات الإيثرنت يبدأ بهذا الشكل 1/fa6 في أمثلتنا :



البورتات 1/6 و 2/6 مرتبط بـ VLAN 1 و البورت 3/6 ينتمي إلى VLAN2 و البورت 4/6 و 5/6 ينتمي إلى VLAN 3 و سنربط البورت 2/6 ببرنامج المراقبة ليقوم بنسخ أي تدفّقات في البورت 1/6 و هذه هي إعدادت السويتش وذلك باستخدام الأمر
Set Span Source_Ports Destination_Port

```
switch (enable) set span 6 / 1   6 / 2
switch (enable) show span
Destination : Port 6 / 2
Admin Source : Port 6 / 1
Oper Source : Port 6 / 1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6 / 2
```



نستطيع باستخدام الأمر Set Span Source_Ports Destination_Port أن نقوم بمتابعة أكثر من Source Port و ذلك بفصل أكثر من بورت بواسطة فاصلة مع العلم أن بورت destination واحد . ففي المثال التالي سنقوم بمراقبة البورت 1/6 و مدى البورتات 3/6 – 5/6 و يكون البورت المراقب هو 2/6.

```
switch (enable) set span 6 / 1, 6 / 3 - 5  6 / 2
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
      for destination port 6 / 2
      Destination : Port 6 / 2
      Admin Source : Port  6 / 1, 6 / 3 - 5
      Oper Source : Port 6 / 1, 6 / 3 - 5
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : -
      Status : active
      switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local
span
      session active for destination port 6 / 2
```

و في هذه السويتشات أيضًا تستطيع مراقبة أكثر من بورت تنتمي لأكثر من VLAN و هو من ميزاته التي تختلف عن سويتشات أخرى مثل 2900 و 3500.

أنواع فيروسات الحاسب

تحدثنا فى العدد السّابق من المجلّة عن فيروسات الحاسب وطريقة عملها وكيف تصيب الجهاز المضيف، ثم تعمّقنا قليلاً فى دورة حياة الفايروس بدايةً من تصميمه بأي لغة من لغات البرمجة، وحتى تدميره بأحد برامج الكشف عن الفيروسات. فى هذا المقال نكمل ما بدأناه فى العدد السابق ولنتعرف على أنواع فيروسات الحاسب وحساب درجة خطورة كل نوع .

فى البداية دعنا نسأل سؤال غريب بعض الشيء وهو : لماذا يتكلف بعض الأشخاص عناء إنشاء الفيروسات ونشرها ؟ الإجابة على هذا السؤال مهما كانت كبيرة أو صغيرة يمكن أن نلخصّها في كلمة واحدة فقط وهي «التخريب» ويمكن أن تضيف بعض التفاصيل على هذه الكلمة مثل : إلحاق الضّرر بالجهاز المضيف كمسح البيانات الموجودة أو إتلافها أو سرقتها على أقل تقدير، هذا إن كان ضحيّة الفايروس مستخدم عادي، أما اذا كان جهة مسؤولة كشركة مثلا فيمكن أن يتطور الأمر الى حد سرقة الأموال أو حسابات الشركة الإئتمانية وأكثر من ذلك بكثير.

وأخيرًا وإن كان هو السائد هذه الأيام يمكن أن يكون مهمة الفايروس هو نشر الذعر فقط كنوع من الإرهاب الإلكتروني واستعراض القوة أو توصيل رسالة ما إلى جهة معيّنة لإرهابهم مثلما حدث مع فايروس «اللهب» الذي ظهر مؤخرًا والذي نشر الذعر فى كثير من الدّول العظمى .

الآن دعنا ننتقل إلى جزءٍ آخر مهم وهو متى أعرف أن جهازي مصاب بفايروس وما هي علامات ظهور الفايروس ؟

مؤشرات ظهور الفايروس

لظهور الفيروسات علامات خاصة يمكن للمستخدم العادي ملاحظتها على المدى البعيد خاصّةً وإن كانت هذه العلامات متكررة لأن في بعض الأحيان يمكن أن تكون تخميناتك لإصابة جهازك بالفايروس خاطئة ولذلك يفضل دائما قبل التصريح بالإصابة أن تكون متأكد من ظهور العلامات أكثر من مرة بنفس الشكل أو بنفس طريقة الظهور . أذكر من هذه العلامات :

1 - بعض العمليّات تأخذ وقتًا أطول من المعتاد فى تشغيلها مع ارتفاع استهلاك مصادر الجهاز مثل ارتفاع استهلاك المعالج أو الذّاكرة بدون سبب .

2 - بطئ ملحوظ في الجهاز عند تشغيل برامج معيّنة أو لعبة ما دون غيرها عن باقي الألعاب .

3 - الجهاز يتجمد تمامًا كل فترة من الزّمن ويجب إعادة تشغيله للرجوع إلى الحالة الطبيعية ثم يعاود في التوقف وهكذا .
4 - اختفاء بعض الملفات أو الفولدرات بدون سبب أو تغير اسمها تلقائيًا لأسماء أخرى بلغات غير مفهومة.
5 - زيادة حجم الفولدرات بشكل غير طبيعى وبدون سبب.
6 - عند تشغيل الجهاز لا يفتح ويستمر فقط بإعطائك أصوات تحذيرية .
7 - لا يستطيع الجهاز التعرف على نظام التشغيل الموجود على القرص الصلب ويستمر فى إعادة التشغيل بشكل أوتوماتيكي .
بالطبع العلامات كثيرة ولكني ذكرت منهم الأشهر التي نستطيع تشخيص حدوثها بسبب أي نوع من الفيروسات التي سأسْردها لاحقًا ولأن الوقاية خير من العلاج.
لنلقِ نظرةً سريعة على أسباب ظهور هذه العلامات .

كيف يصاب الكمبيوتر بالفيروسات

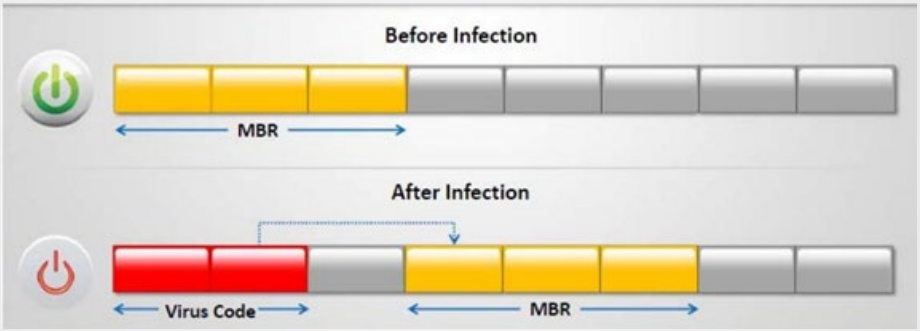
1 - عدم وجود برنامج مضاد للفيروسات على الجهاز.
2 - عدم تحديث برنامج مضاد الفيروسات (فى حالة وجوده) لآخر تحديثاته المتعارف عليها من الشركة المصنعة للتعرف على أحدث الفيروسات واكتشافها .
3 - تنصيب برامج مقرصنة من مصادر غير موثوقة .
4 - عدم فحص البرامج والملفات المرفقة مع رسائل الإيميل قبل فتحها .
5 - استقبال وتحميل أي ملف من أي شخص دون معرفةٍ سابقة به وبمصدره .
يكفينا حديثًا عن أضرار الفايروس ولنتعرف بشيء من التفصيل على أنواع الفيروسات.

أنواع الفيروسات

أنواع الفيروسات ليست منتهية وكل يوم نسمع عن ظهور فايروس جديد يعمل بطريقة مختلفة عن سابقيه لذلك ما سأذكره هو بعض الأنواع فقط أو الأشهر وليس الكل بالتأكيد.

1 - Boot Sector Viruses

يعتبر هذا النّوع الأخطر بسبب صعوبة اكتشافه.
للتّعرف على هذا النوع دعنا أولاً نتعرف على ما يسمى بـ Master Boot Record أو MBR
إذا كنت تؤدي صيانةً لجهازك بنفسك فربّما تكون سمعت هذا الاسم من قبل .. فى بداية تشغيل الحاسب يقرأ البايوس أول مقطع فعلي لأول قرص مرن أو قرص ثابت موجود على النّظام، ثم يقوم بتنفيذه يُسمى أوّل مقطع فعلي للقرص الثابت سجل التشغيل الرئيسي (أو يُسمى في بعض الأحيان جدول الأقسام أو مجموعة التشغيل الرئيسية) ماستر بوت ريكورد الذى نختصره إلى (إم بي أر) يوجد برنامج صغير في بداية هذا المقطع للقرص الثابت. ويتم تخزين معلومات الأقسام مثل عدد أقسام القرص الصلب و نظام الملفات و جدول الأقسام في نهاية هذا المقطع.
يستخدم هذا البرنامج معلومات الأقسام لتحديد القسم القابل للتشغيل ويحاول الإقلاع منه وعادةً ما يكون البارتيشن (سي) هو الأساسي الأول .
ما يقوم الفايروس بعملهِ هو نقل الـ (إم بى أر) من مكانه إلى مكان آخر بداخل القرص الصلب ويقوم بنسخ نفسه مكانه، لذلك كل مرة تقوم بتشغيل الجهاز فإنك تقوم أولاً بتحميل الفايروس ثم بعدها الفايروس يشير إلى مكان الـ (إم بى أر) ليكمل التّحميل ويدخل إلى النظام مثل الصورة التالية :



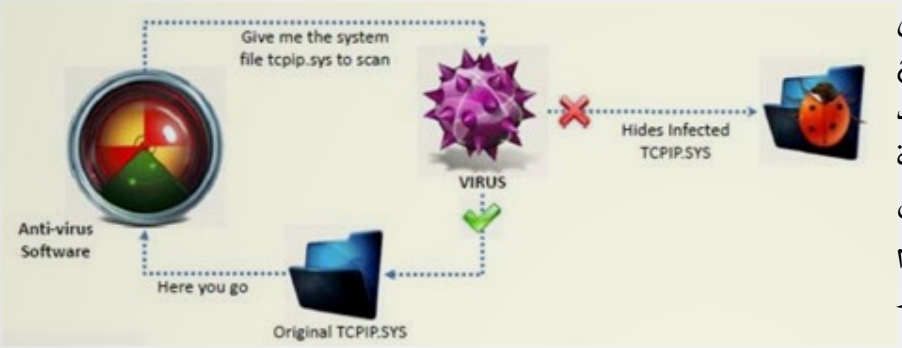
File Viruses - 2

هذا النوع من الفيروسات يصيب الملفات التنفيذية التى تتعامل مع النظام بشكل مباشر مثل ملفات COM, EXE, SYS, VAL, OBJ, PRG, MNU and BAT Files

عن طريق زرع الفايروس خلالها وتشغيلك للفايروس في كل مرة تنفذ بها أحد الملفات التنفيذية التى تنتهي بهذه الإمتدادات مثل الصّورة التّالية :

Stealth / Tunneling Viruses - 3

كما موضح من اسمه بأنه فايروس سري أو فيروسي يعمل بطريقة النّفق . هذا النّوع من الفيروسات يعمل بمنتهى الذّكاء ولا تستطيع كشفه بسهولة فطريقة عمله تعتمد على تملّصه من برنامج كشف الفيروسات عن طريق اعتراض رسائل التحذير المرسلة من برنامج الأنتي فايروس المثبّت على جهازك والتى يرسلها إلى نظام تشغيل وإعادة إرسالها مرة أخرى إلى برنامج الآنتي فايروس على أنها مرسلة من النظام ! ولنتحدث بشيء أكثر توضيحًا أنظر إلى الصورة التالية :



المعروف عن برامج الأنتى فايروس بأنها تعمل بسلْطة من نظام التّشغيل وعند اكتشافها أحد الفيروسات ترسل فورًا رسالة إلى نظام التشغيل يعلمه بما وجده وعلى أساسه يقوم نظام التشغيل بإصدار الأمر بأن هذا الملف مصاب بفايروس وبدوره يقوم الأنتي فايروس بإطلاق رسائل تحذيرية للمستخدم يعلمه بنتائج الفحص التى وصل إليها بمساعدة نظام التّشغيل ويقوم المستخدم بدوره بإعطاء الأمر للآنتى فايروس بالقضاء على هذا الفايروس .

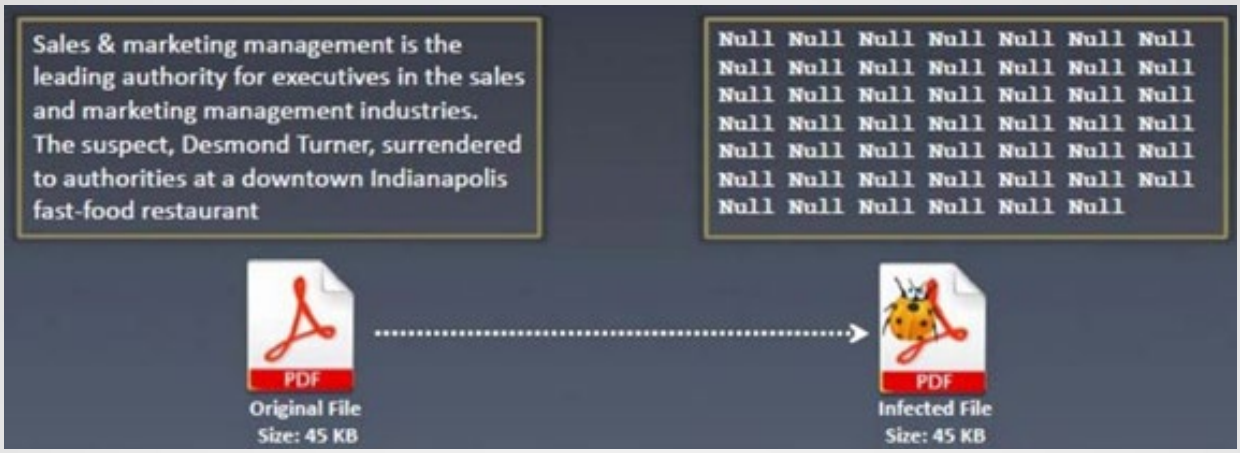
كل هذا الكلام منطقي ومعقول ولكن يستطيع هذا النوع من الفيروسات أن يخدع الآنتى فايروس باعتراضه للرّسائل المرسلة من الآنتى فايروس لنظام التشغيل وينتحل شخصيّة النّظام ويرجع الرّسالة إلى الآنتى فايروس بأن الملف نظيف ولا يوجد به أي ضرر على النظام، وعلى أساسه يطيع الآنتي فايروس الأمر ويسكت ولا يرسل رسائل تحذير للمستخدم !

Encryption Viruses - 4

هذا النوع من الفيروسات يكون مشفر بنوع خاص من التشفير يجعل من الصعوبة على برامج الآنتي فايروس كشفه لأنها لا تعرف مفاتيح تشفيره لتتمكن من فحصه وإن كان وجود مثل هذا النّوع قليل هذه الأيام بسبب التطوير المستمر فى برامج الآنتي فايروس فى فك هذه المفاتيح .

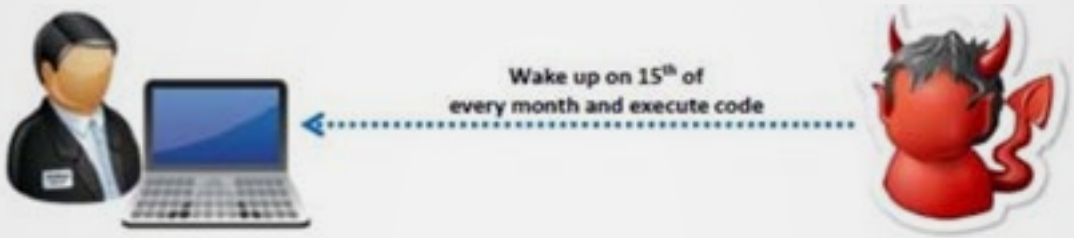
File Overwriting Viruses - 5

وظيفة هذا النّوع من الفيروسات هو إتلاف الملفات المقروءة مثل ملفات البي دي إف أو ملفات الوورد عن طريق ملء الفراغات الموجودة فى الملفات بأي قيمة ثابتة وتكرارها أكثر من مرة وعند فتحك الملف بعد إصابته لا يستجيب لك بسبب تغيير قيمته الكتابية بأخرى مختلفة مثل الصورة التالية :



Sparse Infector Viruses - 6

مثلما يلتزم الشخص ببعض القيم والمبادىء فى حياته نجد أن هذا النوع من الفيروسات أيضًا له مبدأ. فهو لا يظهر تأثيره على الجهاز المضيف إلا عند حدوث شىء معين مثل عند تنفيذك لملف ما أكثر من 3 مرات مثلا أو لا يظهر إلا فى بداية كل شهر ليذكرك بوجوده فقط، ثم يختفى مرة أخرى ! بالطبع مبادئة هذه تجعل من اكتشافه الأمر العسير على برامج كشف الفيروسات.



كما قلت فى البداية بأن أنواع الفيروسات متعددة وكثيرة ولكني ذكرت منهم الأشهر فقط أو صاحب التأثير الأقوى على الساحة.

شهادات شركة VMware

مثل كل الشركات العاملة فى مجال تكنولوجيا المعلومات تقدم شركة VMware عدة كورسات و شهادات فى مجال تكنولوجيا ال VT على منتجاتها فقط
والكورسات والشهادات هذة مقسمة لعدة مستويات ومخصصة لكل شخص على حسب مستواه
وعلى حسب مجال عملة واى منتج يعمل علية من منتجات الشركة

لذلك سوف نقسم الشهادات الى اقسام:

اولا: شهادات مسئولى المبيعات:

VSP VMware Sales Professional

شهادة مخصصة للاشخاص العاملين فى مجال المبيعات لمنتجات شركة VMware . هذة الشهاداه متاحة فقط للاشخاص العاملين فى شركات VMware Partner الكورس الخاص بها والامتحان مجانى من خلال حساب الشركة فى موقع VMware وهى عبارة عن 8 موديول وتمتحن كل مديول على حدى ومن بعدها تشاهد النتيجه لكل مديول على حدى ولك الحق فى دخول الاختبار لعدد لا نهائى من المرات حتى تنجح.

VMware Technical Sales Professional VSTP

شهادة مخصصة للاشخاص العاملين فى مجال المبيعات لكنها تحتلف عن الشهادة السابقه فى موضوع ان الشخص الحامل لها يجب ان يكون له خبرة عملية وفنية فى المنتجات التى يبيعها وهؤلاء نطلق عليهم فى الواقع ال Pre Sales

ويمتاز هؤلاء انهم لهم خلفية فنية عن المنتجات ويستطيعون ان يجيبوا على العملاء من وجة نظر فنية ويقدر ان يحدد احسن حل لمشاكل واحسن تصميم مناسب لهم على حسب حجم اعمالهم

للحصول على هذة الشهادة هو نفس اسلوب الحصول على شهادة ال VSP من خلال حساب الشركات الشركاء لشركة VMware والكورس والامتحان مجانى ويمكنك ان تدخل الامتحان العديد من المرات بشكل مجانى ويمكنك الحصول عليها بدون الحصول على شهادة ال VSP .

ثانيا : شهادات الفنيين والمهندسين:

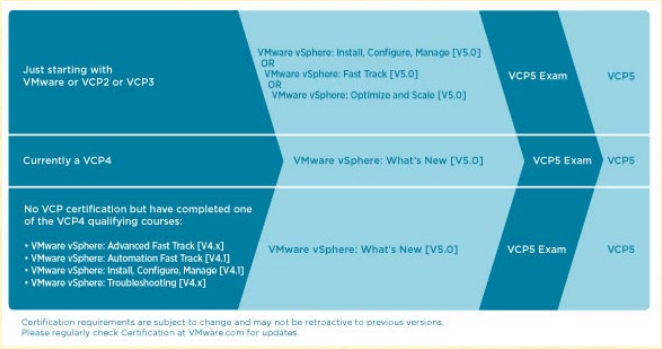
VMware Certified Professional - VCP

هى اشهر شهادات شركة VMware واكثرها انتشارا وهى شهادة خاصة للمهندسين العاملين فى عمل اعداد وأدراة وصيانة منتجات VMware وتحديد ال Vsphere and VCenter وهيا المدخل الحقيقى لكل شخص يريد ان يدير او يحول شركتة الى عالم ال VT

هذة الشهادة لها عدة اصدارات على حسب اصدار ال Vsphere وتحدث باستمرار

له كورس وحيد لكى تؤهلك للدخول للامتحان . لكن يجب ان تحضر الكورس فى مركز تدريب معتمد من شركة VMware وليس باماكانك ان تحصل على الشهادة اعتمادا على درساتك السخصية او خبرتك العملية فقط

يمكنك معرفة المراكز المعتمدة من خلال موقع شركة VMware وهم معدودين



الكورس مدتة 40 ساعة فقط وبعد الحضور يمكنك ان تحجز الامتحان من خلال شركة VUE هوا امتحان اختيار من متعدد وليس عملى .

يعيب هذة الشهادة ان سعر الكورس الخاص بها غالى الثمن لانة سعر موحد على مستوى العالم يوجد حتى كتابة هذا المقال ما يقارن من 40 الف شخص فى العالم حصلوا على هذة الشهادة

VCAP-DCA
VMware Certified Advanced Professional – Datacenter Administration

هذة الشهادة تعتبر شهادت المحترفين الخطوة التالية للاشخاص الحاصلين على شهادة ال VCP وذوى الخبرة الكبيرة فى العمل فى الداتا سنتر العملاقة

للحصول على هذة الشهاده يجب ان يتوفر فى الشخص الحاصل عليها الخبرة الكبيرة فى مجال ال VT

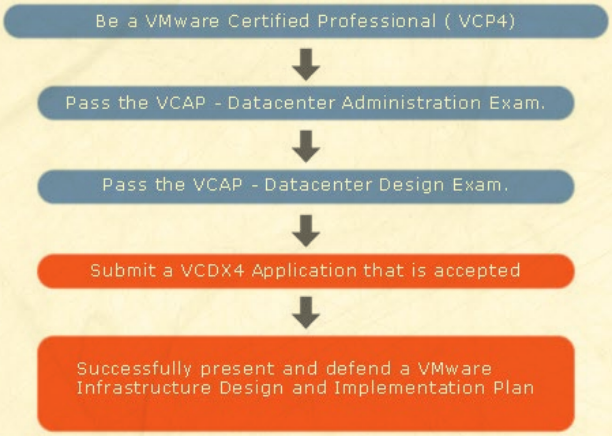
فى جميع نواحية فى الاعداد والادراة والصيانة وحل المشاكل والحماية

لذلك يجب ان يكون ان يدرس هذة الكورسات لكى يكتسب هذة المعلومات وهم عدة كورسات

* VMware vSphere: Advanced Fast Track
* VMware vSphere: Automation Fast Track
* VMware vSphere: Troubleshooting
* VMware vSphere: Manage for Performance
* VMware vSphere: Manage and Design for Security
* VMware vSphere: Automation with vSphere PowerCLI

ليس المطلوب ان تدرسهم كلهم او او تدرسهم فى مركز تعليمى معتمد لكن يكفى ان تكون على دراية بالمعلومات فى هذة الكورسات

لكن يجب الحصول على كورس وشهاده ال VCP لكى تستطيع الحصول على هذة الشهادة



ويحدث اتصال من الشركة للشخص لمراجعة اعماله وعمل مقابلة شخصية مع لمناقشة اعمالة وعلى اساسها يتم اعطائة هذة الشهادة

ثالثا: شهادات مهندسى ال VDI

VCA4-DT
VMware Certified Associate 4 – Desktop

هذة الشهادة مخصصة للعاملين فى مجال ال VDI او على برنامج VMware View الخاص بعمل VM الخاصة باليوزر على السيرفرات ال Vsphere

للحصول على هذة الشهاده يجب ان تدرس هذا الكورس

* VMware View: Install, Configure, Manage

ثم تقوم بحجز الامتحان الخاص بة من خلال شركة VUE

VCAP4-DCD
VMware Certified Advanced Professional – Datacenter Design

هذة الشهادة هى نفس فكرة الشهادة السابقة لكنها متخصصة فى مجال التصميم
بمعنى تصميم الداتا سنتر التى تعمل بتكولوجيا ال VMware وعمل افضل تصميم على حسب احتياجات العمل
للحصول على هذة الشهادة يجب دراسة هذة الكورسات ال

* VMware VSphere: Design Workshop [V4.x]
* DRBC Design - Disaster Recovery and Business Continuity Fundamentals

ليس المطلوب ان تدرسهم كلهم او او تدرسهم فى مركز تعليمى معتمد لكن يكفى ان تكون على دراية بالمعلومات فى هذة الكورسات
لكن يجب الحصول على كورس وشهادت ال VCP لكى تستطيع الحصول على هذة الشهادة

VCDX VMware Certified Design Expert

هذة الشهادة هي شهادة الخبراء فى التصميم الداتا سنتر وهيا تعتبر اعلى شهادة التصميم وادارة الداتا سنتر ايضا
للحصول على هذة الشهادة يجب ان يحصل الشخص على كل الشهادات السابقه

VCP
VCAP-DCD
VCAP-DCA

بعد الحصول على هذة الامتحانات والنجاح فيها يتم ملئ التطبيق الخاص بهذة الشهادة وارساله للشركة ويتم قبولة

VCP5-DT

VMware Certified Professional 5 – Desktop

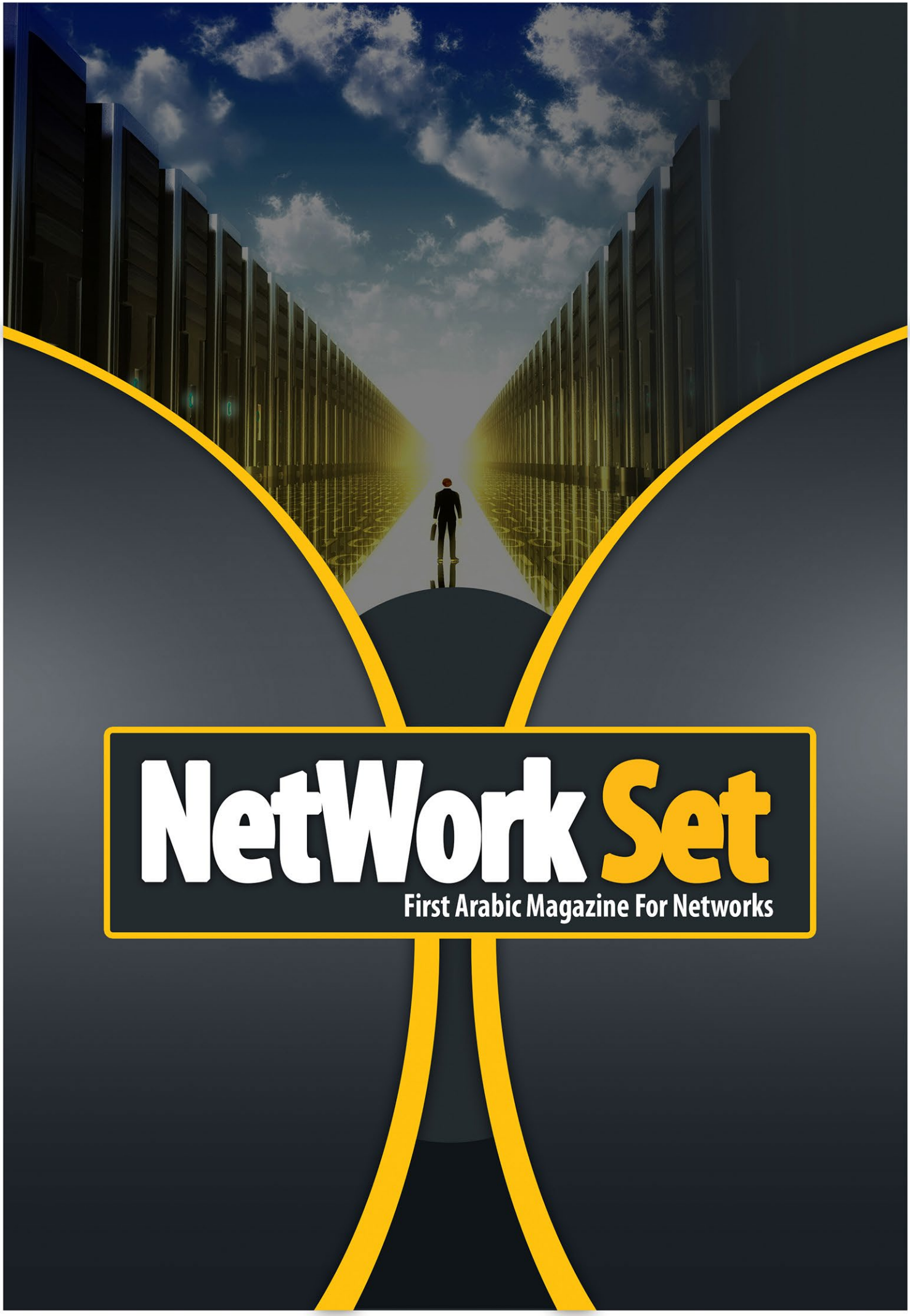
هذة الشهادة هى الخطوة التالية والاعلى للشهادة السابقة
فهى متخصصة فى نفس المجال لكن يزيد عليها ان الذى يريد الحصول عليها يجب ان يكون حاصل على شهادة ال VCP ثم ينجح فى امتحان الخاص بهذة الشهادة VCP5 DT
يجب ان يكون الخاص الحاصل على هذة الشهادة على دراية ب ThinApp

رابعا شهادة الخبراء:

هذة الشهادة تركتها للنهاية لانه تختلف عن كل الشهادات السابقة من حيث انها ليس لها كورس ولا امتحان
انما شروطها لكى تحصل عليها انك يجب ان تسجل فى البرنامج الخاص بها

وان تكون متواجد فى المنتديات والاماكن التى يرسل الناس مشاكل خاصة ببرامج ال VMware وانت تقوم بالرد عليهم ومساعدتهم فى حل هذة المشاكلاو تقوم بعمل مقالات علمية تساعد الاخرين وتجمع جميع اسهاماتك فى حل المشاكل وغيرها وترسلها لشركة VMware وهم يقوموا بعمل تقييم لادائك ويقومون بالموافقة او الرفض لاعطائك هذة الشهادة الحاصلين على هذة الشهادة محدودين ولكنهم منتشرين بكثرة على الانترنت بسبب ان كل شخص منهم له موقع خاص بةالحاصلين على هذة الشهادة لهم وضع خاص مع شركة VMware وتعطيهم مميزات كثيرة وتتيح لهم كل الاماكانيات من البرامج لديها والبرامج الجديدة والمشاريع المختلفة عندهاوالحضور للمؤتمرات الخاصة بالشركة ايضا والتحدث باسمها فى المنتدياتهذا كان عرض سريع ومختصر عن شهادات شركة VMware المختلفة

للمزيد من المعلومات يجب زيارة موقع الشركة والدخول فى قسم التعليم


NetWork Set
First Arabic Magazine For Networks