NO. 25 APRIL 2012 • Price Free • www.networkset.net

# NetWork Set

First Arabic Magazine For Networks

## إبدأ شركتك في الشبكات

Samba Server Series

المخاطر التي سوف تواجه الجيل الجديد من الأيبي IPv6

Access Point Modes in Wireless Cisco Network

كيف يعمل SPI Firewall

أنواع الهوائيات

لمحة على الشبكات الأفتراضية

النسخ الاحتياطي مع Windows Server Backup

أهم قواعد الـ Troubleshooting وفقاً لمنظمة compTIA

Bidirectional Forwarding Detection (BFD)

# السنة الثالثة

نحتفل اليوم معا بمرور عامان كاملان على أصدار المجلة والتى تدخل اليوم عامها الثالث على التوالي بدون توقف أو تأجيل واليوم قررت أن يكون إفتتاحية العدد مخصصة للحديث عن المجلة وعن روادها وعن بعض التفاصيل الآخرى.

في 15 نيسان-أبريل من عام 2010 أنطلق العدد الأول والذي كان نتيجة جهد شخصي كامل والحمد لله وبعدها مباشرة بدأت التواصل مع بعض الأخوة والأصدقاء والمهندسين الذين يملكون حب مشاركة المعلومات وإفادة الآخرين وكانت البداية مع المهندس عادل الحميدي والمهندس محمد التميمي والمهندس أحمد الشحات لتبدأ بعدها الأسماء بالزيادة وتبدأ المجلة تتطور عدد بعد عدد حتى وصلنا إلى هذه المرحلة المتقدمة ولله الحمد, أعداد تحميل المجلة كانت معتدلة نسبيا ولم تشهد نقلات كبيرة كونها مجلة متخصصة ولاتصلح لأي مستخدم كمبيوتر أو مهتم في مجال التكنلوجيا كون الهدف الذي وضعته للمجلة منذ البداية كان بين قوسين مجلة متخصصة وليس مجلة عامة لكل الناس فلقد مللنا من الأسلوب التجاري المتبع في بعض المجلات والذي لايقدم أي إفادة حقيقية للعالم العربي سوا تعريفهم بجديد التكنلوجيا (كمادة إستهلاكية) وبعض المواضيع المختلفة والتى تقرأ لمرة واحدة, بينما مجلتنا كانت منذ البداية تهدف إلى أن تكون مرجع دائم لأي شخص مهتم بهذا العالم الكبير, ولكن بشكل عام أعداد تحميل المجلة على سيرفر المجلة تجاوز المليون مرة منذ فترة قصيرة وهذا العدد مرشح للزيادة بشكل أكبر لو جمعنا أعداد التحميل للمجلة على سيرفرات آخرى أو من خلال عملية التبادل المباشر للمجلة بين متتبعيها وحقيقة الرقم بالنسبة لي كبير ولم أتوقع وصولنا إلى هذا الرقم لكن وصلنا بعون الله وتوفيقه وبمساعدة نخبة متميزة من مهندسي الشبكات في العالم العربي ونطمح للمزيد.

الأسماء التى مرت على المجلة كثيرة وسوف أحاول كتابتها جميعها وأعتذر لو في حال نسيت أسم أحدكم فالمراجعة سوف تعتمد على موسوعة الويكي الخاصة بالمجلة وهي كالآتي (مع حفظ الألقاب) : أحمد الشحات, عادل الحميدي, محمد التميمي, ياسر رمزي, عبد المجيد خالد الكثيري, أحمد بخيت, عمر السويدي, أحمد الجلجولي, محمود عمر, عدنان الشمري, محمد عبدون, محمد ناجي سيد, اسلام محمود, أحمد مصطفى, دبالي لحسن, صالح الصافي, صفا الرمضاني, أنس الأحمد, إسلام محمد, علاء مازن عدي, عبد الرحمن بن داود, نادر المنسي, عمرو يحيى, ميثم مرهج, شريف مجدي, عبد الجليل الوكيل, فادي أحمد الطه, خالد عوض, هيثم إسماعيل, رضوان إسخيطة, مصطفى الحسن, هاني محمد, طارق جغايمي, نزار محمود, مالك سمعان, أنس المبروكي, أمجد العبدالله، مصطفى الهواري، محمد جمال ثابت، أحمد فؤاد منصور، علاء معن الشوا، أحمد مصطفى، نورس جربوع، أحمد غزال, أحمد هيكل, سامي خالد الرجعي, أحمد زهران, تميم نايف أحميش, أحمد فؤاد منصور, عثمان إسماعيل.

كما أرغب من خلال هذا المقال بتوجيه رسالة إلى كل المهندسين المحترفين في العالم العربي والذين يملكون الخبرة الحقيقة التى عمرها يتجاوز السنين بان يشاركونا مقالاتهم وخبرتهم فنحن نطمح للمزيد ونرغب برؤية مجلة آحترافية كاملة من أول صفحة إلى آخر صفحة, وأنا أتوقع كما يتوقع الكثيرين بأن للمجلة مستقبل كبير وسوف تصبح في يوما من الأيام الأسم الاول في عالم الـ IT في العالم العربي لذلك أحرص على أن تكون موجود فيها من الآن وخصوصا أن لدي الآن نقاش حول تبني المجلة من قبل مؤسسة كبيرة ومعروفة في العالم العربي وهو مالم أصرح عنه من قبل وأكتبه لكم اليوم كأعلان أول.

وبغض النظر عن نجاح النقاش مع المؤسسة وتبني المجلة سوف تبقى المجلة هي المجلة الاولى عربيا في هذا المجال والتى سوف تصل إن شاء الله إلى قمة المجلات التقنية في العالم العربي والعالمي كون وراءها فريق متحمس ويرغب بنجاحها مهما كانت التكلفة والوقت, فنحن نخدم الامة العربية ونقدم لهم مرجع متخصص بنوايا حسنة وصادقة وغير مادية لأن صفقتنا الوحيدة هي مع الله عز وجل وهي مهما طالت تبقى تجارة رابحة لنا في الدنيا والآخرة, أتمنى فعلا ومن كل قلبي ان تكون المجلة أفادتكم ولو حتى بكلمة واحدة وأن لاتنسونا نحن فريق عمل المجلة من دعوة صالحة بالتوفيق والتيسير لنا في هذه الدنيا المادية الفانية ودمتم بود.

أيمن النعيمي - سوريا

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


## أسـرة المجلـة

### المؤسس و رئيس التحرير

م.أيمن النعيمي

### المحـررون

م.نادر المنسي | م. سامي خالد الرجعي | م.عبد الرقيب عبده صالح الفقيه

م.خالد عوض | م.أحمد زهران | ---

م.أنس المبروكي | م. أحمد سلطان | ---

م. شريف مجدي | م.أحمد عاشور | ---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : عثمان اسماعيل



جميع الأراء المنشورة تعبر عن وجهة نظر الكاتب ولا تعبر عن وجهة نظر المجلة

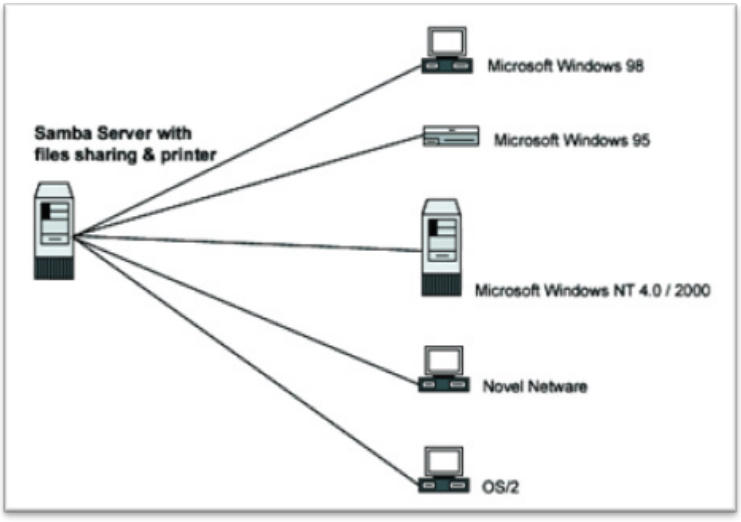
جميع المحتويات تخضع لحقوق الملكية الفكرية و لا يجوز الاقتباس أو النقل دون اذن من الكاتب أو المجلة


www.networkset.net


# Samba Server Series Article 1

فى كل الشركات ستجد انها تعتمد على بيئات مختلفه من انظمه التشغيل فمثلا ستجد ويندوز® سيرفر ويونكس ولينكس لان لكل من هولاء ميزته , فالويندوز® للمستخدمين العادين اسهل, فمثلا محاسب فى الشركه لا يستطيع ان يعمل على اللينكس او اليونكس ولكن الاسهل له هو الويندوز® وعلى الناحيه الاخرى كسيرفر الافضل ان يكون يونكس او لينكس فاليونكس يتمتع بمزايا رائعه كسيرفر لقواعد البيانات او التطبيقات التى تحتاج الى بيئه غايه فى الاستقرار وايضا هناك اللينكس بمميزاته كويب سيرفر. هذا يعنى انه لكل بيئه عمل احتيجاتها الخاصه بها ولكن السوال هنا كيف تتعامل او تفهم هذه البيئات المختلفه بعضها البعض.


حتما انه فى بعض التطبيقات لا يوجد ادنى مشكله فمثلا لو هناك DNS على ويندوز يستطيع اليونكس او اللنكس فهمه لانه DNS برتوكول يعمل من خلال الشبكه بمعنى انه برتوكول فى حزمه برتوكولات TCP/IP لذلك فكل انظمه التشغيل المختلفه تفهمه وتتعامل معه بسهوله اى كان نظام التشغيل الموجوده عليها ولكن هناك ايضا مشاكل تحدث خاصه فى FILE SERVERS فاللينكس واليونكس يستخدمان برتوكول NFS «Network File system» للقيام بهذه المهمه اى لعمل sharing للبيانات الموجوده عليه حتى يستطيع المستخدمين الاخرين سواء كانوا على Unix platform او Windows ® Platform الوصول الى هذه البيانات من خلال الشبكه اما فى الويندوز® فانه يستخده برتوكول اخر وهو DFS «Distributed File System » لذلك فهناك مشكله نظرا لاختلاف البرتوكولات المستخدمه .



# Samba Server Series Article 1

## اذن فما هو الحل ؟

حقيقه هناك حلان لهذه المساله:

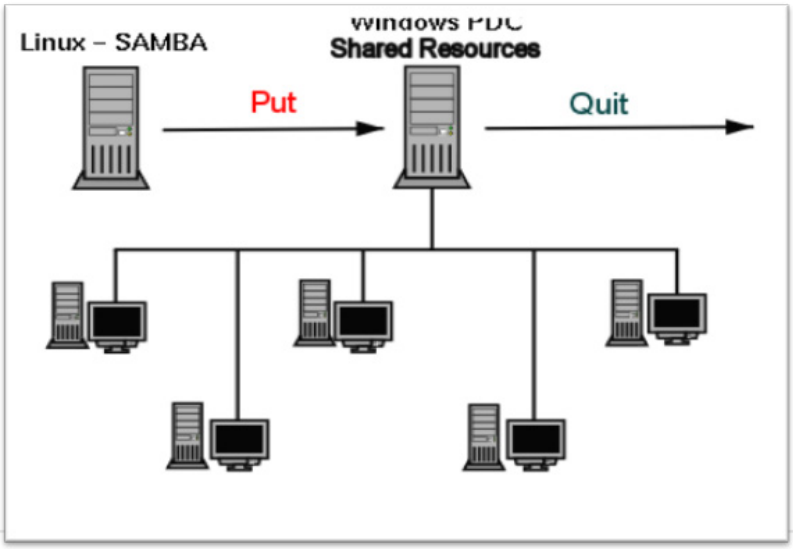
1 - بالنسبه للحل الاول هو انزال agent اسمه services for Unix ® نقوم بانزاله وتنصيبه على كل جهاز ويندوز® او السيرفر الذى يعمل file server حتى يجعل الويندوز® يفهم NFS ولكن المشكله هنا انه بطىء جدا جدا خاصه اذا كانFILE SERVER على لينكس وايضا لو ان هناك مثلا 200 مستخدم ويندوز® فانت ستقوم بتسطيب هذا AGENT على كل هولاء المستخدمين وهذه عمليه فى غايه الصعوبه والارهاق ايضا.

2 - الحل الاخر هو SAMBA SERVER على اللينكس او على ويندوز وهنا انت تقوم باستخدام شىء مثل برنامج يفهم كل من البرتوكلين NFS AND DFS .

وهذا الحل غايه فى الروعه لانه Samba ليست فقط تعمل فى عمليه sharing للملفات فقط لها العديد من الاستخدامات كالتالى :

1. File server
2. Printer sharing: فهى ايضا تقوم بعمل مشاركه للطابعات على الشبكه والتحكم فى الوصول اليها من مختلف انظمه التشغيل الموجوده على الشبكه.
3. Openldap directory:

Ldap فى اللينكس او اليونكس هو مثل Active Directory فى الويندوز® ولكنه اكثر شمولا وروعه فهو يعمل كقاعده البيانات التى يخزن فيها اسماء المستخدمين وحسابتهم وايضا القواعد policies التى تطبق عليهم وهنا يحتاج open Ldap الى samba بجواره فى مثل هذه الاستخدامات. هذه الفكره نستفيد منها فى حاله اذا ما اراد احد ما ان ينقل بيئه عمله من ويندوز ميكروسوفت™ سيرفر الى لينكس ريدهات™ مثلا او اى لينكس اخر .



# Samba Server Series Article 1

## السامبا البدايه وكيفيه الاستخدام:

لقد بدءت السامبا عندما كان هناك استرالى اسمه اندرو يريد ان يقوم بمشاركه sharing طابعه على نظامين احداهما لينكس والاخر ويندوز® وكانت هناك بعض الادوات التى تقوم بمثل هذه العمليه فى هذا الوقت ولكنها كانت غاليه الثمن فبدء فى دراسه طريقه عمل كل من نظامى التشغيل مع الطابعه ومراقبه البرتوكولات المستخدمه فيها ثم انتجت السامبا من هذا الوقت ثم اصبح لها مجتمع community من المطورين يقومون بالتحديث فيها والعمل على الزياده من امكانياتها.

الان تعالوا لنبدء مع السامبا منذ البدايه :

- كيفيه نقوم بانزال السامبا على النظام الذى نستخدمه :

1 - نستطيع انزال السامبا من اى موقع فهى بدون اى مقابل والافضل من الموقع الالكترونى الخاص بها www.samba.org

2 - هى ايضا تكون موجوده مع نظام التشغيل فالانظمه مثل لينكس ubuntu وايضا Unix Solaris® فهى تاتى مدمجه included مع النظام نفسه فكل ما تحتاجه هو ان تقوم بعمل configuration لها حتى تبدء فى العمل مباشره ,» اى انها تكون installed كجزء من النظام نفسه» .

3 - الاشكال التى تكون بها samba package كثيره فهى قد تكون rpm « « Red hat™ package manager وهى هنا ممكن انزالها او تسطيبها على الريدهات لينكس او Unix® AIX فكلاهما يقبلان هذه النوعيه من packages ويكون الامر المستخدم فى عمل تنصيب لها كالتالى :

```
Rpm   -ivh   <path-of-the-package-on-the-system>
```

4 - ايضا قد تكون على هيئه package لها الامتداد التالى .tar.gz والذى يكون مستخدم مع Unix Solaris® ولتنصيب مثل هذه package نقوم بكتابه الامر التالى:

```
tar    -zxvf     samba-version.tar.gz
```

هذه الامر سيقوم بفك الضغط الموجود على package ثم نقوم بالبحث عن ملف يدعى INSTALL او README فسيكون به الخطوات التى يجب اتباعها لتنصبها فيتم تنفيذها.

حاله خاصه :

فى بعض الحالات تكون packages ليست فى صوره binaries فبالتالى لا يتم تنصيبها بالاوامر السابق ذكرها لانه فى هذه الحاله تكون package عباره عن source code نفسه وهنا بالتالى نحتاج الى القيام بعمليه compiling له فى البدايه ثم القيام بعمل تنصيب له وتكون الخطوات كالتالى :

# Samba Server Series Article 1

1 - لو package عباره عن source code of samba. تكون tar.gz الخطوات المتبعه كالتالى:

```
-    tar -zxvf   samba-version.tar.gz
-    ./configure : script inside the package
-     make
-     make install
```

2 - اما لو كانت على هيئه rpm source code فتكون الخطوات المتبعه كالتالى :

```
-      rpm  -ivh   samba-version.src.rpm
-      rpm  -bb   samba-version.spec
-      rpm  -ivh   samba-version.arch.rpm
```

بعد القيام بتنصيب السامبا على السيرفر لديك ستجد انه هناك بعض الملفات زادت فى النظام اهما على الاطلاق smb.conf وهو يكون فى احد المكانين الاتين:

```
1-     /etc/smb.conf
2-     /etc/samba/smb.conf
```

وهذا هو الملف الذى نقوم بكتابه configuration التى نريدها فيه لانه الملف الذى يقرءه samba daemon المسئول عن عمل السامبا سيرفر.

ملحوظه : daemon فى اللينكس او اليونكس هى عمليه لا ينقطع عملها طالما النظام يعمل فهى عباره عن Process تعمل على النظام وفقا لى configuration file خاص بها يوجد به entries التى تحدد طريقه عمله على النظام .

فى مقال قادم ان شاء الله سنعرف كيفيه استخدام السامبا سيرفر فى مشاركه الملفات على الشبكه وايضا محتويات smb.conf .

# NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية

Magazine NetworkSet

أول مجلة عربية متخصصة
في مجال الشبكات

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

أول مشروع عربي لترجمة
المواد العلمية و التقنية

YouTube

قناة المدونة على يو تيوب

قسم خاص بالأسئلة والاجوبة


# الهوائيات
# Antennae

يعتبر الهوائي من أهم العناصر المهمة في الشبكات اللاسلكية لدى المرسل والمستقبل حيث يتم تصنيعها من قبل العديد من شركات التصنيع المتخصصة في صنع الهوائيات تحت معايير عالميه حتى تكون متوافقة معي بعضها البعض .لذلك سوف أحاول في هذا المقال أن أوضح التعريف العلمي للهوائي وأهم الأنواع المستخدمة.

تعريف الهوائي وماهي أنواع الهوائيات ؟

الهوائي هو جهاز يستخدم لتحويل الإشارات الراديوية RF التي تعبر النواقل إلى أمواج كهرومغناطيسية Electromagnetic Wave تنتقل هذه الموجات في الفضاء(الأثير) .

كما تعمل الهوائيات بالاتجاه المعاكس ( عند المستقبل ) حيث تعمل على تجميع الأمواج الكهرومغناطيسية من الفضاء وتحويلها إلى إشارات RF ونقلها الى المستقبل عبر قنة الناقل .

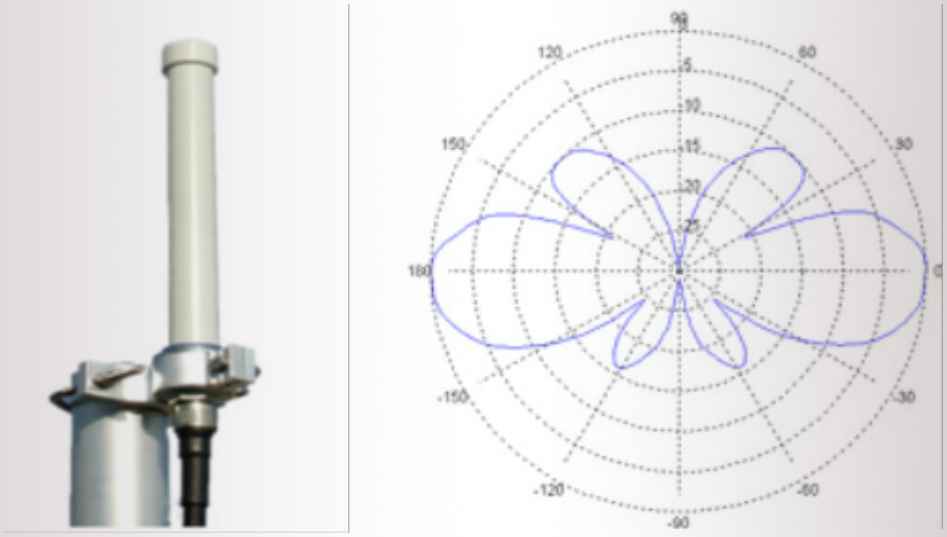
أما بالنسبة لأنواع الهوائيات سيتم توضيحه على النحو التالي :

## أنواع الهوائيات

يمكننا تصنيف الهوائيات ضمن ثلاثة مجموعاتٍ مختلفةٍ تبعاً لطبيعة الاستخدام. تستخدم جميع الهوائيات المذكورة أدناه في الشبكات اللاسلكية الخارجيّة والتي تعرف أحياناً باسم شبكات المناطق الحضرية (Metropolitan Area Networks (MAN .


## أولاً:-الهوائيات متعددة الاتجاهات
## Omni-directional Antennas

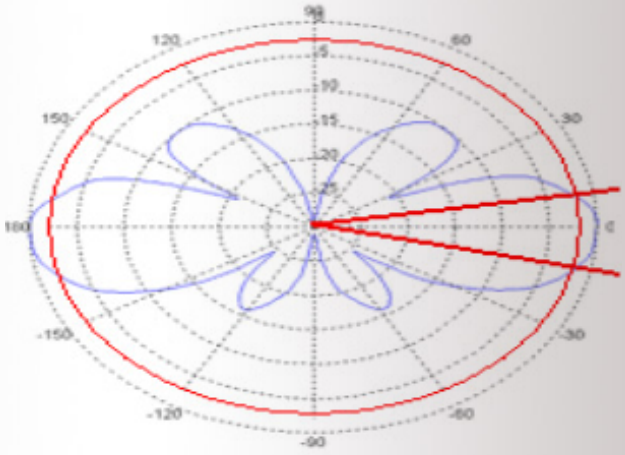
- توصل أحياناً بنقاط الولوج اللاسلكية، وتملك نمط إشعاعٍ يغطّي 360 درجة, تعمل عادةً كمجمعٍ مركزيٍّ أو كبوابةٍ للشبكة.
- تملك الهوائيات متعددة الاتجاهات نمطاً إشعاعياً قدره 360 درجة محيطة بالهوائي، بالإضافة إلى حقل كهربائيً E-field مستقطب شاقولياً. يكون ربح الهوائيّات متعددة الاتجاهات منخفضاً على الأغلب ويتراوح بين 3 – 12 ديسيبل. تستخدم هذه الهوائيّات لبناء الوصلات بين نقطةٍ إلى عدّة نقاط (Point-to-Multi-Point (PtMP وتعمل بشكلٍ جيدٍ لمسافاتٍ تصل حتى 1.5 كيلومتراً، خاصّةً عند استخدامها مع الهوائيّات الاتجاهية عالية الربح في جهة الزبون.



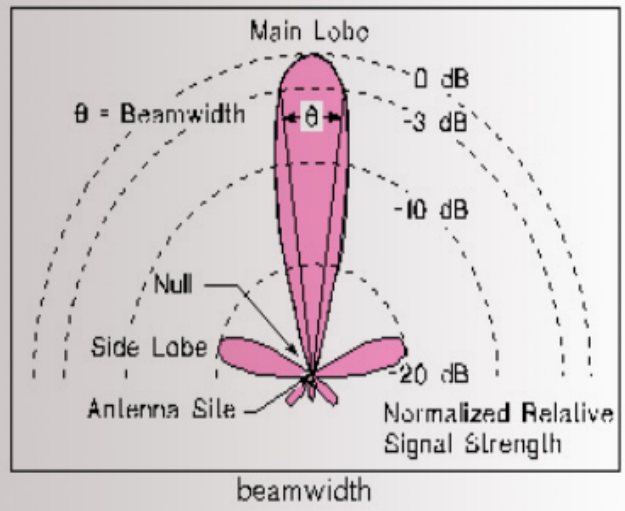
شكل 2: هوائي متعدد الاتجاهات Omni-directional ذو ربحٍ قدره 6 ديسيبل ونمط الإشعاع الموافق

يظهر الشكل 2 أحد الأشكال الشائعة للهوائيات متعددة الاتجاهات من ميزات هذا الشكل من الهوائيّات أنّ مقدار تغطيتها لا يبلغ 360 درجة لكنّها توفّر تغطيةً جيّدةً للزبائن الواقعة ضمن مجالها الأفقي + / - 20 درجة. مما يعني أنّ هذا الهوائي في حال تركيبه على قمة برجٍ ما قد لا يتمكّن من تغطية الزبائن المتواضعة في أعلى أو أسفل البرج مباشرةً. يمكننا باستخدام نمط الإشعاع الموضّح في الشكل 2 حساب المجال الأمثل لزوايا القطّاع الأفقي الذي يعمل هذه الهوائي ضمنه. يعرف هذا المجال بعرض الإشعاع Beamwidth ويشير إلى الفتحة الزاويّة التي يتم ضمنها إشعاع القسط الأكبر من القدرة. من أكثر القيم شيوعاً لهذه الفتحة 3 ديسيبل والتي تمثّل الفتحة الزاويّة (بالدرجات) التي يتم ضمنها إشعاع ما يزيد عن 90 ٪ من القدرة. تبلغ الفتحة الزاويّة الموافقة للقيمة 3 ديسيبل في مثالنا هذا حوالي 22 درجة، من – 10 درجات إلى + 22 درجة.

**كقاعدة عامة : كلما ازداد ربح الهوائي متعدد الاتجاهات كلما صغر عرض الإشعاع الموافق.**



شكل 3 : حساب عرض الإشعاع الموافق للقيمة ديسيل ( 10+ ، 12- درجة )




شكل 4: تظهر الصورة عرض الإشعاع لهوائيٍّ مقارنةً مع ربح هذا الهوائي. كلما ازداد ربح الهوائي كلما صغر عرض الإشعاع الموافق

## ثانياً:- الهوائيات القطّاعية
## Sectorial Antennas

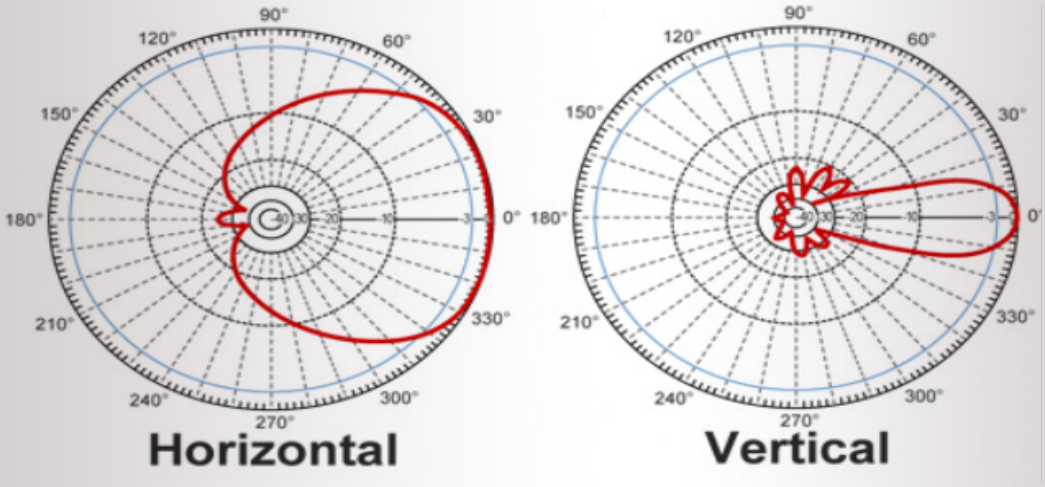
تستخدم الهوائيّات القطّاعيّة (تماماً كما هي الحال في الهوائيّات متعددة الاتجاهات) مع نقاط الولوج اللاسلكية لتخديم الوصلات من نقطةٍ إلى عدّة نقاط Point-to-Multi-Point (PtMP). توجد الهوائيّات القطّاعيّة باستقطابٍ أفقيٍّ أو شاقوليٍّ تبعاً للتقنيّة المستخدمة في التصنيع.

تملك الهوائيات القطّاعيّة عادةً ربحاً أكبر من نظيراتها متعددة الاتجاهات (في المجال 10-19 dBi) في قطّاعٍ أصغر، وتستخدم عادةً لتخديم مناطق تصل حتى 6-8 كيلومتر.

من القيم الشائعة للهوائيّات القطّاعيّة ربحٌ قدره 14 dBi لعرض إشعاعٍ أفقيٍّ يعادل 90درجةً وعرض إشعاع شاقولي يعادل 20 درجةً. يمكن الحصول على قيم أعلى للربحِ في الهوائيّات عبر تضييق عرض الإشعاع الأفقي Horizontal Beamwidth.

يمكن كما هو موضّحٌ في الشكل 5 بناء الهوائيّات القطّاعيّة باستخدام هوائي متعدد الاتجاهات ذو استقطابٍ شاقوليٍّ بالإضافة إلى عاكسٍ على شكل حرف V.

شكل 5: هوائي قطّاعي
Sectorial Antenna (A2.45LP14 180°)



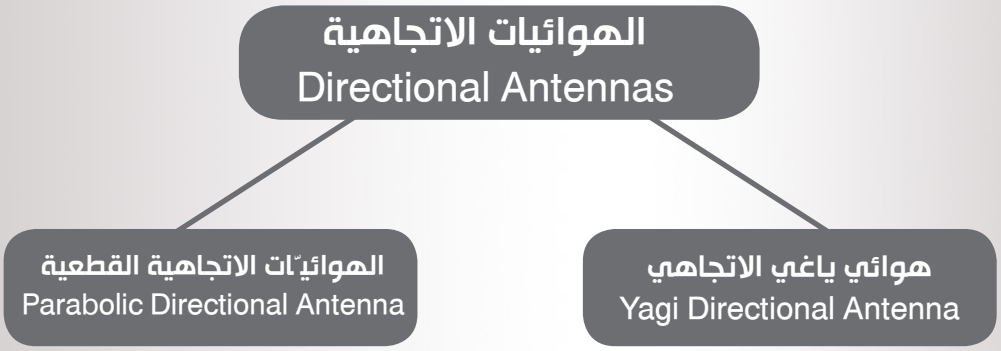

شكل 6: نمط الإشعاع النموذجي لهوائيٍّ قطّاعيٍّ (المصدر: Hyperlink)

يظهر الشكل 6 نمط الإشعاع النموذجي لهوائيٍّ قطّاعي. يتضح من نمط الإشعاع الأفقي أنّ مقدّمة الهوائي تقوم بإشعاع القسط الأكبر من القدرة. يتوقّع إشعاع جزءٍ صغيرٍ جدّاً من القدرة خلف الهوائي القطّاعي. يشبه نمط الإشعاع الشاقولي إلى حدٍّ كبيرٍ الهوائي متعددً الاتجاهات حيث يكون عرض الإشعاع ضيّقاً جدّاً ولا تتجاوز منطقة التخديم 20 درجة. يتم تثبيت الهوائيّات القطّاعيّة عادةً في أعلى برجٍ مرتفع يميل قليلاً للتمكّن من تخديم المنطقة الواقعة تحت البرج.

## ثالثاً:- الهوائيات الاتجاهية
## Directional Antennas

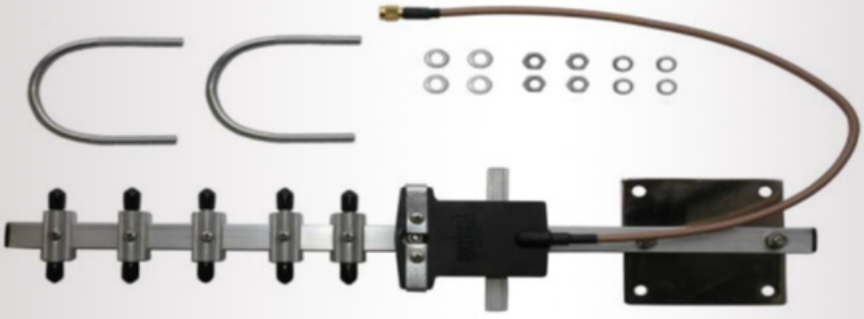
تستخدم الهوائيّات الاتجاهية على الأغلب في مواقع الزبائن أو كجزءٍ من شبكةٍ بعيدة المدى تصل بين عدّة نقاط Backhaul. يتم توجيه الهوائيّات الاتجاهية في موقع الزبون باتجاه نقطة الولوج المركزيّة (المجمّع).

يعتبر النوعين التاليين أكثر أشكال الهوائيّات الاتجاهية شيوعاً:




### هوائي ياغي الاتجاهي
### Yagi Directional Antenna

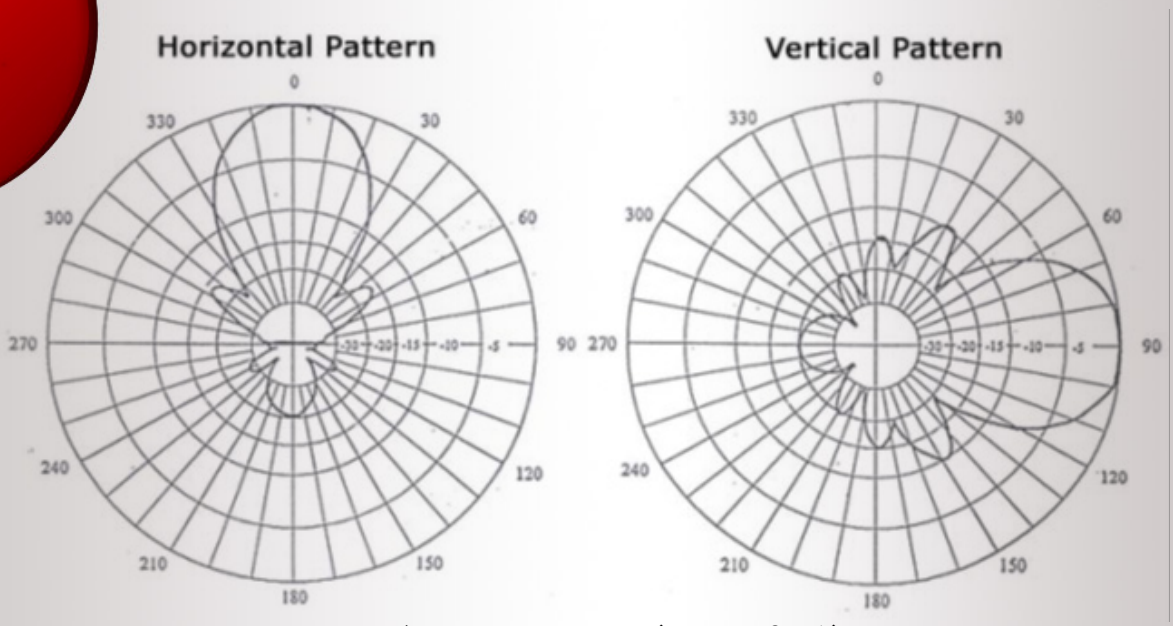
يتألّف هوائي ياغي من هوائيٍّ (ثنائي القطب Dipole) بالإضافة إلى مجموعةٍ من عناصر التوجيه المركّبة أمامه و(اختياريا) عاكس. تتم إحاطة الهوائي عادةً بأسطوانةٍ بلاستيكيّةٍ لحمايته. عرف أسطوانة حماية الهوائي عادةً باسم radom (radar dome) وهي عبارةٌ عن علبةٍ مقاومةٍ للعوامل الجويّة تستخدم لحماية الهوائي من الأمطار، الجليد، الثلج أو العواصف الرملية.



شكل 7: هوائي ياغي الاتجاهي من طراز Terabeam Wireless P2412 (يركّب ضمن أسطوانة حمايةٍ بلاستيكية)

كلمّا ازداد عدد عناصر التوجيه أمام المشعّ كلّما ازداد ربح الهوائي. يمتلك هوائي ياغي الاتجاهي عادةً ربحاً يتراوح بين 7 إلى 19 dBi. يظهر الشكل 7 هوائياً إتجاهيّاً من نوع ياغي طراز 2.4 GHz P-2412 ذو ربح قدره 12 dBi.

يبيّن الشكل 8 نمط الإشعاع النموذجي لهوائي ياغي الاتجاهي. تتميز هذه الهوائيّات بتشابهٍ أنماط الإشعاع الأفقي والشاقولي. يتجّه كلٌ من نمط الإشعاع الأفقي والشاقولي باتجاه عناصر التوجيه، ولا يتم إشعاع أيّ قدرةٍ بالاتجاه الذي يقع خلف الهوائي. كما هو الحال في جميع الهوائيّات، كلّما ازدادت زاوية الإشعاع كلّما انخفض ربح الهوائي. في حالة هوائيّات ياغي الاتجاهية، كلّما قصر الهوائي (أي احتوى على عددٍ أقل من عناصر التوجيه) كلّما ازداد عرض منطقة التخديم.



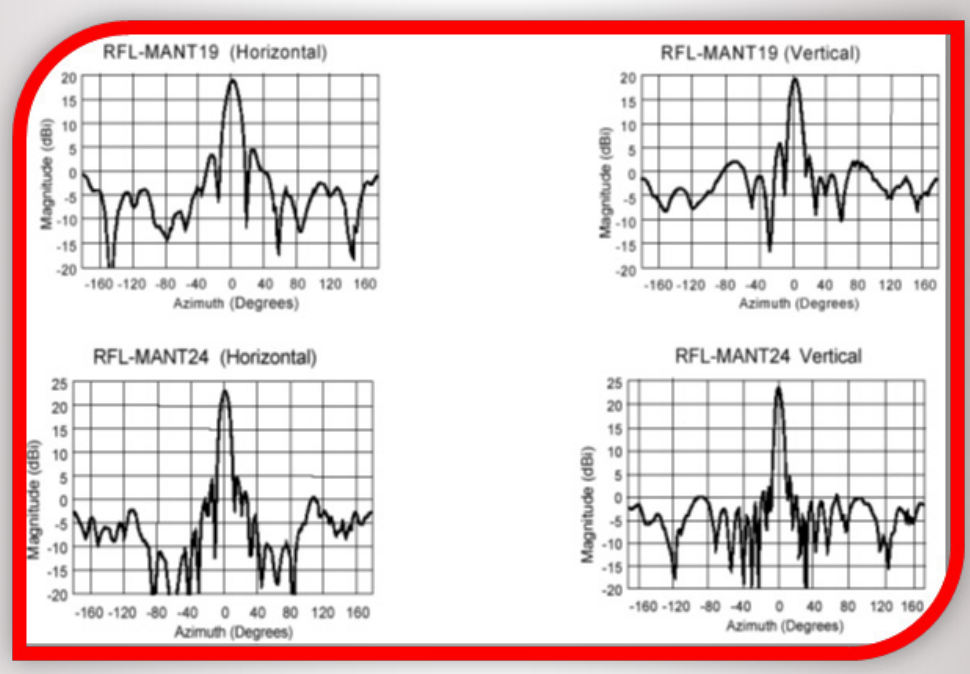

شكل 8: نمط الإشعاع المعياري لهوائي ياغي الاتجاهي

## الهوائيات الاتجاهية القطعية
## Parabolic Directional Antenna

يصعب الحصول على أرباح عاليةٍ (تفوق 14 dBi) بالتوافق مع أنماط إشعاع جيّدةٍ باستخدام هوائيات ياغي الاتجاهية. لذلك يشيع استخدام عاكس للأمواج اللاسلكية على شكل قطعٍ مكافئ (ثنائي القطب Dipole).يملك الهوائي القطعياً ربحاً يتراوح بين 16-28 dBi.

يشابه نمط إشعاع الهوائي القطعي نظيره في هوائيات ياغي الاتجاهية إلا أنه يغطي منطقة تخديم أضيق بكثير. من الصعب جداً توجيه الهوائيّات القطعية نظراً لتوجّه الإشارات اللاسلكية التي ترسلها إلى منطقة تخديم ضيقة للغاية، وبالتالي تعتبر هذه الهوائيّات أكثر حساسيّةً للاضطراباتً الفيزيائيّة والميكانيكيّة، خصوصاً الرياح الشديدة، من هوائيّات ياغي الاتجاهية. لا تعتبر الهوائيات القطعية خياراً جيّداً للوصلات قصيرة المدى (أقل من 2 كيلومتر) بسبب ربحها العالي والذي قد يتسبّب في زيادةٍ كبيرةٍ غير مبررةٍ في قدرة الوصلة اللاسلكية.

يظهر الشكل التالي (10) أسلوباً آخر لتمثيل أنماط إشعاع الهوائيّات. يوضّح الشكل أنماط الإشعاع لهوائيين من نفس الطراز ولكن يملكان ربحين مختلفين (19 dBi و 24 dBi). نلاحظ أنّه وعلى الرغم من التشابه الشديد بين الأنماط الأفقيّة والشاقوليّ إلا أنّ الهوائي ذو الربح 19 dBi يملك زاويةً أوسع لعرض الإشعاع Beamwidth المكافئ للقيمة 3 ديسيبل (17 درجة) في مقابل (8 درجات) للهوائي ذو الربح 24 dBi.




شكل 10: أنماط الإشعاع لهوائيين من طراز RFL-MANT ذوي ربحٍ قدره 19dBi و 24 dBi

لقد وضحنا في مقالنا هذا انواع الهوائيات لمهندسين الشبكات حتى يستطيع ان يفرق بشكل ممتاز كيفية استخدام الهوائي كذلك استخدام الهوائي المناسب في المكان المناسب حسب الطلب من أجل تحقيق الأهداف المناسبة , حيث يوجد هناك العديد من التفاصيل حول عمل واستخدام الهوائيات سنتطرق اليها أنشاء الله في المقالات القادمة . وبهذا نكون قد انتهينا والسلام عليكم ورحمة الله .....

Magazine
NetworkSet
First Arabic Magazine for Networks

ضع أعلانك معنا وساهم في
تطوير واستمرارية أول مجلة عربية متخصصة


انتشار واسع - تغطية شاملة

حزم اعلانية مختلفة تناسب جميع الاحتياجات


# النسخ الاحتياطي مع Windows Server Backup

مقدمة :

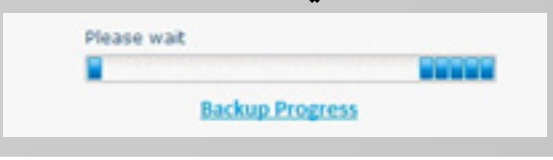

في الإصدارة الجديدة من ويندوز سيرفر وهي W2k8 وايضا W2k8 R2 قامت مايكروسوفت بإضافة ميزة الـ Windows Server backup من أجل ان تجعلك قادر على أخذ نسخ احتياطية ومن ثم استرجاعها وتشمل استرجاع نظام التشغيل والبرامج والبيانات . وعندما تستخدم هذه الأداة التي تأتي مع الويندوز وانت تقوم بإضافتها عن طريق إضافة ميزة Add Features تستطيع ان تحسن عمل الشركة التي تعمل لها عن طريق عمل استعادة للبيانات المفقودة ، وعن طريق هذه الأداة تستطيع أن تعمل لما تريد نسخ احتياطي وايضا اين تقوم بتخزينه وكيف تستطيع عمل استرجاع لها ..

## نظرة حول Windows Server backup

كما قلنا هيا عبارة عن ميزة ومجموعة من الـ Wizards والأدوات لكي تعمل نسخ احتياطي للخوادم servers وهذه الميزة قامت مايكروسوفت بعمل لها تحديث لها في الـ R2 وهي نزلت مع server 2008 . وكما نعلم انه كانت ميزة الـ NTBACKUP في server 2003 وقاموا بحذفها في الـ server 2008 .

عندما نقوم بعمل استعاده للـ Objects عن طريق الـ Windows Server backup فإنها تعود مع بقاء كل الـ attributes والتي هيا خواص الـ Object وتوفر عليك عنا اسناد كل تلك الخواص مرة أخرى على سبيل المثال اسناد مستخدم إلى مجموعة معينة .

عندما تعمل على الـ Windows Server backup من الممكن ان تعمل التالي :




- من الممكن عمل نسخ احتياطي للسيرفر ككل ، وهذا يشمل نظام التشغيل .
- ممكن عمل نسخ احتياطي لبيانات لحالة النظام (System State Data) ، وهي بيانات تحتوي على إعدادات السيرفر وايضا قاعدة بيانات الدليل التي هيا الـ (Ntds.dit) .
- من الممكن عمل استعادة للبيانات الغير موثوقة او كما تسمى بالـ non authoritative data ، وهيا بيانات سوف تضاف إلى الـ Domain Controller لكن عندما يحدث تحديث للبيانات Replication على سبيل المثال من Additional Domain Controller سوف تعود لحالتها الأولى
- من الممكن عمل استعادة للبيانات الموثقة authoritative data ، وهيا بيانات سوف تضاف إلى الـ Domain Controller لكن ستعمل على تحديث كل

الـ DCs الأخرى عن طريق الـ Replication .
تستطيع عمل نسخ احتياطي الـ GUI الخاصة بي الـ Windows Server backup أو عن طريق الـ CLI باستخدام الـ Wbadmin.exe . وايضا النسخ الاحتياطي ليس منفصل فهو يعمل Capture للأقسام الحساسة وهي تشمل التالي :-

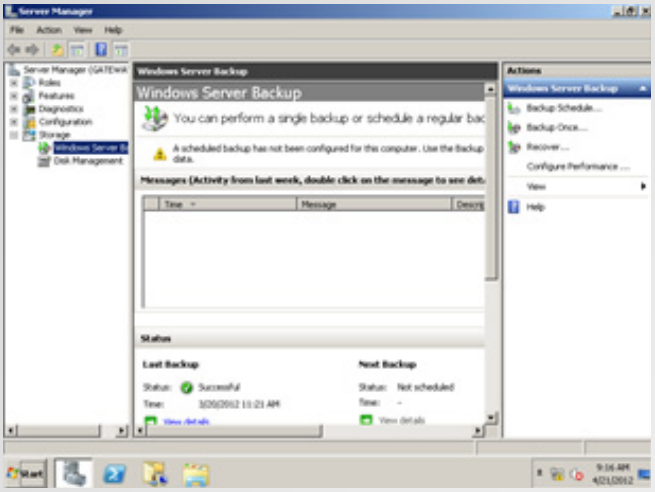
- قسم النظام
- القسم الذي يحتوى على ملفات الإقلاع Boot Files
- القسم الذي يحتوى على ملف الـ Sysvol
- القسم الذي يحتوى على قاعدة بيانات الدليل Ntds.dit
- القسم الذي يحتوى على ملفات الـ Logs

ومن المؤسف انك لا تسطيع عمل نسخ احتياطي إلى Tape Drives أو Dynamic Volumes التي هي عكس الـ Basic Volumes . انت تستطيع عمل نسخ احتياطي إلى Network Drives ، أقراص صلبة خارجية وايضا Basic Volumes ، أو DVDs and CDs .

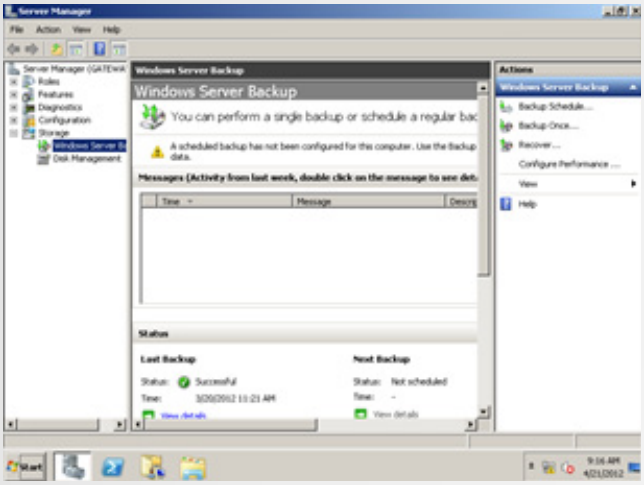
وايضا لا تستطيع عمل نسخ احتياطي لملفات منفصلة ، فقط تستطيع عملها للأقراص كاملة فقط backups full volume . وايضا الأعضاء المتواجدين في مجموعة الـ Backup Operators لا يستطيعون عمل نسخ احتياطي مجدول اي كل فترة زمنية وانما اعضاء الـ Domain Admin Group هم من يستطيعوا عمل هذا الشيء .

اعتقد إلى هنا كفاية كلام ..
عمل نسخة احتياطية للنظام ككل Full System Backup :-
من الممكن عمل نسخة احتياطية للنظام ككل أو عن طريق جدولة معينة ، واي طريقة من الطريق من الممكن عملها عن طريق الـ GUI أو الـ CLI ، وسنستخدم طريقة الـ GUI . بعد تحميلنا لميزة Windows Server backup والتأكد من تنزيلها بشكل جيد كما في الصورة

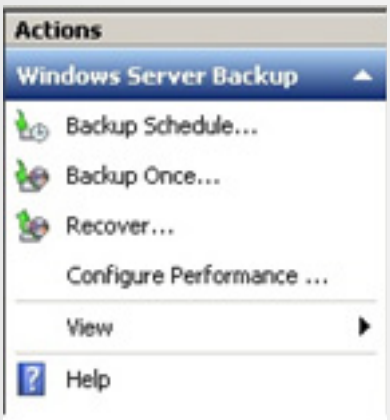
نقوم بعدها بفتح الواجهة من الـ Server Manager ونختار تحت الـ Storage الـ Windows Server backup ستظهر لنا النافذة التالية



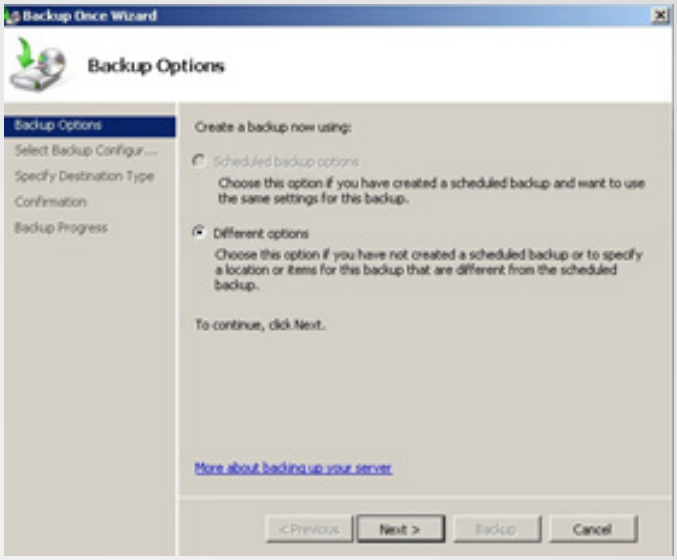

نقوم بعدها بفتح الواجهة من الـ Server Manager ونختار تحت الـ Storage الـ Windows Server backup ستظهر لنا النافذة التالية



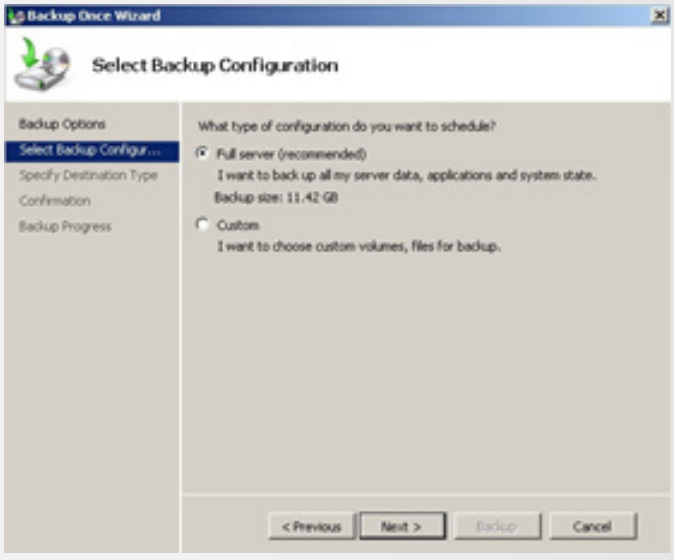

وتأكد من انك عامل login بصلاحيات الـ Domain Admin ، ومن القائمة التي على الجهة اليمنى نختار Backup once كما في الصورة



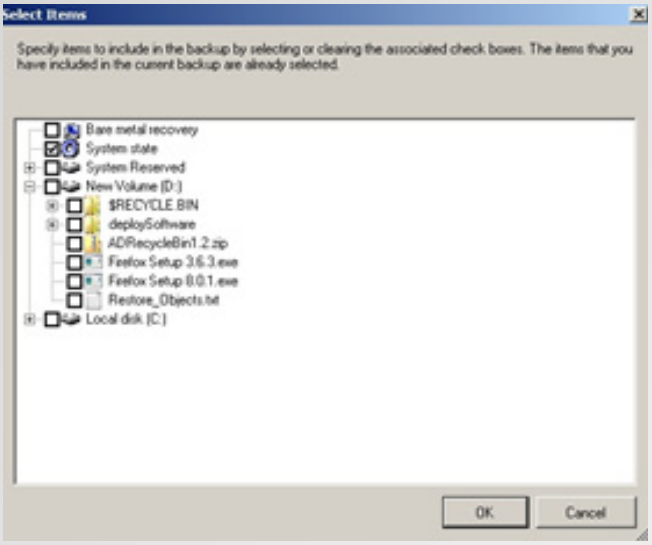
واذا كنا قد عملنا نسخة احتياطية مجدولة من قبل ستلاحظ خيار الـ Scheduled Backup Options محفز ونستطيع اختياره ، ولكن هنا نحن نعمل لأول مرة فنختار الخيار Different Options ثم نضغط Next كما في الصورة




ثم نختار Full Server (Recommended) ثم نختار Next كما في الصورة

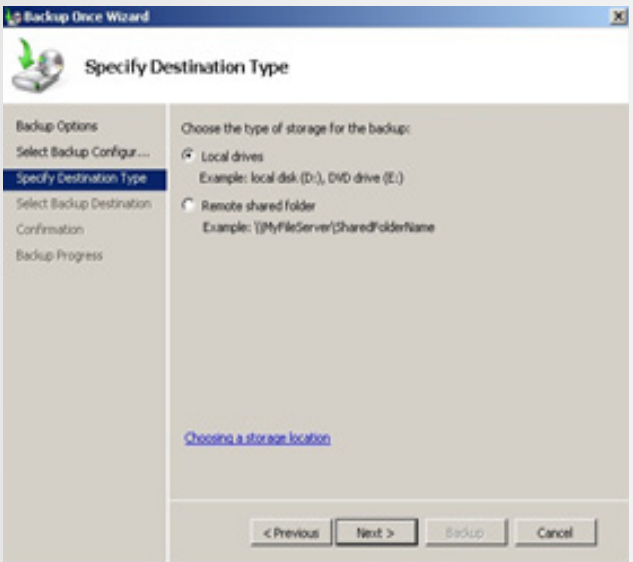



لاحظ انك كنت من الممكن ان تختار Custom وعند اختيارك له والضغط على Add Items تستطيع تحذف اي شيء مثل حذف قسم وتستثنيه من عملية النسخ الاحتياطي أو حذف مجلد او ممكن أن تختار فقط حالة النظام كما في الصورة وكما ذكرناها سابقا

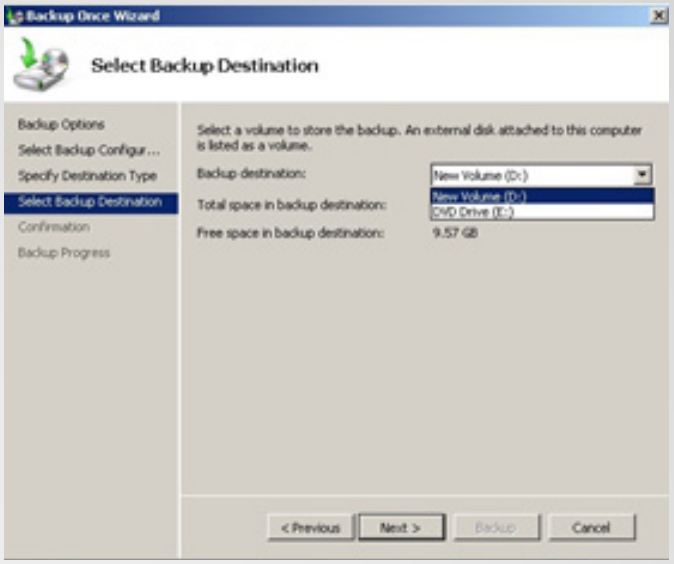



ولاحظ ايضا عند اختيارك Custom من الممكن ان نختار الخيار الذي يدعى Bare Metal Recovery والذي يعمل تلقائيا بنسخ كل البيانات المطلوبة لعمل استعادة للنظام ككل Full System .

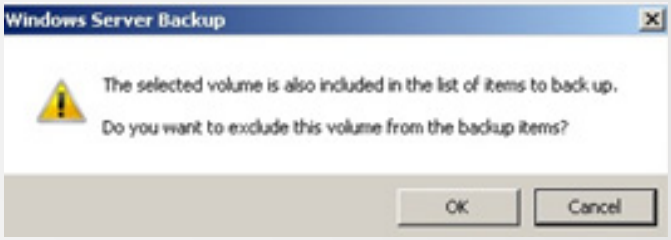
بعد ان اخترنا (Full Server (Recommended ثم Next نقوم بتحديد الوجهة Destination من الممكن أن تكون على الفرص المحلي Local Drive أو على الشبكة كما في الصورة ثم نضغط Next




اذا قمت باختيار الـ Local Drive قم أيضا باختيار القرص المناسب ولاحظ انك لا تستطيع أن تختار القرص الذي يتواجد به نظام التشغيل ، وتأكد ان القرص فيه مساحة كافية ثم أضغط Next



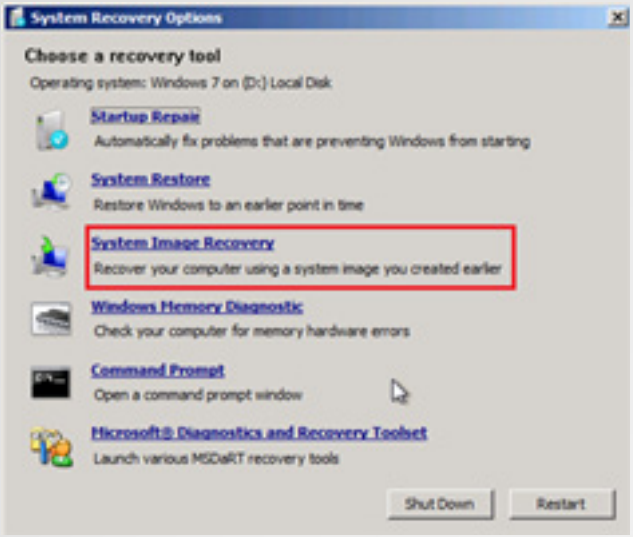

وعندما تختار الخيار Full Server البرنامج يحذرك برسالة مفادها ان القرص الذي أخترته لتخزين النسخة الاحتياطية علية هو ايضا من ضمن النسخة فيجب عليك الضغط على OK ليتم استثناء القرص ليتم عمل النسخة كما في الصورة




وأخيرا نضغط على Backup لبدأ عملية النسخ الاحتياطي ، ثم أضغط Close لأنك لا تحتاج لإبقاء نافدة النسخ مفتوحة لتتم عملية النسخ الاحتياطي لأنه سوف يستمر في العمل خلف المشهد ، ويجب عليك ان تراقب العملية مرة على الأقل

ولنتجه الان إلى عمل استعادة للنظام في حالة ان النظام وقع فيه اي مشكلة .

ولعمل استعادة للنظام نقوم بإدخال قرص الـ Windows Server ونعمل إعادة تشغيل للنظام ونقوم بالإقلاع من الـ DVD ، في أول نافذة تظهر لك نختار اللغة المناسبة والوقت المناسب وشكل العملة وشكل لوحة المفاتيح ثم نضغط Next ، في نافذة التحميل نضغط على Repair Your Computer في ، في نافذة الـ System Recovery Options تحت Choose A Recovery Tool نختار الخيار System Image Recovery كما في الصورة




ومن ثم أختار Select A system Image ثم أضغط Next ، في نافذة اختيار الموقع Select The Location اذا النسخة موجودة على الـ Local Computer وهذا الذي عملناه نقوم باختيار موقع القرص الذ فيه النسخة الاحتياطية ثم نضغط Next ، ثم نختار الوقت والتاريخ الذي عملنا فيه النسخة الاحتياطية ، اذا كنت تريد ان تعمل استبدال كل البيانات في كل الأقراص أختار من نافذة الـ Choose Additional Restore Option قم باختيار Format and Repartition Disks ، ثم أضغط على Next ثم Finish بعد ذلك قوم بالتأكيد واضغط على Yes .

وعندما تتم عملية الاسترجاع كاملة الخادم Server يجب ان يعمل إعادة تشغيل من أجل أن تتم عملية الاستعادة والعملة على النسخة الجديدة ..

شكرا لكم ونلتقى في العدد القادم ان شاء اللّه ..


# أهم قواعد الـ Troubleshooting وفقاً لمنظمة compTIA ؟

أثناء قرأتى لمقال المهندس أيمن النعيمي بعنوان (عيادة... أجهزة أكس بي لاتدخل على شبكة الوايرليس) و اتضح ان المشكلة تكمن فى تحديث تعريف كارت الوايرليس خطر على ذهني عمل مقال عن قواعد الـ Troubleshooting,التى تعلمتها أثناء دراستي لشهادة compTIA A+ وهو ما يعرف بنظرية استكشاف الأخطاء وإصلاحها (Troubleshooting Theory ) قبل ان اخوض فى التفاصيل احب ان وضح شئ مهم ان هذه الخطوات هي خطوات قابله للتغير و التبديل و من الممكن ان ترى نظريات افضل منها, اما هذه الخطوات فهي خاصة بأمتحان شهادة compTIA A+ . و سوف اتناول شرح هذه النظرية و خطواتها

تعريف النظرية : نظرية حل المشاكل هى مجموعة من الخطوات العقلية التى تستخدمها فى عملية الحوسبة لتشخيص وإصلاح جهاز الكمبيوتر ، وتتضمن التحدث الى المستخدمين ، تحديد كيف ومتى حصلت المشكلة ، تحديد السبب ، مرحلة الاختبار ، التحقق ، توثيق النتائج ، و من يركز فى هذا التعريف يستطيع ان يحدد هذه الخطوات و هى كالتالي

1- التعرف على المشكلة .
( Identify the problem )
2 - وضع نظرية للسبب المحتمل . ( السؤال الواضح )
Establish a theory of probable cause -)
( Question the obvious
3 - إختبار النظرية لتحديد السبب .
( Test the theory to determine the cause)
4 - وضع خطة عمل لحل المشكلة و تنفيذ الحل .
Establish a plan of action to resolve the)
( problem and implement the solution
5 - التحقق من كامل وظائف النظام و اذا وجدت تدابير وقائية غير مطبقة يتم تنفيذها .
Verify full system functionality and if applicable)
( implement preventative measures
6 - توثيق الاستنتاجات و الاجراءات و النتائج .
( Document findings , actions , and outcomes)

بعد ان وضحت هذه الخطوات ليس من الضروري تكون خطوات يمكنك ان تزيد عليها و تغير فيها على حسب طبيعة عملك و المكان الذى تعمل فيه كما اوضحت سابقاً و سوف اقوم بشرح كل خطوة على حدى.....

## التعرف على المشكلة

في هذه الخطوة نقوم بجمع المعلومات عن المشكلة و ذلك عن طريق

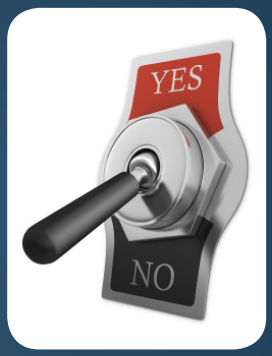
- سؤال المستخدم : تقوم انت فى هذه الخطوة بسؤال المستخدم الذى بلغ عن المشكلة و عن السلوك الغير عادى من جهاز الكمبيوتر
- التعرف على أية تغيرات تم إجرائها على جهاز الكمبيوتر و هنا نحن امام سؤال تقليدي يتم سؤاله للمستخدم « هل هناك اى تغير حدث مؤخرا على جهاز الكمبيوتر هو الذى ادى الى ظهور المشكلة ؟؟ » وهذا التغير من الممكن ان يكون تغير سوفت وير او هاردوير وهنا يجب ان تسخر حواسك عند التعرف على المشكلة فيجب ان تنظر هل هناك شئ اضيف للكمبيوتر او شئ استبدل او شئ ناقص او شئ فى غير مكانه الصحيح و ايضا تسمع لانه فى بعض الاحيان هناك مشاكل تحدث و ينتج عنها صوت فمن خلال هذا الصوت تستطيع تحديد المشكلة و تصل ايضاً فى انك تستخدم حاسة الشم لانه فى بعض الاحيان تنتج رائحة مثل رائحة الحريق قد تكون ناتجة عن حريق فى الباور سبلاي او

قطعة اخرى فى الجهاز

- مراجعة الوثائق ، من الممكن ان تعمل فى شركة كبيرة متخصصة فى صيانة الاجهزة للمستخدمين وان يكون هناك قاعد بيانات لهم فتقوم انت بمرجعة هذه الوثائق لانه من الممكن ان تكون المشكلة التى امامك قد حدثت بالماضي فتستطيع انت التعامل معها بدون اضاعة للوقت ... لاحظ معي انك في هذه الخطوة لاتقوم بأخذ اي اجراء وقبل ان تقوم بعمل اي اجراء هناك خطوة هامه يجب ان تفعلها وهي عمل ( backup )

## - وضع نظرية السبب المحتمل «السبب الواضح»

فى هذه المرحلة يتم تحليل المعلومات التى تم تجميعها من المرحلة السابقة و تضع خطة للمشكلة ودائماً انظر للسبب الواضح ( اعنى بذلك ان لا تنظر الى الشئ الكبير او بمعنى ادق الامور المعقدة, لا بالعكس تماما انظر لابسط الامور واسهلها مثال ذلك عندما لا يعمل الكمبيوتر يجب ان تعتاد على السبب البسيط والواضح فلو وضعنا نظرية على ذلك عندما يبلغك احد ان الكمبيوتر لايعمل من اوئل الاسباب التى يجب ان تأتى على ذهنك هل كيبل كهرباء متصل هل هناك تيار كهربي ام لا ) ما اريد ان اوضحة فى هذه الخطوة دائماً انظر الى ابسط الامور مع التصاعد من الاصغر الى الاكبر




## إختبار النظرية لتحديد السبب

بعد ان وضعت النظرية تقوم بإختبارها وكما وضحت فى المثال السابق اذا كان الجهاز لا يعمل والسبب الواضح هنا انه غير موصل بالكهرباء نقوم بتوصيل الجهاز بالكهرباء فأذا اشتغل الجهاز تتأكد من ان نظريتك صحيحة و بعد ذلك تنتقل الى الخطوة التالية ،،، اما اذا لم يعمل او قمت بتوصيلة و لم يعمل فى هذه الحالة نرجع الى الخطوة الثانية و نقوم بوضع نظرية اخرى ( ملاحظتى ايضاً لا تخرج عن السبب البسيط فمن الممكن يكون هناك مشكلة فى دائرة الكهرباء ، فبعد ان تتأكد ان ليس هناك مشكلة فى الكهرباء ننتقل مرحلة أكبر أربعة ( big four ) و هم ( اللوحة الام – المعالج – كارت الشاشة – الذاكرة العشوئية ) و قس على هذا النحو من المشاكل الى تقابلك دائماً انظر للشئ البسيط )

واذا لم تسطيع ان تأتي بحل للمشكلة حاول الاتصال بالمشرف (supervisor ) لوضع نظريات اخرى لحل المشكلة ....

## وضع خطة عمل لحل المشكلة و تنفيذ الحل

فى الوهلة الاولى قد ترى هذه الخطوة مكررة وعندما درست انا هذه الخطوات و صلت لنفس الاستنتاج ولكن بعد التعمق سوف تجدون غير ذلك ، عندما تم اختبار النظرية و التأكد انها تعمل بنجاح كان هذا على المثال السابق و هذا مثال يعتبر بسيط ولكن فى بعض الاحيان الامر معقد اكثر من ذلك فمن الممكن المشكلة تكون اصلاح عدة قطع فى الجهاز او تكون المشكلة متشابهة و مرتبطة بعدد معين من الاجهز فتقوم انت بوضع خطة عمل لتنفيذها على جميع الاجهزة و بعد ان تقوم بوضع الخطة تقوم بتنفذها ...

## التحقق من كامل وظائف النظام و اذا وجدت تدابير وقائية غير مطبقة يتم تنفيذها

بعد ان قمنا بحل المشكلة نقوم فى هذه المرحلة بالتأكد من الجهاز يعمل بشكل سليم و هذا يتطلب عمل اعادة تشغيل مرة او اثنان و الدخول على الانترنت و فتح البرامج .....الخ ،

وفى هذه الخطوة ايضاً من المهم ان تمنع هذه المشكلة من الحدوث مرة اخرى ايا كانت المشكلة لانه من الممكن ان تكون المشكلة ناتجة عن مشكلة اكبر و هذا هو دورنا هو منع المشكلة من الحدوث فى المستقبل و يعنى ذلك انك لاتتوقف على حل المشكلة فقط اسأل نفسك لماذا حدثت هذه المشكلة هل السبب كبير ام صغير هل مهم ام غير مهم ، و هنا يجب ان اوضح ايا ما كانت التدابير الوقائية التى سوف تأخذ بها يجب ان لا يكون لها تأثير على الانظمة الاخرى او السياسات فأذا وجد يجب الحصول على تصريح لهذه التدابير ...

- توثيق الاستنتاجات و الاجراءات و النتائج

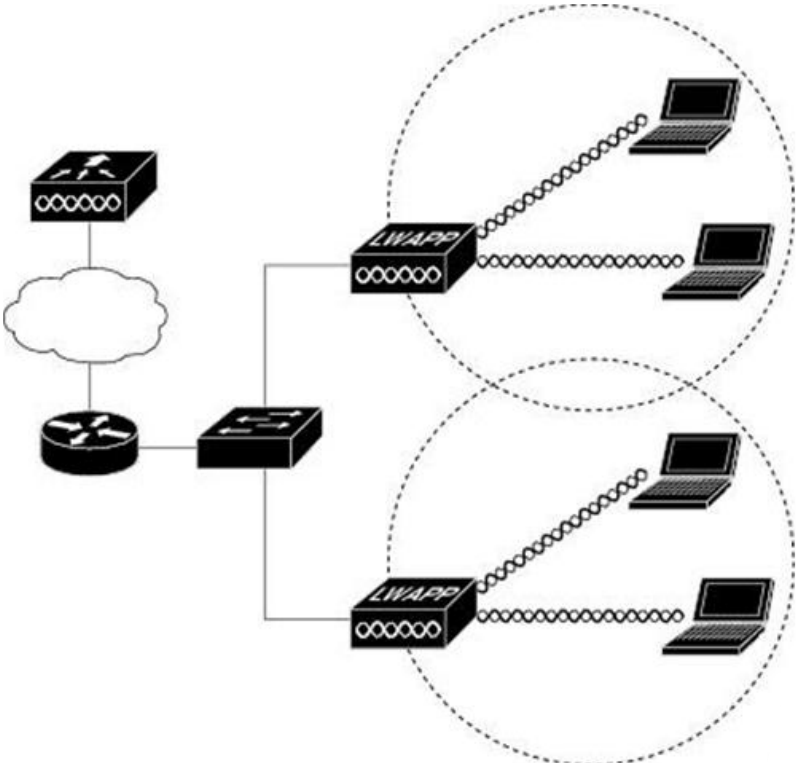
فى هذه الخطوة الاخيرة وهى تسجيل العملية بالكامل و هذه الخطوة تعتمد على الشركة التى تعمل بها سواء كانت تدعم التسجل الورقي او الالكتروني من خلال قاعدة بيانات ، يتم فى هذه الخطوة تسجيل المشكلة ، السبب ، الحل ، التدابير الوقائية ، واي خطوة اخرى تمت فى العملية ، هذه الخطوة نستطيع ان نستفيد منها من جانبين

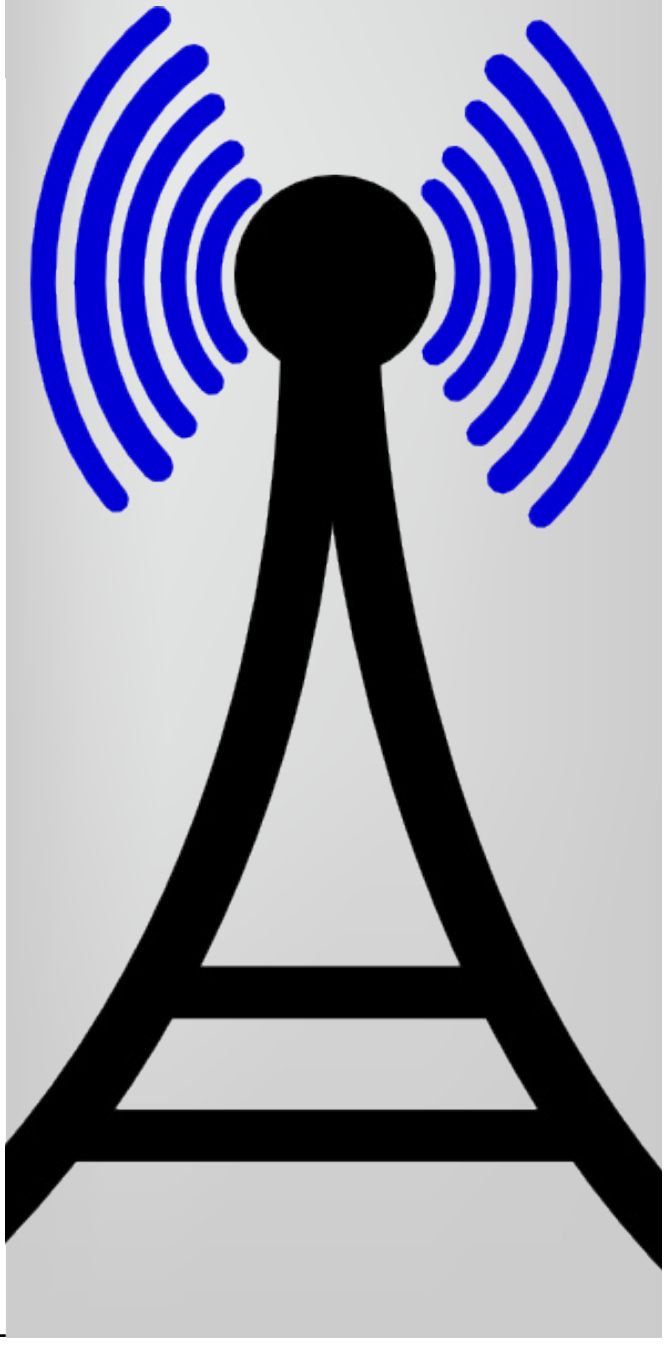
الجانب الاول غلق للمشكلة لك وللمستخدم و تجعل منك خبير تصليح المشاكل فى المستقبل
و الجانب الثانى تستطيع انت او احد من فريق العمل الذى معك الرجوع الى هذه الوثائق و استكشاف الحلول دون تضيع وقت،

و هذا ما حصل مع المهندس ايمن النعيمي لان معظمنا لا يستطيع ان يحفظ جميع الحلول التى يطبقها على المشاكل المختلفة وبالتالى هذه الخطوة تساعد كثيراً , فى النهاية اتمنى من اللّه ان اكون وفقت فى عرض هذا المقال و ان تكونوا خرجتو منه بشئ مفيد حتى اذا كان بسيط «فالدال على خير كفاعلة – صدق رسول اللّه صلى اللّه عليه وسلم »


# Access Point Mode in Wireless Cisco Network

# أوضاع عمل الأكسس بوينت في شبكات سيسكو اللاسلكية



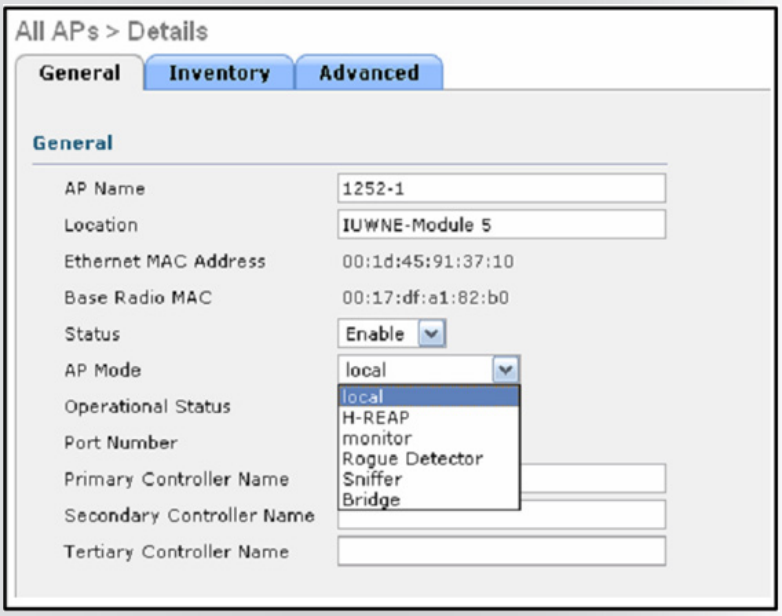
الأكسس بوينت في سيسكو تلعب أدوارا عديدة و لا يقف دوره فقط علي ادخالك الي شبكة الإنترنت كما يظن الكثيرون

و تعتبر أهم وظيفة للأكسس بوينت هي توفير الإتصال اللاسلكي بالأجهزة الا أن الأكسس بوينت قادر علي لعب أكثر من وظيفة أخري مثل مراقبة الشبكة و كشف الدخلاء عليها أو الإتصال بشبكة لاسلكية أخري و يغرها و هو ما سنعرفه حالا الفرق الذي ستجده بين الأوضاع هنا و الأوضاع في أجهزة أكسس بوينت أخري أنك ستتحكم في هذه الأوضاع من خلال الجهازي السحري للشبكات اللاسلكية من سيسكو و هو الكنترولر Wireless Controller

و تستطيع أن تغير وضع عمل الأكسس بوينت من هنا و ذلك بعد تحديدها من شاشة الكنترولر

Wireless > Access points >all APs > Details >

# Access Point Mode in Wireless Cisco Network




و هذه الأدوار نسميها أوضاع عمل Modes و هي في سيسكو الأوضاع التالية كما تري في الشكل

Local
Monitor
Sniffer
Rogue Detector
Hybrid Reap
Bridge

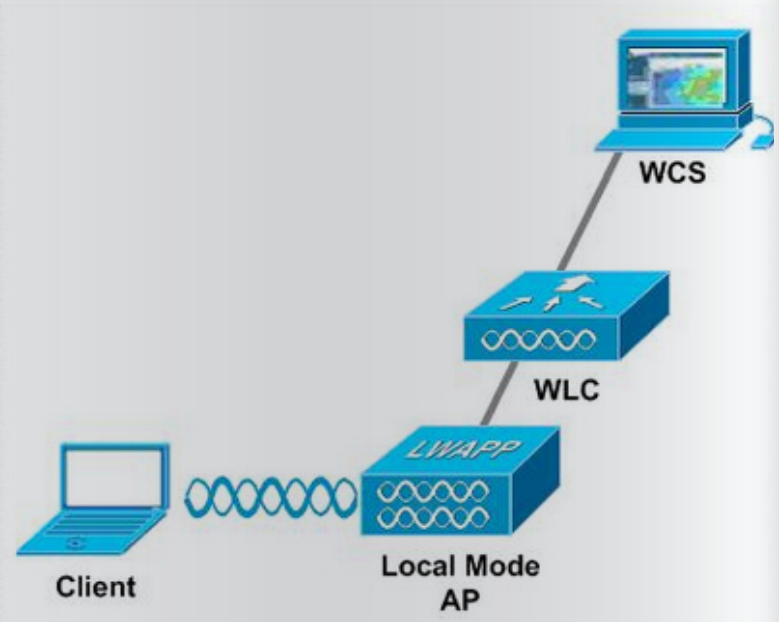
و ليست كل الأكسس بوينت تدعم هذه الأوضاع فمثلا الوضع H) Hybrid Reap) لا يدعم الا في أجهزة 1130AG و 1240 و 1250

## AP Local Mode

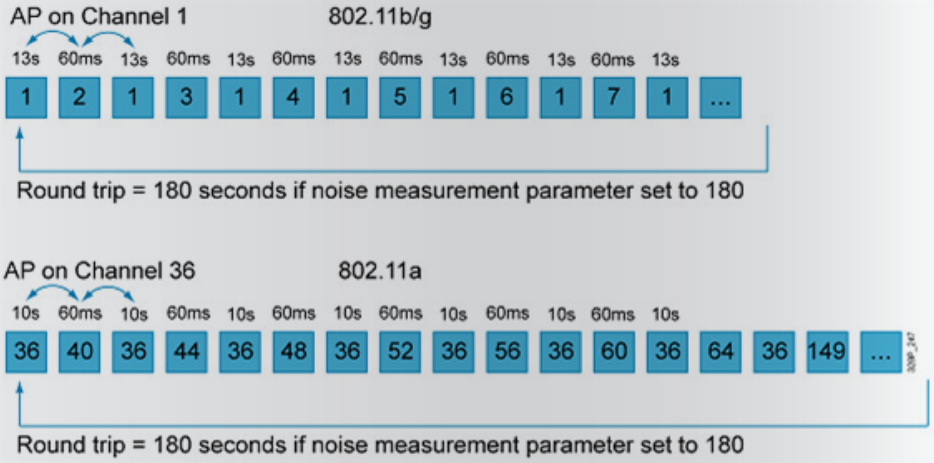
يسمي أيضا normal mode و هو الوضع الشائع و الإفتراضي في عمل الأكسس بوينت من سيسكو حيث يقوم الأكسس بوينت بعمل مسح شامل لكل القنوات كل 180 ثانية و ذلك لفحص management Packets و مشاهدة تدفق البيانات في الشبكة monitoring traffics

عندما يمسح الأكسس بوينت القنوات الترددية channels فإنه يقوم بالذهاب الي القناة التي لا ينتمي اليها مدة 60 ثانية ثم يعود الي قناته الأصلية لمدة 13 ثانية

و لذلك فهو يستخدم في عملية site survey حيث يتم ارسال و استقبال الإشارة من قبل الأكسس بوينت و باقي الأجهزة في خلية الأكسس بوينت و ذلك يحدد قوة الإشارة Received Signal Strength Indicator RSSI و مقدار الشوشرة فيها Signal to Noise Ratio SNR



# Access Point Mode in Wireless Cisco Network

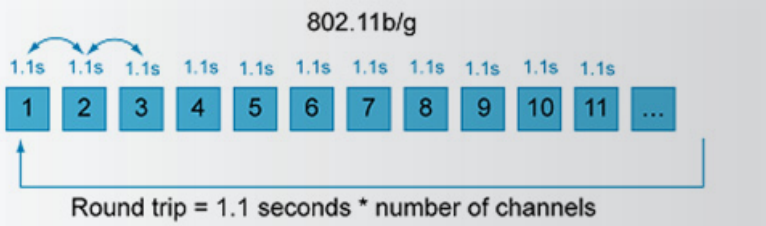


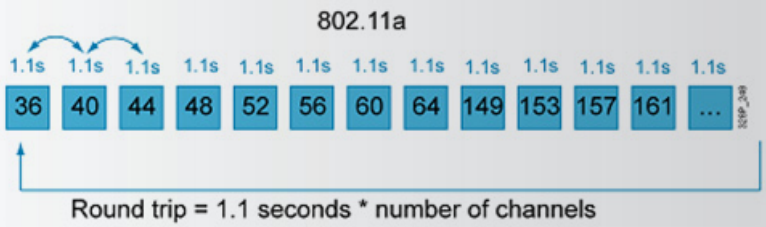

بالنسبة لمعيار IEEE 802.11b/g يقوم الأكسس بوينت بالإنتظار في قناته و لنفترض انها رقم 1 و ذلك لمدة 13 ثانية ثم يقوم بالإنتقال للقناة التي تليها وهي 2 فيمسحها في 60 مللي ثانية ثم يرجع الي قناته رقم 1 مرة أخري و يظل فيها 13 ثانية ثم ينتقل للقناة التالية رقم 3 لمدة 60 مللي ثانية و يظل قوم بهذا الأمر حتي ينتهي من مسح جميع القنوات

هذا الأمر يتم أيضا بشكل متشابه مع معيار IEEE 802.11a الا أن الأكسس بوينت يظل في قناته لمدة 10 ثواني و ليس 13 كما في المعيار السابق و ذلك لكثرة قنوات هذا المعيار

AP Monitor Mode

يطلق علي وضع Monitor mode بالوضع الخامل Passive حيث لا يقوم الأكسس بوينت بإرسال اي بيانات راديوية و لا يسمح بالأجهزة بالإتصال به
و لكنه حيث يقوم بمتابعة الموجات الراديوية لأجهزة الأكسس بوينت الدخيلة Rogue Access Point أو الأجهزة المتسللة أو المخترقة و التي تريد الإتصال بشكل غير شرعي بالشبكة Rogue Clients و يقوم بإعطاء تقرير للكنترولر عن هذه الأجهزة و لذلك فهو يقوم بأداء مهمة Wireless Intrusion Detection System IDS ليقوم بمهام
يقوم هذا الوضع أيضا بعمل Troubleshooting و Site survey و يعطي نقارير عن المشاكل اللاسلكية الحادثة عن التداخلات الراديوية interferences و هذا يفيد مدير الشبكة في فهم البيئة الراديوية للشبكة و تعديل أماكن أجهزة الأكسس بوينت لتفادي حدوث التداخلات



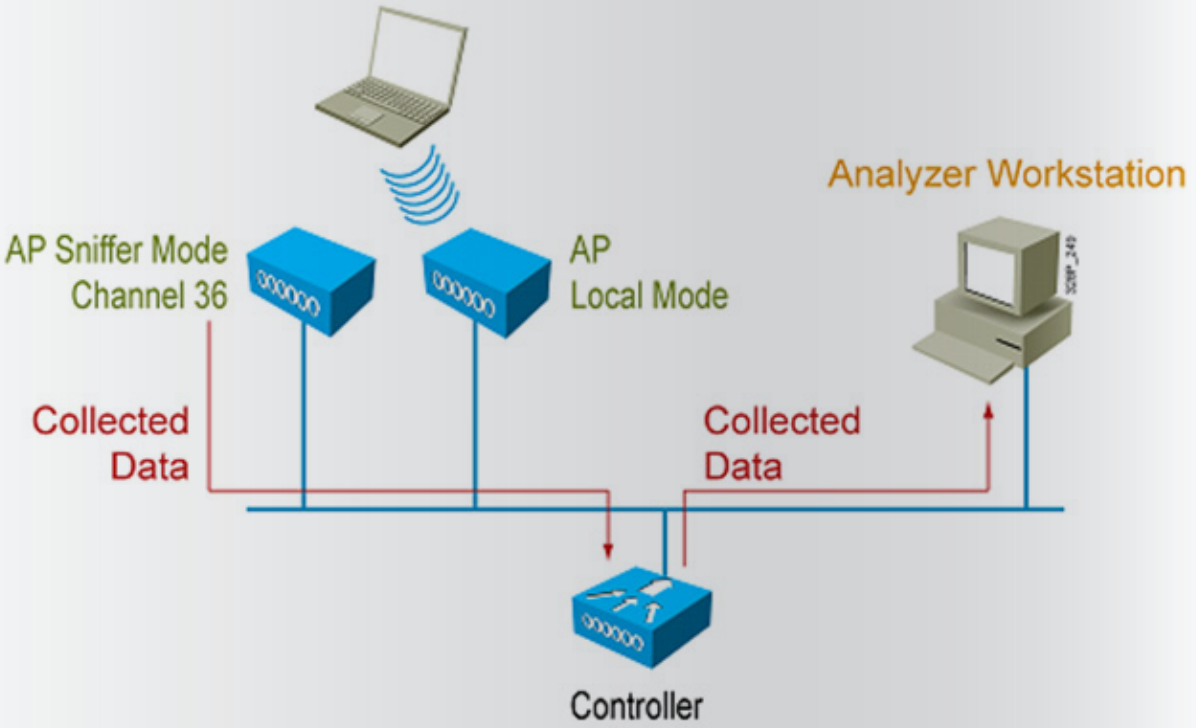




و سنستفيد جدا من هذا الوضع عند استخدام جهاز Cisco Wireless Location Appliance حيث سنقوم بجعل أكثر من أكسس بوينت يعمل في وضع Monitor Mode لتحديد مشاكل و أوضاع الأكسس بوينت

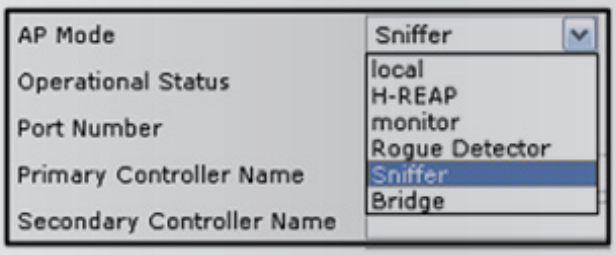
# Access Point Mode in Wireless Cisco Network

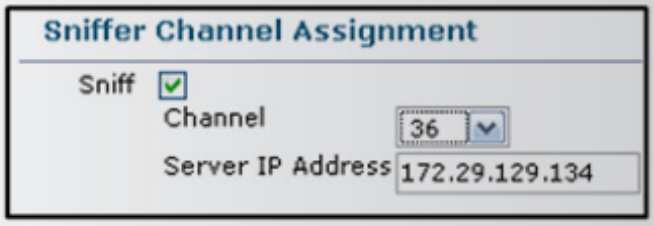
في هذا الوضع يتم مسح كل القنوات الممكن مسحها و ذلك حسب country code لكل دولة و لكنك تستطيع تغيير هذا بإجبار الأكسس بوينت بمسح كامل القنوات و ذلك بعمل الأمر في الكنترولر
Config advanced 802.11b monitor channel-list all
و لضبط المسح ليخص الولايات المتحدة مثلا من 1 الي 11 فسنكتب
Config advanced 802.11b monitor channel-list US

و لضبط المسح ليتم علي القنوات الترددية المعروفة Dynamic Channel Assignment DCA في 802.11b/g فقط و هي 1 و 6 و 11 فنكتب
Config advanced 802.11b monitor channel-list DCA




هذا الوضع يعمل مع سيرفرات برامج OmniPeak أو Airmagent أو Wireshark و هي البرامج المستخدمة في فحص بيانات الوايرلس capture data و لذلك فهو يستخدم في مراقبة البيانات و فحصها

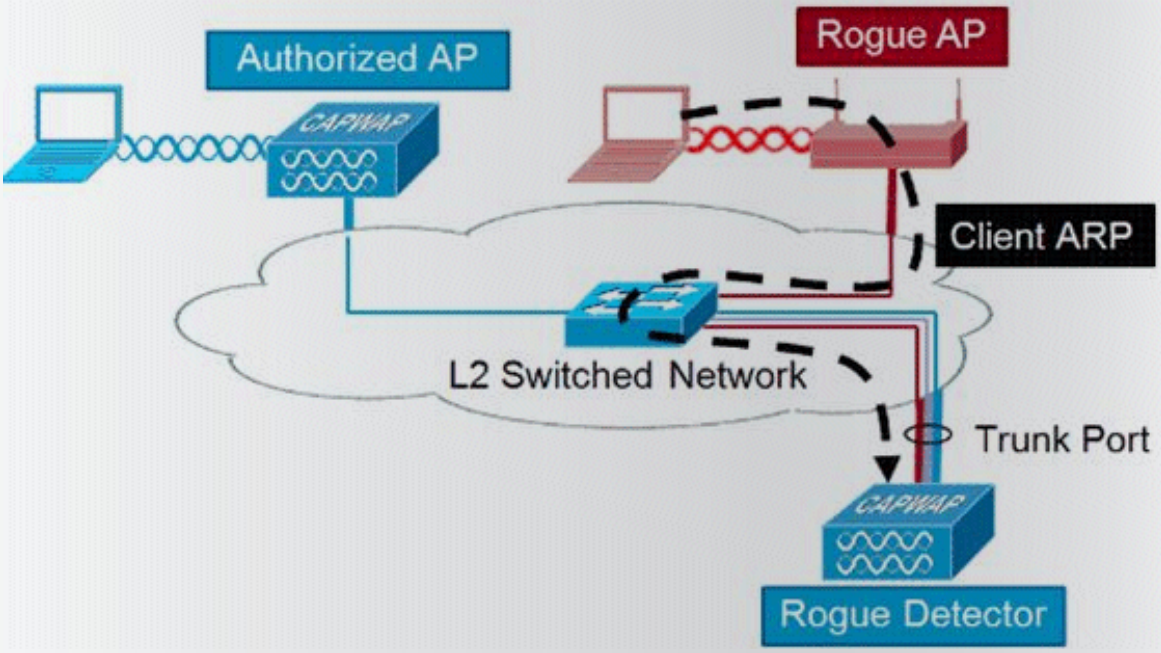


# Access Point Mode in Wireless Cisco Network

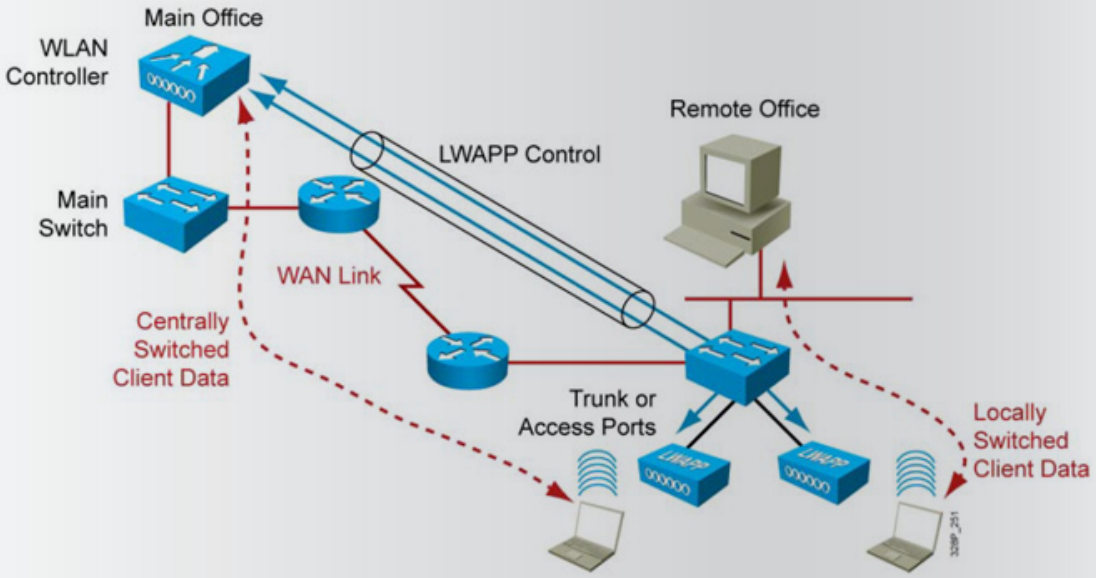
بعد إعداد الأكسس بوينت في وضع sniffer mode سيقوم بإعادة التشغيل Reboot
يقوم الأكسس بوينت الذي يعمل في هذا الوضع بتجميع البيانات من السيرفرات التي جمعتها من الأكسس بوينت التي تعمل في وضع Local ثم يقوم بقبسها encapsulate مع header الخاص بهذه السيرفرات حسب نوعها ثم يرسلها الي الجهاز الذي يقوم بتحليل ها المعطليات

## Rogue Detection Mode




هنا سيتم وقف التراسل بين الأكسس بوينت التي تعمل في هذا الوضع و تقوم بالتصنت علي رسائل ARP الموجودة علي الشبكة السلكية حيث يقارن بين بيانات MAC الخاصة بالأجهزة الدخيلة مع قائمة MAC التي حصل عليها من الكنترولر ثم يقوم بإرسال النتائج الي أجهزة الكنترولر الأخري و التي تقوم بعمل تحذير لباقي الأكسس بوينت بعدم السماح لهذا الأكسس بوينت بالدخول
يتم وضع الأكسس بوينت التي تعمل في وضع Rogue detector mode علي trunk port كي تستطيع التصنت علي كامل VLAN الموجودة في لشبكة السلكية الخاصة بالوايرلس

## H-REAP Mode



# Access Point Mode in Wireless Cisco Network

الوضع H-Reap أو Hybrid remote edge access point يتم استخدامه عندما تريد استخدام الكنترولر للتحكم في أجهزة أكسس بوينت ضمن شبكتك و لكنها تعمل من خلال WAN في مكان آخر و هنا يتم ربط الشبكة اللاسلكية بالكنترولر عبر شبكة WAN و هذا الأمر مفيد عندما تريد أن تدير عدة فروع متباعدة من خلال المركز الرئيسي للشركة بدون الحاجة لوضع كنترولر في كل فرع

و لأن الأكسس بوينت سيقوم بالإتصال بالكنترولر لقيم زمنية صغيره لتحديث بياناته بقيمة 4 ميجابايت فإنه لابد من مراعاة التالي

أولا أن لا تقل سرعة الربط عن 128 Kbps

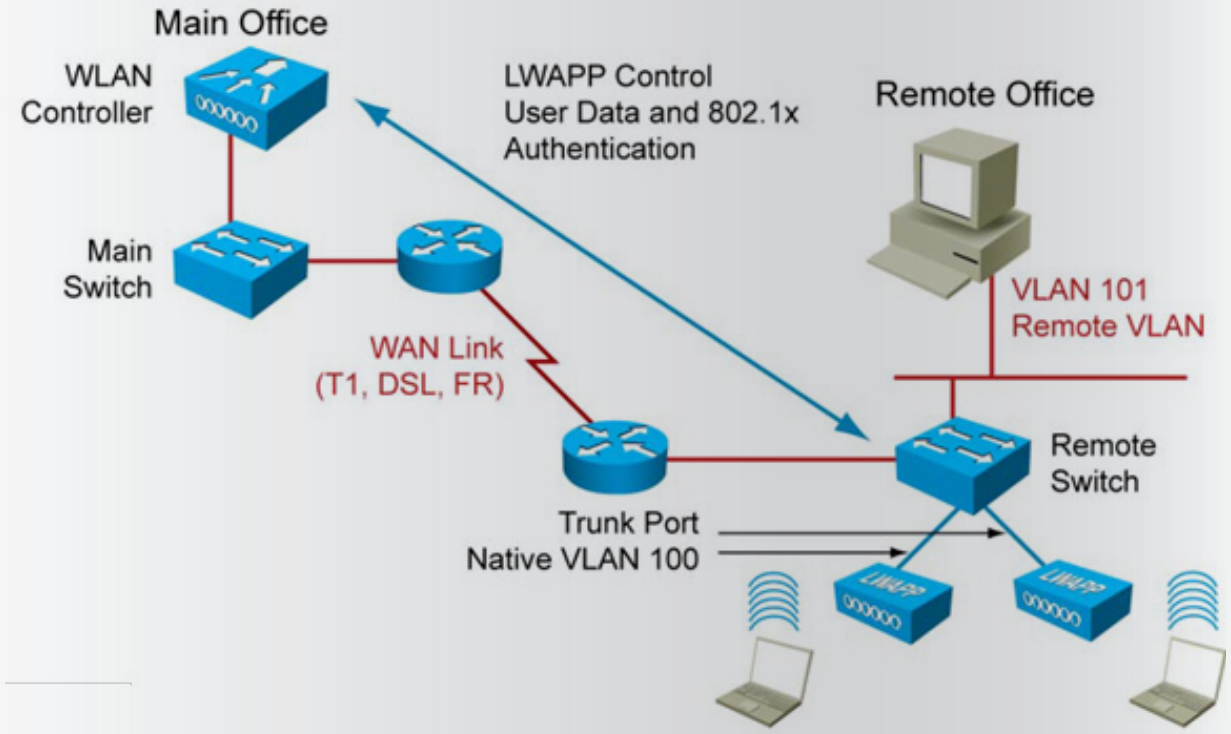
ثانيا يجب أن لا تقل قيمة Round-trip delay أو ما يسمي (Round-trip time (RTT عن 100 ميللي ثانية , علما بأن RTT هي قيمة الوقت اللازم لإرسال اشارة بين طرفين و استقبالها و يعتمد علي البعد بين الطرفين و كذلك عدد المحطات التي يمر بها و كذلك طبيعة الوسط الناقل للإشارة

عند اكتمال تحديث الأكسس بوينت فإنه يقوم بالعمل منفردا بدون الإتصال بالكنترولر أي يعمل في الوضع Stand alone mode و هو الوضع الذي يكون فيه الأكسس بوينت مسؤلا عن الشبكة و لا يحتاج فيها الي الكنترولر و هو مدعوم من قبل أجهزة الأكسس بوينت التالية AP 1240 , AP 1130 AP 1250 , علي أن تكون الذاكرة الموجودة في أي منهم لا تقل عن 32 ميجابايت

و لهذا فإنه عند حدوث انقطاع في خدمة WAN فإن الشبكة تظل تعمل و يتم احالة عمليات التوثيق authentication للأكسس بوينت ذلك في حالة اكتمال تحديث الأكسس بوينت من قبل الكنترولر

اذن فالأكسس بوينت في وضع H-REAP يستطيع العمل وضعي Stand alone أو Connected -Controller based

## أولا الوضع Connected -Controller based



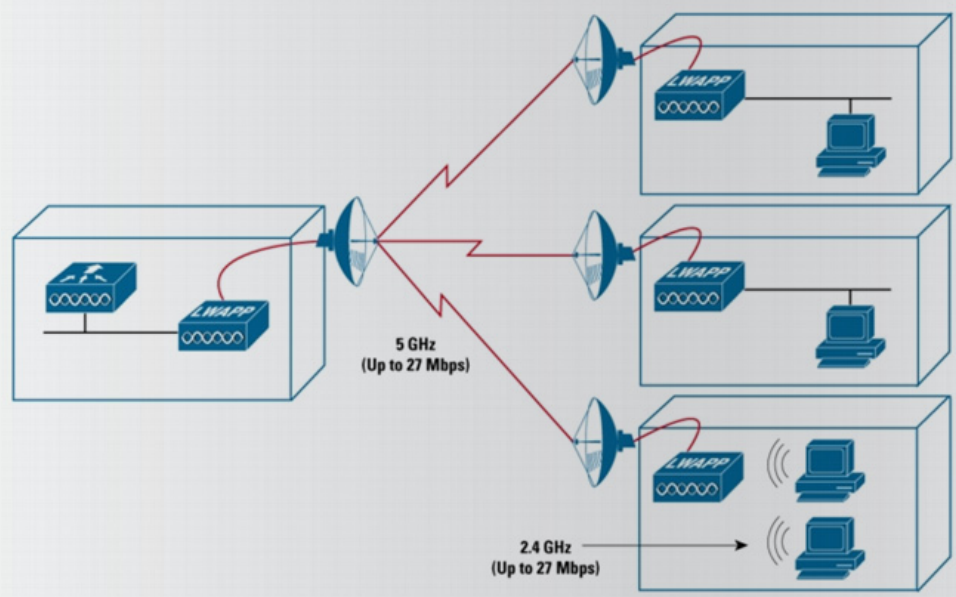
# Access Point Mode in Wireless Cisco Network

عندما يكون الأكسس بوينت في وضع H-REAP فإنه يقوم بتخزين هذه المعلومات من الكنترولر لإستخدامها عند فقدان الإتصال بالكنترولر نتيجة انقطاع الإتصال بشبكة WAN
DTIM : Delivery Traffic Indication Message و هي قيمة تحدد عدد المرات التي سيقوم بها الأكسس بوينت ارسال رسائل broadcast و multicast
Beacon period : الفترة الزمنية بالميليل ثانية و التي سيرسل فيها الأكسس بوينت اشارات beacon و افتراضيا تكون القيمة هي 100 ميللي ثانية
Power Level : قيمة القدرة التي يرسل بها الأكسس بوينت اشاراته
Channel number : القناة التي يعمل بها الأكسس بوينت
Black list : عناوين MAC الغير مسموح لها باستخدام هذا الأكسس بوينت

## ثانيا الوضع Standalone in HREAP

وضع Standalone in HREAP لا يدعم عمل توثيقات IP Secuity IPSEC و Point-to-Point tunneling Protocole PPTP و ذلك لأن هذه البروتوكولات تحتاج اتصال دائم بالكنترولر و لا يستطيع الأكسس بوينت الإنفراد باتخاذ قرار فيها و لكن تم استخدام بدائل لهذه البروتوكولات تعمل علي Standalone in HREAP و هي Backup Raduis server و Local authentication حيث يقوم الكنترولر بتوكيل Backup RADUIS Server بعمل توثيق لأجهزة الأكسس بوينت بعد ارسال قائمة بالأسماء و كلمات المرور لعمل Local authentication

## AP Bridge Mode



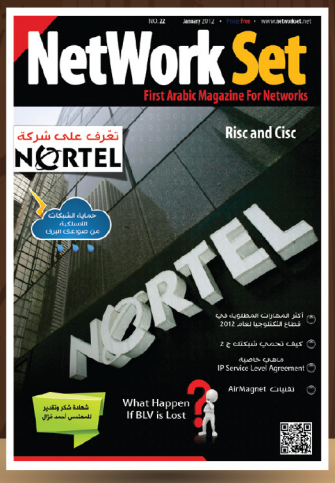

في هذا الوضع سيقوم الأكسس بوينت بأداء دور الجسر اللاسلكي ليربط بين شبكتين لاسلكيتين في وضع point to point أو point to multipoint و كذلك سيسمح بارتباط الأكسس بوينت به كأنه LOCAL و في هذا الوضع سيحتاج الأكسس بوينت «الجسر» الي اختيار أفضل مسار للجسر الذي يليله و يتم ذلك بإستخدام بروتوكول Adaptive Wireless Path Protocol AWPP و هنا لن تحتاج الأكسس بوينت الي الإتصال سلكيا بالكنترولر بل ستقوم بإختيار أفضل مسار للأكسس بوينت لتأخذ منها معلومات الكنترولر
يسمي هذا الوضع في سيسكو أيضا بـ IMesh for indoor APs أو mesh for outdoor APs
يتوفر هذا الوضع في اجهزة الأكسس بوينت من نوع 1500 و 1130AG و 1240

# Network Set Magazine Gallery









# ماهو بروتوكول Bidirectional Forwarding Detection (BFD)؟

في كل من شبكات الشركات وشبكات موزعي الخدمة، هناك بيانات حساسة يجب أن ترسل في وقتها، و نظرا لذلك، يتم بناء هذه الشبكات عادة مع وجود درجة عالية من التكرار ( Redundancy) المرغوب فيه. فعالية هذا Redundancy تعتمد على قدرة أجهزة الشبكة في الكشف عن حالات الفشل(failures) و إعادة توجيه حركة المرور إلى المسار البديل بسرعة.

هذا الكشف يجري عادة عن طريق بعض الآليات التي يوفرهاhardware . ومع ذلك، فإشارات هذه الآليات لا تنقل دائما مباشرة إلى الطبقات العليا. فعندما لا توجد هذه الآليات (على سبيل المثال: إيثرنت) أو عندما لا تصل الإشارات الى الطبقات العليا ،يجب أن تعتمد البروتوكولات على استراتيجياتها الخاصة التي هي أبطأ بكثير من أجل الكشف عن الفشل. هذه البروتوكولات تستغرق عادة أكثر من ثانية واحدة أو أكثر في بعض الحالات للكشف عن مشكل ما في الشبكة . بالنسبة لبعض التطبيقات، فهذا الوقت يعد طويلا.

(Bi-directional Forwarding Detection (BFD يوفر سرعة كبيرة للكشف عن فشل الشبكة في وقت قليل بينForwarding engines ، و ذلك عن طريق overhead صغير. كما يوفر كذلك ، طريقة موحدة للرابط / الجهاز / البروتوكول للكشف عن فشل الشبكة في أي طبقة بروتوكول وفي أي نوع منmedia .

## 1.وصف بروتوكول : BFD

يكشفBFD عن فشل الاتصالات مع data plane next hop . البروتوكولات الزبونة التي تدعم حاليا هذه الخاصية هي Open Shortest Path First (OSPF) ، Intermediate System-to-Intermediate System (IS-IS) ، Enhanced (Interior Gateway Routing Protocol (EIGRP و (Border Gateway Protocol (BGP.

بعد بدء تشغيلBFD ، يقوم البروتوكول الزبون بتقديم طلب للBFD لإنشاء adjacencies مع neighbor . BFD process ينشئ adjacency structure ويحاول إنشاء session . الفاصل الزمني الأول لرسالة hello هو ثانية واحدة، عندما يتم تأسيس session وتتحول حالتها إلىup ، بعد ذلك يتم استخدام قيمتيtransmit وreceive المعدة. و لضمان انتقال حزمBFD control في الوقت المناسب ، يتم معالجة هذه الحزم من قبل pseudo-preemptive BFD process. في معظم الحالات، يتم إرسال واستقبال حزم BFD control عن طريق مسار Cisco Express Forwarding switching لتجنب التأخير التي يمكن تكبده في عمليه queuingعلى مستوى process. حزم BFD ترسلunicast مباشرة بينneighbors .

يعملBFD في وضعين: Asynchronous mode وDemand mode ، نظامIOS الخاص بسيسكو يدعم حاليا فقطAsynchronous mode ، والذي هو بمثابة الوضع الأساسي. في الوضع الغير المتزامن، الأنظمة ترسل حزم BFD control لبعضها البعض.

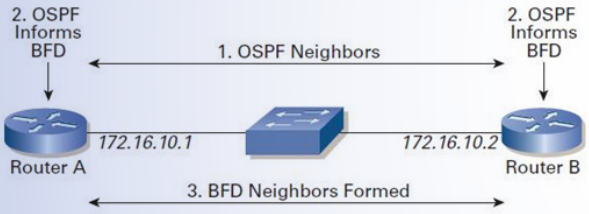
إذا لم يتم تلقى عددا من حزم BFD control المتفاوض عليها مسبقا على التوالي من قبل النظام آخر، يتم إعلانdown للsession . بروتوكول BFD يعتمد على إرسال حزم مكونة من 24 بايت و تتضمن القيم المحددة للlocalDiscriminator، min_TxInterval، remoteDiscriminator ، min_RxInterval وDetectMultiplier. وتعرف هذه القيم كما يلي:

- localDiscriminator : يستخدم لتعريف BFD session، يجب أن يكون وحيد في هذا النظام وغير صفري (non-zero ).
- remoteDiscriminator : هذا هو Discriminator الذي اختاره النظام الأخر وهو شفاف تماما على النظام المحلي.
- min_TxInterval : الفاصل الزمني الأدنى بالميكروثانية، بين انتقال حزمBFD control الذي يريد هذا النظام استخدامه. يتم التفاوض حول هذا الفاصل الزمني بين النظامين.
- min_RxInterval : الفاصل الزمني الأدنى بالميكروثانية، بين استقبال حزمBFD control الذي يريد هذا النظام استخدامه.
- DetectMultiplier : قيمةالفاصل الزمني المتفاوض عليه لإرسال حزمBFD control مضروب في هذا المتغير، سوف يكون الوقت المستغرق للكشف عن فشلsession ؛ Detection time أو الوقت المستغرق للكشف ( هو مرور فترة من الزمن دون تلقي حزمBFD control

بعد ذلك يمكن قول بأن session توجد في حالة (down هذا الوقت لا يتم نقله في حزم BFD control المتبادلة. بدلا من ذلك، يتم حسابه بشكل مستقل في كل اتجاه من قبل الجهاز المستقبل على أساسtransmit interval وdetection multiplier المتفاوض عليهما. في الوضع الغير المتزامن، قد يكون هناك أوقات كشف مختلفة في كل اتجاه، أما في الوضع المتزامن، وقت الكشف الجهاز المحلي يساوي قيمة المرسلDetect Mult من الجهاز الأخر مضروب فيtransmit interval المتفق عليه

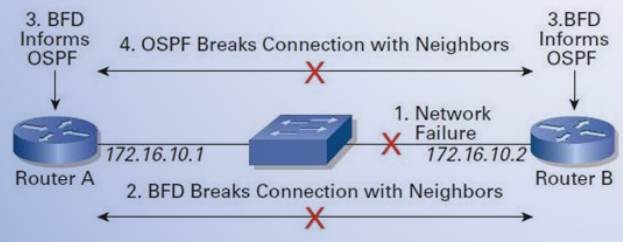
## 2. أمثلة عن بروتكول: BFD

الشكل أدناه يظهر شبكة بسيطة تتكون من جهازي توجيه يستعملان OSPF وBFD . عندما يكتشف OSPF أحد الجيران أو neighbors (الخطوة 1)، يرسل طلب إلى BFD process المحلي لإنشاء sessionمع الروتر المكتشف في الخطوة الأولى (الخطوة 2) بعد ذلك يقوم BFD process بإنشاء session معOSPF neighbors (الخطوة 3).




Bidirectional Forwarding Detection

يظهر الرسم التالي ما يحدث عند حدوث فشل في الشبكة. إذا كان هناك مسار بديل متاح، فأجهزة التوجيه تبدأ فورا بتوجيه الترافيك نحو المسار البديل. عند حدوث فشل في الشبكة (الخطوة 1)، تتحولBFD session إلى حالة down (الخطوة 2) . يقوم BFD بإشعار OSPF process المحلي بأن BFD neighbor لم يعد reachable (الخطوة 3) وفي الأخير يقوم OSPF process بهدمOSPF neighbor relationship (الخطوة4 ) .




هدم OSPF NEIGHBOR RELATIONSHIP

الآن دعونا ننظر كيفية استخدام بروتوكولات التوجيه لBFD وكيفية إعدادBFD.

### 3. BFD مع OSPF :

يسجلOSPF جميع neighbors المهتمين باستخدام BFD فيBFD process . بعد تسجيل أحد الجيران، يبدأBFD بإنشاءsession معه (إذا كانت غير موجودة). عندما يكتشفBFD أن الاتصال قد فقد مع أحد الجيران ، فإنه يرسل إشعار. إذا كانBFD مشغلا مع هذهOSPF interface ، فإنه يفرض علىOSPF هدم OSPF relationship . هذا يولدneighbor down event الذي يؤدي لإحداث إصدارات جديدة من link-state advertisements (LSAs) المطلوبة. كل هذا يتسبب في تشغيل Shortest Path First (SPF)، مما ينتج عنه إعادة توجيه حركة المرور إلى مسارات أخرى بديلة.
يمكنك إعدادBFD للOSPF فيrouter mode مما يؤدي إلى تفعيلBFD على كافةinterfaces :

```
router ospf 1
no] bfd all-interfaces]
```

ويمكن أيضا أن تقوم بتفعيلBFD علىinterface خاصة، يمكنك تفعيل أو تعطيلBFD باستخدام الأوامر التالية:

```
[no] ip ospf bfd [disable]
```

الأوامر التالية تقوم بتفقد حالةBFD :

```
0/RouterA#sh ip ospf int e2
is up, line protocol is up 0/Ethernet2
Area 0 ,16/Internet Address 172.16.10.1
Process ID 1, Router ID 172.16.10.1, Network Type BROADCAST, Cost: 10
,Transmit Delay is 1 sec, State BDR, Priority 1
BFD enabled
Designated Router (ID) 172.16.10.2, Interface address 172.16.10.2
,Backup Designated router (ID) 172.16.10.1
Interface address 172.16.10.1
,Timer intervals configured, Hello 10, Dead 40
Wait 40, Retransmit 5
```

Show ip ospf neighbor detail تخبرك ما إذا كان يتم رصده من قبلBFD .

```
RouterA#sh ip ospf nei 172.16.10.2 det
Neighbor 172.16.10.2, interface address 172.16.10.2
,0/In the area 0 via interface Ethernet2
BFD enabled
Neighbor priority is 1, State is FULL, 6 state changes
```

في المثال التالي، شبكة ODPF بسيطة تتكون من جهازي توجيهA و 2 Ethernet interface 0/B. في الروترA موصلة في نفس الشبكة مثل 1 0/Ethernet interface في الروترB . في هذا المثال، تم إعداد BFD في كل من روترA و b على جميعinterfaces المرتبطة بـOSPF process.

- إعداد روتر A :

```
0/interface Ethernet2
ip address 172.16.10.1 255.255.0.0
bfd interval 50 min_rx 50 multiplier 3
!
router ospf 1
log-adjacency-changes detail
network 172.16.0.0 0.0.255.255 area 0
bfd all-interfaces
```

- إعداد روتر B :

```
0/interface Ethernet1
ip address 172.16.10.2 255.255.0.0
bfd interval 50 min_rx 50 multiplier 3
!
router ospf 1
log-adjacency-changes detail
network 172.16.0.0 0.0.255.255 area 0
bfd all-interfaces
```

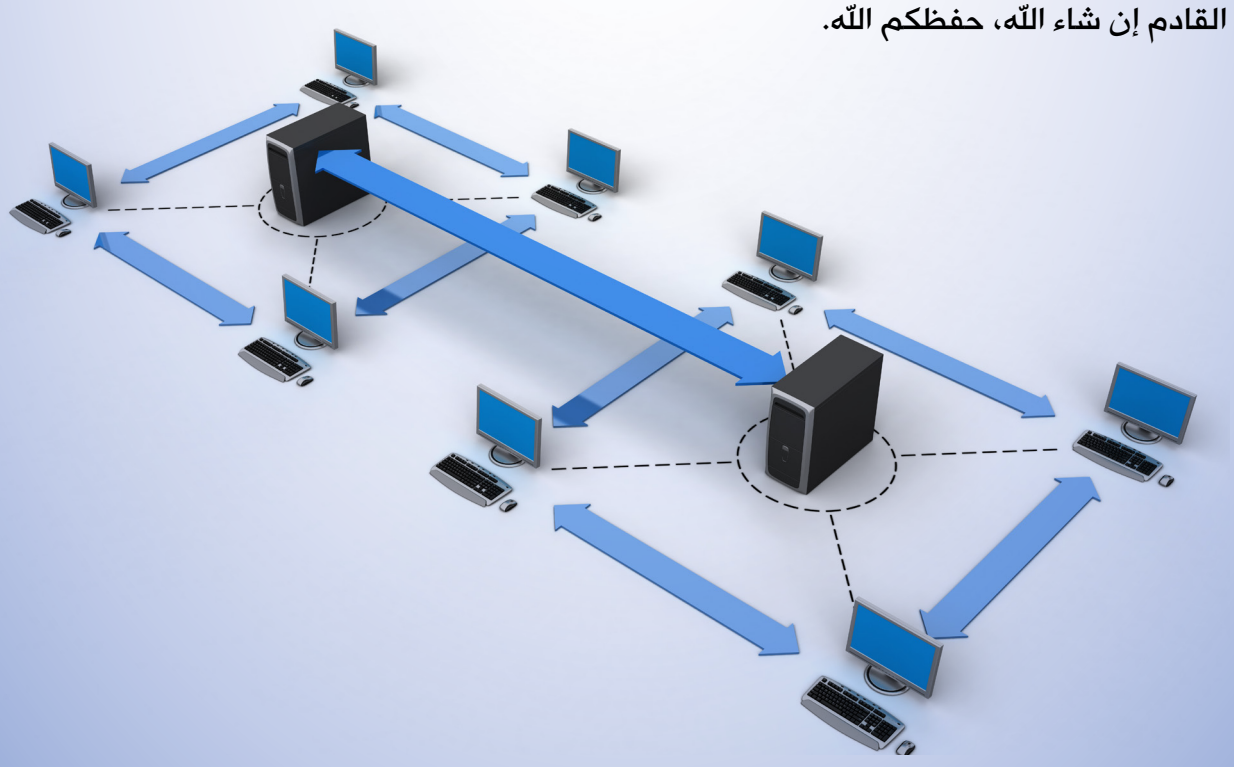
show bfd neighbors details تتحقق من أنه تم إنشاء BFD session و من أن OSPF يشغل BFD .

```
RouterA#sh bfd neighbors details
(OurAddr NeighAddr LD/RD RH Holdown(mult
State Int
( 3) 94 1 2/2 172.16.10.2 172.16.10.1
0/Up Et2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
(Holdown (hits): 150(0), Hello (hits): 50(8605
:Rx Count: 8607, Rx Interval (ms) min/max/avg
last: 56 ms ago 49/72/32
:Tx Count: 8609, Tx Interval (ms) min/max/avg
last: 16 ms ago 49/72/32
Registered protocols: OSPF
Uptime: 00:07:08
Last packet: Version: 0 - Diagnostic: 0
I Hear You bit: 1 - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 2 - Your Discr.: 2
Min tx interval: 50000 - Min rx
interval: 50000
Min Echo interval: 0
#RouterA
```

النتيجة نفسها بالنسبة لروتر : B

```
RouterB#sh bfd neighbors details
(OurAddr NeighAddr LD/RD RH Holdown(mult
State Int
( 3) 142 1 2/2 172.16.10.1 172.16.10.2
0/Up Et1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
(Holdown (hits): 150(0), Hello (hits): 50(10131
:Rx Count: 10137, Rx Interval (ms) min/max/avg
last: 8 ms ago 49/64/32
:Tx Count: 10135, Tx Interval (ms) min/max/avg
last: 36 ms ago 49/64/36
Registered protocols: OSPF
Uptime: 00:08:24
Last packet: Version: 0 - Diagnostic: 0
I Hear You bit: 1 - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 2 - Your Discr.: 2
Min tx interval: 50000 - Min rx
interval: 50000
Min Echo interval: 0
#RouterB
```

يوفر طريقة لمديري الشبكات لاكتشاف فشل الشبكة في (Bidirectional Forwarding Detection (BFD الطبقة 2 بين جهازين متجاورين. وعلاوة على ذلك، فإنه يمكنهم إعدادrouting protocols للإجابة على إشعاراتBFD ، والبدء في البحث عن مسار آخر لترافيك على الفور . إذا تم إعدادBFD جيدا ، فيمكنه أن يكون أداة قوية وجزأ مهما من خطةHigh availability للشبكة . . وبهذا نكون قد انتهينا أتمنى لقاءكم في العدد القادم إن شاء اللّه، حفظكم اللّه.




# إبدأ شركتك فى الشبكات

تعودت دائما أن أسرد أى موضوع أو شرح على هيئة قصة لها أبطال تدور حولهم الأحداث حتى ينجذب القارىء ويتفاعل مع أحداث القصة واليوم ستكون انت عزيزى القارىء البطل ...
وكما هو معروف فى الأفلام الغربية وحتى العربية بأن البطل يجب أن ينتصر فى النهاية وتنتهى القصة على صورته وهو واقف شامخ يبتسم ابتسامة النصر لذلك قم بتجهيز نفسك لالتقاط صورة لك فى نهاية المقال


## فى البداية جاوبنى على هذه الأسئلة السريعة :

كم عدد الحاصلين على شهادة CCNA فى العالم ؟ اذا عرفت اجابة هذا السؤال فبالتأكيد ستعرف عدد الحاصلين على CCNP و MCITP وغيرهم من الشهادات التقنية فى الشبكات

ولكن لماذا اسألك هذه الأسئلة ؟ لاننا فى الوطن العربى دائما ننظر الى الأمور من جانب واحد فقط كأنى بالظبط أحضرت لك صورة وقمت بتغطيتها بالكامل ما عدا جزء بسيط منها ثم سألتك عن رأيك فى هذه الصورة ؟!

بالطبع يجب أن تخبرنى بأنك لا تستطيع أن تحكم عليها الا بعد أن أكشف لك الصورة كاملة ولكننا نحن العرب دائما نتسرع فى الحكم على الأمور لذلك سأجدك تخبرنى عن رأيك في الصورة كاملة اعتمادا على الجزء الذى رأيته فقط !!

الأن وقد جذبت انتباهك لماذا تكلف نفسك عناء تكاليف الامتحانات الدولية الكثيرة لتقم فى النهاية بتعليقهم على الحائط لمجرد أن يعلم الجميع أنك حاصل على هذه الشهادات فقط ! ما الذى استفدته من هذه الشهادات كواقع عملى فى حياتك ؟

أعرف ان بعض الشركات تشترط عليك أن تكون حاصل على كذا وكذا و .... حتى تعمل لديهم ويمكن أن يقبلوك أو لا حتى وان قبلوك سيكون دورك بسيط جدا بالنسبة للشركة أو فى جزء معين فقط حتى تقول لنفسك يا ليتنى لم أتكلف مصاريف الشهادات وقمت فقط بدراسة الجزء الذى أعمل به الأن أو قمت بإنهاء الكورس التدريبى لها على الأقلCCNAولكن لماذا لا تفكر خارج الصندوق ؟ كمثال انت الأن حاصل على هذه الشهادة أعطتك أساسيات للشبكات فى جميع التخصصات بداية من الراوتينج والسويتشنج مرورا بالوايرلس والفويس والحماية وانتهاء بجزء الشبكات الكبيرة لماذا لا تبدأ شركتك الخاصة كـ

شركة حلول شبكات تقوم بتقديم حلول الشبكات فى المنطقة الموجود بها
ومع مرور الوقت ستكبر شركتك ويكون لها اسم مشهور محليا وربما فى المستقبل ستنافس عالميا شركات مثل سيسكو وميكروسوفت وجونيبر وأفايا كلها بدأت بواحد أو اثنين اقتنعوا بعلمهم وبدلا من أن يطرقوا أبواب الشركات أملين فى توظيفهم وبدلا من الانتظار فضلوا أن يبدأوا عملهم الخاص ويقوموا هم بتوظيف الأشخاص !
ابحث عن من هم فى نفس حماسك وعلمك وابدأوا سويا شركة فى تخصصك وقم بالتوسع تدريجيا حتى تحقق حلمك بأن تكون شركتك عالمية معروفة .
اذا استمتعت بهذه المقدمة وفى حال نويت أن تفكر فى انشاء شركتك الخاصه فربما يهمك أن تتعرف على بعض النقاط الأساسية أولا قبل بداية رحلتك :

## التخطيط:

مثل أى مشروع جديد تقدم على عمله ينبغى عليك فى البداية التخطيط لمشروعك ووضع النقاط الأساسية التى ستبنى عليها مشروعك مثل :

هدف الشركة: يجب أن تضع لشركتك هدف تصل اليه أو ما غايتك من الشركة
تحديد هدف الشركة يساعدك فى تحديد رأس المال الذى ستبدأ به مشروعك وعدد العاملين بالشركة والأهم معرفة متى تتوقف فى حالة مر عليك فترة من الزمن ولم تحقق الشركة الهدف المطلوب منه

دراسة السوق ينبغى عليك قبل الخوض فى مشروعك دراسة السوق ومعرفة اتجاه العملاء للشبكات بمعنى هل تكون شركتك شركة تدريب مثلا لكورسات الشبكات مثل سيسكو وميكروسوفت وجونيبر أم تكون شركة حلول شبكات تقدم خدمات مبيعات وتركيب الشبكات وحل المشكلات والدعم الفنى للشبكات .

التخصصية: اختيار تخصص الشركة شىء فى غاية الأهمية فعلى أساس التخصص يتجه العميل الى الشركات ،على سبيل المثال اذا كنت شركة حلول شبكات فيجب أن تضع قائمة كاملة بكل المهام التى تقوم بها شركتك فى حلول الشبكات سواء مبيعات أو حلول تطبيقية خاصة بالشبكات ولا تغوص فى تخصصات أخرى مثل حلول البرمجة أو تطوير المواقع . هذه الخطوة تساعدك فى اختيار فريق العمل المتخصص وستكون على دراية كاملة بسير العمل فى الشركة .

اختيار المكان: المكان المناسب هو بداية انطلاق شركتك وظهروها الى النور . اختر المكان بعد دراسة سوق العمل ومعرفة أين يقع عملائك كن على مقربة منهم لتصبح دائما فى الصورة ولا تشغل بالك حاليا بالتوسع فى أكثر من مكان لأنها مرحلة قادمة بإذن الله فى حال أثبتت وجودك .

الدعايا: على حجم دعايتك يكن حجم العملاء . فى بداية الشهور الأولى من شركتك كثف الدعايا حتى تصل الى أكبر شريحة ممكنه ويكون اسم شركتك مسموع ولا تبخل بالمال المصروف على هذه الدعايا واعتبره كـ مصاريف ضرورية لاتمام الشركة لأنك يمكن أن تظل عدة شهور من غير عميل واحد وذلك لأنك لم تنتشر بالشكل المطلوب .

كل هذه الخطوات يجب أن تضعها فى تخطيطك قبل بدأ مشروعك وتأكد أن ما ستمر به من تعب أو مصاريف لن تتذكرها عندما تنجح شركتك وتكبر يوما بعد يوم أمامك كالطفل الصغير .
الأن وقد أتممت عملية التخطيط وأنرت الطريق أمامك وعزمت الجهد على اتمام مشروعك دعنا ننتقل للخطوة التالية وهى مرحلة :

## التنفيذ

الأن ستحول كل ما كتبته على ورق الى واقع فعلى . فى مرحلة التنفيذ سوف يظهر لك عدو اسمه «الوقت» لذلك أنصحك بمصادقته حتى تنتهى من اتمام مشروعك . الكثير منا عند عمل أى شىء يتحجج دائما فى الوقت وقلته على الرغم من أن كل البشر لديهم فقط 24 ساعة فى اليوم مثلك تماما ! ضع لنفسك جدول زمنى تنتهى فيه من مرحلة التنفيذ مع تحديد مهام كل يوم مع ذكر مهام احتياطيه لكل يوم فى حال فشلت المهام الأساسية .

فى هذه المرحلة ستتعامل مع فئات كثيرة من البشر نظرا لم تكن تتصور انكم ستحتاجهم فى يوم من الأيام ولكن هذا هو حال الدنيا كل منا له دور فى الحياة .

عليك بالصبر والتفاؤل فهذه المرحلة مؤقتة فقط وعندما تنتهى ستكون لك شركتك وحلمك لذلك ضع دائما فى حسبانك حكمة «أتعب قليلا اليوم وأرتاح غدا أفضل من أرتاح اليوم وأتعب باقى العمر» .

## ما بعد التنفيذ

مبارك عليك شركتك . الأن ستشعر بارتياح رهيب ومخيف فى نفس الوقت فأنت قد أنهيت المرحلة الصعبة وانتقلت الى المرحلة التالية وهى ادارة الشركة .

فى بداية الشهور الأولى فى شركتك عاملها كـ طفل صغير فى أسابيعه الأولى ينبغى عليك متابعته باستمرار وألا تغفل عنه حتى يستطيع أن يقف على قدميه . شركتك الأن فى حالة للرعاية والاهتمام والتواجد باستمرار فى مكان العمل والتواجد بين الموظفين والمتابعة الدورية لحال العمل . لا تستعجل الربح فـ كل المطلوب منك الأن هو الحفاظ على الشركة فى شهورها الأولى حتى تقوى على المنافسة فى السوق وحينها الربح سيأتى إليك دون أن تعلم .

لا تشغل بالك بالشركات المنافسة واشغل بالك بالعميل نفسه وحاول دائما أن تلبى رغباته وتكون عندحسن ظنه لأن العميل دائما على صواب وأنت فى احتياج المال اللازم لشركتك أما هو فيمكنه أن يتركك ويذهب لشركة غيرك .

فى حال تحقيق الأرباح وأردت أن تتوسع فى نطاق عمل الشبكة فلا أنصحك بذلك قبل مرور سنة على الأقل لان خلال هذه السنة سوف تمر بكل الأحداث السعيدة والحزينة فلا تغرك بعض الأرباح فى شبح التوسع فربما تمر عليك بعض الشهور بدون ربح للشركة حينها ستضطر لاستخدام مال الأرباح لضمان سير عجلة الشركة .

# بعض النصائح الضرورية لضمان استمرار شركتك

_ كلما استغرقت وقت أطول فى مرحلة التخطيط كلما كان أفضل لضمان رؤية الصورة كاملة من كل الزوايا بكل تفاصيلها حتى لا ترجع اليها مرة أخرى فى حال نسيت بعض تفاصيل الصورة .
_ يجب أن يسود روح الحب والتعاون بين أفراد فريق العمل وأنكم جميعا فى مركب واحدة اما أن تسير بكم فى هدوء وتصل بكم الى بر الأمان واما أن تكون رحلة شاقة تسودها الكراهية وحب السلطة فـ ستغرق السفينة قبل حتى أن تقطع نصف الطريق حينها سترجع لنقطة البداية .
_ قيم شركتك كل فترة زمنية ثابته سنة مثلا وقارن بين حال شركتك منذ البداية وحتى الأن وقرر هل أنت راضى عن حال الشركة أم لا وان كانت الشركة فعلا أثبتت نفسها أم أنها مجرد تضييع وقت .
_ لا تقف عند حد الشركة وحاول تطوير نفسك باستمرار لتواكب التطور وسوق العمل وتقدر على المنافسة .
_ استغل قدرة الشباب فى انعاش شركتك فعندهم طاقة رهيبة نتيجة سنين طويلة أمضوها فى التعليم ولديهم القدرة على التعلم وإثبات الذات لذلك لا تحرمهم من صعود سلم المجد عن طريق شركتك لربما تجد منهم من ينضم الى طاقم ادارة الشركة .


هذا كل ما لدى فى هذه المقالة
اذا كنت شعرت بأنك البطل فعلا فى هذه القصة فقم بالتقاط صورة لك وارسلها لى
,, تحياتى

Magazine
NetworkSet
First Arabic Magazine for Networks

ضع أعلانك معنا وساهم في
تطوير واستمرارية أول مجلة عربية متخصصة


انتشار واسع - تغطية شاملة

حزم اعلانية مختلفة تناسب جميع الاحتياجات

# المخاطر التى سوف تواجه الجيل الجديد من الأيبي IPv6



من يتابع أخبار الأنترنت وعالم التقنيات سوف يعلم أن اليوم هو يوم تحول كبير في عالم الانترنت لان الثامن من حزيران/ يونيو هو اليوم العالمي للـ IPv6 أما أعتبار أن اليوم هو تحول كبير في عالم الأنترنت فهو بسبب تحول أكبر شركات العالم في مجال الأنترنت إلى الجيل الجديد من الأيبي ومن أشهر هذه المواقع غوغل فايس بوك مايكروسوفت سيسكو والكثير من الشركات المعروفة.

لكن لأطرح عليكم سؤال طرحته منذ عام بالضبط وتحديدا في أفتتاحية العدد الثاني من المجلة حينما تحدثت عن نظرية التمييز وسألت في آخر المقال من منكم بحث عن المخاطر التى سوف تهدد الـ IPv6 وبحث عن حلول لها ؟؟؟

فالكل مجمع أن الجيل الجديد من الأيبي مؤمن بشكل جيد ولايحوي أي ثغرات لكن الواقع والخبير يقول أن هذا الجيل ليس بتلك الصورة التى تتخيلها, فمن خلال دراسة بعض النقاط وطرح بعض الأسئلة وجدت الكثير من النقاط الحساسة التى تهدد مستخدمي هذا الجيل من الأيبي وتهدد الاجهزة التى تعمل من خلالها , وما سأطرحه اليوم سوف يكون عن المشاكل التى يستطيع الجميع فهمها مبتدأ كان أم محترف وخصوصا أن النقاط المطروحة يجب أن تكون في عقلية كل مهندس شبكات لأنه الوحيد القادر على تحليل مثل هذه الأمور.

- النقطة الأولى التى يجب أن نضعها أمام أعيينا هو حجم الهيدر الخاص بالباكيت فكما هو معروف أن حجم الباكيت الخاص بالجيل الجديد من الأيبي هو أربع أضعاف الجيل القديم ولكن ماذا يعني ؟؟؟ وإلى ماذا يقودنا ؟؟؟ حقيقة أنا وضعت أمامك معلومة خطيرة وتحتاج

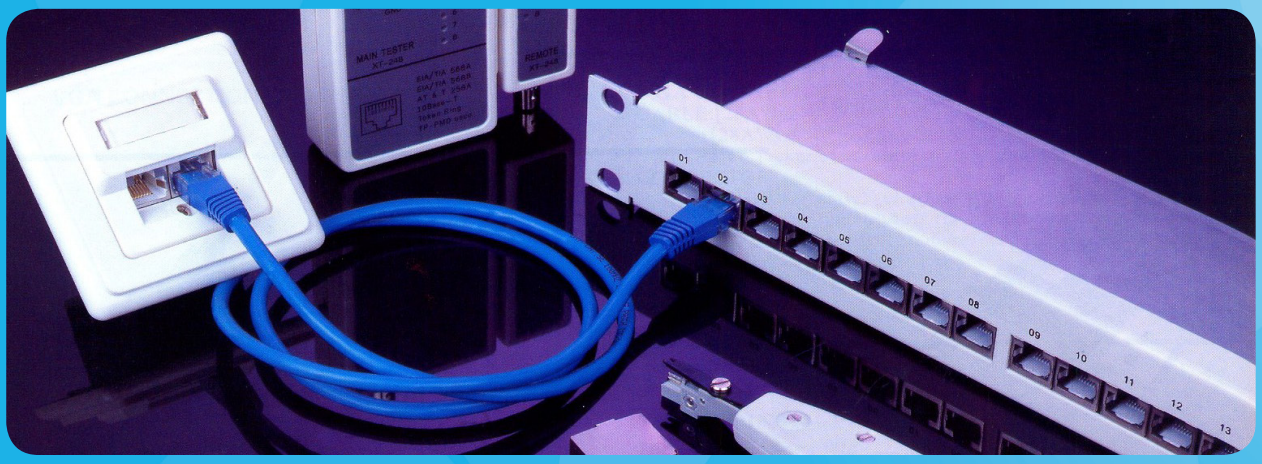
منك التفكير والتحليل قليلا للوصول إليها, فكما نعلم أن الروتر هو مسؤول عن عملية إدارة الباكيت!!!. هل توصلت إلى النتيجة ؟؟؟ طيب لنواصل وكون الباكيت أصبحت أربع أضعاف الجيل السابق فهذا يعني جهد أكبر من الروتر للمعالجة!!!. مارائيك هل بدأت تفهم الفكرة ؟؟؟ لنواصل بشكل أعمق , ياترى مارائي الروتر عندما يكون عليه هجوم مثل هجوم الـ DOS أو الـ DDOS ؟؟؟ وهي لب الفكرة الأولى فالباكيت سوف تكون بحجم أكبر وبأربع أضعاف وبالتالي الروتر سوف يعمل بشكل أكبر وزد على ذلك هجوم مثل الـ DOS أو الـ DDOS ؟؟؟ الهجوم الأول ليس خطيرا وطرق الحماية منه بسيطة لكن الـ DDOS هجومها خطير ولو أستهدفت روتر أو جهاز معين في شبكة فنسبة الدمار سوف تكون بشكل أسرع وأكبر لأن حجم الهيدر أكبر بأربع مرات وبالتالي أستهلاك أكبر لطاقة المعالج وهنا المشكلة.

- فكرة أستبدال الـ ARP بي الـ Neighbor discovery لن تحل المشكلة وسوف تبقي المستخدمين معرضين لنفس مخاطر الـ ARP الموجودة في الجيل السابق لأن عملية الـ Neighbor discovery غير مؤمنة ويمكن التلاعب بها بسهولة وبذلك نكون قد عدنا إلى نقطة الصفر وقد أعود لكي أتحدث عنها لاحقا.
- العدد الغير محدود الذي يقدمه لنا الجيل الجديد سلاح ذو حدين فهو قدم لنا حل فعال لمشكلة الأيبيات وزودنا بي 340 ترليون ترليون ترليون أيبي لكن لو أردت أن تعمل شبكة داخلية في الشركة التى تشرف عليها وأعتمدت على الـ Prefix الذي ينصح به دائما وهو /64 هل تعلم عدد الأيبيات المتاحة لك ؟ كوينتليون!!!. هل سمعت بهذا الرقم من قبل؟؟؟ نعم هو بعد كوادريليون!!!. لاتعلم الكوادريليون؟؟؟ طيب هو بعد الترليار واللي هو بعد الترليون والخ.... خلاص أنا لن أتابع لأني أعلم أن هذا الموضوع سوف يرفع ضغطك لذلك سوف أعود إلى الكوينتليون والذي هو 10 أوس 18 أيبي متاح لك في الشبكة ؟؟؟ طيب ماذا يعني هذا ؟؟؟ تصور أنك تريد القيام بعمل مسح للشبكة للبحث عن الثغرات والمشاكل الأمنية ياترى كم من الوقت تحتاج لمسح الكوينتليون هذا ؟؟؟ سنة على الأقل لتنتهي من المسح.... نقطة مفيدة لك ضد الأشخاص الذين يريدوا عمل مسح للشبكة لمعرفة الأيبيات والاجهزة الموجودة ولكن مضرة لو في حال أردت أنت ان تبحث عن الثغرات لذلك لا أنت ولا الهكر سوف يستطيع عمل مسح لشبكتك.
- النقطة الرابعة تتعلق بعملية الـ Translation التى سوف تحدث بين الجيل الجديد والقديم فنحن نعلم أن التحول الذي سوف يحدث لن يكون شامل لكل الانترنت بل لبعض الشركات وبالتالي يجي أن يكون لدى الشركات آلية تقوم بعمل ترجمة بين الجيلان ففي كل مرة تحتاج الاتصال إلى المواقع التى تعمل بالجيل الجديد تحتاج إلى عملية ترجمة معقدة تحتاج أجهزة قوية لتنفيذ المطلوب مع غض النظر أن هناك الكثير من المشاكل التى سوف تحدث أثناء عملية الترجمة وبالتالي المزيد من الثغرات والهفوات.

حقيقة هناك الكثير من النقاط لكن لم أتعمق بها كثيرا ومنها أستخدام الـ IPsec مع الجيل الجديد فنحن نعلم أن هذه الميزة كانت موجودة في خيارات الجيل القديم لكن مع الجيل الجديد هي جزء من الباكيت, هل ياترى سوف تكون إيجابية أم سوف يكون لها سلبيات؟؟؟ هذا مالدي اليوم بمناسبة اليوم العالمي للـ IPv6 أتمنى أن تكونوا قد أستفدتوا وبأنتظار تعليقاتكم وأرائكم حول هذا الموضوع ودمتم بود.


# لمحة على الشبكات الأفتراضية

تقنيات
الشبكات
الافتراضية الخاصة VPN أصبحت
الأن من أشهر التقنيات الشائعة لربط الشبكات وهى
بديل للحلول التقليدية المكلفة ذات الأسعار الباهظة ,فطالما يمكن
الحصول على نفس مستوى الحماية بتكلفة أقل بكثير من خطوط Leased-Line وطرق
التشبيك التقليدية إذن فلماذا لا يتم استخدام هذه التقنية ,ليس هذا فحسب بل فإن هذا النوع
من الشبكات له قائمة عريضة يمكنك منها اختيار النوع الذى تريده و حتما ستجد إحداها يتوافق
مع متطلباتك ومتطلبات الشبكة,خلال هذه المقالة نتعرف على أشهر أنواع هذه الشبكات الشائع
إستخدامها فى بيئة شبكات سيسكو .



**مفهوم الشبكات الإفتراضية بشكل غير تقنى :**

بعيدا عن المصطلحات التقنية والفنية التى قد لا تهم الكثير ,فببساطة شبكات ال VPN ما هى إلا قناة سرية مؤمنة أشبه بنفق يمكنك استخدامة لحماية بياناتك عند مرورها بمنطقة غير أمنة مثل شبكة الأنترنت ,فهناك وسيلة اتصال -وهى الانترنت- يمكنك من خلالها ربط أى جهازين مهما كان موقعهما ببعضهما ,ولكن يعيب تلك الوسيلة أنها تعج بالمخترقين والمخربين بالاضافة إلى عدد كبير من التهديدات التى لا مجال لذكرها هنا ,فبياناتك التى تتناقلها عبر تلك الشبكة يمكن أن يتم اختراقها بسهولة او الحصول عليها ,هنا كانت الفكرة فى إنشاء نفق له طرفين فقط ,هذا النفق يربط بين نقطتين محددتين الأولى هى شبكتك المحلية والأخرى هى الشبكة الهدف التى تريد ربطها مع الشبكة الأولى لتصبح الشبكتين كيان واحد متصلين عن طريق الأنترنت الذى لا يمثل أكثر من مجرد Link يربط الفرعين ,وعند رغبة أى من الطرفين فى تبادل أى بيانات فما عليه إلا أن يقوم بدفعها إلى هذا النفق لتصل إلى طرفه الأخر بأمان .

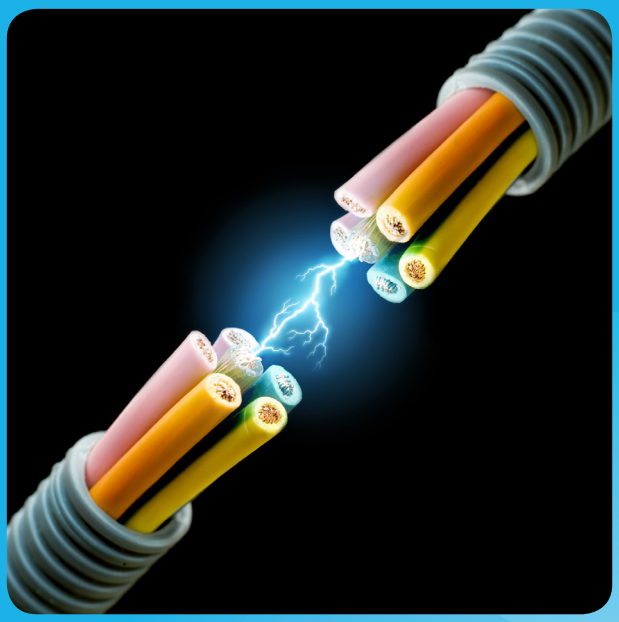
أما لمن يعنى بالتفاصيل التقنية :

شبكات ال VPN هى تطبيق بحت لعلوم التعمية والتشفير ,فغالبا ما تجد مقدمة عن التعمية Cryptography فى مقدمة أى كتاب يتناول شرح هذه الشبكات ,الفكرة تكمن فى استخدام مجموعة من الخوارزميات والبروتوكولات التى تم جمعها فى حاوية تسمى IPSec ,هى أشبة بمجموعة بروتوكولات TCP/IP لكن يميزها أنها تتعلق فقط بالحمايةوالتشفير ,وباستخدام هذه البروتوكولات يتم تشفير البيانات المتناقلة بين أطراف الشبكة الافتراضية ولهذا سميت افتراضية لأنها لا وجود لها على أرض الواقع بل هى عملية نظرية يتم تطبيقها على سيل البيانات والحزم فتنطلق عبر الأثير السايبيرى مع الحزم الأخرى لا فرق بينهم سوى مستوى التأمين , \ومن متطلبات هذه العملية خوارزميات التشفير Encryption Algorithm - خوارزميات فك التشفير Decryption Algorithm - خوارزميات لتبادل المفاتيح ISAKMP - وأخيرا منظومة للتحقق من الهوية سواء عن طريق شهادات الموثقية الرقمية Digital Certificate أو عن طريق مفاتيح Pre-shared Key, هذه هى البنية التحتية لشبكات ال VPN التى تعتمد عليها فى ضمان سرية البيانات .

## أشهر أنواع الشبكات الأفتراضية :

### VPN Site-To-Site

هذا هو اكثر الأنواع شيوعا للشبكات الأفتراضية حيث يكون هناك اتصال بين طرفين يكونوا فى العادة إما روترين أو روتر وجدار نارى يدعم إتصالات ال VPN , ومن متطلبات هذا السيناريو وجود عناوين ثابتة لكل طرف من الطرفين ويتم إعداد كل طرف لتعريفه بالوجهة الأخرى التى سيقوم بتشفير البيانات لها ,فأى بيانات سيتم ارسالها بين الطرفين يتم عمل Encapsulation لها بعناوين ثابتة لا تتغير وتحتوى بداخلها على الحزمة نفسها بالعناوين الحقيقية التى من الممكن أن تكون من نطاق العناوين الخاصة لأن كل هذا المحتوى يكون مشفر ,فالحزمة نفسها



تبحر فى الانترنت بعناوين طرفى النفق وهى أجهزة الشبكة .

وبالطبع لابد من وجود اليه للتحقق Authentication, فاذا كانت الشبكة صغيرة يمكن الأعتماد على مفاتيح Pre-shared Key أما إذا كانت تتعدى العشر روترات فعندها لابد من الأعتماد على الشهادات الرقمية Digital Certificate ووجود موزع لها Certificate Authority على الشبكة .

أحد عيوب هذا النظام هو عند التوسع فى التوصيلات ,فعلى سبيل المثال إذا زادت عدد الفروع عن عشرة فروع مطلوب ربطها ببعضها Full-Mesh Topology أى ان كل فرع يكون متصل بكل الفروع الأخرى مباشرة ,عندها ستكون الاعدادت معقدة وصعبة الادارة والصيانة اذا ما حدث أى مشكلة فى الاتصال .

### DMVPN (Dynamic Multipoint VPN)

هذا النوع هو شبيه بالنوع الأول ويمكن القول أنه يعتمد على نفس الأليات والبروتوكولات فى العمل إلا أن الفارق فى ادارة الاتصال , ففى هذا النوع يتم الاعتماد على روتر يسمى Hub وهو قلب الشبكة ,بينما بقية الروترات يطلق عليها Spoke, ويتم تعريف كل Spoke بعنوان ال Hub الذى لابد أن يكون Static IP بينما عناوين ال Spokes من الممكن أن تكون Dynamic IPs ,فكرة هذه الشبكة تعتمد على عنصرين :

## بروتوكول Next Hop Resolution Protocol (NHRP).

فى البداية يقوم كل Spokes بعمل Registeration على ال Hub بحيث يكون ال Hub هو الوحيد الذى لديه معرفة بعناوين كل ال Spokes على الشبكة وهذا يتم عن طريق هذا البروتوكول ,وعندما يصل إلى أى روتر من ال Spokes طلب للوصول إلى شبكة أخرى عن طريق ال DMVPN ,وهذه الشبكة موجودة على Spoke اخر عندها يطلب من ال Hub عنوان هذا ال Spoke ليتم فتح قناة مباشرة تسمى Spoke-To-Spoke Tunnel وهى لا تمر بال Hub .

## Routing Protocol

فائدة الروتنج بروتوكول أنه يقوم بالربط بين عناوين ال Spokes المحلية وعناوينهم الحقيقة التى تستخدم فى الاتصال ,ولابد من وجود نفق GRE لكى تستطيع بيانات ال Multicast العبور فيه ,ويمكن فى مقالات قادمة شرح الموضوع أكثر بشكل عملى للتوضيح .

مميزات هذا النوع هى فى سهولة إضافة فروع أخرى ,فعند إضافة فرع جديد إلى الشبكة كل ما عليك فعله هو اعداد هذا ال Spoke الجديد بالاشتراك عند ال Hub ليتولى هو عملية إخبار باقى الشبكة ,وكل هذا يحدث بشكل ديناميكى أى أنك لن تحتاج إلى تغير اعدادات كل روترات الشبكة مثل النوع السابق .

وهذه أمور يجب أن تضعها فى الإعتبار قبل التفكير فى ال VPN :
قبل أن تقرر أى من الأنواع تختار ضع فى اعتبارك ما يلى واعتمد عليه لتحديد أى نوع هو الأفضل لك

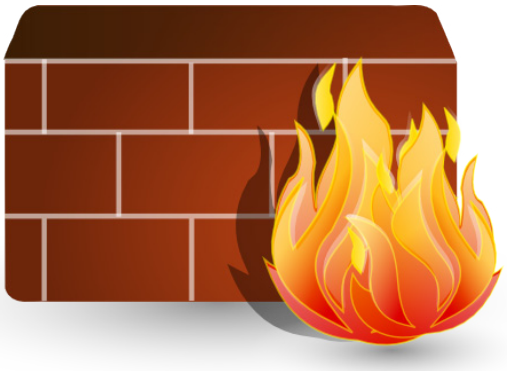
- عدد المستخدمين .
- الباندويث المتاح .
- مستوى الأمن المطلوب .
- التكلفة وهل ستحتاج إلى أجهزة أو رخص إضافية أم لا .

وقبل محاولة تطبيق هذا النوع حاول أن تتوسع فى القراءة عنه لأن الموضوع لا يقتصر على نجاحك فى اعداده بل على قدرتك على حل أى مشاكل قد تحدث لاحقا فى هذا النوع من الشبكات لأنها تكون فى الغالب معقدة ويصعب كشفها .
وفى نهاية هذا الجزء أتمنى أن أكون قد قدمت ما يفيد ,وتابعونى فى الأعداد القادمة لإلقاء نظرة على أنواع جديدة من هذه الشبكات مثل GET VPN - SSL VPN - Remote Access VPN ومواضيع أخرى وإلى اللقاء فى العدد القادم .


# كيف يعمل SPI Firewall

هنالك أنواعا متعددة من الـ Firewalls أو الجدران النارية التي تستخدم لحماية الشبكات وصد هجمات الهاكرز . إلا أننا في هذا المقال سنتكلم بإسلوب مبسط عن SPI Firewall وكيف يعمل .

بالإضافة إلى مقارنة بنوع أخر من الجدران النارية .

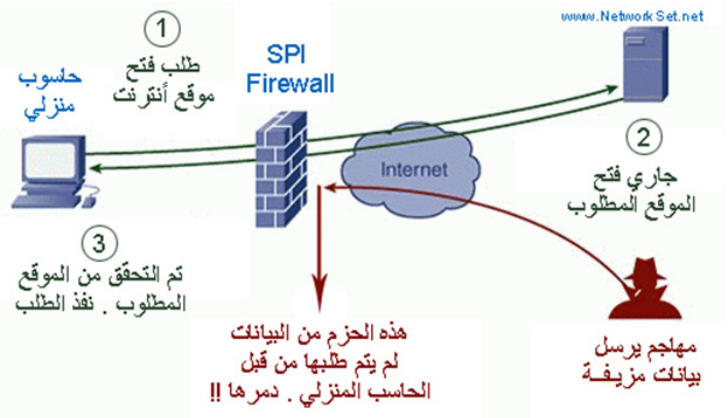


يقوم هذا النوع من الجدران النارية بفحص الـ Packets أو حزم البيانات المتدفقة من الشبكة الداخلية والشبكة الخارجية أو الأنترنت . حيث يقوم SPI Firewall بالتحقق من هذه الـ Packets ما إذا كانت تنتمي بطريقة شرعية لحزم البيانات المتدفقة بين الشبكة الداخلية والخارجية . كذلك يقوم بفحص Destination Address أو عنوان الجهاز المستقبل و Source Address أو عنوان الجهاز المرسل . بالإضافة إلى تحققه من عنوان المنفذ أو Port Address . كما أنه يقوم بالتحقق ما إذا كانت البيانات أثناء الإتصال تصل في الوقت المتوقع أم لا . ولتوضيح العملية أكثر دعنا نأخذ هذا المثال المبسط .

تخيل أن (المهندس أيمن ) يجري محادثة مع (المهندس نادر) وكان الحديث كالتالي :
المهندس أيمن : «مرحبا مهندس نادر».
المهندس نادر : «أهلا وسهلا مهندس أيمن».
المهندس أيمن : «كيف حالك ».
المهندس نادر : «أهلا وسهلا مهندس أيمن».
المهندس أيمن : «هل تسمعني؟؟».
المهندس نادر : «أهلا وسهلا مهندس أيمن».

ماذا إتضح لك من خلال المحادثة التي جرت بين المهندس أيمن والمهندس نادر ؟؟ لاشك أن لاحظت بأن المهندس نادر كان يكرر عبارة « أهلا وسهلا مهندس أيمن» عدة مرات متتالية . وهنا شي من الشك !! لأن حزم البيانات لا تصل للجهة الأخرى في الوقت المتوقع وهذا ما يفحصه الـ SPI Firewall كما ذكرنا سابقا. أي يشكك الجدار الناري بأن هنالك شي يسبب تأخر في حزم البيانات .

ومن خلال هذا المخطط سنتعرف بشكل أوضح كيف يعمل هذا النوع من الجدارن النارية :



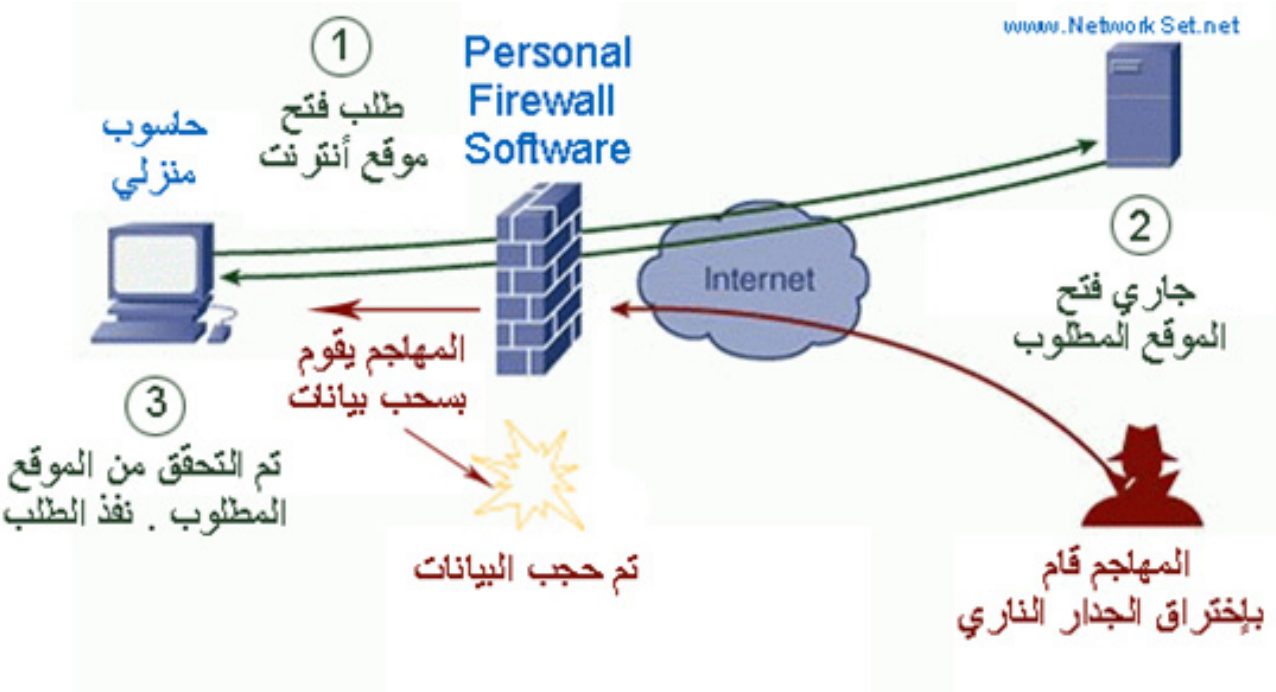

كما يتضح لك من خلا المخطط بالأعلى أن الخطوط السوداء تمثل عملية تنفيذ الجهازالمنزلي لطلب من الشبكة الخارجية أو الأنرنت. حيث أن هنالك SPI Firewall يقع بين الحاسب المنزلي وشبكة الأنترنت. أو بالأصح الشبكة الداخلية (المنزلية) والشبكة الخارجية (الأنترنت). حيث يقوم الحاسب المنزل هنا بطلب فتح احد مواقع الأنترنت وتبدأ حزم البيانات تتدفق من الحاسب المنزل عابرتا الجدار الناري SPI Firewall ثم إلى سيرفر موقع الأنترنت كما هو واضح بالمخطط

وعندما تعبر حزم البيانات من خلال الجدار الناري ، يقوم SPI Firewall بالتحقق من حزم البيانات وينتظر الإستجابة من سيرفر الموقع كما يظهر في الخطوة 2 على المخطط . بعد أن يستجيب سيرفر الموقع ، ويتم التحقق من الطلب بشكل صحيح ، ثم يتم تفيذ

طلب الحاسب المنزلي وفتح الموقع المطلوب كما هو موضح في الخطوة 3 .

لكن ماذا لو قام مهاجم بإرسال بيانات مزيفة بغرض خداعك وإرسال بيانات توهمك بأنها الموقع الذي طلبت فتحه ؟؟ هنا يتدخل الـ SPI Firewall ويقوم بحجب البيانات المزيفة ثم تدميرها قبل دخولها الشبكة الداخلية كما يتضح في المخطط .

يعتبر SPI Firewall حل جيداً للتقليل من مخاطر الهجمات . لكن لو تم أختراقه بطريقة عبقرية ، فأن ملفات التجسس يمكنها أن ترسل معلومات عنك إلى المهاجم مما يسهل حينها إختراق جهازك . ولكن هنالك نوع أخر من الجدارن النارية يسمى Personal Software Firewall . هذا النوع من الجدران النارية يتميز بميزة أفضل من SPI Firewall والتي سنوضحها في المخطط التالي :




يعتبر SPI Firewall حل جيداً للتقليل من مخاطر الهجمات . لكن لو تم أختراقه بطريقة عبقرية ، فأن ملفات في هذا المخطط جرت نفس العملية السابقة ولكن هنا تمكن المهاجم من التحايل على الجدار الناري ودخول الشبكة الداخلية والهجوم على الحاسب المنزلي لسرقة بياناته .بعد أن قام المهاجم من أختراق الشبكة الداخلية ، قام بمحاولة سحب بيانات الجهاز المنزلي إلا أنه فشل .
لأن الـ Personal Firewall Software يتميز عن SPI Firewall بأنه يتمكن من حجب الهجمات والواردة من خارج الشبكة ومن داخلها . بينما SPI Firewall فقط يستطيع حجب الهجمات الواردة من خارج الشبكة. فلو كان هنالك SPI Firewall لما تمكن من منع المهاجم من سحب بيانات الحاسب المنزلي.

ختاما لهذا المقال ، نتمنى أن نكون قد أوضحنا أن هنالك أنواع من الجدارن النارية تختلف في ألية عملها وقوة حمايتها . فقد أوضحنا لكم أبسط أنواع الجدارن النارية وربما مستقبلا نكتب لكم عن أنواع أخرى أكثر تقدما.


# مقدمة عن سويتشات شركة HP

## الجزء الثاني

نستكمل اليوم ما تكلمنا عنه في المقال الماضي من سويتشات HP ونسال اللّه أن ينفع بهذا المقال كل من لديه رغبة في دخول عالم HP , ومقالي لهذا العدد سوف يكون عن نوع محدد من سويتشات HP المعروف بإسم

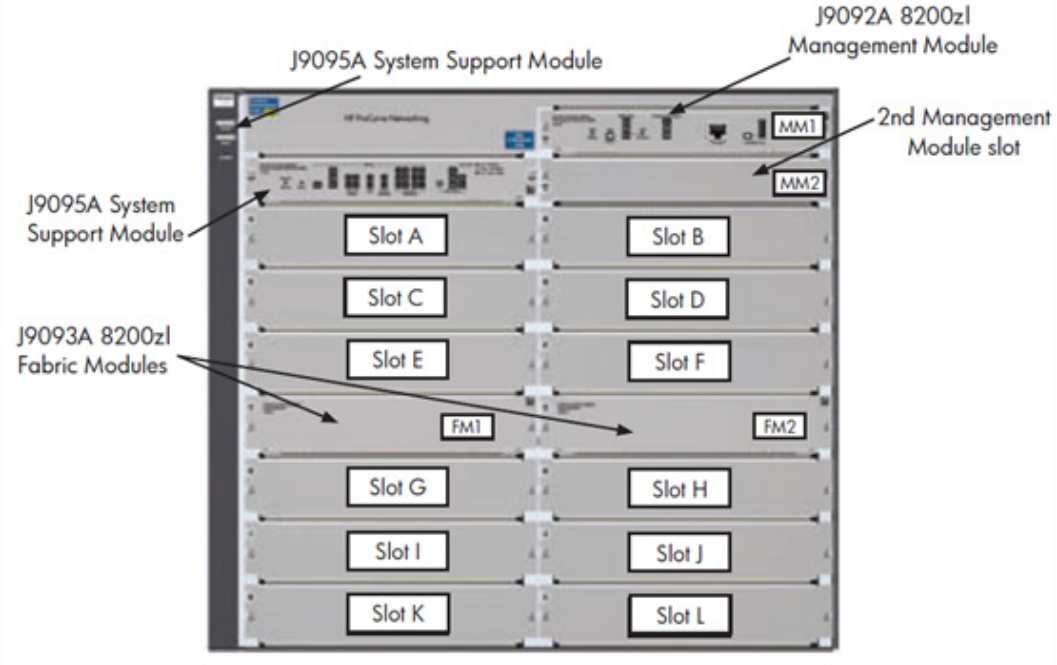
HP ProCurve Switch 8200zl Series

طبعا هذا السويتش يتكون من مجموعة من Slots
يتم تركيب Module في كل Slot

Switch 8206zl Chassis layout

The Switch 8206zl is a rack-mountable, 6U-height chassis. The interface modules are inserted in the front slots, labeled A through F. Management and fabric modules are labeled MM1/MM2 and FM1/FM2, respectively

يحتوي ال Module على port 24 وهذه صورة للتوضيح




1 - كما بالشكل يتكون السويتش من عدد من Slots وهي بالترتيب من A-B-C-D-E-F-G-H-I-J-K-L

2- Fabric Modules

وهو المسئول عن ربط Modules بعضها ببعض داخل السويتش حتي يصبح كل Modules كأنها سويتش واحد ويتم عن طريق Tunnels موصله بعدد 2 Links كل Link يكون سعته 14.4 Gbps فيكون مجموعهم 28.8 Gbps

3 - Management Module

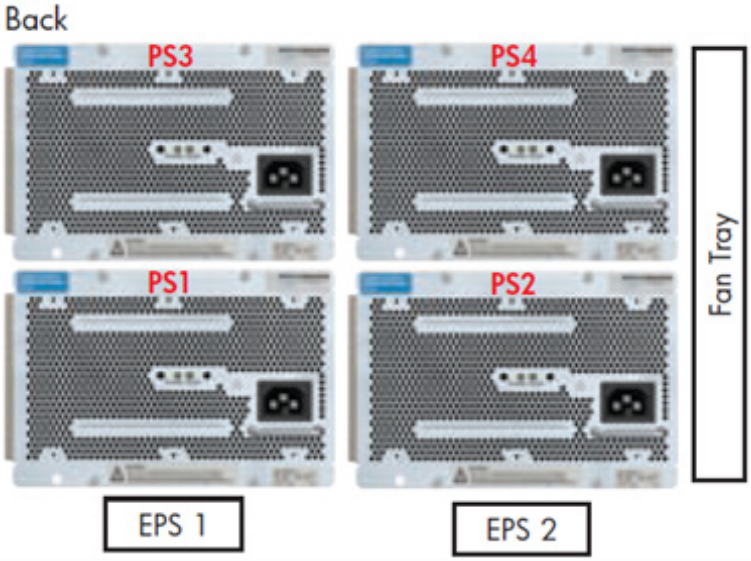
وهو المسئول عن إدارة السويتش بالكامل وهو يتكون من CPU , RAM, Console Interface, بالاضافة الي LEDs

4 - System Fan Tray

وهي المسئولة عن عملية التبريد للسويتش من الداخل – وتعتمد سرعة دوران هذه المراوح على درجة حرارة Chassis وتزداد سرعة الدوران كلما ارتفعت درجة حرارة Chassis

5 - Power Supplies

وتستخدم في حالة Power Redundancy (وهو امكانية تغيير اي Power Supply أو Management Module أثناء عمل السويتش ) طبعا مع الاحتفاظ بوجود Power Supply واحد يقوم بالعمل أثناء التغير ) ويستخدم ايضا في اي خصائص اضافية في حالة Power Over Ethernet

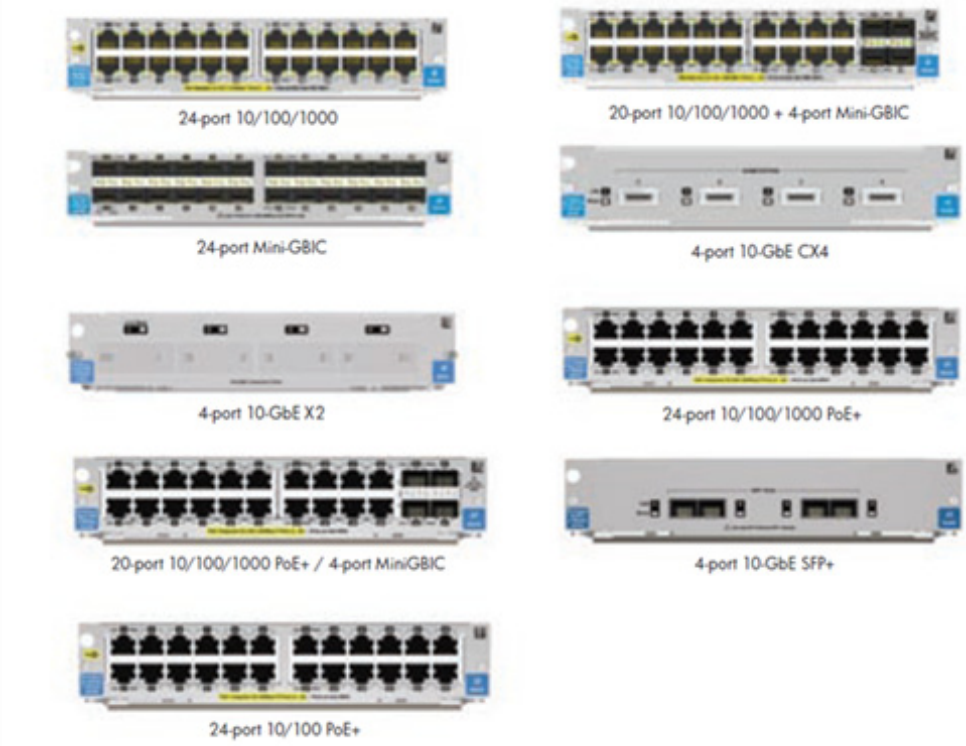



ولا بد ان يحتوي السويتش علي في أقل الحالات علي 2 Power Supplies

و أقصي عدد يكون 4 Power Supplies

ولا بد أن يكون واحد فقط يعمل حتى يكون السويتش يعمل بشكل طبيعي لتشغيل 6 Slots وهذه صور ال Power Supplies

- والان سوف ناتي الي معرفة أنواع وأشكال Modules مع التوضيح بالصور :
طبعا هذه مداخل Fast Ethernet وأيضا مداخل فايبر GBIC - وتكون حسب إحتياجك للشبكة




وآخيرا لنسعرض بعض مميزات هذا السويتش HP ProCurve Switch 8212zl

1-High Performance
2- Security ACLs (per-port)
3- IP Routing
4- Supported for IPv4/IPv6 dual stack
5- Resiliency- Redundant Power Supplies, Hot-Swappable

وهذه مميزات هامة جدا لهذا السويتش حيث انه يملك High Capacity مع Fabric Modules
عن طريق Tunnels موصله بعدد 2 Links كل Link يكون سعته 14.4 Gbps
بالاضافة الي امكانية عمل Access list علي السويتش وعمل بعض الاعدادات لحماية السويتش من عمليات الهاكرز
بالاضافة الي امكانية عمل Routing علي السويتش حيث تم التوضيح في المقال السابق ان السويتش يعمل Layer 3
بالاضافة الي انه يدعم IPV4 and IPV6
ثم انه من أهم مميزات هذا السويتش هو عملية Resiliencyعن طريق تغيير Power Supply أو Module أو Fabric Module دون إطفاء السويتش عن الكهرباء .

*Magazine*

# NetworkSet