MAGAZINE
NETWORK SET
السنة الأولى - شهر آب/أغسطس الموافق لعام 2010
أول مجلة عربية تختص بأمور الشبكات تصدر من موقع WWW.NetworkSet.net

الشبكات وأنظمة المراقبة

- أكتشف علاقة الشبكات بأنظمة المراقبة
- قم بمراقبة عملك عن بعد
- راقب كل شيء من خلال شاشة واحدة

نتائج الأستفتاء

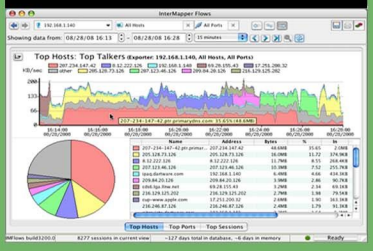
ماهو أكثر مجال في الشبكات يروق إليك؟

- شبكات سيسكو 56%
- كل مايتعلق بالشبكات 35%
- شبكات مايكروسوفت 29%
- شبكات جونيبر 9%

تعرف على أداة فحص الشبكات PathPing

networkset.net

تقرأون في هذا العدد



شاهدوا أيضا أقسام

5

أفتتاحية العدد

الخبرة ثم الخبرة!!!

الخبرة ثم الخبرة أول مطلوب نجده في كل إعلان عمل وسؤال يؤرق كل مهندس شبكات أنتهى من تعليمه وأراد أن يبدأ مشوار العمل والتى تفأجئه بمطلب غريب أن كل الأعمال المتوفرة في الأسواق تطلب من المتقدم أن يكون ذو خبرة سنتين على الأقل ,ولنكن صريحين أكثر أنا اجد هذا الطلب من الأشياء الـ******(رقابة) في عالمنا العربي بشكل كبير فهي تحد من تمييز الأشخاص في كل المجالات ومن ضمنها مجال الشبكات لذا أولا سوف أتوجه إلى شركات التوظيف بأن تراعي قليلا هذه الأمور مع المتخرجين الجدد والذين لايملكون إلا الخبرة المقيتة التى كسبها من خلال دراسته في الجامعات العربية والتى لن توصله إلى أي وظيفة مرموقة في أحد الأيام لذا أنا أود أن أطلب من أي شخص مسؤول عن أمور التوظيف أن لاتوقف أي متقدم جديد لايملك أي خبرة للتقدم للوظيفة فقد يكون هذا المتقدم أفضل من شخص لديه خبرة 10أعوام بذكائه وقدرته على التأقلم مع العمل بشكل سريع وبالأخص قدرته على تطوير هذه الشركة فنحن نعلم أن جيل الشباب هم الأكثر ثراء من غيرهم من ناحية التطوير لان الحماس هي من أكثر الصفات الموجودة في هذا الجيل بالأضافة إلى رغبته في أثبات نفسه بقوة والذي يمده بقدرة أكبر على تطوير عمل الشركة بعكس الخبير الذي همه الأول هو تنفيذ عمله بافضل وبأسرع صورة ممكنه وبالتالي تطوير الشركة سوف يبقى يراوح في مكانه لذا أخواني الأعزاء أرجو مراعاة هذه النقطة بتمعن وبعمق أكبر .

أما التوجه الثاني فهو لك أخي العزيز المتخرج بدون خبرة والذي دائما أحب أن ألومه بسبب تقصيره في أداء عمله إتجاه دراسته وإتجاه تطوير نفسه فالكل يريد أن يكسب الخبرة من خلال كتاب أو بعض النقاط الذي يعتقد أنه لو فهمها فقد كسب الخبرة اللازمة فكثيرا جدا هي الرسائل التى وصلتني تطلب مني أن أنصح ماهي الكتب أو الفيديوهات التعليمية التى تعطي الطالب خبرات العمل وكان دائما جوابي لهم أن مثل هذه الأشياء غير موجودة في الحياة فكلمة خبرة لاتدل في لغتها العربية إلا على معنى واحد وهو السنوات التى يقضيها الشخص في عمله لكي يحصل على شيء يدعى خبرة لذا أخي العزيز أنسى وجود مثل هذه الأشياء في حياتك وأعلم أخي العزيز أن الحصول على الخبرة من أبسط الأشياء الموجودة في حياتك ولكي تحصل عليها عليك أتباع أحد الخطوات التالية

أ-أحرص على إيجاد عمل أثناء دراستك فهو أفضل شيء سوف يؤهلك للحصول على الوظيفة المرموقة إن شاء الله وحتى لوكان العمل بشكل مجاني والذي أحثك عليه أيضا, أبحث عن عمل بدون مقابل ولو أطررت لأن تدفع من جيبك لكي تعمل فما سوف تزرعه اليوم سوف تحصده غدا إن شاء الله .

ب-أحرص دائما أن تكون دراستك لأي شيء يخص الشبكات أن تكون بشكل معمق وخصوصا فهم الأساسات فهي التى سوف تجعلك من الأشخاص الذين يحصلون على الخبرة بشكل أسرع من غيرك والتى سوف تنعكس عليك بشكل إيجابي وتعطيك الثقة في نفسك أثناء عمل أي مقابلة توظيف لا البحث على الأنترنت عن الأسئلة التى يتوقع أن تسأل عنها أثناء عمل المقابلة !!!! .

ج-ولو اغلقت كل الأبواب بوجهك ولم تستطتع إيجاد عمل فالخبرة مازالت متواجدة أمام عينيك وبشكل مجاني بس لازم تفكر كيف تجده وهي الأنترنت فهو أكبر وأفضل مكان تجد فيه الخبرة وأفضل مكان هو المنتديات والمدونات فوالله المنتديات فيها خبرة 10سنوات بس تحتاج منك معرفة كيفية تحويلها لصالحك وسوف تسألني كيف ؟ والجواب بسيط أشترك في أقوى المنتديات العربية الخاصة بالشبكات وكن عضو نشيط ولاتكتفي فقط بالقراءة فهي لن توصلك لأي شيء بل حاول أن تجد أي سؤال وقم بالأجابة عليه مباشرة وحتى أن لم تكن تعرف الأجابة أفتح محرك البحث غوغل وحاول أن تبحث عن المشكلة باللغة العربية أو باللغة الأنكليزية وحاول أن تفهمها وبعدها قدم الأجابة للشخص السأل ولاحظ مع الوقت الحجم الهائل من الخبرة التى سوف تحصل عليها وكن دائما السباق في الرد على الأسئلة وهذا الأمر أعطيكم أياه عن خبرة أكيدة في هذا المجال .

خلاصة هذا الكلام أخي العزيز أن الخبرة شيء بسيط جدا ويمكن الحصول عليه لكن يحتاج منك بعض الجهد والتعب وأهم نقطة أن لاتضع أمامك أي معوقات أو مبررات لكي تقنع نفسك أنك شخص لايستطيع أن يفعل شيء أمام أبواب العمل التى يا أما تحتاج خبرة أو تحتاج واسطة وثق دائما أنك سوف تصل إلى أعلى المراتب إن شاء الله

أيمن النعيمي

المحررون الدائمون

- الدكتور محمد التميمي
Yarra_link@yahoo.com
- المهندس أيمن النعيمي
www.networkset.net
- المهندس أحمد الشحات
warior10@hotmail.com
- المهندس عادل الحميدي
adel_husni2000@hotmail.com
- المهندس ياسر رمزي
www.yasserauda.com
- المهندس أحمد بخيت
www.abakhiet.info
- المهندس محمود عمر
mahmoudomr@gmail.com

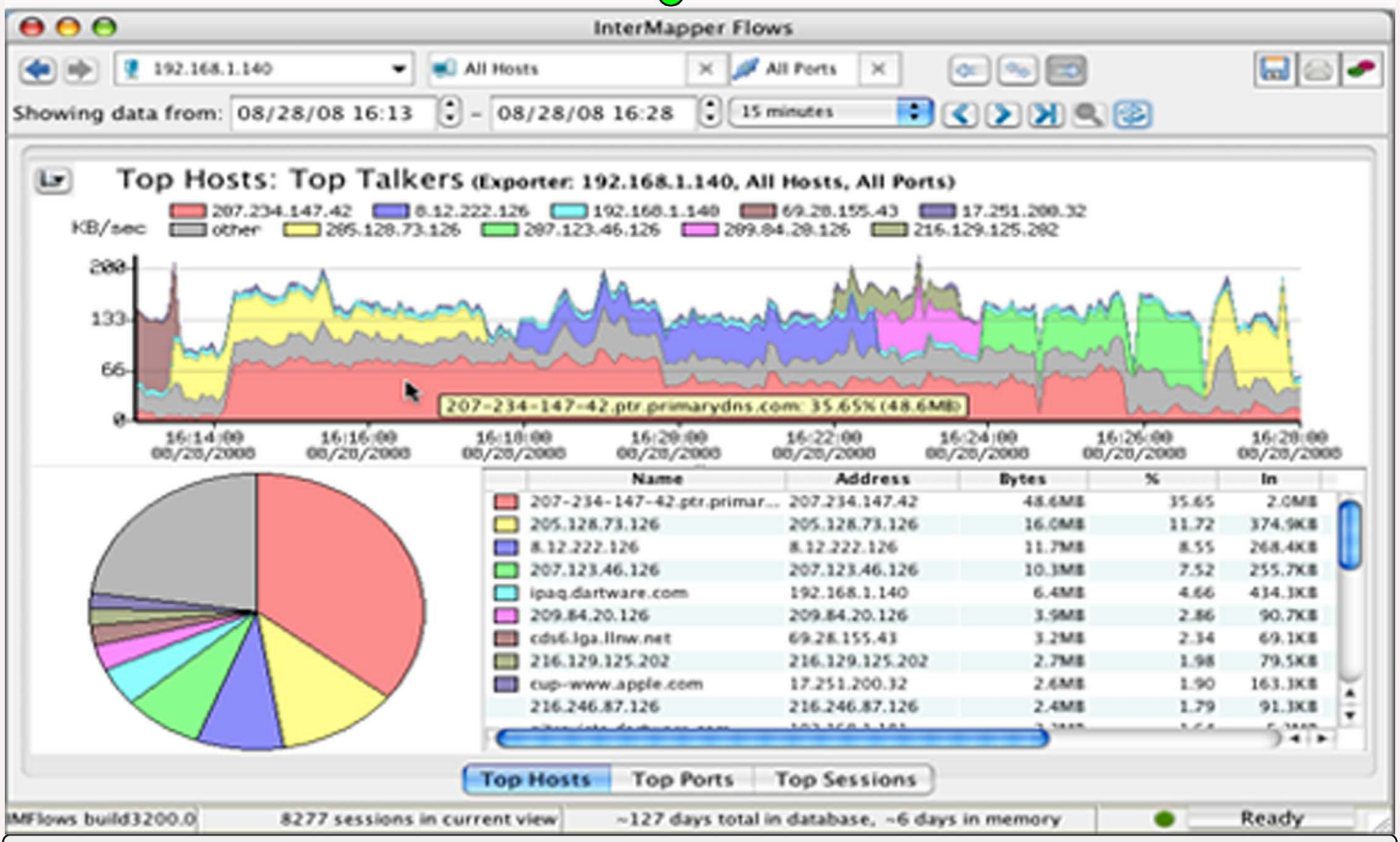
المحررون الضيوف

- المهندس عمر سويدان
om18899@gmail.com
- المهندس أحمد الجلولي
ahm_ijal@hotmail.com

موقع المجلة
www.networkset.net
بريد المجلة
magazine@networkset.net
بريدي الخاص
admin@networkset.net

محتويات آب 2110

الشبكات وكاميرات المراقبة (الصفحة رقم 12



شرح الـNetflow مع توضيح أوجه الأختلاف بينه وبين SNMP

بقلم: أيمن النعيمي

تحدثت في العدد السابق عن أحد أهم البروتوكولات التى تستخدم عادة من قبل مدراء الشبكات بهدف متابعة ومراقبة الأجهزة على الشبكة أما اليوم فسوف يكون حديثنا عن أحد البروتوكولات التى قامت سيسكو بتطويره وهو الـNetflow وهو بروتوكول شبيه بي الـ SNMP ووظيفته مراقبة الشبكة والأجهزة من خلال تحليل الترافيك ومراقبة الباندويث في الشبكة والذي يساعدنا في رفع أداء الشبكة والجميل في هذا البروتوكول بأنه ليس حصرا على أجهزة سيسكو فهو مدعوم من شركات آخرى لكن بمسميات مختلفة وهذه بعض الأمثلة :

Jflow or cflowd for Juniper Networks
NetStream for 3Com/H3C
NetStream for Huawei Technology
Cflowd for Alcatel-Lucent
sFlow for Foundry Networks/Brocade

بعكس الـ SNMP الـ Netflow يستطيع أن يقدم لنا تحليل ومتابعة الـ Flow Traffic من خلال تحديد منفذ معين مثلا أو من خلال تحديد أيبي معين وهذا كله يتم من خلال الأعدادات التى نقوم نحن بها وسوف أعود لأتحدث عنها بشكل أفضل, بعد جمع المعلومات يقوم البروتوكول بتخذينها على الـFlow Cache ليتم دفعها فيما بعد إلى الـ Netflow analyzer أو يتم حذفها في حال لو أنتهى الزمن المسموح ببقائها (times out) على الكاش وأرجو منك كقارئ أن تركز على كلمة دفعها(PUSH) لانها سوف تعطيك أحد أكبر الأختلافات بين الـ Netflow و الـ SNMP لان الثاني يقوم بسحب أو جذب المعلومات إليه)ULLP(من خلال الـNMS أو Network Manage- ment Station راجع موضوع الـ SNMP لفهم هذه التفاصيل بشكل أكبر بينما الـNetflow يقوم بدفعها نحو مركز التحكم أو مركز المراقبة والذي يحوي البرنامج المسؤول عن تحليل هذه البيانات ونستطيع أيضا ان نصف هذا الأختلاف بأن الأول يقوم بتصدير المعلومات Export من خلال الجهاز الذي يقوم بجمع المعلومات والثاني يقوم بأستيراد المعلومات Import من خلال الجهاز المسؤول عن أستلام المعلومات

أما الأختلاف الثاني فهو يتمحور حول أمكانية كل بروتوكول لان بروتوكول الـ SNMP يقوم بجمع أحصائيات أكثر عن الجهاز نفسه مثل platform وهذا resource utilization, traffic counts, and error counts يشمل أحصائيات حول المعالج والرامات والأخطاء التى حدثت على الجهاز أما الـ Netflow فهو يقوم بجمع معلومات مفصلة حول الترافيك الذي يمر عبر هذا الجهاز.

يعتمد الـNetflow على سبع طرق لجمع المعلومات وهذه الطرق كالآتي

Source IP address
Destination IP address
Source port for UDP or TCP, 0 for other protocols
Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
IP protocol
Ingress interface

وتستطيع أن تلاحظ معي الامكانيات التى يعطيها لك البروتوكول للقيام بعملية جمع المعلومات اللأزمة وطبعا هي متاحة بحسب أمكانية الجهاز المستخدم مثل أن يكون L2\L3\L4

أصدارات الـNetflow

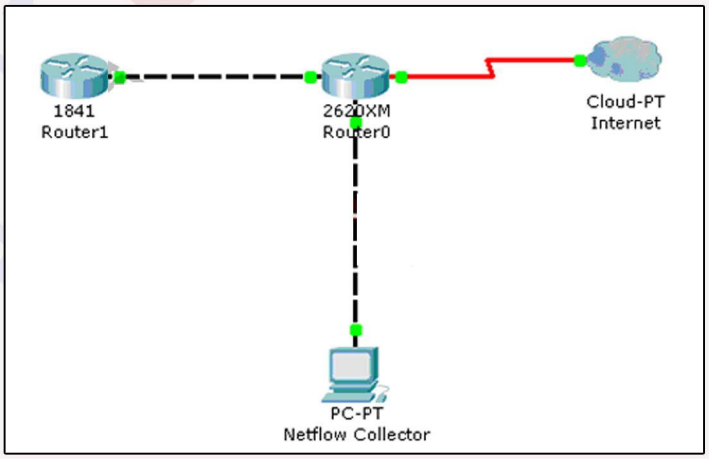
حتى الآن هناك تسعة أصدارات للـNetflow بحسب موقع سيسكو ويعد الأصدار الخامس منها هو الأكثر أستخداما والأكثر شيوعا حتى وقتنا الحالي وهذه نظرة مبسطة عنها منقولة من موقع الويكيبديا

Version	Description
V1	First implementation, now obsolete, and restricted to IPv4 (without IP mask and AS Number).
V2	Cisco internal version, never released.
V3	Cisco internal version, never released.
V4	Cisco internal version, never released.
V5	Most common version, available (as of 2009) on many routers from different brands, but restricted to IPv4 flows.
V6	No longer supported by Cisco. Encapsulation information.(?)
V7	Like version 5 with a source router field. Used (only?) on Cisco Catalyst switches.
V8	Several aggregation form, but only for information that is already present in version 5 records
V9	aka v10; IETF Standardized NetFlow 9 with several extensions like Enterprise-defined fields types, and variable length fields.

إعداد الـ Netflow

قد يكون أعداد الـ Netflow معقد بعض الشيء كون وجود أمكانيات كبيرة للبروتوكول من حيث كيفية ونوعية الترافيك الذي من الممكن جمع المعلومات عنه بالأضافة إلى نوعية الجهاز نفسه لذا سوف أقدم مثالان أثنان

المثال الأول



سوف نتوجه إلى الروتر 0ونقوم بمراقبة المنفذ المتصل مع الروتر 1وخطوات الأعداد كالآتي

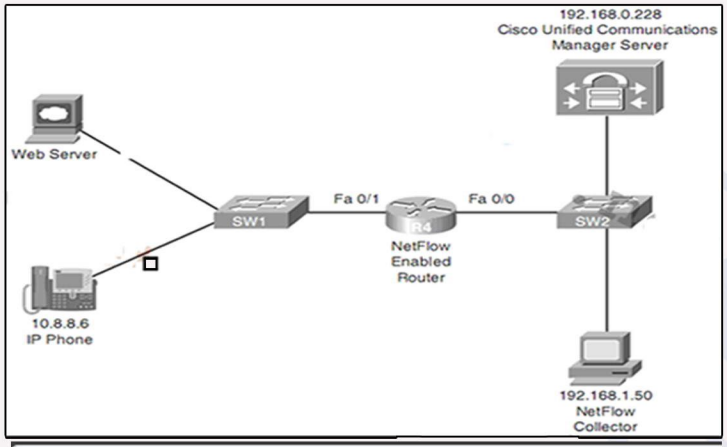
```
Cisco's IOS
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip route-cache flow
```

من خلال هذا الأمر نقوم بتفعيل الـNetflow على المنفذ وبعدها نتوجه إلى المنفذ المتصل مع جهاز الكمبيوتر والمسؤول عن عملية تحليل البيانات ونقوم بالأعدادات التالية :

```
Cisco's IOS
router(config)# ip flow-export version 5
router(config)# ip flow-export destination <ip_address> 2000
router(config)# ip flow-export source FastEthernet 0/0
```

في الأمر الأول قمنا بتحديد الأصدار الذي سوف يستخدم والأمر الثاني قمنا بتحديد أيبي الكمبيوتر الذي سوف يتم أرسال المعلومات إليه وهو هنا PC-PT وبعدها قمنا بكتابة الرقم 2000وهي ملاحظة هامة جدا أحب أن أعطيك أياها وهي تعني البورت الذي سوف يتم أرسال المعلومات من خلاله لان الـNetflow لايوجد له بورت مخصص للأرسال لذلك نقوم بأختيار بورت معين والعملية تتم من خلال بروتوكول الـUDP والأمر الآخير من أجل تحديد المكان الذي سوف نقوم فيه بجمع المعلومات منه وأرسالها إلى الكمبيوتر

المثال الثاني




```
Cisco's IOS
R4# conf term
R4(config)# int fa 0/0
R4(config-if)# ip flow ingress
R4(config-if)# exit
R4(config)# int fa 0/1
R4(config-if)# ip flow ingress
R4(config-if)# exit
R4(config)# ip flow-export source lo 0
R4(config)# ip flow-export version 5
R4(config)# ip flow-export destination 192.168.1.50 5000
R4(conig)# end
```

سوف تستطيع من خلال هذا المثال ان تلاحظ أننا أخترنا أكثر من بورت لكي يتم مراقبتهم وبالتحديد مراقبة الترافيك الذي يدخل من خلال 0/0و 1/0 وبالتالي أمكننا من مراقبة كل الترافيك الذي يعبر من خلال الروتر وباقي التفاصيل مفهومة ,أما الأوامر التالية فهي من أجل تحديد الوقت التى سوف نسمح فيه للـflow بالبقاء في الكاش كما ذكرنا من قبل (Times out)

```
Cisco's IOS
router(config)# ip flow-cache timeout active 5
router(config)# ip flow-cache timeout inactive 30
```

وآخيرا وليس آخرا الأوامر المستخدمة لعرض حالة الـ netflow على الروتر أو من أجل الـTrubleshooting

```
Cisco's IOS
router# show ip flow export
router# show ip cache flow
router# show ip cache verbose flow
```

أمكانيات وابعاد مدير تعريف مركز نظام مايكروسوفت
(SCCM2007 -Microsoft System Center Configuration Manager 2007)

بقلم: محمد التميمي

كما وعدناكم في عدد شهر (July- 2010) بتخصيص المزيد من الوقت لعائله سيرفرات النظم المركزيه لمايكرسوفت هانحن اليوم مع هذا التقرير الشامل المختص بامكانيات نظام(SCCM2007)والذي تم تخصيص الامتحان(اختصاص تكنلوجي)MCTS 70-401مما يوحي بامكانيه الانتقال الى شهادات اعقد مثل (MCITP) في الاصدارات المستقبليه لهذا النظام او ان يكون هذا النظم باصداراته القادمه جزء من مسار الحصول على شهادات خبراء النظم لاصدارات السيرفر القادمه.

في هذا التقرير سنتناول دوره حياه النظام والفوائد العمليه من استخدامه ثم السير باتجاه متطلبات التنصيب وتطوير العمليات وصولا الى عمليات اعقد يتيحها هذا النظام بهدف ان يكون لمهندس النظم فكره اوليه كافيه للبدء مرحله التعلم بصوره اشمل لاحقا.

مقدمه الى نظام SCCM.

في هذا الجزء نتناول اولا الخبرات الاساسيه التي يجب امتلاكها قبل البدء في التوسع في دراسه الـSCCM2007 بنوع من التفصيل , والمهارات المطلوبه تقسم الى اساسيه وثانويه وهي:-

- خبره في سيرفرات الوندوز (اساسي).
- خبره في نظام (SMS) والذي يعتبر النسخه الاقدم من نظام (SCCM2007) (ثانوي).
- خبره في الاكتف دايركتوري (اساسي).
- خبره في خدمات التطوير للوندوز (WDS) وخدمات التحديث (WSUS) (ثانوي).
- خبره في التعامل مع حزمه البرامجيات (SW Packaging) (ثانوي).
- خبره في التعامل مع تعريف الريجستري (ثانوي).

وفي القسم الثاني من هذا الجزء نسلط الضوء على الامتحان المخصص لـ SCCM2007 وهو الامتحان (MCTS 70-401)والذي تتوزع فيه اهميه المواضيع مع النسب المئويه لكل موضوع من ضمن ماده الامتحان كما يلي:-

- تنصيب وتطوير سيرفر الـ SCCM2007 (9%).
- تعريف معماريه الـ SCCM2007 (91%).
- أداره الموارد (41%).
- توزيع التطبيقات (17%).
- تطوير وتوزيع انظمه التشغيل (31%).
- حمايه معماريه الشبكه (31%).
- اداره وصيانه معماريه الـ SCCM2007 (15%).

ولمزيد من التفاصيل حول مكونات كل موضوع في القائمه اعلاه برجاء ملاحظه الشكل الاتي:-

```
Deploying a SCCM 2007 Server (9 percent)
-----------------------------------------
Set up and configure an Active Directory schema.
Migrate from an SMS 2003 hierarchy to SCCM 2007.
Configure an SCCM hierarchy.
Set up and configure security accounts.

Configuring an SCCM Infrastructure (19 percent)
-----------------------------------------
Configure client agents.
Configure site boundaries.
Configure core site system roles.
Configure discovery methods.
Configure client installation.
Configure SCCM infrastructure for Internet-based client management.

Managing Resources (14 percent)
-----------------------------------------
Build an SCCM collection by using queries.
Meter software usage.
Manage assets.
Manage inventory flow.
Manage client agents.

Distributing Applications (17 percent)
-----------------------------------------
Manage packages.
Manage programs.
Manage advertisements.
Schedule distribution.
Track success and failure rates for distribution.
Manage distribution points.
```

```
Deploying Operating Systems (13 percent)
-----------------------------------------
Capture a reference computer image.
Manage task sequences.
Configure site system roles related to deploying operating systems.
Deploy operating system packages.
Customize user state migration.
Deliver applications.

Securing a Network Infrastructure (13 percent)
-----------------------------------------
Configure Network Access Protection (NAP).
Maintain NAP.
Migrate from ITMU to WSUS.
Deploy software updates.
Manage vulnerability compliance.

Managing and Maintaining an SCCM Infrastructure (15 percent)
-----------------------------------------
Manage system health.
Configure automatic maintenance tasks.
Create custom reports.
Maintain clients.
Manage systems by using configuration management.
Manage Wake on LAN.
```

اجزاء SCCM.

اجزاء الـSCCM2007 هي:-

أ- المكونات SCCM Components.

• الموقع Site: نعني به حدود الموقع الذي سنقوم بادارته هل هو موقع تم تعريفه بواسطه حدود الـSubnet IP ام بواسطه الـAD site وذلك لمعرفه السيرفرات والكمبيوترات التي ستتم ادارتها ضمن حدود الموقع او الشبكه.

• السيرفر Site server: نعني به السيرفرات التي ستكون ضمن حدود الموقع وذلك للتمهيد لتقسيم الادوار فيما بينها.

• النظام Site System: يتم تعريف قسم من السيرفرات على انها Site System والهدف من هذا هو تفعيل الادوار بحيث يكون لكل نظام عدد من الادوار مما يحقق سلاسه الاداء في الشبكه بشكل عام.

• الهيكليه Site Hierarchy: هيكليه المواقع بحيث اقوم بتعريف امكانيه معالجه الموقع الثاني وتوفير خدمات الـSCCM2007 (ريموتلي).

• العميل The Client: يجب تنصيب مدير التعريف (Configuration Manager) على كل جهاز كمبيوتر خاص بالعملاء داخل الشبكه ومن اجل تسهيل المهمه يتم عمل كشف (Discovery) لمعرفه الاجهزه المرتبطه بالشبكه تمهيدا لتنصيب مدير التعريف رغم ان هذه الطريقه تعاني من بعض المشاكل حينما تكون بعض الاجهزه مثلا غير مفعله خلال اوقات عمل الكشف مما يمنع انضامهما لاحقا الى قائمه الاجهزه التي تنضم لقائمه المعالجه بواسطه الـSCCM2007.

ب- الادوار Site System Roles.

الادوار هي الفعاليات التي يقوم السيرفر بتنفيذها وتقسم الى:-

• سيرفرات الموقع Site Server: تستخدم في عمليه اداره الاجهزه Device Mgmt .

• نقاط التوزيع Distribution Point: نقطه خدمه يشير اليها العميل للوصول الى الخدمات مثال ذلك خدمه تنصيب نظم التشغيل باستخدام PXE.

• نقاط الاداره Management Point: للحصول على خدمات الترقيه لنظم التشغيل مثال ذلك نظام WSUS.

• نقاط التقارير Reporting Point: نقطه تتم الاشاره اليها لعرض التقارير على شكل صفحه انترنت.

• نقاط التحديد Server Locator Point: عند عدم رغبه توسعه السكيما الخاصه بالاكتف دايركتوري AD تتم الاستعانه بهذه النقاط من قبل العملاء لمتابعه حاله الانظمه لديهم , مثال ذلك المتابعه من خلال SHV-System Health Value للتاكد من ان نظام العميل حاصل على جميع التحديثات الضروريه لنظام التشغيل لديه.

• سيرفر قواعد البيانات Data Base Server: يحتوي على قاعده بيانات تحتفظ بالمعلومات اللازمه لعمل الـSCCM2007.

الشكل الاتي يعطينا فكره عن انواع الادوار التي يمكن لسيرفر الـSCCM2007 ادارتها.

Roles	Type
ConfigMgr component server	Server
ConfigMgr device management point	Server
ConfigMgr distribution point	Server
ConfigMgr management point	Server
ConfigMgr PXE service point	Server
ConfigMgr reporting point	Server
ConfigMgr site server	Server
ConfigMgr site system	Server
ConfigMgr software update point	Server
ConfigMgr site database server	Server
ConfigMgr system health validator point	Server

ت- الهيكليه Site Hierarchy.

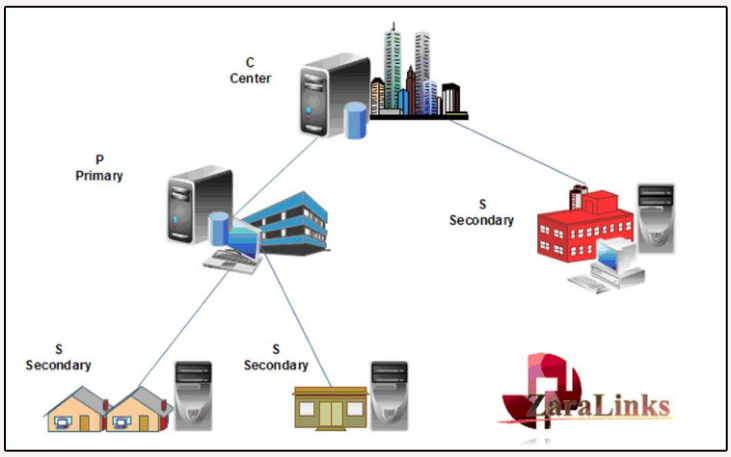
تقسم الهيكليه الى ثلاثه اقسام هي:-

• المركز (Center) وهو المقر الرئيسي الحاوي على قاعده بيانات جميع بقيه المواقع ويعتبر قلب الـSCCM.

• الموقع الرئيسي (Primary) ويحتوي على قاعده بياناته الخاصه ويدار من قبل فريق المهندسين الخاص بالموقع.

• الموقع الثانوي (Secondary) لايحتوي على قاعده بيانات خاصه به ويدار من قبل فريق المهندسين في موقع المركز او الموقع الرئيسي المتصل به مباشره.

في الشكل التالي توضيح لكيفيه ترابط المواقع :-



تنصيب SCCM او الترقيه من SMS2003.

عمليه تثبيت او تنصيب الـSCCM تحتاج اولا الى اعدادات مهمه تسبق محاوله التنصيب وهذه الاعدادات تشمل

أ . اعداد العتاد المادي (الهاردوير) : بالنسبه للسيرفر سرعه المعالج تفضل GHZ2.0 والذاكره GB1 ومساحه فاضيه من القرص الصلد (الهارد دسك) تبلغ حوالي 15GB اضافه الى نوع نظام التشغيل يجب ان يكون على الاقل Win Server2003 SP1. اما بالنسبه للكمبيوترات التي ستتم ادارتها من خلال الـSCCM فمواصفاتها هي سرعه المعالج تفضل MHZ300 والذاكره يخصص منها 384MB ومساحه فاضيه من القرص الصلد (الهارد دسك) تبلغ حوالي 350MB اضافه الى نوع نظام التشغيل يجب ان لايكون احد الانظمه التاليه

الشكل الاتي يوضح الانظمه التي لايدعمها الـSCCM:-

- Windows 95
- Windows 98
- Windows Millennium Edition
- Windows XP Media Center Edition
- Windows XP Starter Edition
- Windows XP Home Edition
- Windows XP Professional, with less than Service Pack 2 applied
- Windows Vista Starter Edition
- Windows Vista Home Basic Edition
- Windows Vista Home Premium Edition
- Windows NT Workstation 4.0
- Windows NT Server 4.0
- Windows 2000 Server, Service Pack 3 and earlier
- Windows 2003 Server, with no service pack installed
- Windows CE 3.0
- Windows Mobile Pocket PC 2002
- Windows Mobile SmartPhone 2002

ب . المتطلبات البرمجيه وتشمل تنصيب البرمجيات الاتيه

• MMC3.0.
• Net Frame work 2.0.
• SQL SP2（Full Version / Not express）.

• التحديثات الكامله لكل سيرفر من موقع مايكروسوفت الرئيسي.

• متطلبات اضافيه موضحه في الشكل ادناه:-

- Internet Information Services (IIS) 6.0 or later is required if the system will perform any of the following site systems roles:
  - Background Intelligent Transfer Service (BITS)-enabled distribution point. This role requires BITS server extensions and Web Distributed Authoring and Versioning (WebDAV) extensions. IIS is not required if the distribution point will not be BITS-enabled.
  - Management point. This role requires BITS server IIS extensions and WebDAV IIS extensions.
  - Reporting point. This role requires Active Server pages.
  - Software Update Point
  - Server locator point.
- All Configuration Manager distribution point systems using BITS bandwidth throttling require BITS 2.0 or later.
- Management points and server locator points configured to be part of a Network Load Balancing (NLB) cluster are supported.
- All site servers require Internet Explorer 5.0 or later.
- Windows Server 2008 is the only supported operating system for hosting the System Health Validator point site system role.

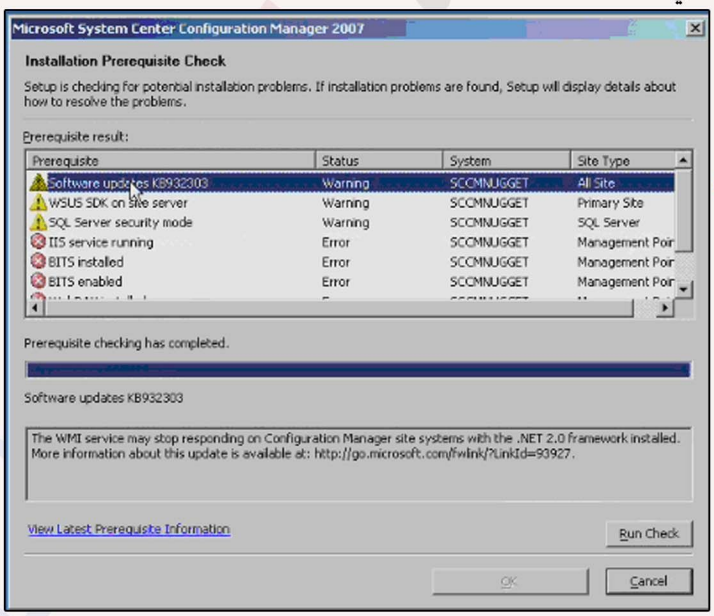
بعد الانتهاء من اعدادات الهاردوير والسوفت وير الضروريه تبداء المرحله الثانيه والتي تشمل تهيئه السيرفر لتنصيب الـSCCM وكالاتي

أ-توسعه السكيما : يتم توسعه سكيما الاكتف دايركتوري من خلال الاداه EXTADSCH.EXE والتي تنفذ على جهاز السيرفر الذي يحتوي جذر الغابه الشبكيه (NW Forest Root) حيث ينفذ الامر من سطر الاوامر وهذه الاداه تكون متوفره في نفس دي في دي الـSCCM.

ب-يتم اضافه حافظه (كونتينر) باسم (System Management) ضمن المسار(cn=system) وذلك من خلال استخدام الامر (ADSIEDIT.MSI)من سطر الاوامر لتفعيل شاشه معالجه السكيما.

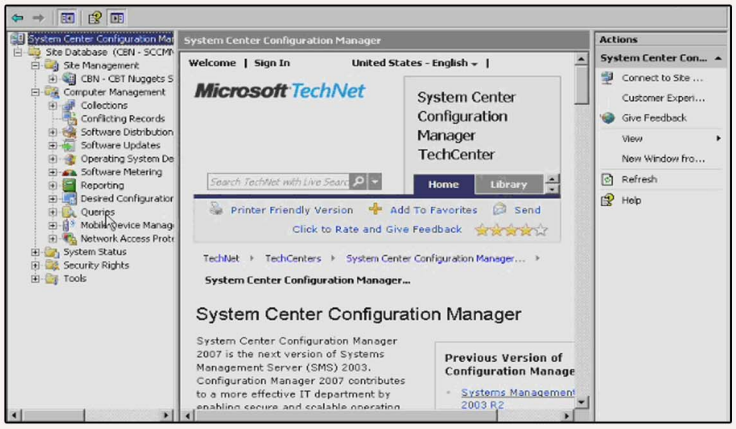
ت-تنصيب قاعده البيانات الـ (SQL2005 or 2008)في حاله عدم وجودها مسبقا.

ث-تنفيذ مدقق المتطلبات وهو برنامج متواجد ضمن دي في دي الـSCCM يفضل تنفيذه للتاكد من ان كل الاعدادات سليمه قبل البدء بعمليه التنصيب , لاحظ الشكل الاتي:-



ج- البدء بتنصيب الـSCCM حيث تظهر عدة شاشات يتم اختيار التعاريف الضروريه تمهيدا لتنصيب النظام.

بعد الانتهاء من تنصيب الـSCCM يصبح بالامكان تفعيل مدير تعريف مركز النظام (SYS Center Conf Mgr) الذي يستخدم اداره الشبكات وكما نلاحظ في الشكل الاتي



اما في حاله ترقيه الـ SMS 2003الى SCCM2007 فان عمليه الترقيه تشابه الى حد ما عمليه التنصيب ولكن يجب ملاحظه الامور التالي وكما هو ملاحظ في الشكل قبل اجراء عمليه الترقيه:-

```
- SCCM sites cannot be child sites of SMS 2003 sites.
- SMS 2003 sites can be child sites of SCCM sites.
- Native mode SCCM sites cannot be child sites of mixed mode SCCM sites
- SCCM clients cannot be assigned to an SMS 2003 site.
- SMS 2003 clients can be assigned to an SCCM site.
- SMS 2003 primary sites cannot be managed through the SCCM console.
- SMS 2003 secondary sites can be managed through the SCCM console.
      - only when the SMS 2003 secondary site is directly below an SCCM site.

- SMS 2003 clients must be upgraded after their site server.
- SMS 2003 sites to be upgraded must be set to advanced security.
- SMS 2003 clients must be advanced clients.
- All SMS 2003 feature packs must be uninstalled (except for ITMU).
- SMS_def.mof customizations will not automatically survive the upgrade.
- Start with the central site, then work your way down the hierarchy.
- A parallel SCCM instance in some cases is a better option.
```

بهذا ينتهي الجزء الاول من التقرير الشامل لنظام الـSCCM وموعدنا الشهر القادم مع الجزء الثاني للتعرف على (اكتشاف المصادر, تطوير عملاء SCCM, مرحله جمع المعلومات الاساسيه).

لماذا لايقوم التلنت بأظهار رسائل الـ Log ؟

بقلم: أيمن النعيمي

مقالة بسطية ومخصصة للمبتدئين في عالم سيسكو والتى تدور حول أحد الأوامر التى يجب أن يعرفها أي شخص حاصل على شهادة في سيسكو وهو الأمر Terminal monitor وسبب كتابتي عنه يعود إلى سبب واحد وهو أهمية وبساطة هذا الأمر ولا أخفيكم أني دائما ماأختبر أي شخص حاصل على شهادة CCNA بهذه السؤال وهو لماذا لا أستطيع أن أشاهد الـ Log message عندما أستخدم التلنت أو الـ SSH وماحصل معي مؤخرا أجبرني على الكتابة عن هذا الموضوع وهو توجيه هذا السؤال إلى ثلاث أشخاص أنتهوا من دراسة الكورس ولكنهم لم يعلموا لماذا وكيف نقوم بحل هذه المشكلة وطبعا عدم معرفتهم لاتعني أن دراستهم كانت سيئة لكن قد لايكون قد أعطوا للامر أهمية كبيرة ولندخل في الموضوع بشكل أعمق

كما هو معروف عند الجميع أن للأتصال بالروتر هناك طريقتان مشهورتان الأولى تكون عن طريق الـ Console Port والثانية عن طريق الـ VTY ولنقف لحظة عند كلمة VTY ماذا تعني Virtual TeletYpe وكلمة Teletype كلمة قديمة يعود معناها إلى اداة قديمة لها لوحة مفاتيح وتقوم بطباعة كل ما أنت تضغط عليه مثل هذه الآلة في الصورة

طيب ماذا سوف نستنتج من كل هذا الكلام ؟ الفكرة بسيطة كل ماتكتبه من خلال الـ VTY سوف يظهر أمامكم على شاشة الكمبيوتر لكن لن يظهر أي شيء أنت لم تقم بكتابته ومن هنا نستنتج لماذا الـ VTY لايقوم باظهار ملفات الـ Log وحتى لوقمت بكتابة الأمر debug لمتابعة بعض التفاصيل لن يخرج أي شيء لك لو كنت متصل من خلال التلنت ومن هنا وجد الأمر Terminal Monitor الذي سوف يسمح للتلنت بأخراج رسائل الـ Log مباشرة على شاشة الكمبيوتر وهو يكتب في الـ Privileged Mode ولايقافه نقوم بكتابة الأمر التالي terminal no monitor وهي الفائدة الوحيدة من هذا الأمر أتمنى ان لا أكون قد أطلت كثيرا في هذا الموضوع وقدمت لك شيئا جديدا وياريت أعرف منكم هل كنت تعرف بهذا الأمر أم لا ؟ أي هل كنت تعلم أن التلنت(by default)لايقوم بأظهار رسال الـ Log ؟

من أين أبدأ وكيف أبدأ في الشبكات ؟؟؟
سؤال لطالما حيرني !!!

بقلم: عادل الحميدي

كيف حالكم اليوم؟ الله أسأل أن تكونوا بخير وعافية وأسأله سبحانه أن يجعل أيامكم كلها خير وعافية.

بداية عندي لكم منكم شكوى؟ العدد السابق من المقالة في الشهر الماضي كان به سؤال؟ أردت منه تنبيه البعض إلى المدة الزمنية والتي نحاول فيها تحقيق هدفنا الأول من غايتنا الكبيرة ألا وهو مهندس محترف في ثلاث سنوات، ، لكن للأسف لم يراسلني على الإيميل ويجيب على هذا السؤال سوى شخص واحد وذلك كان شيئاً سلبياً جداً، أعرف أن بعضكم يقول أن السؤال كان للتنبيه على هذا الشيء وللفت الإنتباه وأننا لم نظن أنك تريد عليه إجابة، لكني أريد أن أقول لكم شيء آخر لم يلاحظه إلا شخص واحد وهو الذي أجاب على التساؤل، إن السؤال الهدف منه قياس مدى التفاعل مع المقالة، كـ عدد المتابعين والمتحمسين لها وفي الحقيقة في البداية كانت ردود الفعل مناسبة جداً، لكن الآن... أعرف أن البعض سيقول لي لا والله ردود الفعل قوية وأنا أعرف أناس كثيريين يقرأون المقالة وكم إستفادوا منها، أنا أيضاً أعرف هذا، ولم أرد هذا المعنى أيضاً، سامحني اليوم إذا كنت هلامي وغير واضح، ولكي أكون أكثر وضوحاً، دعني أسألك سؤال... هل تريد لهذه المقالة وهذه المجلة بشكل عام أن تستمر؟ طبعاً أريد ذلك، إذن يا أخي الكريم لا تحرم القائمين عليها من الشكر ولو كان بكلمة أو رسالة على الإيميل لن تستغرق من وقت سعادتك سوى لحظات لشخص ظل ساعات يكتب لك مقال، لا أريد أن أقول ولو بدعوة بظهر الغيب فهم يستحقون ذلك وأكثر، وهذا لسببين في رأيي، الأول: أن الله تبارك وتعالى لا يشكر لعبد لا يشكر للناس، والذي قيل أن معناه أن من لا يشكر الناس كان كمن لا يشكر الله معاذ الله، الثاني: أن ذلك يا أخي هو دافع لنا في الإستمرار، أتعرف أن الإنسان عنده حب الثناء وبه تعلو همته، أعرف أني صريح أكثر من اللازم ﷺسميها زي ما تسميها ﷺ فمن منا لا يحب الثناء، دعني أضرب لك مثالاً ولتكن أنت فيه الحكم، لي 6حلقات فيديو منشورة على الإنترنت شرحت فيها IP Address v4 (أرقام وعناوين الأجهزة تشبه رقم جواز السفر ذلك الرقم الفريد والمميز للإنسان) متوفرة على هذا الرابط:

http://www.4shared.com/dir/36232010/d4530059/AdelAl-Hamedi.IP.Address.html

هل تعرفون كم وصل عدد مرات تحميل هذه المادة ما يقرب من أربعة آلاف شخص ولله الحمد، لكن كم منهم رد حوالي الخمسين أكثر تلك الردود عبارة عن إستفسارات)لو لم يكن عنده إستفسار لما رد لا أعرف(وإثنين منهم إنتقاد أحدهم لاذع والبقية وهم قليل شكر سريع من كلمات، نسأل الله الإخلاص أعرف أنك ستقول لي يا أخي ﷺمعليش ﷺ وجزاك الله خيراً، وأنت تعمل هذا العمل لله ولا تنتظر الجزاء من الناس، أقول لك وهذا هو الدافع إلى الاستمرار حتى الآن ولولاه ما واصلت، والآن دعوني أكون أنا أول من يبدأ بهذا... وإني لا أسمح للمهندس أيمن النعيمي أن يحذف الكلمات التالية من المقالة...

أتوجه بالشكر من كل قلبي للمهندس أيمن النعيمي، ذلك الشاب العبقري ذو الهمة العالية والمدونة الأكثر من رائعة، وصاحب فكرة تلك المجلة، والذي كنت له متأثراً جداً عدد الشهر الماضي لما حدث له من ضياع المجلة قبل موعد نشرها بيوم أو يومين ثم عكوفه عليها لليال لإعدادها من جديد، وكم تمنيت أني علمت قبل ذلك لأساعده بأي شيء ولكني علمت متأخراً، أسألكم بالله ألا ترون أن هذا الرجل يستحق منا الثناء والدعاء، فالله أسأل أن لا يحرمه الأجر وأن يغفر له ويرحمه ويهديه ويعافيه ويرزقه... اللهم آمين اللهم إستجب...

وأرجو منكم أن تسامحوني على تلك المقدمة والتي قد لا تروق للبعض، ولكنها مشاعر وأحاسيس أردت أن أصارح بها إخواني وأحبابي في الله، وأرجو منكم أن تتحملوني...

والآن نرجع للمقالة فاليوم ستكون مختلفة عن كل عدد حيث أني سأكمل المقالة أولاً ثم أجيب عن الإستفسارات التي وصلتني على الإيميل والتي هي في نقصان)لكن أعتقد أنها هذا الشهر سترجع لسابق عهدها وأكثر(، ولعل السبب في تأخير الاستفسارات أن تلك التساؤلات تحتاج مني أن أكمل المقالة أولاً ثم أجيب عليها وهذا سيكون أنسب ويجعل الأمور في نصابها.

تكملة المقالة: كورسات مايكروسوفت... CSEM>CSA-M>MCP-

في الحقيقة (كما ضربت لذلك مثال في المقال السابق) لو أنك انتهيت من كورسات سيسكو CCNA (زميل شبكات سيسكو المعتمد) ثم CCNP (محترف شبكات سيسكو المعتمد) ستجد نفسك مع هذا ضعيف وعندك عجز وقصور في العمل على أنظمة التشغيل مثل ويندوز إكس بي Windows XP وإن قلت هذه سهلة)ولعلي أرفع لكم كورس Windows XP فديو تعليمي من أحد أكبر مراكز التدريب في العالم وأشهر المدربين لتعلم أن الموضوع كبير(، فتأتيك أنظمة التشغيل الخاصة بالسيرفرات)أجهزة الكمبيوتر الضخمة التي تدير الشبكة(، وإن قلت لي هذه أخذت عنها فكرة في كورس A+، فأقول لك أنت واهم، فأنا أقصد تشغيل تلك الأنظمة وإدارتها للشبكات والأمان و... وأمور أخرى معقدة (لكن بسيطة بالتعلم) ليس هذا أوان ذكرها، ولست أقصد نبذة مختصرة تصلح أن تكون عنوان لكتاب أما محتويات الكتاب فأنت لم تقرأها بعد...

المسار الثاني: مايكروسوفت

الشهادة الخامسة: والبداية في مايكروسوفت تكون بـ MCP (Microsoft Certified Professional) محترف معتمد من مايكروسوفت، عندما تدرس أي كورس من كورسات مايكروسوفت وتختبر وتنجح تحصل على هذه الشهادة، نعم أي كورس في أي تخصص... لكننا هنا نتكلم عن كورسات الشبكات فسنبدأ بـ ويندوز إكس بي Windows XP... وهي تستغرق شهر تقريباً

ثم الشهادة السادسة: MCSA (Microsoft Certified Systems Administrator) مدير أنظمة معتمد من مايكروسوفت، وهي عبارة عن ثلاث كورسات بثلاث اختبارات، ومدتها ثلاثة أشهر.

ثم الشهادة السابعة: MCSE (Microsoft Certified Systems Engineer) مهندس أنظمة معتمد من مايكروسوفت، وهي عبارة عن ثلاث كورسات بثلاث اختبارات، ومدتها ثلاثة أشهر.

وعندئذ أنت أصبحت محترف حقاً في أنظمة التشغيل والشبكات الخاصة بمايكروسوفت، ولا تنسى أن الراتب في زيادة ولله الحمد، فالله سبحانه يقول: "إنا لا نضيع أجر من أحسن عملا" وأنت اجتهدت وإن شاء الله تستحق... والثلاث سنوات مر منها الكثير صحيح فيه عناء لكن لذة النجاح تنسي المشقة.

ولكن ما هو ترتيب أخذ تلك الشهادات مع غيرها من الشهادات السابقة، هذا هو استفسار اليوم والذي عنه سأجيب حالاً فكن معنا...

الاستفسار الأول: (وهو كما يقولون استفسار "في الجون" أو "جه على الجرح" كنت سأبينه في تلك الحلقة فسأل عنه أخونا فجزاه الله عنا خير الجزاء فالاستفسارات حقيقة تضيف للموضوع لمسة جمالية) وهو تحت عنوان كثرة الكلام قد ينسي بعضه بعضاً

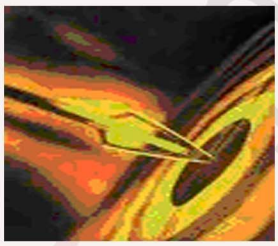
سألني أحدهم قائلاً: "أنا إتلخبطت" عندي تشويش فأنا فهمي بطيء وأريد منك أن

تتحملني (أقول له بل أنت إنسان ناجح وذكي وشديد التركيز ومهتم بالأمر) يعني لو أحدنا يريد أن يسير في المسار الأول وهو سيسكو يعمل إيه واحد إثنين ثلاثة في كلمة ونصف، ولو أحدنا يريد أن يسير في المسار الثاني وهو مايكروسوفت يعمل إيه واحد إثنين ثلاثة في كلمة ونصف، وشكراً؟

الإجابة في كلمة ونصف: (المختصر المفيد)

1) A+, N+, CCNA, MCP, MCSA, CCNP –> Cisco Certified

2) A+, N+, MCP, MCSA, CCNA, MCSE –> Microsoft Certified



1) Cisco: 3years (36month) -]3m(A+) + 3m(N+) + 2m(CCNA) + 1m(MCP) + 3m(MCSA) + 6m(CCNP)[= 36 – 18 = 18 month.

2) Microsoft: 3years (36month) -]3m(A+) + 3m(N+) + 1m(MCP) + 3m(MCSA) + 2m(CCNA) + 3m(MCSE) = 36 – 15 = 21 month.

وللعلم هناك ملاحظات على تلك المدة فهذه المدة مثالية نوعاً ما وهذا ما سنوضحه في الحلقة القادمة فانتظرونا...

الإستفسار الثاني: وهو تحت عنوان حقيقة أم خيال/ سألني أحدهم هل هذه الخطة مجربة أم ضرب من المثالية؟ يعني أنت حصلت على تلك الشهادات؟ أم أن تلك أحلام تريد تحقيقها؟

ولعلي أجيب للمرة الألف أنها واقعية وعن تجربة وحقيقية، فأنا حاصل على بكالوريوس علوم الحاسب الآلي وعلى وشك الإنتهاء من الماجستير تخصص نظم معلومات، كما أني حاصل على الشهادات التالية:

A+, N+, CCNA, CCNP, MCP, MCSA, MCTS, MCSE

والآن أرجو أن تكون الصورة واضحة...

الاستفسار الأخير: يقول الأخ نصحني أحدهم بأن أذاكر A+, N+ وليس من الضروري أن أختبرهم، وأدخل مباشرة على CCNA؟

وأنا أقول لك لا تسمع له وسر على الخطة التي نضعها سوياً، لأن الكورسات التي تحصل عليها تثقل سيرتك الذاتية ولا تستطيع أن تكتب مثل هذه الكورسات في سيرتك الذاتية إلا إذا كنت إختبرتها فحصلت على شهادتها.

إلى اللقاء في الحلقة القادمة

تقرأون في هذه الحلقة :::

أنظمة التشغيل الخاصة بالسيرفرات ...

1) A+, N+, CCNA, MCP, MCSA, CCNP –> Cisco Certified ...

2) A+, N+, MCP, MCSA, CCNA, MCSE –> Microsoft Certified ...

تقرأون في الحلقة القادمة :::

ملاحظات على المدة الزمنية ...

تكملة المسارين سيسكو ومايكروسوفت ...

الفرق بين شهادة حضور كورس وشهادة اجتياز كورس ...

أهمية السيرة الذاتية ... وكيف تسوق نفسك؟

How to sell yourself?

كيف تقوم بعمل مقارنة بين الأعدادت من خلال موجه الاوامر في سيسكو

بقلم: أيمن النعيمي

أثناء تصفحي للانترنت صادفني على موقع سيسكو أحد الأوامر الرائعة وهو من أجل مقارنة التغييرات التى حدثت بين أعدادات الـ Startup-configuration و الـ Run-configuration وأثرت أن أتحدث عنها اليوم لما لها من فائدة كبيرة في أكتشاف بعض أخطاء المهندسين الذي يعملون أحيانا على الأجهزة.

بداية أحب أن أقول ان لهذا الموضوع فوائد كثيرة وأحد اهم هذه الفوائد هي عمل مقارنة بين الأعدادات الموجودة على الـ NVRam مع الأعدادات الموجودة في الـ RAM وسوف تسألني لماذا أنا يجب علي عمل مثل هذه المقارنة ؟ للإجابة على هذا السؤال سوف أطلب منك أن تفرض أنك كنت تكتب بعض الأوامر على الروتر وأنك نسيت ماهي الأوامر التى قمت بكتابتها وتريد أن تعرف لو قمت بنسخ الأعدادت من الـ Ram إلى الـ NVRam لن يحدث معك أي مشكلة أو تعارض في الأعدادات

الفائدة الثانية لنفرض أيضا ان الروتر قد حدثت فيه مشكلة وأنك تريد أن تسترجع نسخة من الأعدادات الموجودة على سيرفر TFTP ولكن قبل أن تقوم بهذا الشيء تريد أن تعرف ماهي الأعدادات التى تم تغييرها وسببت هذه المشكلة عندها سوف نلجأ إلى هذا الأمر لمقارنة الأثنان مع بعضهما البعض وتعرف مكان الخلل بالتحديد وطبعا هناك الكثير من الفوائد لأستخدام هذا الامر وهو يختلف بحسب عملك ومتطلبات عملك بس أنت فكر فيه ! ؟

وقبل أن أكتب الأمر سوف أذكر بعض النقاط التى تخطر على بالك مثل ان تقول لي سوف أقوم بعمل Show run وبعدها Show start وسوف أقارن بين الأثنان وطبعا تستطيع بنفسك تقدير الوقت الذي سوف تضيعه طلوعا ونزولا بين الأعدادات وقد يتساءل أحدكم بأني سوف أقوم بنسخ الأعدادت على ملف تكست وأقوم بمقارنته وطبعا الفكرة معقولة لكن أيضا سوف تأخذ منك وقت طويل ولو كنت من مستخدمي هذه الطريقة أنصحك بتحميل برنامج Compare It الذي يستطيع أن يقوم بمقارنة الأثنان وأظهار أماكن الأختلاف بينهم لذا لنتعرف على الطريقة التى أتاحتها سيسكو لك لكي تقوم بهذه العملية في سرعة البصر ومن دون تضييع أي وقت ولكي أوضح الفكرة قمت بعمل بعض الأعدادات على الروتر ومن بينها أعطاء أيبي للمنفذ Fastethernet وقمت أيضا بتغيير أسم الروتر من Cisco إلى NetworkSet لذا سوف ألجا الإن إلى كتابة أمر المقارنة وهو يكتب بهذه الطريقة وعلى الـ Privilege Mode

show archive config differences system:running-config nvram:startup-config

وأعتقد أن من خلال مشاهدتك للأمر سوف تفهم الفكرة من دون الحاجة إلى أي تفسير فقد قمت بتحديد المقارنة بين الـ Run و الـ Start والنتيجة سوف تكون على الشكل التالي

```
NetworkSet#show archive config differences system:ru
NetworkSet#show archive config differences system:running-config nv
NetworkSet#show archive config differences system:running-config nvram:sta
NetworkSet#$e config differences system:running-config nvram:startup-config
Contextual Config Diffs:
+hostname Cisco
interface FastEthernet0/0
 +no ip address
 +shutdown
-hostname NetworkSet
interface FastEthernet0/0
 -ip address 192.168.10.1 255.255.255.0

NetworkSet#
NetworkSet#
NetworkSet#
NetworkSet#
NetworkSet#
NetworkSet#
NetworkSet#
```

ماذا سوف نلاحظ من هذه الصورة ؟ اول شيء سوف تلاحظه إشارة الزائد "+" وهي تعني الأعدادات الموجودة على الـ NVRam أما إشارة السالب "-" فهي خاصة بأعدادت الـ Ram أو الـ Run config ويتضح لك ماهي الأعدادت الجديدة التى قمت بها ولم أحفظها بعد على الـ NVRam وهي كما اوضحت سابقا الأيبي وأسم الروتر

وهذا الأمر لايقتصر فقط على المقارنة بين الـ NVRam والـ Ram بل يمكننا أن نقوم بعمل عدة مقارنات ومن اماكن مختلفة ومن بينها الـ TFTP وهذه لائحة بالأماكن التى تستطيع اللجوء إليها

```
Dynamips(0): R1, Console port
NetworkSet#show archive config dif
NetworkSet#show archive config differences ?
  archive:   [file1 path]
  cns:       [file1 path]
  flash:     [file1 path]
  ftp:       [file1 path]
  http:      [file1 path]
  https:     [file1 path]
  null:      [file1 path]
  nvram:     [file1 path]
  pram:      [file1 path]
  rcp:       [file1 path]
  scp:       [file1 path]
  slot0:     [file1 path]
  slot1:     [file1 path]
  system:    [file1 path]
  tftp:      [file1 path]
  xmodem:    [file1 path]
  ymodem:    [file1 path]
  |          Output modifiers
  <cr>
```

شرح إستخدام أداة فحص الشبكة PathPing

بقلم: عمر السويدي

نتكلم في هذه المقالة عن أحد الأدوات الهامة من أدوات فحص الشبكة، اسمها الـ Pathing

أولاً.. يجب على من يقوم بعمل كمسؤول عن الشبكة، أن تكون له أجهزة وبرامج تساعده على القيام بعمله على أكمل وجه، ذلك لأنه الخط الأول في حالة حدوث مشاكل.

الآن، الكثير يعرف عن أداة الـ Ping و وكذلك أداة الـ tracert المستخدمات في الوندز، أما أداة الـ pathping فهي تجمع بينهما ولكي نفهم كيفية عمل هذه الأداة سوف نلقي نظرة أقرب لمفهوم أداة الـ Ping و الـ Tracert.

الأداة الأولى ping تعنى بحساب الوقت من المرسل إلى المرسل إليه، بجانب التعرف على حالة وجوده، أما الأداة الثانية الـ tracert فهي تعنى بالكشف عن الطريق الذي استخدمته الرزم التي تقوم أنت بإرسالها وتفيد هذه الطريقة في معرفة الطريق المستخدم للوصول إلى الهدف، هذا إذا ما كان هناك أكثر من طريق. كذلك تفيد هذه الطريقة في معرفة السرعة من المرسل إلى أجزاء الشبكة، بمعنى، أنت تعلم أنه توجد راوترات كثيرة بينك وبين الهدف، فإذا ما أردت أن تعرف الوقت الذي ستحتاجه إلى كل هدف من هذه الأهداف، فكيف ستعرف؟ الجواب عن طريق استخدام tracert , وكلا الأداتان تستخدمان بروتوكول ICMP من المرسل إلى المرسل إليه.

ننتقل الآن إلى أداة اليوم، pathping، ما علاقتها بالأدوات التي ذكرت الآن؟

في الحقيقة هذه الأداة الأخيرة، ما هي إلا مزج بين الأداتين المذكورتين.

الـ pathping هي أداة لمعرفة الطريق من المرسل إليه، وكذلك هي أداة لقياس مدى البعد وفعالية الطريق بين المرسل والمرسل إليه.

وقبل البدء في شرح طريقة عمل هذه الأداة، أو البريمج، سنتكلم عن فوائد استخدامه.

مصاعب الشبكة لا تكمن في عمل تضبيط (configuration) لجهاز من أجهزتها، لكن باتساع وكبر حجم الشبكة التي أنت تكون مسؤولاً عنها، فالمشاكل التي هي في الحقيقة صغيرة، كرداءة سلك شبكي مثلاً، تكون صعبة الاكتشاف، حتى مع عملية التوثيق التي هي مطلب أساسياً، لكن في الحقيقة المشاكل في غالبها لا يكون حلها عن طريق التوثيق وما شابه، وأنا لا أدعو إلى تقليل الاهتمام بعملية التوثيق، لا، لكن إن أردت أن تجعل عملك صعباً جداً فلا توثق، فالذي أغرب بقوله سيتضح بمثال،

أحياناً يكون هناك سلك مشتركاً بين فرع مثلاً وجهة ثانية، لا يتعدى طوله الأمتار الخمسة، وأنت عندما صممت هذه الشبكة، لم تتوقع أبداً أنه سيكون مصدراً للمشاكل، ولكن بعد الفحص، وجدت أنه يعمل بشكل جيد، لكن عند استخدام نوع معين من الأنظمة التي تتطلب جودة عالية جداً، مثل للصورة، فإنه يتعثر ولا يستطيع العمل بشكل جيد.

لذلك من المطلوب حتى تكون مسؤول شبكة لا يمكن الاستغناء عنه، أن تكون لك أجهزة وبريمجات وبعضاً من البرامج في حقيبتك تساعدك في الكشف عن الغموض.

نرجع إلى محور كلامنا، وبالمثال يتضح المقال:

```
Tracing route to yahoo.com [209.191.122.70]
over a maximum of 30 hops:
  0  NICE1 [192.168.1.100]
  1  192.168.1.1
  2  195.229.244.43
  3  195.229.245.146
  4  194.170.0.234
  5  195.229.1.101
  6  195.229.1.173
  7  nyc-r1-atm64-0-0-0.emix.net.ae [195.229.0.82]
  8  198.32.160.121
  9  UNKNOWN-216-115-100-92.yahoo.com [216.115.100.92]
 10  UNKNOWN-216-115-96-21.yahoo.com [216.115.96.21]
 11  ae-1-d111.msr2.mud.yahoo.com [216.115.104.103]
 12  te-6-1.fab2-a-gdc.mud.yahoo.com [209.191.78.137]
 13  te-9-1.bas-c2.mud.yahoo.com [68.142.193.11]
 14  ir1.fp.vip.mud.yahoo.com [209.191.122.70]

Computing statistics for 350 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           NICE1 [192.168.1.100]
                                 0/ 100 =  0%   |
  1    4ms      0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 1/ 100 =  1%   |
  2   53ms      1/ 100 =  1%     0/ 100 =  0%  195.229.244.43
                                 0/ 100 =  0%   |
  3   53ms      1/ 100 =  1%     0/ 100 =  0%  195.229.245.146
                                 0/ 100 =  0%   |
  4   59ms      1/ 100 =  1%     0/ 100 =  0%  194.170.0.234
                                 0/ 100 =  0%   |
  5   58ms      1/ 100 =  1%     0/ 100 =  0%  195.229.1.101
                                 0/ 100 =  0%   |
  6   58ms      1/ 100 =  1%     0/ 100 =  0%  195.229.1.173
                                 0/ 100 =  0%   |
  7  261ms      1/ 100 =  1%     0/ 100 =  0%  nyc-r1-atm64-0-0-0.emix.net.ae [19
5.229.0.82]
                                 0/ 100 =  0%   |
  8  487ms      3/ 100 =  3%     2/ 100 =  2%  198.32.160.121
                                 0/ 100 =  0%   |
  9  397ms      3/ 100 =  3%     2/ 100 =  2%  UNKNOWN-216-115-100-92.yahoo.com [
216.115.100.92]
                                 0/ 100 =  0%   |
 10  419ms      1/ 100 =  1%     0/ 100 =  0%  UNKNOWN-216-115-96-21.yahoo.com [2
16.115.96.21]
                                 1/ 100 =  1%   |
 11  419ms      2/ 100 =  2%     0/ 100 =  0%  ae-1-d111.msr2.mud.yahoo.com [216.
115.104.103]
                                 1/ 100 =  1%   |
 12  419ms      3/ 100 =  3%     0/ 100 =  0%  te-6-1.fab2-a-gdc.mud.yahoo.com [2
09.191.78.137]
                                 0/ 100 =  0%   |
 13  420ms      3/ 100 =  3%     0/ 100 =  0%  te-9-1.bas-c2.mud.yahoo.com [68.14
2.193.11]
                                 0/ 100 =  0%   |
 14  417ms      3/ 100 =  3%     0/ 100 =  0%  ir1.fp.vip.mud.yahoo.com [209.191.
122.70]

Trace complete.
```

في الصورة أعلاه هي نتيجة مخرجات الأمر pathping، الأمر الملفت للانتباه هو إعادة الترقيم مرة ثانية، والسبب في ذلك لأنه يعمل العملين معاً. أعني ping و tracert

فأولاً الترقيم من 0إلى 14هي المسافة بالراوترات من المرسل إلى المرسل إليه. ثم بعد ذلك، يقوم بعمل قياس للفترة الزمنية بين كل وصلة والوصلة التي تليها.

لكن هنا فرق بسيط بين الـ pathping و الـ tracert وهو اختلاف طريقة عرض الـ RTT بين الأمرين، بمعنى في الـ tracert الـ RTT فالنتيجة في الـ pathping المتوسط، بينما في الـ tracert لا يكتب المتوسط، بل تكون هناك محاولات ثلاث ويظهر نتيجة المحاولات الثلاث وحتى نوضحه أكثر هذه صورة لنتيجة عمل أداة الـ tracert:

```
Tracing route to yahoo.com [209.191.122.70]
over a maximum of 30 hops:

  1    2 ms     2 ms    <1 ms  192.168.1.1
  2   49 ms    48 ms    51 ms  195.229.244.43
  3   51 ms    50 ms    51 ms  195.229.245.146
  4   51 ms    49 ms    51 ms  194.170.0.234
  5   53 ms    52 ms    53 ms  195.229.1.101
  6   54 ms    55 ms    54 ms  195.229.1.166
  7  260 ms   253 ms   259 ms  195.229.0.194
  8  355 ms   353 ms   438 ms  198.32.160.121
  9  382 ms   405 ms   409 ms  UNKNOWN-216-115-100-92.yahoo.com [216.115.100.92
]
 10  430 ms   410 ms   408 ms  UNKNOWN-216-115-96-21.yahoo.com [216.115.96.21]

 11  430 ms   408 ms   410 ms  ae-2-d101.msr1.mud.yahoo.com [216.115.104.107]
 12  431 ms   368 ms   362 ms  te-8-2.fab1-a-gdc.mud.yahoo.com [209.191.78.149]

 13  367 ms   361 ms   360 ms  te-9-1.bas-c2.mud.yahoo.com [68.142.193.11]
 14  368 ms   365 ms   409 ms  ir1.fp.vip.mud.yahoo.com [209.191.122.70]

Trace complete.
```

فالأوقات التي بجنب الأرقام تراها ثلاث مرات، وذلك لأنه أعاد المحاولة ثلاثاً، يكتبها جميعاً في كل مرة، وتم التأكد من هذا عن طريق الوايرشارك،
أما في حالة الـ pathping فستتضح هنا:

```
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                            NICE1 [192.168.1.100]
                                 0/ 100 =  0%   |
  1    4ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 1/ 100 =  1%   |
  2   53ms     1/ 100 =  1%     0/ 100 =  0%  195.229.244.43
                                 0/ 100 =  0%   |
  3   53ms     1/ 100 =  1%     0/ 100 =  0%  195.229.245.146
                                 0/ 100 =  0%   |
  4   59ms     1/ 100 =  1%     0/ 100 =  0%  194.170.0.234
                                 0/ 100 =  0%   |
  5   58ms     1/ 100 =  1%     0/ 100 =  0%  195.229.1.101
                                 0/ 100 =  0%   |
  6   58ms     1/ 100 =  1%     0/ 100 =  0%  195.229.1.173
                                 0/ 100 =  0%   |
  7  261ms     1/ 100 =  1%     0/ 100 =  0%  nyc-r1-atm64-0-0-0.emix.net.ae [19
5.229.0.82]
                                 0/ 100 =  0%   |
  8  487ms     3/ 100 =  3%     2/ 100 =  2%  198.32.160.121
                                 0/ 100 =  0%   |
  9  397ms     3/ 100 =  3%     2/ 100 =  2%  UNKNOWN-216-115-100-92.yahoo.com [
216.115.100.92]
                                 0/ 100 =  0%   |
 10  419ms     1/ 100 =  1%     0/ 100 =  0%  UNKNOWN-216-115-96-21.yahoo.com [2
16.115.96.21]
                                 1/ 100 =  1%   |
```

هنا الذي قام بعمله هو أخذ المتوسط بعد عدد من المحاولات.
أما الآن فالنشرع في شرح عمل هذه الأداة

```
                Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                            NICE1 [192.168.1.100]
                                 0/ 100 =  0%   |
  1    4ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 1/ 100 =  1%   |
  2   53ms     1/ 100 =  1%     0/ 100 =  0%  195.229.244.43
                                 0/ 100 =  0%   |
  3   53ms     1/ 100 =  1%     0/ 100 =  0%  195.229.245.146
                                 0/ 100 =  0%   |
  4   59ms     1/ 100 =  1%     0/ 100 =  0%  194.170.0.234
                                 0/ 100 =  0%   |
  5   58ms     1/ 100 =  1%     0/ 100 =  0%  195.229.1.101
                                 0/ 100 =  0%   |
```

لنأخذ المثال في الأعلى.
تحت الـ hop يذكر عدد أرقام الراوترات بين المرسل والمرسل إليه، وعند كل hop يقوم بحساب الـ RTT ، فإن كنت تعرف مسبقاً كم الوقت بالتقريب بين النقطتين، فإذا ما حدثت مشكلة ثم قمت بعمل نفس هذا الفحص مرة ثانية ووجدت اختلافاً كبيراً في منطقة معينة، فستتمكن من معرفة شيئاً عن المشكلة.
الذي يهمنا كثيراً هنا هي الأرقام تحت Lost/Sent =This node/Link.... Pct
فالبرنامج يقوم بإرسال 100رزمة إلى كل وصلة، وعدد المفقود منها يخصمه من الناتج العام عن طريق النسبة. فكلما زادت نسبة المفقود في وصلة، لا بد أن يثير ذلك من انتباهك.
لا بد أنك لاحظت أن هناك أرقام بجنب الـ IP addresses وأرقام أخرى بين الأرقام وبالتحديد عند علامة | ، وأعني الأرقام بعدد 100
فما هو الفرق؟
الفرق أن الأرقام الـ 100الموجودة بجنب الـ ip addresses، هي تحدد كم ذلك الجهاز قد فقد من رزم، بينما الأرقام الـ 100بين الـ Ips هي تتحدث عن الوصلة، فإن ارتفعت أرقام الوصلات، فهذا معناه المشكلة في الأسلاك مثلاً، أو بسبب الضغط على تلك الوصلة، بينما الأرقام الـ 100بجنب الـ IP addresses فهي إن ارتفعت فهي تعني أن الجهاز لا يستطيع التعامل مع العدد الكبير من الرزم، فهو يسقطها، وقد يرجع السبب إلى الضغط الكبير على الجهاز أو بدء عطل في الجهاز. وهكذا.

بعد أن عرفنا مخرجات أو نتائج استخدام هذه الأداة، لنتحدث عن إمكانيات هذه الأداة. والصورة في الأسفل تظهر إمكانياته.

```
C:\>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]
                [-4] [-6] target_name

Options:
    -g host-list      Loose source route along host-list.
    -h maximum_hops   Maximum number of hops to search for target.
    -i address        Use the specified source address.
    -n                Do not resolve addresses to hostnames.
    -p period         Wait period milliseconds between pings.
    -q num_queries    Number of queries per hop.
    -w timeout        Wait timeout milliseconds for each reply.
    -P                Test for RSVP PATH connectivity.
    -R                Test if each hop is RSVP aware.
    -T                Test connectivity to each hop with Layer-2 priority tags.
    -4                Force using IPv4.
    -6                Force using IPv6.

C:\>
```

هذه هي أوامر الأداة هذه، كما ترى ليست كثيرة. هي أداة واحدة لها استخدام واحد، لكنه لا يمكن الاستغناء عنها لمن أراد العمل باحترافية.
لن أتحدث عن جميع الأدوات بل سأترك فرصة التعلم والاستفادة والحصول على المعرفة.
سأتحدث عن بعض الأوامر التي قد تبدوا صعبة.
مفتاح g-
لو كانت هناك طرق متعددة بين المرسل والمرسل إليه، لكن محلل نظم الشبكة يود في فحص طريق واحدة بعينها، فهذا الأمر يمكنه من تحديد العناوين Ips التي سوف يستخدمها للوصول إلى الهدف.

مفتاحان P- و R-
هما يقومان بفحص الأجهزة والوصلات والأسلاك إذا ما كانت جاهزة لنوع معين من البروتوكولات مثل المختصة بالبث المباشر للصورة أو للصوت.

مفتاحان 6- 4-
من أجل أختيار الـ Internet Protocol الذي يجب إستخدامه.

وإلى لقاء آخر، إن شاء الله والذي سوف يكون عن كيفية تحليل الشبكة ومعرفة الأسباب التى تؤدي إلى بطئ الشبكة

الشبكات وأنظمة المراقبة

بقلم: أحمد الجلجولي

انظمه المراقبه بالكاميرات , ماذا نعني بها وماذا نعني بقولنا بأن هذا الموقع مراقب بالكاميرات , اولا وقبل كل شيء اود التعريف بأنظمه المراقبه بالكاميرات : وهي ذلك النظام الذي يتكون من عدد من الكاميرات وعملها تصوير الاحداث في الموقع ونقلها على شكل اشاره كهربائيه عبر الكوابل الى جهاز يستقبل هذه الاشاره ويقوم بتحويلها الى صور تعرض على شاشه العرض , والان فقد تعرفنا الى مكونات هذا النظام ولنلقي نظره على كل مكون ونستوضح عمله .

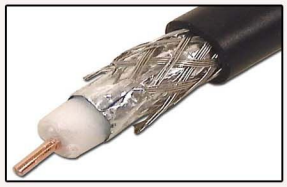
اولا سوف ابدأ بالكاميرات وتنقسم الى عده اقسام رئيسيه وسأقوم بتصنيفها حسب ظروف العمل وتنقسم الى داخليه وخارجيه Indoor & Outdoor

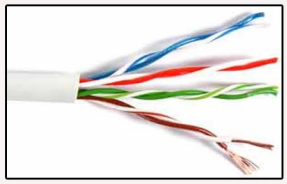
, فالكاميرا الداخليه تقوم بتصوير الاحداث من حولها وإما ان تكون ليليه او نهاريه ويطغى على شكلها نوع القبه Dome Camera والسبب في استخدامه هو انه عند الرؤيه إليه لا يتم التعرف عليه كأنه كاميرا , وإما ان تكون ايضا الكاميرا الداخليه ثابته او متحركه .

اما بالنسبه للكاميرا الخارجيه فتوضع في الاماكن ذات الظروف الخاصه مثلا ان تكون مضاده للماء والحراره وهكذا وايضا يطغى على شكلها النوع الخارجي الليلي المكون من معدن الالنيوم وتسمى بـ IR Box Camera , وهنالك بعض الانواع الخارجيه الاخرى حيث انه يتم وضع الكاميرا في علبه مستطيله الشكل Housing وتكون هذه العلبه معزوله جيدا وبداخلها مروحه تبريد وجهاز طرد للحراره , وقبل ان ندخل في المكون الثاني لم لا نلقي نظره على متطلبات تشغيل الكاميرات وهو الـ Power Supply والمقصود به هو محول الكهرباء او الشاحن او مزود التيار او ..... , وفي انظمه الكاميرات نحتاج الى ثلاث فولتيات (220v,24v,12v) فهنالك كاميرات تحتاج الى 12v وهي الكاميرات العاديه (IP cam,cam,IR box, Dome) وهنالك كاميرات تحتاج الى 24v وهي الكاميرات المتحركه Dome PTZ وهنالك كاميرات تحتاج الى 220v وهي متحركه (مع ملاحظه ان فولتيه الكاميرا عاديه ولكن الحاجه الى مثل هذه الفولتيه هي للمحرك Motor وليست للكاميرا) .

اما بالنسبه للتيار (أمبير) الذي تحتاجه الكاميرات فهو إما ان يكون 500ma (للكاميرات النهاريه) أو ان يكون 1A (للكاميرات الليليه) ونظرا لقوانين التيار الكهربائيه فلا يوجد أي تأثير من استخدام 1A لجميع الكاميرات وذلك لان الكاميرا تستخدم ما تحتاجه فقط .

أما المكون الثاني من هذا النظام وهو الجزء الذي يقوم بنقل الاشاره وبالحقيقه هنالك نوعان رئيسيين من هذه الكوابل وهي : الكوابل المحوريه Coaxial Cable , وكوابل الازواج الملتفه Twisted Pair cable





نعم نستطيع استخدام كوابل الـUTP وكوابل الـSTP وهي نفسها التي تستخدم لعمل شبكات الحاسوب وهنا نستخدم توصيلات خاصه تسمى Video Balun وتقوم هذه القطعه بتحويل الاشاره من احاديه الى ثنائيه (اي لتسير الاشاره داخل كيبل الUTP) وتتكون من طرفين طرف يشبك بالكاميرا(توصيله BNC تقليديه) والطرف الاخر يشبك بالكيبل

وهنالك أيضا نوع خاص من الكاميرات لاتحتاج إلى أي محول لانها مزودة بمخرج التي RJ45 وتدعى IP Camera وتربط على شبكه الكمبيوتر مباشره ويتم مراقبتها في حال كانت كاميرا مفرده باستخدام متصفح الانترنت اما في حال لم تكن مفرده اي انه يوجد اكثر من كاميرا في نفس الموقع يستخدم ما يسمى بي Network Video Recorder:NVR والذي سوف نتحدث عنه لاحقا.

أما المكون الثالث من مكونات نظام المراقبه والذي يعد الجزء الاكثر اهميه ويسمى بجهاز العرض والتسجيل ويرمز له بالرمز DVR اي وهي اختصار لـDigital Video Recorder ومعناها بالعربيه جهاز التسجيل الرقمي , وعمل هذا الجهاز هو القيام بعمليه التسجيل وايضا يقوم بعرض الاحداث مباشره على شاشه عرض , وإما ان يكون مبني على جهاز الكمبيوتر Computer Based اي عباره عن بطاقه PCI يتم تركيبها على جهاز الكمبيوتر ويتم إنزال برنامج خاص به يسمى بـDVR Server Software , اما النوع الاخر فيكون جهاز قائم لوحده Standalone DVR وهو جهاز مختص يؤدي نفس العمل ولكن يكون عمله فقط للكاميرات , وسواء أكان جهاز المراقبه مبني على الكمبيوتر ام قائم لوحده فطريقه شبكه ومراقبته من مكان اخر واحده .

ويستخدم لتوصيل نظام المراقبه على شبكه الحاسب سلك ازواج ملتفه (سلك الشبكه التقليدي) ويتم إعطاءه رقم اي بي خاص به على الشبكه ويتم التعامل معه كأنه جهاز كمبيوتر , والان لتتم المراقبه يجب علينا تجهيز الجهاز الذي سوف نراقب عليه ببرنامج يسمى ببرنامج المراقبه للعميل Client Software وبالعاده يأتي مع جهاز العرض والتسجيل على قرص مدمج , وفي حاله عدم توافر هذا البرنامج يمكننا استخدام متصفح الانترنت بدلا منه , ويجب تزويد هذا الجهاز باخر إصدار من DirectX و ActiveX .

استخدام متصفح الانترنت بدلا منه , ويجب تزويد هذا الجهاز باخر إصدار من DirectX و ActiveX .

ومن الناحيه الفنيه يجب علينا معرفه بعض المعلومات قبل القيام بالمراقبه عن طريق الشبكه وهذه المعلومات هي رقم الاي بي الخاص بجهاز العرض والتسجيل وايضا اسم مستخدم وكلمه مرور يتم اخذهما من برنامج العرض والذي سوف نتحدث عنها في الفقرة القادمة .

المراقبه عن طريق الشبكه (LAN & WAN)

في بعض الاحيان يقوم البعض بتركيب نظام المراقبه بالكاميرات لينوب عن تواجده في الموقع المراقب , ولا يستدعي ذهابه الى الموقع إلا لمشاهدة التسجيل ورؤيه ما حصل في غيابه ,ولكن تأتي ظروف العمل وتحكم علينا بالسفر او الذهاب الى منطقه بعيده ويتمنى البعض لو انه يستطيع اخذ جهاز المراقبه معه ليرى ما يحصل , وبالتأكيد جاءت الرغبه لمراقبه الموقع من موقع اخر او مراقبه عده مواقع من موقع اخر مركزي بعيد .

وطبعا في ظل هذا التطور التكنولوجي في مجال الاتصالات تم تلبيه هذه الرغبات جميعها فيمكن عمل ذلك , وايضا تمكننا هذه الخاصيه من مراقبه المواقع حتى بدون توفر جهاز كمبيوتر فيمكننا ذلك من خلال اجهزه الهواتف النقاله .

وهذا ما يسمى بـتقنيه البث على الشبكه سواء أكانت محليه ام موسعه

وبإذن الله تعالى سوف أقوم بشرح كافه الامور المتعلقه بهذا الموضوع وعلى الترتيب التالي :

★ Static IP ما هو وما دوره .

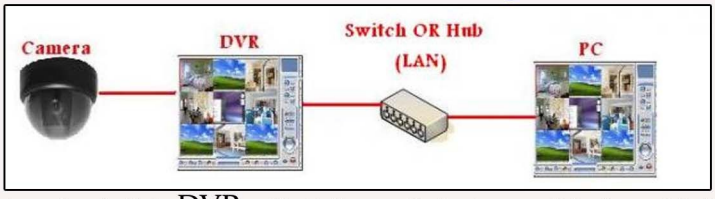
★كيفيه تفعيل الخدمه على جهاز العرض والتسجيل وطرق توصيله بالانترنت .

★ كيفيه المراقبه من الخارج وما هي البرامج المستخدمه لذلك وطرق المراقبه .

اولا الـ Static IP هو عباره عن رقم اي بي يتم حجزه لك من مزود خدمه الانترنت ISP ويكون رقم اي بي ثابت للاشتراك , وعند الدخول عليه من موقع اخر فإنك تقوم بالدخول الى الجهاز الذي قام بالشبك (إما ان يكون جهاز كمبيوتر او راوتر او .....) , وله اكثر من اسم (public IP ,Real IP ,static IP) .

وبالطبع لكل اشتراك على الانترنت رقم مثل هذا ولكنه يكون متغيرا فأنت تستطيع الحصول عليه من بعض المواقع على الانترنت او من خلال جهاز الراوتر لديك ولكن عند فصل الانترنت والشبك مره اخرى فهذا الرقم يتغير , ويجب الحصول عليه من مزود خدمه ISP الانترنت لديك حتى تتمكن من برمجه الاجهزه مره واحده فقط .

المراقبه من نفس الموقع على الشبكه الداخليه (LAN) :



نستخدم هذه الخاصيه عندما يكون جهاز المراقبه DVR في الموقع ونريد ان نشاهده من نفس الموقع مثلا : جهاز الـ DVR تم تركيبه عند الحارس ويريد المدير ايضا مشاهدة الكاميرات واستخدامه .

والطريقه هي كالتالي :

سواء أكان جهاز الـDVR مبني على كمبيوتر Computer Based أو كان جهاز قائم لوحده Standalone DVR فعند شراءه فيجب ان تأتي معه اسطوانه تحتوي على برنامج الـClient وإذا لم تكن متوفره ايضا يمكننا المتابعه دونها وذلك باستخدام متصفح الانترنت .

★اولا يتم ربط جهاز الـDVR على الشبكه وإعطاءه رقم اي بي ثابت) حسب الشبكه (مثلا : 192.168.1.50.

★عمل حساب Account على الـDVR وبالعاده أقوم بتسميته Remote ووضع باسوورد له مثلا 1234 وتحديد الصلاحيات له (يمكن عمل ذلك من خلال البرنامج الخاص بالـDVR وعلى ما اعتقد فإن جميع برامج المراقبه تدعم هذه الخاصيه) والحساب يتم عمله على برنامج المراقبه وليس على الويندوز .

الان اصبحت لدينا المعلومات التاليه :

DVR IP : 192.168.1.50
Username : Remote
Password : 1234

نقوم بتدوينها وحفظها

أ- الذهاب الى الجهاز المراد المراقبه عليه وتنزيل برنامج الـClient وبعد تنصيبه فإنه بالتأكيد سوف يطلب منك المعلومات التي قمنا بتدوينها , ونقوم بإدخالها وبهذا نكون قد انهينا .

ب- إذا لم يتوفر برنامج الـClient الخاص بجهاز الـDVR :

وبهذه الطريقه نستخدم متصفح الانترنت ونقوم بعمل التالي :

أولا الذهاب الى إعدادت المتصفح ومن ثم إعدادت الامان ونقوم بإضافه رقم الـIP الخاص بالـDVR الى خانه الـTrusted Sites .

ثانيا بعد الانتهاء نقوم بوضع رقم الـIP الخاص بالـDVR في العنوان والدخول إليه

ثالثا سوف يطلب المتصفح أمر بتنزيل : ActiveX ونسمح له ذلك.

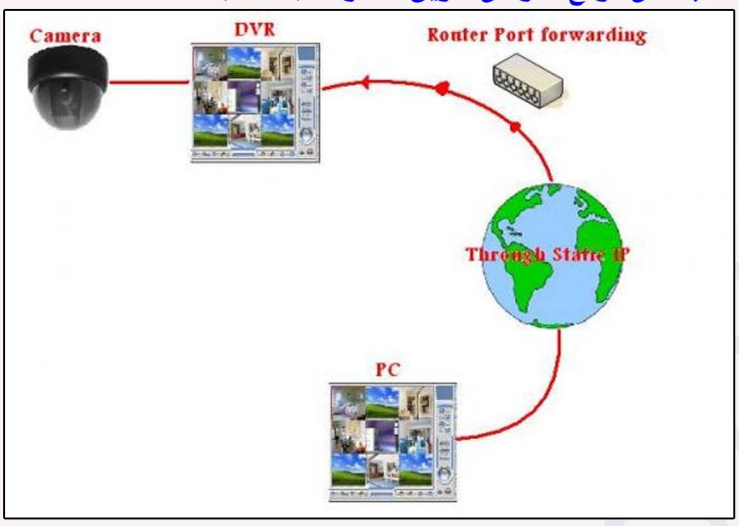
رابعا بعد الانتهاء نقوم بعمل Refresh للصفحه وسوف تفتح صفحه تطلب منا المعلومات التي حفظناها ومن ثم ندخلها وبهذا نكون قد انتهينا .

ملاحظات هامة

★بعض اجهزه المراقبه تطلب معلومات إضافيه مثلا : Site Code ,Site Name .

★للحصول على أفضل نتيجه يجب تنزيل اخر إصدارات الـDirect X واخر إصدار من تعريف كرت الشاشه والـActiveX .

الشبك من موقع اخر عن طريق الانترنت (WAN)



في الأتصالات البعيدة WAN يجب اولا حجز رقم static IP من مزود خدمه الانترنت وهذه هي اول معلومه يجب تدوينها مثلا :

Static IP : 172.180.50.20

ثانيا يجب إضافه حساب على جهاز الـDVR مثلا :

Username : Remote
Password : 1234

ثالثا يتم وضع رقم IP لجهاز الـDVR ثابت حسب الشبكه الداخليه مثلا :

DVR IP : 192.168.1.50

رابعا برمجه الجهاز الذي يشبك على الانترنت في الشبكه ليقوم بتحويل الاتصال الخارجي الى جهاز الـDVR .

إذا كان جهاز راوتر نفعل خدمه الـDMZ ونقوم بإدخال رقم الـIP الخاص بجهاز الـDVR على الشبكه وهو في هذه الحاله : 192.168.1.50.

والان اصبحت لدينا المعلومات التاليه

Static IP : 172.180.50.20
Username : Remote
Password : 1234

خامسا الذهاب الى الموقع المراد المراقبه منه وعمل نفس الطرق التي قمنا بعملها سابقا وهي :

أ- الذهاب الى الجهاز المراد المراقبه منه وتنزيل برنامج الـClient وبعد تنصيبه فإنه بالتأكيد سوف يطلب منك المعلومات التي قمنا بتدوينها , ونقوم بإدخالها وبهذا نكون قد انهينا .

ب- إذا لم يتوفر برنامج الـClient الخاص بجهاز الـDVR :

وبهذه الطريقه نستخدم متصفح الانترنت ونعيد تكرار نفس الخطوات السابقة التى ذكرناها في إعداد الـ LAN

نتائج الأستفتاء الشهري

مداخلتي لهذا الشهر على نتائج الأستفتاء سوف تكون بسيطة نوعا ما وقبل أن أقدم مداخلتي لهذا الشهر أحب أن اوضح الأسباب التى دفعتني للقيام بمثل هذا الأستفتاء .

لا أخفي عليكم أن أحد الأسباب التى دقعتني هي الرسائل والملاحظات التى إستلمتها مؤخرا من بعض الأخوة يسألونني عن سبب إعطاء سيسكو الحيز الأكبر من المواضيع في المجلة وأردت أن أرد عليهم من خلال نتائج الأستفتاء فهي توضح أن أكبر توجه او ميول لمهندسي الشبكات العرب يتجه نحو سيسكو وأجهزتها لذا فنحن في المجلة نحاول أن نركز على سيسكو أكثر من غيرها لاننا نعلم أن سيسكو ليست مجرد شركة مبيعات فقط فجميعنا يعلم أنواع البروتوكولات والتقنيات التى قامت سيسكو بتطويرها وتنفيذها بغض النظر أن كل ماتقوم سيسكو بتطويره يعد حكرا عليها وعلى أجهزتها أما النقطة الثانية فهي تتمثل في عدم إنكار حقيقة أن سيسكو هي الشركة الأولى عالميا في مجال الشبكات وللآسف جونيبر لن تستطيع أن تجاريها لان أهتمام جونيبر ينصب أكثر على أجهزة الـ Core بعكس سيسكو التى تراعي كل المتطلبات الموجودة في السوق .

أما بخصوص مداخلتي على النتائج فأحب أن اقول لكم أن توقعاتي كانت في مكانها تماما فقد توقعت ان سيسكو سوف تحتل المرتيبة الأولى من ناحية التقنية والسبب أوضحته من قبل وهو مراعاة كل متطلبات السوق أما بخصوص التخصص فهو شيء أعرفه وتوقعته منذ العدد الأول عندما كتبت في أفتتاحية المجلة عن الطفرة التى نعاني منها كعرب في مجال الأمن والحماية فهي تحتل قلوب اغلب مهندسي ومتتبعي عالم الشبكات والأسباب قمت بتوضيحها من قبل لذا أنا مازلت أعارض قليلا هذه التوجهات وخصوصا أن سوق الوظائف العربي لايتطلب هذا المقدار الكبير من المتخصصين وأنصح الجميع أن يحاول التركيز في شيء آخر مثل الـVoice أو الـWireless فهي التقنيات التى أراها الاقرب للمستقبل الوظيفي والعملي ودمتم بود

المهندس: ايمن النعيمي

نتائج الأستفتاء

ماهو أكثر مجال في الشبكات يروق إليك؟

- شبكات سيسكو 56%
- كل مايتعلق بالشبكات 35%
- شبكات مايكروسوفت 29%
- شبكات جونيبر 9%
- Security 26%
- Voice 18%
- Wireless 17%

مقارنة بين AppleTalk & IP & Novell IPX

بقلم: أيمن النعيمي

AppleTalk

هو أحد انظمة الشبكات الذي قامت شركة Apple بتصميمه ونشره لمستخدمي كمبيوترات الماكنتوش MACINTOSHوالذي يعد احد الانظمة المصنعة من قبل Appleوقد تم ضمه أول مرة في أجهزة ماكنتوش عام 1984حتى عام 2009عندما قررت شركة Apple التخلي عنه في أصدارها الاخير MAC OS X V10.6لصالح TCP/IPوتتبع Apple نفس التصميم المتبع في OSI Modelمع الاختلاف في البروتوكولات المستخدمة فيه وهذه صورة توضيحية

OSI Model	Corresponding AppleTalk layers
Application	Apple Filing Protocol (AFP)
Presentation	Apple Filing Protocol (AFP)
Session	Zone Information Protocol (ZIP) AppleTalk Session Protocol (ASP) AppleTalk Data Stream Protocol (ADSP)
Transport	AppleTalk Transaction Protocol (ATP) AppleTalk Echo Protocol (AEP) Name Binding Protocol (NBP) Routing Table Maintenance Protocol (RTMP)
Network	Datagram Delivery Protocol (DDP)
Data link	EtherTalk Link Access Protocol (ELAP) LocalTalk Link Access Protocol (LLAP) TokenTalk Link Access Protocol (TLAP) Fiber Distributed Data Interface (FDDI)
Physical	driverLocalTalk driverEthernet driverToken Ring driverFDDI

وكما نرى من خلال هذا الجدول ان AppleTalk يدعم التقنيات التالية ال Ethernet and Token Ring and FDDI

لكن ضمن بروتوكولاته الخاصة والموجودة في ال Physical Layerلتصبح على مثل ...EtherTalk..بالأضافة الى وجود LocalTalkالمملوك لشركة Apple والذي يعمل بتقنية twisted-pair media access system

ومن أهم التطبيقات المستخدمة في AppleTalkهي

AppleTalk Address Resolution Protocol – AARPوأتوقع أن الجميع قد فهم ماهو هذا البروتوكول وماذا يفعل ,لان الاسم مشتق من نفس البروتوكول المستخدم في IPوهو ARP والمسؤول عن إيجاد الماك دريس لايبي معين

Name Binding Protocol – NBPوالذي يعمل بتفس عمل ال DNS مع الاختلاف قليلا في آلية العمل

AppleTalk Transaction Protocol – ATP

وهو المسؤول عن ضمان وصول الداتا بشكل صحيح ويقابله طبعا في IP ال TCP

AppleTalk Echo Protocol – AEPوهو البروتوكول المسؤول عن ال Ping

Routing Table Maintenance Protocol RTMPالبروتوكول المسؤول عن أعطاء معلومات حول التبلوجي الخاص بالشبكة لباقي الروترات وهو يقوم بشكل دوري بالارسال كل عشر ثواني وعلى شكل Broadcast

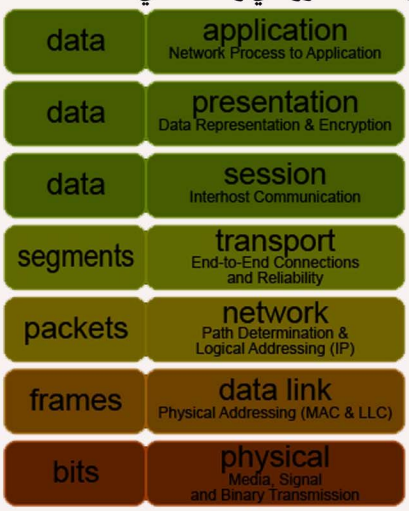
Datagram Delivery Protocol DDP

It provided a datagram service with no guarantees of delivery. All application-level protocols

وأخيرا أحب أن أذكر أن سيسكو تدعم Appletalk

IP

طبعا أغلبنا يعرفه ويعرف كيفية عمله لذلك لن أتطرق اليه كثيرا وسوف أقول أنه من أقدم البروتوكولات المستخدمة ويعد أول بروتوكول تم أستخدامه للربط بين شبكتين في عام 1960ويعمل ضمن ال OSI المعروف في وقتنا الحالي



وهو يستخدم بروتوكولان للنقل الأول TCPأو اختصار لـ Transmission Control Protocol

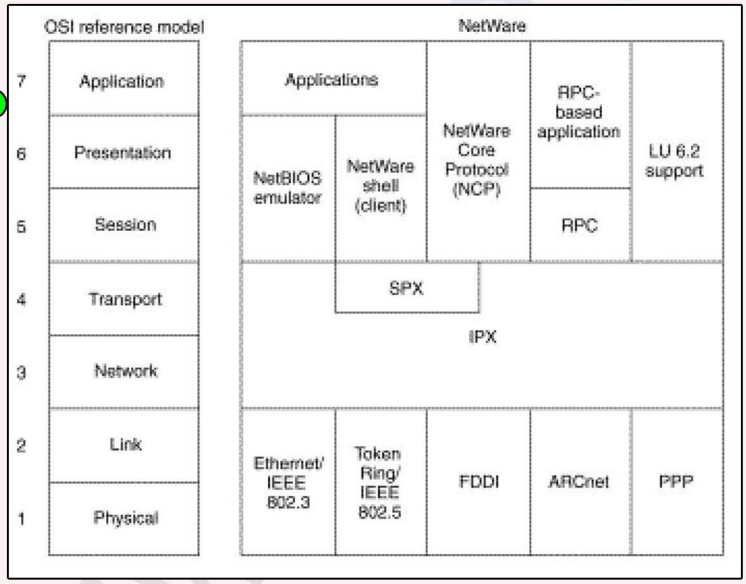
وهو جزء من بروتوكول الإنترنت حيث ينتمي للطبقة الرابعة transport layerوهو يقوم بتأمين الاتصال والتأكد من وصول الداتا بشكل صحيح أما الثاني فهو يدعى UDPوهو أختصار لـ user datagram protocolهو بروتوكول يستخدم في إرسال واستقبال الباكيت عبر الشبكة وهو جزء من بروتوكول الإنترنت حيث ينتمي للطبقة الرابعة transport layerولا يستخدم في نقل المعلومات الهامة ويكثر استخدامه في الاستماع لملفات الصوتوالفيديو عبر الإنترنت أو عبر الشبكة بشكل عام streaming audio and videoحيث يهتم بالسرعة أكثر من اهتمامه بالداتا المنقولة

Novell IPX

NetWare is a network operating system (NOS)

وهو يدعم الخدمات المعتمدة من Novell وقد تم بدا التسويق له لأول مرة عام 1980عندما كانت الشبكات بعدها صغيرة وتعد التكنلوجيا المستخدمة في NetWare بشكل عام مأخوذة منXerox Network Systems (XNS)

وهو نظام شبكات قديم تم عمله لأول مرة عام 1970ماذا نفهم من كل هذا الكلام نفهم ان IPX والذي يدور محور الحديث عنه يستخدم مع نظام NetWareفي بداية الامر لنتعرف على توزع الطبقات في النوفل مقارنة مع توزيع الطبقات في OSI Model



تعتمد شبكات الـ Novell على بروتوكولان أثنان الأول هو IPX وهو يعتبر البروتوكول الرئيسي المستخدم في عمليات الاتصال الخاصه بالشبكة(الطبقه الثالثه) وبما أنه أحد بروتوكولات المستخدمه في نقل البيانات في عمليات الاتصال التي لا تتطلب إعداد مسبق لكونه Connectionless Datagram Protocol

فإنه يتشابه مع عمليات التسليم غير الموثوق فيها لوحدات البيانات التي تتم عبر بروتوكول IP كما إنه يتماثل معIP بمعنى يجب أن يكون Unique ويتكون عنوانه من جزأين 32بت للشبكة بالهكساديسيمال من النطاق1×0 0xFFFFFFFE–و 48بت للهوست والDefault سوف يكون الMAC ADDRESS

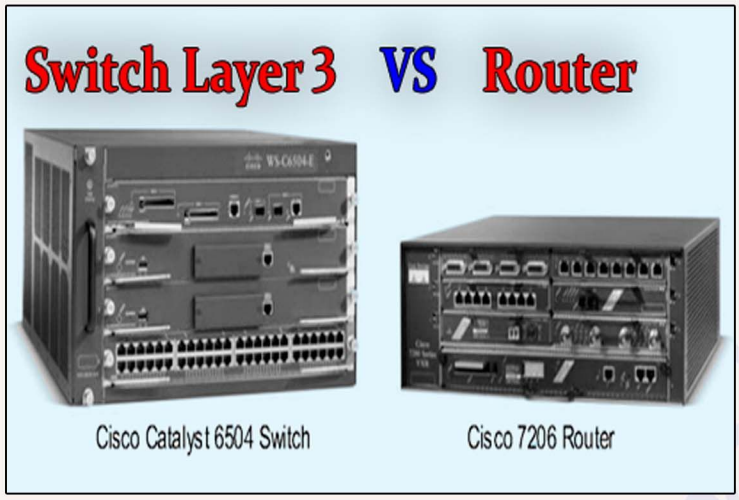
مثال على ذلك :48F30106:00A024F9173B

الهوست : الشبكه أكثر أنواع التضمين شيوعا :Novell Proprietary والمعروف أيضا بإسم Novell Ethernet802.3و Raw 802.3 802.3وهو IEEE STANDARD والمعروف بإسم Novell 802.2 Ethernet II و Ethernet SNAP وهو إمتداد للنوع 802.3

ثانيا SPX

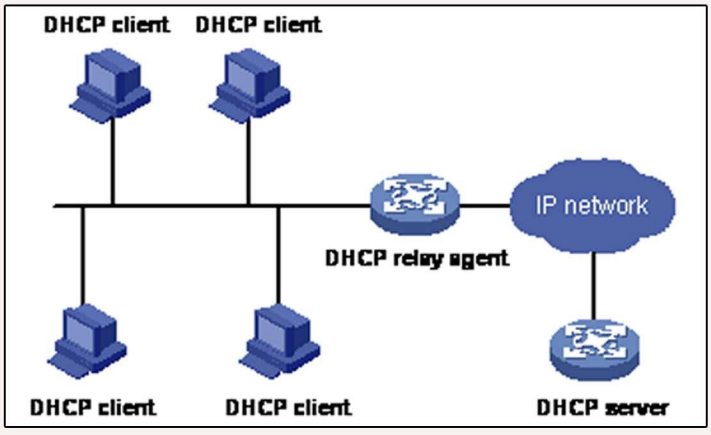
وهو بروتوكول يتم إرساله في مقدمة بيانات خاصة ببروتوكول IPXفي الطبقة الرابعه لنموذج OSI وكما هو الحال في TCPيوفر بروتوكول SPX خدمه مؤمنه لتسليم البيانات حيث يقوم بتعويض خدمة البيانات الغير مؤمنه في IPX يعتبر بروتوكول SPX بمثابة بروتوكول للتحكم في توجيه حزم البياناتفهو Connection-Oriented وله مقدرة على إكتشاف الأخطاء وتصحيحها

مقارنة بين الروترات وأجهزة السويتش لاير 3



كما وعدتكم في العدد الآخير من المجلة بأني سوف أخصص مقالة تتحدث عن أهم الفروقات بين أجهزة الروتر وأجهزة السويتش لاير 3من خلال قرأتي لصفحات الأنترنت ومتابعة بعض والمحللين الذين هم أخبر مني في مجال الشبكات وجدت أن أغلبهم مجمع على أن فكرة السويتش Layer 3ليس إلا Marketing أي من أجل زيادة التسويق فهو روتر لكن مخصص للإيثرنت فقط وهذا يقودنا إلى أول مفارقة بين الأثنان وهي أن السويتش لايملك أي منافذ من نوع Serial وكل المنافذ الذي يحويها من نوع إيثرنت فقط وبالتالي يقودنا هذا الأستنتاج إلى أن السويتش 3 لايدعم الأتصالات بعيدة المدى Wan وهو الفرق الثاني بينهم أما الفرق الثالث فهو يقوم على أن السويتش يعتمد على الهاردوير في عملية تمرير البيانات بينما الروتر يعتمد على السوفت وير بينما نجد الفرق الرابع بينهم صريح وهو عدم دعم الكثيرمن البروتوكولات والخواص الهامة على سويتشات لاير 3مثل الـ Nat, BGP, NBAR, Netflow, VPN, Encryption خلاصة هذا الكلام يعد إستخدام هذا النوع من السويتشات مفيداً في الشبكات الداخلية Lan فهو يوفر سرعة وأداء أكبر من نظيره الروتر لكن لن يستطيع أن يحل مكان الروتر بشكل كامل كون فقدان هذا النوع من السويتشات بعض المميزات الهامة

طريقة إعداد الـDHCP Relay Agent على أجهزة جونيبر




```
Juniper's JUNOS
edit forwarding-options helpers bootp]]
root# show
server 192.168.10.1;
maximum-hop-count 2;
minimum-wait-time 1;
interface {
em0.0;
}

[edit forwarding-options helpers bootp]
root# commit
```

ماهو الـ DHCP Relay Agent ؟

بداية كلمة Relay تعني باللغة العربية النقل على مراحل أو التعاقب في عمل أو إعادة البث فكما يعلم جميعنا أن الروتر لايقوم بتمرير البرودكاست وهذا سوف يجبرنا على وضع سيرفر DHCP في كل شبكة وطبعا هذا شيء غير مرغوب به لما له من مصاريف زائدة بالأضافة إلى الوقت الضائع الذي سوف نقضيع في متابعة إداء وعمل كل سيرفر لذا قامت سيسكو أولا بعمل خاصية تدعى IP-Helper والتى تسمح للروتر بتمرير طلبات الـ DHCP التى تكون على شكل برودكاست إلى السيرفر مباشرة وطبعا هذه الخاصية متاحة فقط على أجهزة سيسكو وفي حقيقية الأمر سيسكو قامت أساسا بتطوير الخاصية القديمة وهي التى نتحدث عنها اليوم DHCP Relay Agent والتى تقوم بنفس العملية تماما وهي نقل البرودكاست من شبكة إلى شبكة آخرى وهي متاحة على كل أنواع أجهزة الشبكة وبما فيها جونيبر والتى سوف أخصها لكي أتحدث عن طريقة إعدادها على أجهزة جونيبر وسوف نتوجه أولا إلى المسار التالي ونقوم بكتابة الأوامر التالية

أعتقد أن الأوامر تشرح نفسها قمنا أولا بكتابة أيبي السيرفر وبعدها (ليس أجباري) قمت بتحديد أقصى عدد للهوب بالأضافة إلى تحديد المدة الزمنية التى سوف ينتظرها الروتر من سيرفر الـ DHCP وفي حال لم يرد خلال ثانية سوف يعاود الأرسال مرة ثانية وآخيرا قمت بتحديد المنفذ الذي سوف يتم إستلام طلبات الـ DHCP Request وهو المنفذ em0.0

LDAP Server

بقلم: أحمد بخيت

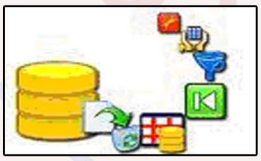
هو عبارة عن بروتوكول مثل كل البروتوكولات على الشبكة يقوم بأداء وظائف غاية في الأهمية تتعلق اغلبها بتأكيد الدخول حيث يستخدم مع أكثر من سيرفر آخر لتنفيذ هذا الغرض مثل سيرفرات البريد حيث العدد الكبير من المستخدمين الذي يكون متواجد على هذه السيرفرات كمان انه يتميز بسرعة كبيرة في الـ Read حيث أن هذا يجعله يستطيع التعامل مع طلبات كثيرة مما يؤدي إلى سرعة في الأداء.

LDAP: هو اختصار لكلمة Lightweight Directory Access Protocol حيث انه يمتاز بالسرعة والخفة وهذا ما يميزه عن استخدام قواعد البيانات العادية مثل SQL – MySQL – Oracle – وحتى نكون منصفين أكثر لابد وان نوضح من أين استمد هذا البروتوكول سرعته هذه عن قواعد البيانات.

للإجابة عن هذا التساؤل لابد لنا أن نعرف ما هي البنية لكل منهما:

قواعد البيانات:

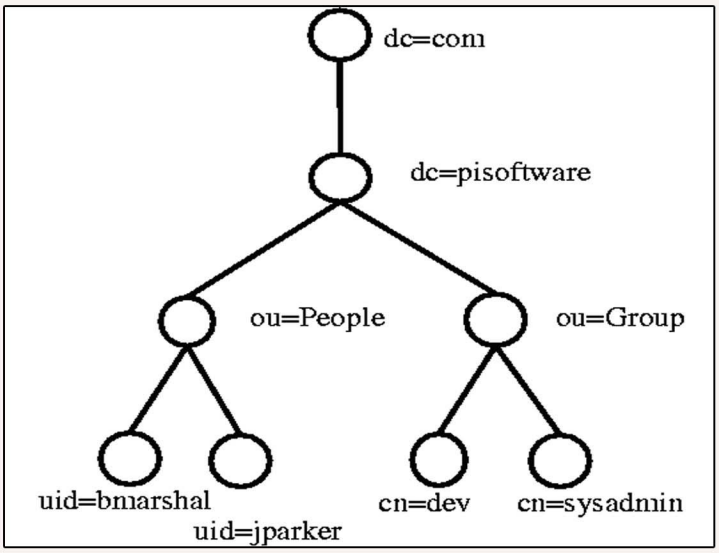
بنية قواعد البيانات تكون معتمدة في الأصل على الجداول Tables حيث يتم إدخال المعاملات لدينا داخل هذه الجداول ومن هنا يتم بناء قاعدة البينات من مجموعة من المعاملات داخل مجموعة من الجداول، كما انه يمكن ربط أكثر من معامل وكذلك ربط أكثر من جدول مع بعضهم لتكون تطبيق يقوم بأداء وظيفة معينة.



ومن ثم يتم استدعاء هذه البيانات بطريقة أو بأخرى لاستخدامها في العمليات المختلفة، ولذلك يتم البحث من قبل البرنامج عن الجدول الذي يريد داخل هذه القواعد مما يتطلب وقت اكبر ثم بعد ذلك يبحث عن المعاملات التي تهمه ويأخذها.

LDAP:

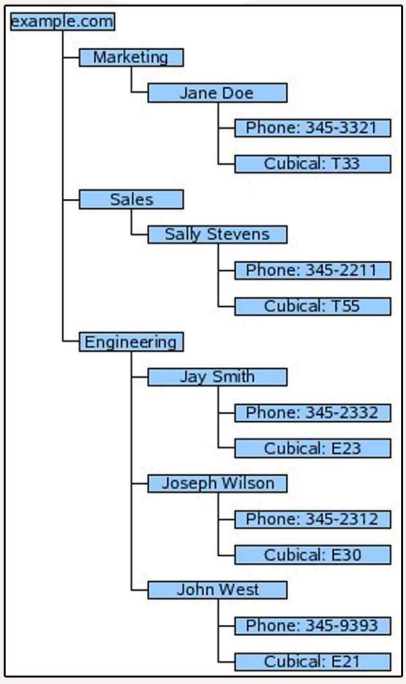
بالنسبة إلى هذا البروتوكول نجد انه يعتمد طريقة أخرى في التعامل مع المعاملات لديه إذ انه يعتمد طريق الشجرة ذات الفروع، حيث انه يقوم بترتيب الجداول فيما سبق في قواعد البيانات وكأنها أفرع رئيسية في المؤسسة وبعد ذلك تحت كل فرع معلومات عدة مثلاً عن المستخدمين Users أو عن المجموعات من المستخدمين Groups وكذلك الخدمات والبروتوكولات وهكذا وهذه الطريقة توفر الوقت على البرنامج أو السيرفر الذي يريد طلب المعلومة.



وهكذا يستطيع هذا البروتوكول إخراج أية معلومة لأي سيرفر بسرعة فائقة نستطيع تشبيهه بطريقة البروفايل Profile حيث انه يضع مجموعة من المعلومات التي تخص شئ معين في مكان واحد.

نظرة تاريخية إلى هذا النوع من البروتوكولات:

في هذا المجال يوجد ليدنا حوالي ثلاثة أنواع هامة في تأكيد معلومات الدخول وهي NIS – X.500 – LDAP – بداية بالنوع الأول وهو NIS كان من الأنواع الهامة والمؤثرة لكن في الشركات ذات الحجم الصغير حيث انه كان ضعيف في الأمن نوعاً ما وبطئ في التعامل مع الطلبات، وهذان السببان جعلا الشركات تسعى إلى تطوير نوع آخر من البروتوكولات هو X.500 أما هذا النوع فانه يمتاز عن سابقه بشئ مهم جداً وهو الأمن الذي جعله يتصدر الحلول الخاصة بتأكيد الدخول لكن مازال هناك عيب آخر مهم خاصة مع تضخم أحجام الخدمات على الانترنت خاصة خدمات البريد مما دفع الشركات إلى البحث عن السرعة ثم الأمن لأنهما مترافقان وهنا ظهر هذا البروتوكول LDAP حيث



بالنسبة إلى السرعة قد فصلناها سابقاً إلا انه بالنسبة إلى الأمن فانه يستطيع تشفير وتأمين معلوماته أثناء الانتقال من قواعده إلى الوصول لبرنامج العميل باستخدام أكثر من وسيلة على سبيل المثال انه يقوم بعمل تشفير MD5 لحساب هذا العميل مثلاً GMail يقوم بطلب معلومات من هذا السيرفر فانه هناك شفرات لفتح الاتصال وبعد ذلك يكون هناك نوع آخر من التأمين وهو من خلال استخدام الشهادات مثل TLS وهو نوع أكثر تعقيداً من الأول لكنه يمد الاتصال بنوع من القوة والصعوبة في تسريب المعلومات.

من أهم السيرفرات التي يستطيع هذا البروتوكول التعامل معها هي:

Mail – Radius – DHCP – DNS – VOIP Asterisk – Domain Controller

كل هذه السيرفرات تستخدم هذا البروتوكول في عمليات تأكيد الدخول مع ملاحظة انه يمكن وجود اكونت واحد لأكثر من هدف، مثلاً فانه بالنسبة إلى خدمات Google وربط الحسابات لمختلف الخدمات فانك تستطيع ربط حسابك ف الخدمات التالية التابعة له مثل: Gmail – Youtube – Blogspot – Webmaster Tool وهكذا فانه حساب واحد بأكثر من صلاحية حسب التطبيق المرجو منه، هذا أضاف ميزة لكل من Google وكذلك المستخدم، حيث أن جوجل تستطيع عمل خدمات مرتبطة ببعضها البعض وتجذب مستخدمين أكثر وأما بالنسبة إلى المستخدمين فانه من المهم الناحية التنظيمية إذ انه بحساب واحد أستطيع تنفيذ أكثر من مهمة.

مثال عملي:

كما انه من أهم مميزات هذا البروتوكول انه يستطيع ربط الاكونت الواحد بأكثر من سيرفر أو جهاز حيث هذه الميزة جعلت مزودي الخدمة يحتاجونه في تطبيقات كثيرة لديهم، هذه التطبيقات جعلت قسم من أقسامهم مثل Network Operation Center =NOC هذا القسم يكون مسئول عن خدمات الدعم الفني لدى العملاء ولهذا فانه يتطلب الدخول المتكرر على أجزاء وأجهزة معينة لدى هذه الشركات ولذلك الهدف انه نريد امتلاك شئ معين يستطيع إدارة عدد معين من الطلبات لمجموعة معينة من الأفراد تكون لها صلاحيات محدودة لحد ما تمكنهم من القيام بالوظيفة على أكمل وجه.

وكذلك يمكن عمل Group يجمع مجموعة من الأفراد يكون اسمه NOC حيث انه يتم عمل مجموعة من الصلاحيات لهذا الـ Group كله بدلاً من عمل صلاحيات لكل مستخدم على حده، وهذا يوفر في الوقت وكذلك شئ جميل من الناحية التنظيمية.

هدف آخر يدفع الشركات إلى استخدام مثل هذا النوع من البروتوكولات وهو إمكانية عمل حفظ لنسخ احتياطية من بيانات العملاء لديها مع العلم أن الحجم النهائي لهذه الملفات يكون غاية في الصغر.

منن هنا نجد أن هذا المثال يصلح لجميع أنواع الشركات الكبرى لأن تستطيع الشركة من خلاله إدارة كل عمليات تأكيد الدخول سواء على خدمات أو سيرفرات أو راوترات لديها مهما كان عددها وكذلك مع إمكانية المركزية والأمن المتوافر فإنها في مأمن تام من عمليات الاختراق.

إلى هنا نكون قد وصلنا إلى نهاية الموضوع ونتمنى بان يكون أضاف لكم وان شاء الله مستمرين في تقديم المزيد والله الموفق.

بقلم: أيمن النعيمي

طريقة أعداد الـ DHCP Server على أجهزة سيسكو وجونيبر

CISCO JUNIPER

Cisco's IOS

```
Router> enable
Router# config t
Router(config)# ip dhcp pool NetworkSet
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# domain-name mycompany.com
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 100.100.100.1
Router(dhcp-config)# netbios-name-server 192.168.1.2
Router(dhcp-config)#lease 3
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.2
```

Juniper's JUNOS

```
edit system service dhcp]]
set pool 192.168.1.0/24
set address-range low 192.168.1.3 high 192.168.1.254
set maximum-lease-time 14400
set default-lease-time 14400
set name-server 100.100.100.1
set wind-server 192.168.1.2
set router 198.168.1.1
exit
```

أعتقد أن كل الأمور واضحة ومفهومة بأستثناء الأمر الآخير وهو من أجل أستثناء بعض الأيبيات وعدم إعطاءها من قبل السيرفر .

لعرض حالة السيرفر ومشاهدة حالة الأيبيات إستخدم الأمر التالي

Cisco's IOS

```
Router#show ip dhcp binding
```

من أجل متابعة حالة السيرفر أستخدم الأوامر التالية

Juniper's JUNOS

```
show system services dhcp pool
show system services dhcp binding
```

بعض أسرار الأمر Show run على أجهزة سيسكو

قد يلجأ أي شخص يعمل على أجهزة سيسكو إلى أمر الـ Show Run كأول أمر يحاول من خلاله التعرف على مايقوم به الجهاز من عمل لذا فهو يعد من أكثر الأوامر إستخداما لذلك أحببت اليوم أن أقدم لك بعض المعلومات التى تساعدك في إستخدام هذا الأمر واما سبب كتابتي لهذا العنوان (أسرار) فهو بسبب جهل الكثيرين لهذا الأوامر البسيطة ونبدأ بي أول سر سوف أقدمه لك هو كيفية البحث عن كلمة معينة في الأعدادت الموجودة على الروتر وهي تتم من خلال كتابة الإشارة "/" فلو قمت مثلا بكتابة الأمر Show run سوف تظهر لك أول الأعدادات الموجودة كما هو موضح بالصورة

```
Router#show run
Building configuration...

Current configuration : 892 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
!
 --More--
```

وكما تشاهد معي ان آخر كلمة موجودة هي More وهي من أجل عرض المزيد من الأعدادات لذا نحن لن نقوم بالضغط على زر الأنتر أو سبيس بل سوف نقوم بكتابة "/" وبعدها سوف نقوم بأضافة الكلمة التى نريد أن نبحث عنها او التى نريد ان نرى ما هي الأعدادات التى تخصها ولتكن مثلا أعدادات التلنت لذا سوف أكتب بعد الأشارة كلمة line ليقوم بعدها بفلترة الأعدادات وإيجاد الأعدادات التى تخص الكلمة السابقة ولتكن النتائج كما هو موضح بالصورة

```
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
!
/line
filtering...
line con 0
line aux 0
line vty 0 4
!
!
end

Router#
```

السر الثاني الذي سوف أقدمه لك وهو شيء مهم جدا وهو كيف أقوم بعرض كل الأعدادات من دون الحاجة إلى ضغط انتر أو سبيس من أجل عرض الأعدادات بشكل تدريجي وبكلام آخر عرض كل الأعدادات مرة واحدة وهي تتم من خلال كتابة الأمر التالي terminal lenght وبعدها قم بكتابة الرقم صفر لتظهر لك كل الأعدادات ومن دون أي توقف أو Break وسوف تكون صيغة الامر بشكل كامل

terminal lenght 0

السر الثالث وهو من أجل عرض الأعدادات المهمة فقط لان أحيانا تحوي الأعدادات أشياء غير ضرورية مثل الـ Certificate أو encrypt التى تظهر في أول الأعدادات لذا تستطيع أن تقوم بفلترتها مباشرة من خلال كتابة الأمر show run brief ليقوم بعرض الأعدادات من دون ذكر الأشياء السابقة التى تحدثنا عنها

```
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

Router#show run | ?
  append    Append redirected output to URL (URLs supporting append operation
            only)
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output to URL
  section   Filter a section of output
  tee       Copy output to URL

Router#show run |
```

السر الرابع وهو أعتقد ان الكثير منكم يعلمونه وهو أستخدام البايب "|" فهو يقوم بالفلترة بشكل رائع جدا ومفيد مثل أن نخبر الروتر بعرض الأعدادات إبتداء من أو نقوم له أستثني شيء ما أو نقوم بحفظ الأعدادات في ملف معين وهذه الصورة توضح وظيفة كل أمر منها

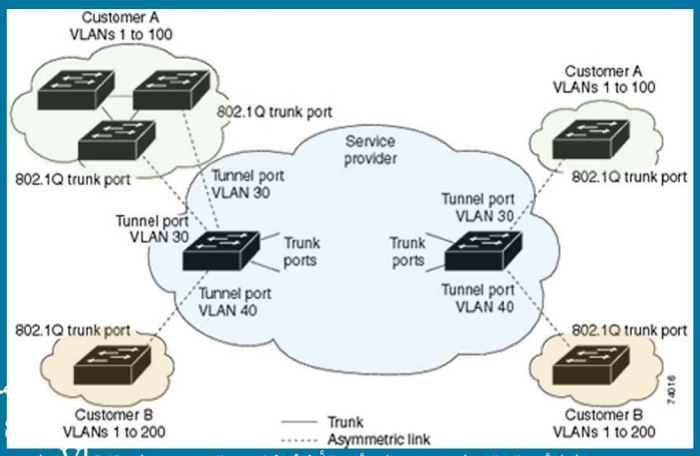
وآخيرا أحب أن أضيف أن هذه الأشياء ليست حصرا على الأمر Show run بل يمكن تطبيقها أيضا على الأمر Show start

مفهوم الـ Vlan في الشبكات البعيدة Wan وكيف يتم نقلها

بقلم: أيمن النعيمي

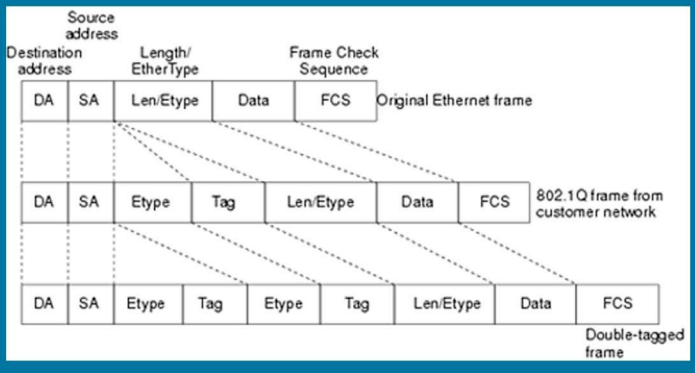
أغلبنا وأن لم يكن كلنا تعلم مفهوم الـ Vlan في الشبكات وجميعنا يدرك حقيقة واحدة وهي أن الـ Vlan يستخدم في شبكات الـ Lan لعزل المستخدمين عن بعضهم بهدف الحماية والامن بالأضافة إلى رفع أداء اشبكة من خلال عزل الـ Broadcast في السويتشات ومن هنا سأطرح عليك سؤالا هل تعتقد أن هناك أمكانية لتفعيل الـ Vlan بين عدة فروع لشركة ما من خلال الـ Wan ؟؟؟الجواب بالتأكيد هو نعم وهو ماسوف أطرحه عليكم في هذا المقال.

بداية أحب أن أوضح شيئ مهم وهو أني لن أتحدث عن طريقة الأعداد لانها لاتعنيني بقدر ماتعنيني فهم إلية العمل وهي تهم مخدمي الأنترنت أو ISP فقط لذا سوف أتطرق إلى المفهوم النظري لسير هذه العملية ولكي نبدأ الشرح لنأخذ هذا الصورة أولا

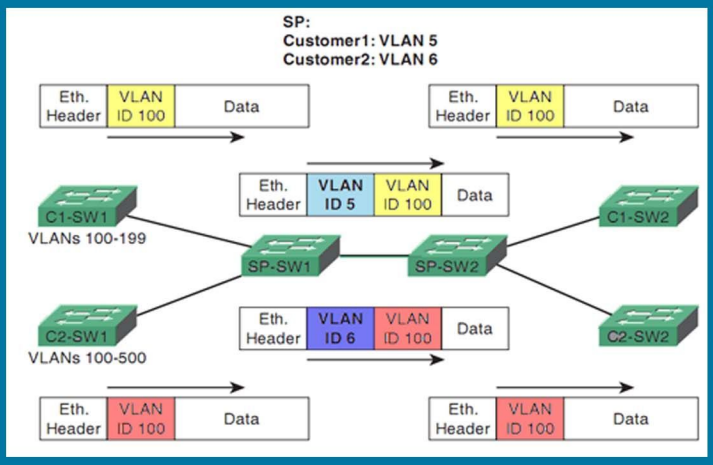


ويريد لها أن ترتبط ببعضها وأن تأخذ نفس تصميم الـ Vlan الموجود في الشبكة الرئيسية أو يريد أن يستفيد من فوائد الـ Vlan من خلال ربط وعزل الأقسام الموجودة في الفرع الرئيسي مع نفس الأقسام الموجودة في الفرع الآخر وطبعا نستطيع أن نقدر مدى أهمية هذا الموضوع بهذا الشكل أو بشكل آخر بحسب مفهومك وتعمقك في مجال الشبكات لذا ماهو الحل ؟ حقيقة الحلول الموجودة كثيرة بعض الشيء يعني على حد علمي هناك ثلاث طرق الأولى من خلال 802.1Q-in-Q أو من خلال (Ethernet over MPLS EoMPLS) والـ VMPLS Vlan MPLS وسوف أتحدث اليوم عن الطريقة الأولى وسوف أترك الطرق الباقية لأشرحها عندما أبدا دراسة كورس CCIP إن شاء الله .

802.1Q-in-Q يمكن أختصارها إلى Q-in-Q ويطلق عليها مسمى آخر وهو Layer 2 Tunneling مفهوم هذه التقنية بسيط جدا ولكي أقدمها لك سوف أطلب منك الأطلاع على هذه الصورة



توضح هذه الصورة ثلاثة أشياء القسم الأول منها يوضح الـ Ethernet Frame الذي يخرج من الأجهزة الموجودة في الشبكة ويتجه نحو السويتش والقسم الثاني يوضح كيفية حقن السويتش للفريم برقم الـ Vlan في خانة الـ Tag أما القسم الآخير فهو يتم من خلال سويتشات مقدمي الخدمة وهو ببساطة يقوم بحقن هذه الفريم بي Tag آخر يحمل رقم Vlan مختلف ومخصص للعميل نفسه ويقوم بأرساله إلى جهاز آخر مربوط مع الفرع الثاني وطبعا يقوم السويتش الثاني بإزالة الـ Tag الثاني ويقوم بأرساله إلى داخل الفرع الثاني لتقوم بعدها سويتشات الفرع الثاني بأرساله إلى الـ Vlan المخصص له وهذه صورة توضح كيفية سير العملية بشكل كامل



ونستطيع أن نلاحظ ان للعميل رقم واحد تم تخصيص الـ Vlan 5 بينما تم تخصيص الـ Vlan 6 للعميل الثاني ولاحظ أيضا أن الأثنان يرسلان نفس رقم الـ Vlan (100) وهذا يقودنا إلى أن أستنتاج أن مقدم الخدمة لايتأثر بي الـ overlapping بين العميلان .

النقطة الآخيرة التى أحب أن أشير إليها وهي أن الـ Q-in-Q يقوم أيضا بنقل الـ CDP and VTP Frame بين الفرعان أيضا وبالتالي أمكانية التحكم في كيفية توزيع الـ Vlan من خلال إعداد أحد السويتشات لكي يعمل كا VTP server

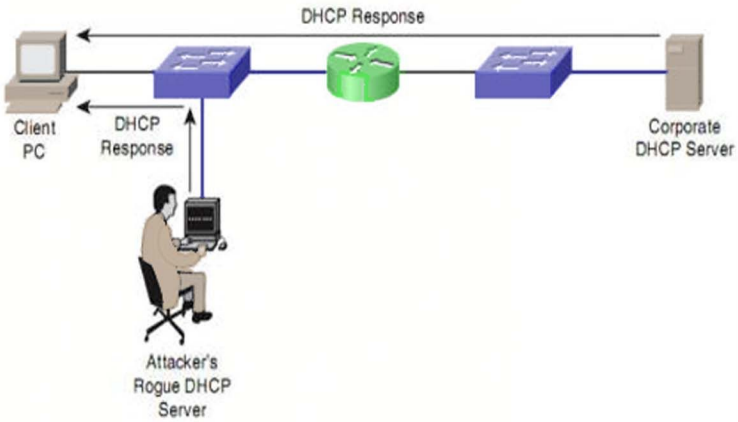
قسم أمن وحماية الشبكات

هذا القسم سوف يتم عرض فيه كل الأمور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التى تحدث على الشبكة وأرجو منك أن تدقق على كلمة تخفيف لان النظرية العامة تقول لايوجد جهاز أمني خالي من الثغرات مهم كانت قوته!

هجوم الـ DHCP Spoofing وطريقة التصدي له

مقدمة عن هجوم الـ DHCP Spoofing

أستكمالا للموضوع الذي بدأته من قبل حول أنواع الهجوم التى تستهدف الـDHCP والذي تحدث في جزءه الأول عن موضوع الـ DHCP Starvation وأثره الضار على الشبكة ونستكمل اليوم حديثنا حول موضوع أخطر من هذا وهو الـDHCP Spoofing والذي يمكن المهاجم من التنصت على كل الترافيك الذي يعبر من خلال الشبكة وبكلام آخر هجوم الـ Man In The Middle

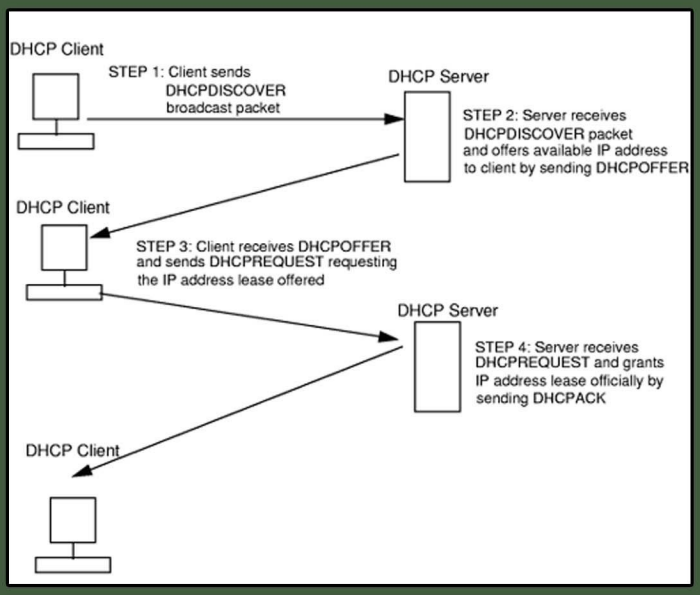


ماهو هجوم الـ DHCP Spoofing ؟ وكيف يتم ؟

يعد هذا الهجوم احد الهجمات الخطيرة على الشبكة والحماية منه أمر مهم جدا على الشبكة وفكرته بسيطة جدا وتنفيذها أسهل وهي ببساطة تقوم من خلال قيام المخترق بتشغيل سيرفر DHCP على جهازه يملك نفس المعلومات التى يقوم السيرفر الرئيسي بتزويدها للأجهزة لكن مع أختلاف بسيط جدا وهو الـ Gateway للشبكة فهو يقوم بتغييره بحيث يكون هو جهازه نفسه ومن خلال أحد البرامج مثل الـ ettercap يقوم بتحويل الترافيك المار عبر جهازه إلى الـ Gateway الحقيقي للشبكة وبهكذا كل مايتم أرساله من خلال الأجهزة الموجودة على الشبكة سوف يعبر من خلال جهاز المخترق ومن خلال أحد برامج تحليل البيانات مثل الـ Wire Shark سوف يشاهد كل تفاصيل الترافيك وطبعا هذه تعد كارثة كبيرة للشبكة وخصوصا أي هجمة تندرج تحت هجمات الـ MITM ولو أراد المهاجم أن يكون الهجوم كاملا فهو سوف يقوم أولا بتنفيذ هجوم الـ DHCP Starvation على السيرفر الرئيسي ويقوم بحجز كل الأيبيات الموجودة عنده وعندها سوف يضمن بأن كل الأجهزة الموجودة على الشبكة وعلى سويتشات آخرى بأنه سوف تلجأ إليه للحصول على المعلومات اللأزمة للأتصال بالشبكة مما يزيد من كمية المعلومات المارة عبر جهاز المخترق وبالتالي دمار أكبر للشبكة

كيفية الحماية من هذا النوع من الهجمات ؟

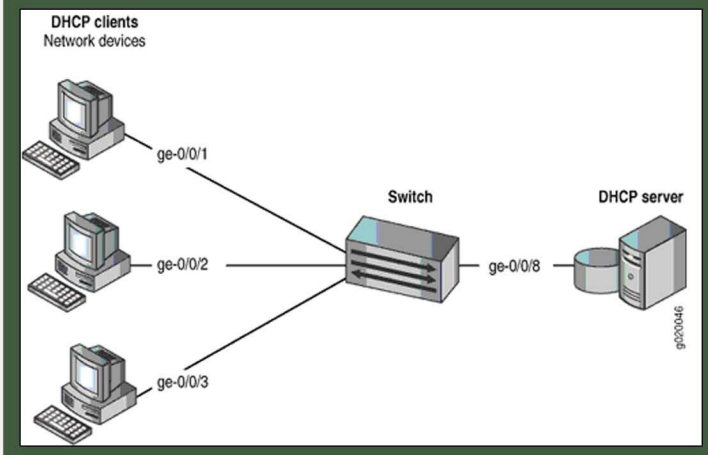
الحل الذي قدمته سيسكو كان عبارة عن خاصية تدعى DHCP Snooping هذه الخاصية ببساطة تعرف السويتش ماهي البورتات الموثوقة وماهي البورتات الغير موثوقة وبكلام آخر تعرف السويتش ماهي المنافذ التى يسمح لها بتوزيع طلبات الـ DHCP فنحن نعلم أن عملية طلب المعلومات من الـ DHCP تمر بعدة خطوات تبدأ بقيام جهاز العميل بأرسال برودكاست إلى الشبكة يسأل فيه عن سيرفر الـDHCP وبعدها يرد عليه السيرفر بعنوان الأيبي الخاص فيه وعندها تأتي خطوة الطلب من العميل إلى السيرفر (طلب الأعدادات) وبعد وصول الطلب إلى السيرفر يقوم بأرسال المعلومات اللأزمة له من أيبي وماسك ودي ان اس وطبعا الـ Gateway وهذه صورة توضيحية لسير العملية



من خلال فهمك لهذه العملية سوف تستنتج معي بأن هذه الخاصية تقوم بأخبار السويتش من هو المنفذ الموثوق والذي يسمح له بالرد على طلبات الـ DHCP التى تتم من خلال المستخدمين الموجودين على الشبكة ومن هنا أتت كلمة Snooping والتى تعني تفتيش أي تفتيش الطلبات ومن أين وصلت والخ.....(لهذه الخاصية إستخدامات جيدة جدا سوف نتعرف عليها تباعا في المواضيع القادمة إن شاء الله)

طريقة الأعداد (سيسكو)

سوف أقوم بكتابة كل الأوامر اللأزمة وبعدها سوف أقوم بتفسير كل أمر على حدى وسوف أستعين أيضا بهذه الصورة التوضيحية




```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10 32 104
Switch(config)#interface range gigabitethernet 0/0/1 – 0/0/3
Switch(config-if)#ip ghcp snooping limit rate 3
Switch(config-if)#interface gigabitethernet 0/0/8
Switch(config-if)# ip dhcp snooping trust
```

أول امر أعتقد بأنه واضح للجميع وهو من اجل تفعيل الـ DHCP Snooping على السويتش وقبل ان نكمل يجب أن نتفق على شيء مهم جدا وهو مجرد تفعيلك لهذه الخاصية على السويتش يقوم هو بشكل أوتماتيكي بوضع كل البورتات على شكل Untrusted أي غير موثوقة

أما في الأمر الثاني فنحن نقوم بتحديد الفي لان التى نريد أن نقوم بتفتيشها وهذا شيء مهم أيضا وأساسي ومن خلا هذا الأمر نستطيع ان نكتب كل الفي لان التى نريدها وقد قمت في هذا المثال بأضافة 3في لان 10,32,104الأمر الثالث من أجل تحديد مجموعة من البورتات وقد أخترت 3منافذ التى تشكل اجهزة العملاء لدي في الشبكة وبعدها أقوم بتحديد عدد الطلبات التى يسمح له بطلبها وهي تحسب بعدد الباكيت كل ثانية PPS ويمكنك زياد هذا الرقم كما تشاء لكن لاينصح بهذا كثيرا وآخيرا أدخل على المنفذ المرتبط مع سيرفر الـDHCP وأخبر السويتش بان هذا المنفذ موثوق به Trusted والسبب أوضحته من قبل

وآخيرا لمشاهدة تفاصيل عن حالة الـ DHCP Snooping نستخدم الأوامر التالي

```
Switch#show ip dhcp snooping
Switch# show ip dhcp snooping binding
```

طريقة الأعداد (جونيبر)

أحب أن اوضح بأن هذه الأوامر لم أقم بتجربتها بشكل شخصي وهي مأخوذة من موقع جونيبر وعلى نفس المثال السابق وهي كالآتي

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/8 dhcp-trusted
set vlan users-vlan examine-dhcp
```

في الأمر الاول أخبرت السويتش بأن البورت 0/0/8بأنه آمن كما فعلنا نفس الشيء مع سيسكو وبعدها أخبرته أن الفي لان التى أسمها users يجب تفتيشها وعلى فكرة هذه الفي لان تجمع الثلاث بورتات السابقة لذلك لايوجد أي سبب لكتابتها مرة ثانية (ياسلام عليكي ياجونيبر)

أنتهى موضوعنا لليوم وأنتظرونا في دروس قادمة تتحدث أكثر عن موضوع الـ Spoofing الذي يحدث على الشبكة ودمتم بود

هل انت مستعد لتصبح محترف سيكورتى و ان تكون هاكر اخلاقى !!!!!!!!!!

هل تعلم ان عملك في مجال الاختراق القانونى يدر عليك اموالا طائلة !!!!!!!!!

الطريق طويل وليس بالسهل لتكون اخصائى سيكورتى و تعمل كاخبير امنى Penetration tester و تكشف الثغرات الموجودة بالشبكات الخاصة بي الشركات .

بداية سوف ينقسم موضوعنا الى عدة حلقات سوف نتكلم فيها عن ما قبل دراسة السيكورتى و متطلباتة الى طريقك للمذاكرة و الشهادات المتاحة لخبير السيكورتى و الهاكر الاخلاقى التعريف بهم تفصيلا و شرح مواضع كثيرة فى السيكورتى و الهجمات المحتملة و شوف اشرح تطبيق بعض الهجمات و الحماية منها .

اولا هل انت مستعد الان لى تكون هاكر او خبير فى الامن و الحماية ؟

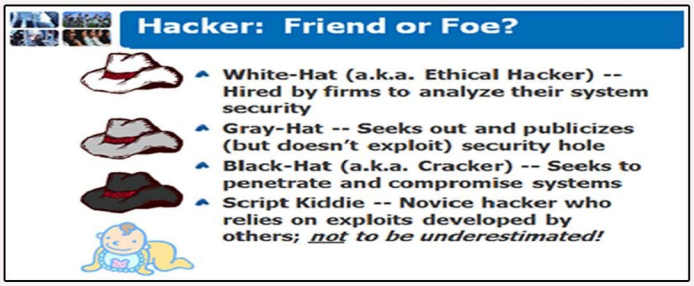
لى الاجابة على هذا السوال يتوجب علينا ان نفهم ما معنى كلمة سيكورتى و انواعها

احب هذة المقولة جدا Security is a process, not a product

اى ان السيكورتى ليس منتج بمجرد ان تضعة فى النتروك و شركتك سوف تحصل على حماية 100% من الاختراقات وليس معنى ان نركب cisco ASA او ISA server او الاثنين معا نكون حصلنا على حماية متاكملة ضد الاختراق بل السيكورتى ليست الا عملية او عمليات نقوم بتنفيذها لتجنب اختراق الشبكة و الحفاظ على بيانات الشركة من الضياع و الاختراق . كما سوف نرى لاحقا ان هناك انواع كثيرة من السيكورتى

فا اولا من هم الهاكرز و ما هى انواعهم ؟

سوف نرى فى الشكل القادم



الهاكر هو بالمفهوم العام ليس بالشخص الشرير و المخرب ولكن هو شخص يحب البرمجة و فاهم جدا لى طبيعة الانظمة بمختلف انواعها أو كما أفضل أن أعبر عنه باللغة الأنكليزية :

A person who enjoys learning details of a programming language or system

و كل جريمته انة احيانا يكون فضول

انواع الهاكرز وهو ما سوف يدور حولة حلقتنا اليوم

1-White Hat

فما هو الا شخص خبير بالانظمة و طبيعتها و لة خبرة بالبرمجة و يستطيع ان يحلل الانظمة و اكتشاف ثغرات خطيرة للدخول على الانظمة بدون اى صلاحيات ومنها الحصول على معلومات لا يحق لة الحصول عليها او تخريبها.

يقوم بتعينة فى الشركة لتحليل نظامها و محاولة اكتشاف ثغرات النظام و بعدها سد هذة الثغرات

2- Gray Hat

هذ الهاكر يصعب تعريفة و تحديد نوعة فهو ما بين القبعة البيضاء و السوداء يصعب تحدد نوعة ولكنهم لا يخترقون بدافع شخصى ولكن بدافع تحقيق حماية افضل .

3- Black Hat

و هو شخص محترف كل عمله تدقيق وتحليل الانظمة و اختراقها و تخريبها بدافع الشهرة او الابتزاز

4- Script kiddie

وهو من وجهة نظرى الاخطر على الاطلاق ويطلق عليهم عادة بى اطفال المخترقين فهم ليس لهم دراية بالأنظمة او البرمجة و الاختراق بشكل عام ولكنهم يذهبوا إلى المواقع الامنية و التى تعلن عن وجود ثغرات و طريقة استغلالها و كل ما هم يفعلونة اختيار هدف عشوائى و يطبقوا علية الهجمة دون اى وعى منهم .

بذلك نكون انتهينا من اولى حلقات الطريق على خبير امن و حماية .

انتظرونى في العدد القادم لكي نتحدث بشكل أعمق حول الأمن والسكيورتي

Cisco Systems

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

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

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

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

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

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

Juniper NETWORKS

Aggregate Half-Duplex Throughput
* 10 Gbps

FPC Slots and Full Duplex Throughput **per Slot**
* 1 built-in, 4 Gbps additional 1 Gbps for FIC

PICs per Chassis
* 4, plus 2 additional fixed FE, or 1 fixed GE ports

Chassis per Rack
* 24

Redundancy
* No

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

Mounting
* Front or center

Maximum Weight
* 38.2 lbs / 17.3 Kg

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

Router M7i

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

Maximum Number of IP Addresses in Trusted Interfaces
Unrestricted

Maximum Throughput
* 10 Gbps FW
* 5 Gbps 3DES VPN

Maximum Number of Sessions
1,000,000

Maximum Number of VPN Tunnels
25,000

Maximum Number of Policies
40,000

Maximum Number of Virtual Systems
0 default, upgradeable to 500

Maximum Number of Virtual LANs
4094

Maximum Number of Security Zones
16 default, upgradeable to 1,016

Maximum Number of Virtual Routers
3 default, upgradeable to 503

Routing Protocols Supported
OSPF, BGP, RIPv1/v2

High-Availability Modes Supported
* Active/Passive
* Active/Active
* Active/Active Full Mesh

IPS (Deep Inspection FW)
Yes

Integrated / Redirect Web Filtering
Yes

NetScreen-5200

Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
* **Junos Software Version Support: Junos Software 9.1**	* Fixed I/O: 4 x 10/100/1000	* BGP, OSPF, RIP, Static, ECMP: Yes
* **Firewall Performance (Large Packets): 600 Mbps**	* Maximum PIM Slots: 3	* Multicast, PIM SM, SSM,IGMP: Yes
* **Firewall Performance (IMIX): 400M**	* Maximum EPIM Slots: 0	* Maximum Number of Security Zones: 40
* **Firewall and Routing PPS (64 Byte): 175, 000 pps**		* Maximum Number of Virtual Routers: Yes
* **3DES and SHA-1 VPN Performance: 140 Mbps**		* Maximum Number of VLANs: 256
* **Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512**		* PPP, FR, MLPP, MLFR, HDLC: Yes
* **Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K**		
* **New Sessions/Second: 5,000**		

Router J2320

Data Rate
* 480 Gbps

Throughput
* 357 Mpps (wire speed)

10/100/1000BASE-T Port Densities
24 (dual-mode 1/10GbE network ports)

10GBASE-X Port Densities
24

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

Resiliency
Dual load-sharing internal autosensing AC power supplies

Power Options
Autosensing; 110/220 VAC; 60/50 Hz

Operating System
JUNOS

QoS Queues / Port
8

Traffic Monitoring
N/A

MAC Addresses
16,000

Jumbo Frames
9216 Bytes

IPv4 Unicast / Multicast Routes
N/A

Number of VLANs
1,024

Switch EX2500

مصلحات تقنية

إعداد: أيمن النعيمي

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

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

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

IS-IS : وتعني Intermediate system to intermediate system وهو أيضا احد بروتوكولات التوجيه ويندرج تحت الـ Linl 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 Intergrated IS-IS يدعم بروتوكول الـ IP

BGP : وتعني Border Gateway Protocol يعد هذا البروتوكول أيضا أحد بروتوكولات التوجيه لكن ليس للأستخدام الداخلي كما هو حال جميع البروتوكولات التى ذكرناها من قبل لانه إستخدامه 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 التى تحدث في عالم الأنترنت مثل تصفح المواقع أو الأتصال عن بعد وهو يعد path-vector ويعتمد على عدة اشياء تدعى Attribute تساعده في أختيار أفضل مسار للباكيت .

EBG : وتعني Exterior Gateway Protocol وهو بروتوكول آخر من بروتوكولا ت التوجيه ويستخدم في الأنترنت وفي الشبكات العالمية وهو بروتوكول قديم وبطئ بعض الشيء ظهر عام 1982 وأحيل للتقاعد بعد ظهور بروتوكول الـ BGP .

مشاكل وحلول

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

سؤال: ما أهمية الـProcess-id في الـOSPF ؟

للأجابة على هذا السؤال يجب أن نعرف أن الـProcsee ID في الـOSPF لايتعلق بباقي الروترات وهو خاص بي الروتر لوحده وبمعنى آخر local to the router only أي أن روتران في نفس الأريا سوف يعملان حتى لوكان الـProcess id مختلف وهي تفيد في حال كان الروتر يملك multiple OSPF على نفس الروتر ونريد أن تكون كل عملية منعزلة عن الآخرى لذا نلجأ لأعطاء كل عملية منها ايدي مختلف عن الآخر والرانج الخاص بها يبدأ من واحد وينتهي بي 65535
والأمر يكتب على الشكل التلي Router OSPF 3
وطبعا الأمر مختلف في EIGRP لان الـProcess idهناك يجب ان يكون موحد على كل الروترات

سؤال: ماهو local port and remote port وماهو الفرق بينهم ؟

جواب: عند دراستك للـOSI Layer وخصوصا في الطبقة الرابعة Transport Layer سوف تجد جوابك وبشكل عام هذه الطبقة كما هو معروف عنها أنها تقوم بتحديد نوع البروتوكول المستخدم TCP أو UDP بالأضافة إلى وظائف آخرى وطريقة الأختيار ترجع إلى نوعية التطبيق الذي تستخدمه فاذا كنت تستخدم تطبيق الـ HTTPوتريد ان تتصفح أحد المواقع فأنت تستخدم أحد البورتات العشوائية الموجودة عندك للأتصال مع البورت 80وكما هو معروف ان عدد البورتات هو 65536أول 1023بورت محجوز لخدمات معينة مثل http,ftp,dns,dhcp الخ .... وباقي البورتات تعتبر للأستخدام العام فمنها من يستخدم لبعض البرامج مثل الماسنجرات أو اي برنامج يتطلب استخدامه الأنترنت
لذا الفكرة ببساطة هي ان local Port هو Source Port الذي يتم كتابته في الهيدر الخاص بي الـTCPاو UDPبينما الـRemote Port هو الـ Destination Port
فعندما تتصفح الأنترنت أو اردت طلب صفحة معينة فأنت تضع في الهيدر الخاص بي الـTCPرقم بورت عشوائي وليكن 1025وهو يمثل السورس بورت أو لوكال بورت بينما تضع البورت 80ليكون هو الريموت بورت أو الـDestination Port والسبب يعود كون التطبيق الخاص بي الـHTTPفي السيرفر الي يحوي الموقع يكون مفتوح على البورت 80ويتسمع على انواع الترافيك الذي يصل اليه وعندما يصل الطلب سوف ينظر الى الهيدر ليكتشف أن هذا الطلب قادم لخدمة HTTPفيأخذ الطلب ويضع المطلوب بداخله ويعيد ارساله لكن هذا المرة سوف يرد بان يضع اللوكال بورت رقم عشوائي بينما الريموت بورت سوف يكون 80

مشكلة :انا عندى فى الشغل روتر سيسكو .1841وأريد أن طريقة أقوم بوصل الأنترنت مع الروتر من خلال مودم DSL فماهي الأعدادات اللازمة للقيام بهذا الموضوع ؟

الحل: كل ماعليك ان تقوم به على الروتر هو default route للشبكة من خلال الأمر ip route 0.0.0.0 0.0.0.0 192.168.1.1بحيث الأيبي يكون أيبي المودم وبعدها أتجه إلى السويتش وقم بكتابة الأمر التالي ip default-gateway 172.16.1.1والايبي طبعا خاص بالمنفذ الموجود على الروتر والمتصل مع السويتش (الخطوة الثانية تقوم بعملها في حال كان السويتش عندك قابل للأعداد)
ملاحظة صغيرة تقنية الـ PAT مفعلة على الروتر By Default