

April 2011

Issue 12

Magazine

NetworkSet

First Arabic Magazine for Networks

القواعد الذهبية لتمديد كابلات الشبكة

مقارنة هامة بين VLSM & CIDR

Spanning Tree Protocol

معايير معهد مهندسي الإلكترونيات

و الكهرياء للشبكات اللاسلكية

www.NetworkSet.net

NetworkSet

وأعود وأذكر مرة أخرى أن المجلة مفتوحة للجميع فنحن هدفنا نبيل ولوجه الله تعالى فساهم معنى في رفع مستوى الأمة العربية فكتابة مقال لن تأخذ معك أكثر من يوم واحد وسوف يقرأها ويستفيد منها الآلاف ومئات الآلاف فهل هناك خير أفضل من هذا العمل؟

النقطة الأخيرة وهي موضوع الدعم المادي. و حقيقة منذ إنشاء المجلة أول مرة وضعت خطط لن أعرضها عليكم حاليا حتى نتمكن من إنجاح الخطة الحالية وكانت تتمثل الخطة الحالية بأن يصبح لدينا عدد جيد من المحررين ونجد شركات أو مؤسسات تدعمنا لإكمال المشوار، وللأسف الشديد لم نجد لا هذا ولا ذاك، وكنت أيضا أتمنى أن يكون لدينا دعم لكي نخصص قسم منه للمحرفين كشيء رمزي ومشجع في نفس الوقت، لكن تجرى الرياح بما لا تشتهي السفن.

وأخيرا أسمحوا لي بالتطرق لموضوع آخر وهام وهو الويكي أو الموسوعة العلمية التي أطلقها NetworkSet منذ ثلاث أشهر ولم تجد مساهمين حقيقيين فنحن جميعنا يدرك مدى أهمية هذه الموسوعة وباللغة العربية العلمية وثق تماما أن كل ماتكتبه سوف يستفيد منه غيرك وحتى لو كان مجموع ماتكتبته ثلاث اسطر ولا تنسى أيضا المقولة المعروفة زرعوا فأكلنا نزرع فيأكلون وهي عبرة جيدة لمن يبحث عن مصلحة عامة تخدم كل أفراد المجتمع العربي ودمتم بود.

في مثل هذا اليوم كتبت لكم خبر إطلاق العدد الأول من المجلة، والحمد لله وبرغم كل الظروف والأقوال والرسائل التي وصلتني بشكل مباشر وغير مباشر تقول لي أن ما بدأت فيه هو مرحلة حماس فقط وسوف تتوقف بعد مضي بضعة أشهر. لكن وبفضل الله خالفنا كل التوقعات واستمرينا لسنة كاملة وبدون توقف. وهذا لم يكن لولا توفيق الله، ثم مساعدة بعض الأخوة الأعزاء، والذين هم برأيي السبب في نجاح المجلة، وساعدوا على استمراريتها وهم مع حفظ الألقاب:

أحمد الشحات، عادل الحميدي، ياسر رمزي، مح مدالتميمي، عبد المجيد خالد الكثيري، أحمد بخيت، عمرا السويدي، أحمد الجلجولي، محمود عمر، عدن انالشمري، محمد عبدون، نادر المنسي، محمد ناجي سيد، إسلام محمود، أحمد مصطفى، دبالى الحسن، صالح الصافي، صفا الرضائي، أنس الأحمد، إسلام محمد، علاء مازن عدي، عبد الرحمن بن داود، عمرو يحيى، عبد الجليل الوكيل، شريف وجدي، وأخيرا أنس الأحمد كمصمم للمجلة، وأسامة الشرقاوي كمدقق إملائي ومترجم للمجلة.

أما إحصائيات المجلة فلقد وصل عدد مرات تحميل المجلة إلى ١٣٠٠٠٠ مرة تحميل مسجلة من خلال المدونة، وهذا العدد يقل عن الرقم الحقيقي للمجلة لأن المجلة إنتشرت على بعض المنتديات بروابط مباشرة، وعلى مواقع تحميل مختلفة وعملية تبادل بين الناس وحقيقة أنا لا أبحث عن أرقام أبدا فهذا العدد كافي بالنسبة لمجلة متخصصة وموجهة لنسبة معينة من الناس. ويكفينا شرف أننا قمنا بعمل أول مجلة عربية متخصصة واستمرت لعام كامل وبدون توقف.

المؤسس ورئيس التحرير
م. أيمن النعيمي

المحررون
م. أنس الأحمد

م. نادر المنسي

م. أسامة الشرقاوي

م. عبد الرحمن بن داود

م. أحمد الشحات

م. شريف مجدي

التصميم والإخراج الفني

صدا

حلول تقنية متكاملة

eng.Anas kh al-Ahmad

eng.Salah Baybars

سوريا - دير الزور

00963 51 215452

00963 967 962 665

الآراء المنشورة تعبر عن وجهة نظر الكاتب ولا تعبر عن وجهة نظر المجلة // جميع المحتويات تخضع لحقوق الملكية الفكرية // ولا يجوز النقل أو الاقتباس دون إذن من الكاتب أو المجلة

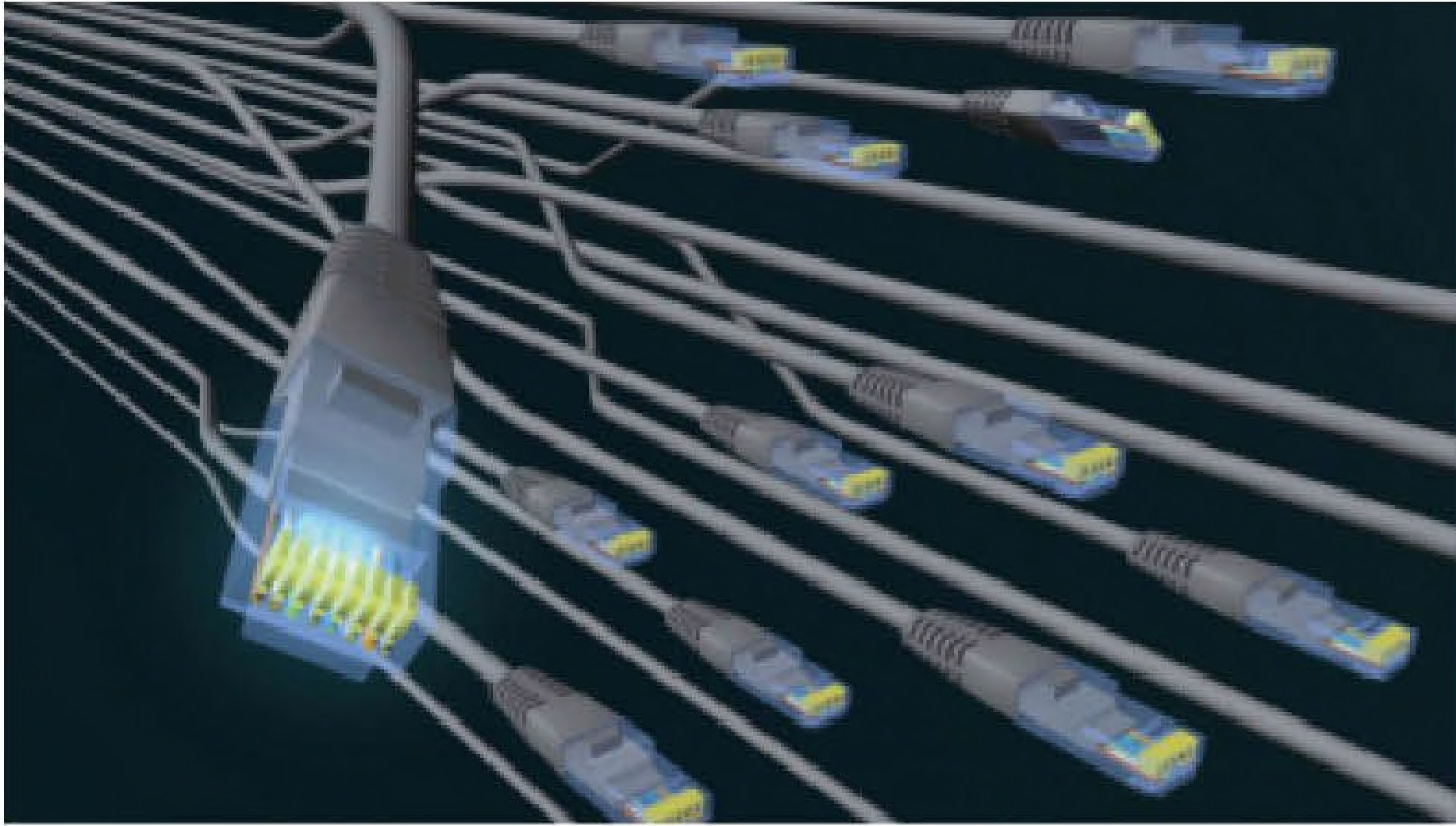
نعنذر في هذا العدد من قراننا الأعزاء أشد الاعتذار إذا كان العدد الحالي لا يرتقي إلى المستوى التصميمي والفني المطلوب وذلك نظر الظروف خارجة عن إرادتنا وإن شاء الله سيتم تعويض ذلك الأمر

ملحوظة

التنفيذ
والإخراج الفني

المحتويات

الصفحة	الموضوع
٣	المحتويات
٤	القواعد الذهبية لتمديد كابلات الشبكة
٦	المشاكل ٢٥ للشبكات وحلولها
١٠	مقارنة هامة بين VLSM & CIDR
١٢	Cryptography – PART I Security Principles
١٦	Spanning Tree Protocol
١٨	Cisco Certified Systems Instructor
٢٠	طريقة توقيت عمل الأكسس ليست على أجهزة سيسكو
٢٢	ال الحلقة الثالثة من تقنية الVirtualisation مع الVMware ماهية الvSphere
٢٥	معايير معهد مهندسي الاللكترونيات و الكهرياء للشبكات الالاسلكية
٢٨	Call Coverage



The GOLDEN RULE

القواعد الذهبية لتمديد كابلات الشبكة

ففي حال كونك أحد هؤلاء المتخصصين في تكنولوجيا المعلومات IT pro، أو مديرا لإحدى قطاعاته، أو حتى من الفنيين المبتدئين في تمديد الكابلات، أو من غير المختصين في هذا المجال وتريد أن تقوم بتمديد شبكتك بنفسك ومن مديني منطقتي HYS = help your self، إذا لابد أن يكون تمديد كابلات شبكتك غير باهظ الثمن لك لا يثقل ميزانيتك أو ميزانية المؤسسة التي أنت مسؤول عن تمديد الكابلات بها، و إلا يكون بالطبع إمساكك عن إنفاق بعض المال علي حساب الجودة. وهذا فقد سرد صاحب كتاب (Cabling the complete guide to network wiring) عدة قواعد نعتها بالذهبية وهي بديهي عند يدك في التفكير في إنشاء شبكتك وقد ألفت الكثير إليها .

- ١- إجعل مسار الكابلات بعيدا عن أماكن تمديد الكابلات الكهربائية ذات الضغط العالي، وبعيدا عن الأماكن التي بها أجهزة كهربية تصدر ترددات ناشئة عن وجود ملفات أو موتورات.
- ٢- لابد وحتما أن يكون مسار الكابلات بعيدا عن أماكن تمركز الطفرات الحرارية مثل السخانات أو المكيفات لأن التغير في درجة حرارة الكابل يغير من مقاومته وبالتالي يؤثر علي تناقل البيانات التي هي في الأصل إشارات كهربية.
- ٣- خريطة تمديدات الكابلات هي المنقذ الرئيسي، والمرجع الأول والأخير عند حدوث معظم مشاكل الكابلات.
- ٤- إجتهد في توصيل كابلاتك إلي الأماكن التي ستعلم أنك ستحتاجها مستقبلا، ولا تقتصر علي الأماكن التي تحتاجها حاليا.
- ٥- تتبع وإعرف المواصفات القياسية العالمية لتمديد الكابلات وذلك لحماية بيئتك أولا من مزار الكابلات الغير مرخص إستخدامها، وثانيا لضمان جودة أعلى في نقل البيانات.
- ٦- إستخدم كابلات ذات مواصفات جودة عالية، وليس شرطا أن تكون الأعلى سعرا هي الأفضل جودة.
- ٧- لا تبخل في إنفاق المال مختارا علي شبكة ذات جودة عالية، فربما ستنفق هذا المال وأكثر منه علي صيانتها فيما بعد مضطرا.
- ٨- إنظر إلي متطلبات شبكتك ونوع البيئة التي سوفتقوم بالتمديد فيها ثم إختار نوع الكابلات التي تناسبها.

٩- العمر الافتراضي لكابلات الشبكة متوسطة العمر (١٦ سنة) وهي بهذا الشكل أطول أجزاء الشبكة عمرا، و لذلك فإن إنفاقك عليها عشر قيم الشبكة الكلية ليس بالكثير.

١٠- سبعون بالمئة من مشاكل الشبكات ناشيء عن التمديد السيء للكابلات، فحاول أن تستخدم أشخاص أو جهات ذوي خبرة في تمديد الكابلات إذا كانت كابلاتك سيتم

١٢- إدرس الطبيعة التي ستمد فيها الكابلات

عند توليك مهمة مد كابلات في إحدى المباني فإنه لا بد أن تدرس الهيئة المعمارية للمكان، وأن تعرف الأماكن التي ستمد إليها الكابلات وأنواع الشبكات التي ستصل إليها بل والغرض من استخدام تلك الأماكن للشبكة ومدى أهمية كل موقع علي الشبكة كي يتسني لك معرفة أنواع الكابلات التي ستستخدمها. نعم هذا ضروري جدا فنحن لن نقوم بتمديد فقط شبكة في قهوة إنترنت، بل ربما تخدم وزارة كاملة أو مؤسسة إقتصادية أو حتي مدينة صغيرة وهذا هو الغرض من هذه الدورة. وعندما نتكلم مثلا عن ربط شبكة في إحدى قري محافظة الشرقية بمصر فإنها ستختلف قطعاً عن ربط نفس الشبكة في إحدى المباني العملاقة بإمارة دبي، وهناك أنظمة شبكية تتطلب أنواع كابلات خاصة.



١٣- هل ستحتاج لسرعات

قديما أذكر أنني كنت أتعامل مع نظام تشغيل الدوس ورأيت البرمجيات التي كان يدعمها مثل لوتس ١٢٣ و db و gwbasic وكانت هذه البرمجيات لا تحتاج إلي مواصفات كبيرة للأجهزة وبالتالي فإن البيانات الخارجة منها تستطيع أن تنقلها علي أقراص مرنة بسعة ٥١٢ كيلوبايت، وكانت إذ ذاك تتحملها شبكات هذا العصر والأمن نجد أن برمجيات الكمبيوتر قد أودعت الكثير من أجهزتنا في صناديق القمامة لقصورها عن تلبية إحتياجات تلك البرمجيات. لا تنتظر كثيرا أن تقف تكنولوجيا صناعة الكابلات مكتوفة الأيدي في ظل ذلك التطور الهائل فلا بد أن تتطور الكابلات بلو تكنولوجيا النقل عامة

١٤- في أي مكان ستستخدم الكابلات (Backbone cables)

ترجمتها الحرفية العمود الفقري و هي الكابلات التي أهميتها في الشبكة مثل أهمية العمود الفقري في الإنسان وهي كذلك فعلا لأنها تربط بين ال PC و أجهزة الشبكة الرئيسية مثل servers, switches, routers بالأجهزة ولذلك يفضل لها كابلات سريعة مثل الألياف البصرية.

(Horizontal cables)

وهي الكابلات التي تصل الحجلات بالمخارج التي في الحائط wall outlets وتستخدم فيها الكابلات النحاسية. كي تستطيع أن تتحمل ذلك الكم الهائل من البيانات التي تمر من خلالها ويخطط المصممون الآن للحصول علي تكنولوجيا تكون قادرة علي نقل ١٠ جيجا بايت لكل ثانية عبر الكابلات.

THE TOP 25 NETWORK PROBLEMS AND THEIR BUSINESS IMPACT

3- سهل قواعد على الجدار الناري وعدم إستخدامها، وإدخال هذخلات فى ال (ACL) بدون فائدة

تؤدى إلى ضعف أداء الجدار الناري. جعل الجدار الناري مفتوح، والقواعد غير المستخدمة، يؤدى إلى إحداث مشاكل حماية. لكي يكون الجدار الناري فعال بشكل أكثر فى شبكتك ويؤدى الحماية المطلوبة، فعليك أن تفعل القواعد المناسبة فيه وتتجنب عمل أى قواعد بدون فائدة فعلية.

4- تجاوز العدد المسموح به من علاقات الإتصال عبر الجدار الناري

فشل محاولات الإتصال الجديدة مع الجدار الناري. تعرض برامج العمل لإخفاقات متقطعة عند الضغط العالى على الجدار الناري.

إخفاق الشبكات الخاصة الافتراضية (VPNs).

يرفض الجدار الناري المشغول أن يتعامل مع محاولات الإتصال الجديدة. وفى هذه الحالة عند محاولة البرامج الإتصال بالشبكة عبر الجدار الناري فإنها تفسل.

5- إستخدام خط الإتصال فى تحميل ملفات صوت أو فيديو

بطء إستجابة البرامج مما يؤثر على عمل المستخدم. عندما يستحوذ برنامج ما أو مستخدم على أغلب سعة الخط، فإنه يؤثر على باقى البرامج والمستخدمين الآخرين لهذا الخط. وتستخدم (NetMRI) برنامج (Getflow) الخاص بها لتجمع بيانات حالة عن أى خط إتصال إرتفع معدل إستخدامه بشكل مفاجئ. إستعراض البرامج والمستخدمين الذين يستخدمون هذا الخط يسمح لمهندسين الشبكات أن يحلوا سبب بطء عمل البرامج و أيها يستحوذ على سعة الخط وما هو الإجراء المناسب لحل هذه المشكلة.

6- إختناق مخرج الربط بالبيانات

أداء غير متوقع للبرامج، يؤثر على عمل المستخدم. عندما تزدحم البيانات عند مخرج الربط (Router Interface)، فإنه يبدأ فى نبذ بعض الحزم لذا فإن مراقبة الحزم التى تم نبذها

من المهم دائماً توضيح المشاكل التى تقابلنا فى مجال الشبكات وإيجاد الحلول السريعة والمناسبة لها وتبادل الخبرات. فتعلم الشبكات والتعامل معها لا يقتصر فقط على معرفة و دراسة البنية التحتية للشبكات أو التصميمات المختلفة لها فقط، ولكن ركن أساسى فى مسيرة مهندس الشبكات أو من يتعامل معها يتمثل فى تعلم كيفية تحليل المشاكل التى تقابلنا ومعرفة أسباب هذه المشاكل وتعلم الحلول المناسبة والسريعة لها حتى لا تؤثر هذه المشاكل على سير العمل. وهذا المقال يتحدث عن المشاكل ال 25 الأهم فى مجال الشبكات، وتأثيرها على العمل.

وقد أرسل لى أوى أيمى هذه المقالة وهى من تأليف (Terrance Slattery) أول شخص حاصل على (CCIE) فى العالم، والذي تحدثنا عنه فى مقال سابق وهو مؤسس شركة Nectordia للحلول البرمجية فى عالم الشبكات

<http://www.netcordia.com/>

1- عدم حفظ التعديلات فى ذاكرة الجهاز (NVRAM)

إعادة تشغيل الجهاز ستتسبب فى فقدان التعديلات الجديدة. إذا لم تحفظ التعديلات التى أدخلتها حديثاً على جهاز ما وحدث إنقطاع للتيار، فإن الجهاز عند إعادة تشغيله يعود إلى التعديلات التى كانت محفوظة عليه من قبل، متجاهلاً تلك التعديلات التى أدخلت عليه ولم تحفظ. وفى هذه الحالة ستتأثر الشبكة لأن التعديلات القديمة لا تتماشى مع احتياجاتها الحالية.

2- التعديلات المحفوظة لا تتماشى مع سياسات الشركة

هذا الأمر يسبب العديد من المشاكل، مثل مشاكل الأداء والكفاءة والحماية.

تتبع بعض الشركات فى شبكاتها الخاصة سياسات قياسية ك (PCI، HIPAA، SOX)، وشركات أخرى تطبق ما يطلق عليه أفضل الممارسات. ومن الصعب أن تتحقق من تطبيق هذه السياسات على مئات الأجهزة فى شبكتك بإستخدام يديك.

11- عدم استخدام تقنية جودة الخدمة (QoS)

برامج العمل المهمة يجب أن يكون لها الأولوية في إرسال وإستقبال البيانات وإلا سوف تعامل البيانات الخاصة بها مثل باقي البيانات في الظروف العادية أو في الظروف الخاصة، كإختناق مخرج الربط. إن التطبيقات مثل (VoIP) أو (SAP) عرضة للإضطراب الشديد في الإرسال (Jitter) وفقد الحزم في حالة عدم إستخدام تقنيات جودة الخدمة (حيث أن هذه التطبيقات حساسة فيما يتعلق بالوقت). ولذلك فإن الإعدادات التي تطابق سياسة الشركة أمر مهم يجب مراعاته (راجع 2).

12- الحزم التي تسقط من طابور الحزم (Queue) عند إستخدام تقنيات جودة الخدمة (QoS)

بطء برامج العمل المهمة. تغيير إحتياجات العمل منذ ظهور مصطلح (Queue). ال (VoIP) يتأثر على وجه الخصوص بهذه المشكلة. الشبكة التي تصمم لتحمل أربعة مكالمات مكالمات (VoIP) في نفس الوقت، لن تكون مناسبة عندما يتم توظيف أشخاص آخرين ويزيد عدد المكالمات التي يجب أن تتم في نفس الوقت (أى مع زيادة الضغط). سقوط حزم من طابور الحزم مؤشر مبكر على مشاكل تتطلب تغييرا في الشبكة.

13- تقلبات الهسار (Route Flaps)

يؤدى إلى أداء متواضع للبرامج، حيث تتخذ الحزم مسارات خاطئة أو غير فعالة في الشبكة. ربما يسبب هذا خط غير مستقر، أو عدم ضبط عدادات (Timers) بروتوكولات التوجيه بشكل صحيح (إنظر 2، 7)، أو وصول الحزم غير مرتبة مما لا يصلح مع بعض البرامج. تغيير المسارات يسبب أيضا الإضطراب الشديد في الإرسال، مما يؤثر على التطبيقات الحساسة للوقت مثل (VoIP) أو (SAP). لقد أثبتت الدراسات أن الأشخاص يمكن أن يتحملوا التأخير في إرسال واستقبال البيانات طالما أن مدة هذا التأخير ثابتة. ولكن التفاوت العالى في إستجابة البرامج سوف يدفع الأشخاص إلى الجنون. تحديد وتصحيح هذه المشاكل سيخدم شبكة العمل بشكل أفضل.

14- قيام ال (OSPF) بإعادة حساباته لإختيار أفضل المسارات

عدم إستقرار بروتوكول التوجيه، مما يؤدى إلى أداء ضعيف وغير ثابت للبرامج. إستقرار الخط، الأخطاء على الخط، أو عدم إستقرار ال (STP) يمكن أن يجعل مخطط الشبكة غير مستقر على مسارات محددة (إنظر 7، 20). فيبروتوكول التوجيه (Routing Protocol) يمكن أن يختار مسار ما مرة وعند حدوث تغيير في الشبكة أو في حسابات بروتوكول التوجيه يختار مسار آخر، هذا التقلب يعرض البرامج لمشاكل في إرسال البيانات أو لفقد الإتصال.

يدل على أن البرامج التي تستخدم الخط تحتاج إلى سعة أكبر، أو أن برنامج ضار يستحوذ على أغلب سعة الخط التي تحتاجها البرامج الأخرى.

7- مشاكل الخط وإستقراره

الأخطاء التي تحدث على خط الإتصال، أو في البروتوكول المستخدم للإتصال، تسبب أداء بطئ أو متقطع للبرامج. إستقرار الخط أو إستقرار مخرج الربط قد يؤدى إلى التأثير على (Routing & Spanning Tree)، وإنظر (13، 14، 15، 16، 20).

لن تتمكن البرامج من العمل بفاعلية إذا كانت هناك أخطاء على الخط أو كان الخط غير مستقر. ونقصد بالأخطاء على الخط أى الأخطاء التي تنتج عن مشاكل فى ال (Routing & Spanning Tree)، وتؤثر على باقى أجزاء الشبكة وذلك تبعاً لتصميمها.

8- المشاكل الناتجة عن عتاد الأجهزة أو العوازل البيئية

توقف مروحة التبريد، تلف مزود الطاقة، ودرجة الحرارة العالية، كل هذه المشاكل قد تحدث وتدفع بالأجهزة لإعادة التشغيل من جديد، مما يؤثر على البرامج أو المستخدمين المعتمدين على هذا الجهاز. تحديد وتصحيح هذه المشاكل، سوف يجعل الشبكة والبرامج المعتمدة عليها موثوقة بشكل أكبر.

9- إستنفاد الذاكرة

قد تؤدى علة فى نظام التشغيل إلى إستهلاك المزيد من الذاكرة، وعند إستهلاك جميع الذاكرة فإن الجهاز سيعاود التشغيل من جديد (لأنه لن يجد مساحة م ن الذاكرة ليستخدمها للقيام بوظائفه الأساسية)، مما سوف يقاطع عمل البرامج التي تستخدم هذا الجهاز. إن مثل هذه المشاكل قد تعاود فى الظهور كل فترة، وهذا أمر مشاهد فى بيئة العمل. ونقول أن العمل يتأثر بناء على مدى إستمرار المشاكل فى الظهور وكذلك تتأثر البرامج بظهور مثل هذه المشاكل.

10- عدم ضبط إعدادات مخرج الربط السيريال (Serial Interface) بشكل صحيح

يجعل بروتوكولات التوجيه تختار مسارات توجيه ليست الأفضل. إذا كانت إعدادات السعة على مخرج الربط السيريال (Serial Interface Bandwidth Settings) منخفضة، فإنها يمكن أن تؤثر على عمل بروتوكول التوجيه نفسه، جاعلة المسارات غير مستقرة. فالفروع البعيدة ستواجه عدم إستقرار فى عمل البرامج، وهذا الأمر حقيقة يصعب معالجته، إذ يتعين عليك أن تدركه أو تلاحظه وقت وقوعه. فإذا أردت لبروتوكول أن يختار مسار معين فعليك أن تستخدم تقنية (PBR)، و ألا تلجأ لتعديل قيم (Serial Interface Bandwidth).

15- ضعف جودة ال (VoIP)

ينشئ عن اضطراب الإرسال، التأخير، أو فقدان الحزم. المكالمات الصوتية المتقطعة. إنتهاء المكالمات بشكل غامض.

يرجع ضعف جودة ال (VoIP) للعديد من المشاكل مثل: التأخر على الخط، اضطراب الإرسال، وفقدان الحزم. فإذا تمت مراقبة هذه المشاكل، فإنه يمكنك تقليص عدد الإعدادات التي يجب عليك مراجعتها لمعرفة ما الذي يؤثر على جودة الصوت. وبتحديد مجموعة التليفونات التي تعطى أداءً ضعيفاً، فسوف تتمكن من وضع يديك على أصل المشكلة.

16- تغيير الجيران بشكل مسترر (Routing Neighbor Changes High)

(والمقصود بالجيران: أى الأجهزة التي يكون مفعّل عليها نفس البروتوكولات ونفس الإعدادات فى شبكة واحدة) البرامج التي تستخدم مسارات عبر مثل هذا الروتر (الذي يتغير

عليه الجيران بشكل مستمر) سوف تكون بطيئة أو غير مستقرة. يؤثر على بروتوكولات مثل (OSPF, EIGRP, and BGP) المرور عبر هذا الروتر يتأثر سلباً بتغيير الجيران الناتجين عن بروتوكولات مثل (OSPF, EIGRP, and BGP). وكما ذكرنا فى النقطتين (13 and 14) فإن هناك عوامل تؤدي إلى تغيير علاقات الجيرة باستمرار، مما يؤثر على إستقرار ومصداقية بروتوكول التوجيه. وكنتيجة لذلك فإن البرامج قد تتعرض لإضطراب الإرسال أو وصول الحزم غير مرتبة. لذلك فإن إكتشاف وإصلاح أسباب تغيير الجيران يجعل الشبكة أكثر إستقراراً وفاعلية.

17- منطقة (OSPF) غير متصلة بالمنطقة الأساسية (area 0)

إذا كانت هناك منطقة (OSPF) غير متصلة بالمنطقة الأساسية (area 0)، فإن الأجهزة فى مناطق ال (OSPF) الأخرى لن تتمكن من التواصل معها، مما يؤثر على البرامج التي تحتاج للتواصل عبر المناطق.

التوجيه (Routing) داخل منطقة من مناطق ال (OSPF) يعتمد على إتصالها بالمنطقة الأساسية (area 0). وعندما ينقطع إتصال إحدى المناطق مع المنطقة الأساسية، فإن الإتصالات تتم بين الأجهزة التي داخل هذه المنطقة المعزولة، ولكن الإتصال بين الأجهزة داخل هذه المنطقة و الأجهزة داخل المناطق الأخرى تنقطع (لأنه لن توجد لديهم مسارات لهذه المنطقة فى ال (Routing Table)).

18- تدفق حركة البيانات أحادي الوجة (Unidirectional Flooding)

عادة ما يكون نتيجة لعدم ضبط إعدادات بروتوكول توجيهه. يتسبب فى بطء البرامج وفشلها، كما أنه يصعب معالجته.

حركة البيانات سوف تتخذ مسارات ليست هى الأفضل، مما سوف يؤدي إلى رفع معدل التأخير، وزيادة التحميل على خطوط أخرى، و التأثير على أداء البرامج. وأحياناً يكون التوجيه غير المتماثل (asymmetric) مرغوباً فيه، ولكنه يزيد التعقيد فى الشبكة، ويصعب من عملية تحليل المشاكل.

فالخوادم تكون مجهزة ب (incoming & outgoing Interfaces) وكل منهما له (MAC) مختلف عن الآخر، مما قد يتسبب فى إرسال البيانات فى إتجاه واحد (Unicast flooding)، وهى العملية التي تحدث عندما لا يعرف السويتش ال (Destination MAC Address) فيرسل الإطارات لكل المنافذ فى ال (VLAN) حتى يعرفه ويسجله فى ال (CAM). وينتج عن ذلك حركة تدفق عالية للبيانات، مما يؤدي للإختناق ويؤثر على عمل الأجهزة فى ال (VLAN). وفى ال (Routed Networks) فإن عدم توجيه حزم فى أحد الإتجاهات على خط ما لمدد طويلة يشير إلى إحتمالية وجود إعدادات توجيه غير صحيحة (Routing misconfiguration).

19- مخرج الربط لروترها مغلق (Router Interface Down)

أى مخرج ربط على روتر و يظهر ك (administratively up) ولكنه لا يعمل (line protocol down)، فمن المحتمل أنه يعمل كمخرج ربط إحتياطي، لئلا يحدث قصور فى الإتصال إذا أغلق المخرج الرئيسى لأى سبب، الأمر الذي قد يؤثر على جميع البرامج التي تستخدمه.

الشبكات الإحتياطية تخفى إخفاقات الشبكات الأساسية، لذا فإنه من المهم تحديد وعلاج مشاكل الشبكات الأساسية قبل أن تخفق الشبكات الإحتياطية أيضاً فيحدث قصور. و أفضل الممارسات فى الشبكة تقضى بأن تغلق إدارياً ال (interfaces) التي لا تستخدمها، بحيث أنك إذا وجدت أى (interface) فى حالة (up/down) يكون هذا دليلاً على وجود خلل ما قد حدث.

20- عدم إستقرار أو عدم تحديد الجسر الأساسى (Root Bridge)

عدم ضبط أولوية الجهاز الذي أريده أن يأخذ دور الجسر الرئيسى فى الشبكة، يتسبب فى تذبذب أداء البرامج فى ال (VLAN). إذا لم نضبط إعدادات سويتش قوى لكى تجعله يأخذ دور الجسر الرئيسى، فإن أى سويتش ضعيف يمكن أن يستولى على هذا الدور إذا كان لديه (MAC Address) أقل من السويتش القوى. ففى شبكات ال (VLAN) التي عليها ضغط شديد، تحتاج لأجهزة ذات معالجات قوية وسعات إرسال وإستقبال عالية، لأنه إذا فقدت العديد من ال (BPDU)، فإن السويتشات تختار سويتش آخر ليأخذ دور الجسر الرئيسى، وعند حدوث هذا فإنه يجب على السويتشات كلها أن تتفق على هذا الإختيار فيما يعرف ب (STP Pre-convergence). هذا الأمر سوف يؤثر على الإتصال بين

البرامج فتبدو متقطعة، هذا التغيير في إختيار الجسر الرئيسي يصعب تحليله حيث أنه يحدث بسرعة.

21- عدم تطابق الثنائية (Duplex Mismatch)

يؤدي إلى تزايد أخطاء الخط.

تصبح البرامج أبطأ عند زيادة مقدار تدفق البيانات.

أخطاء ال (CRC)، والتصادمات المتأخرة (late collisions)، وأخطاء ال (FCS) دلائل على عدم تطابق الثنائية (Duplex Mismatch). إذا تم تنصيب سيرفر وكان ال (Ping) يتم منه و إليه فهو سيرفر قائم ويعمل في الشبكة. ولكن إذا زاد تدفق البيانات إلى السيرفر فأدت إلى حدوث أخطاء، فمن المحتمل أن يكون السبب الرئيسي هو عدم تطابق إعدادات الثنائية (Duplex) بين الجهاز المرسل والسيرفر (أي الجهاز المستقبل للبيانات). و مما يزيد من تفاقم الوضع أن الشركات المنتجة تختلف إعدادات الثنائية بين منتجاتها فمثلا:

Microsoft: auto-negotiate -

Cisco: fixed full duplex -

22- الهجوع أو السويتش النقل كفاءة (أو ليس على الدرجة المطلوبة)

أجهزة غير مصرح لها تضاف إلى الشبكة.

تعريض سلامة الشبكة وأمنها للمشاكل.

إنظر 20، عدم إستقرار أو عدم تحديد الجسر الرئيسي.

الروتاتر اللاسلكية، السويتشات، المجمعات (Hubs)، و الأجهزة الأخرى للشبكات يجب أن تكون تحت إدارة موحدة لكي توفر الحماية المثلى. يمكن لسويتش أخر أن يتحصل على أولوية أقل، مما يجعله الجسر الرئيسي ل (VLAN) و مسببا مشاكل في الإستقرار (إنظر 20). خوادم ال (DHCP) الضارة في الروتاتر اللاسلكية يمكن أن تسبب مشاكل تقطع الإتصال داخل شبكة فرعية (Subnet)، إلا إذا حالت إعدادات معينة ضد وقوع ذلك.

23- وجود المنافذ في حالة (ErrDisabled)

مجموعة الأجهزة الطرفية (End Stations) المتصلة بواسطة هذا المنفذ تفصل عن الشبكة إلى أن يتم تفعيله (إما أوتوماتيكيا أو بفعلا لمستخدم).

العديد من إختيارات الإعدادات (Configuration Options) (تتيح لمنافذ السويتشات أن تغلق (تطفئ) عند حدوث أمور معينة، كإستلام (BPDU) أو إستلام إستجابات من (DHCP) (إنظر 20،22). بعض المنتجين يجعل المنافذ تغلق إذا تعرضت هذه المنافذ للعديد من الأخطاء. تحديد هذه المنافذ تلقائيا يمكن أن يجنبك (كمهندس شبكات) التعرض لكاملة من مستخدم أو مدير سيرفر لديه مشاكل في الإتصال بسبب أن منفذ مغلق.

24- قنوات الأثير (EtherChannels) الغير متوازنة أو الغير مستخدمة

التأثير المتزايد و الإضطراب الشديد في الإرسال يؤثر على التطبيقات الحساسة مثل ال (VoIP).

تعرض الشبكة التعزيزية للمشاكل.

توزيع الحزم عبر قنوات الأثير ربما يصبح غير متوازن إذا إختيرت خوارزمية لتوزيع الحزم ليست الأمثل. وبتغيير الخوارزمية، يصبح توزيع الحزم بقناة الأثير أكثر توازنا ويزيد إجمالى السعة الفعلية. قناة الأثير الغير متوازنة سوف يحدث بها إختناق بسهولة، مما سوف يؤدي إلى أداء البرامج أداء أقل من المتوقع (منها).

25- نظير ال HSRP or VRRP غير موجود (HSRP or VRRP peer not found)

خاصية التعزيز (Redundancy) مفعلة ولكن لا تعمل بشكل صحيح.

التعطل عندما يحدث فشل آخر في الشبكة.

تعرض الأجهزة التعزيزية للمشاكل.

في ال (HSRP & VRRP) يوجد جهاز أساسى يقوم بمهمة ال (Gateway) وجهاز إحتياطى أو تعزيزى تحسبا لحدوث أى مشاكل للجهاز الأساسى. ولهذا فإن المستخدمين داخل شبكة ما قد لا يشعروا بوجود مشكلة إذا فشل الجهاز الأساسى فى القيام بمهمته، لأن الجهاز الإحتياطى سوف ينوب عن الجهاز الاساسى فى أداء وظيفته. ولكن قد يحدث ألا يظهر الجهاز الإحتياطى للمستخدمين، إما بسبب خط ربط معطل بين الأجهزة، أو أن الجهاز الإحتياطى لم ينصب بعد فى الشبكة، أو أن الجهاز الإحتياطى أو مخرج الربط خاصته قد حدث لأحدهما عطل. فإذا حدث قصور آخر للجهاز الإحتياطى (أى بعد القصور الأول الذى حدث للجهاز الأساسى)، تنقطع الشبكة عن العمل مؤثرة على برامج العمل المهمة. و لهذا فإن إكتشاف ومعرفة أن الإعدادات الإحتياطية لا تعمل، يساعدك على تدارك المشاكل وتصحيحها قبل وقوعها حتى لا تؤثر على عمل البرامج المهمة.

ترجمة وتعليق

أسامة الشرقاوى

VLSM

VS

CIDR

مقارنة هامة بين VLSM & CIDR

VLSM

أو Variable Length Subnet Masking قد يكون الحديث عنها شيء غير هام كون الجميع يعرف أهميتها وفوائدها. وسوف أتحدث عنها بشكل بسيط وسريع، فعادة عندما أقدم تعريف لهذه الخاصية أقول عنها بالإنكليزية Subnetting the subnet ولا تسألني عن معناها فهي بسيطة، المهم تم تطوير هذه الخاصية لتقضي على مشكلة كبيرة في طريقة بناء ال IPv4 فجميعنا يعلم أن لل IPv4 خمس تصنيفات أو Classes وهي (A,B,C,D,E)، تم إتاحة أول ثلاث تصنيفات منها للإستخدام، ونعلم أيضا أن لكل تصنيف من هذه التصنيفات قواعد ثابتة تتحكم في عدد الشبكات و ال IPs المخصصة لكل شبكة. فلو أخذنا على سبيل المثال شبكة تنتمي لل Class C ولتكن (192.168.1.0). ماسوف أطلبه منك لكي تحدد لي من هذه الشبكة هو الماسك؟؟؟ طبعا الماسك الطبيعي لل Class C هو 255.255.255.0 !!! .طيب شيء جميل ماهو عدد ال IPs المتاحة لهذه الشبكة ؟ أكيد 254 ! .طيب السؤال الآن: هل ياترى أنا بحاجة إلى كل هذه ال IPs

مقالتي لهذا العدد سوف أخصصها للإجابة على أحد الإستفسارات التي وصلتني تسأل عن الفرق بين ال VLSM وال CIDR. وحقيقة هذا السؤال طرح في الصفحات الإنكليزية والعربية آلاف المرات، وهناك من كان يعقد المقارنة بينهما وهناك من كان يجيب عليها بغموض أو يجيب عليها باللغة الإنكليزية. فتعالوا نتعرف على هذه المقارنة لنضع حدا لهذا السؤال باللغة العربية على الأقل.

قد يكون كتاب Sybex الخاص بكورس ال CCNA هو من سبب هذه المشكلة عند الطلاب والمهندسين لأن الشرح الذي قدمه الكتاب كان معقدا بعض الشيء وغامضا، مع أني أحد أكثر الأشخاص إعجابا بهذا الكتاب لكن أعترف أن الموضوع معقد بعض الشيء هناك. وإن شاء الله سوف تخرج من هذا الموضوع وأنت فاهم الفرق تماما، ولكن لنتفق على شيء مهم قبل أن نبدأ وهو أن كلا الإثنين يعملان بشكل مختلف، وكلا الإثنين يحلان مشكلة في ال IP.

لشبكتي ؟ الجواب بحسب شبكتك. شبكتي تحوي 30 جهاز فقط ؟ أكيد لا تحتاج. إذا سوف يبقى لدي (224 IPs) غير مستخدمين ؟ نعم.

لنفرض مثال من نوع آخر مثل ربط روتران ببعضهم البعض، كم عدد الـ IPs التي نحتاجها ؟ إثنان طبعا وبالتالي الخسارة في الـ IPs أكبر. ما الحل برأيك ؟ الحل كان ببساطة من خلال استخدام خاصية الـ VLSM والمدعومة من أغلب بروتوكولات الشبكات.

ببساطة تقوم هذه الخاصية بتقسيم الشبكة التي تحوي (254 IPs) إلى عدة شبكات، فبدلاً من أن يكون عندي شبكة واحدة تحوي (254 IPs) أستطيع أن أقسم هذه الشبكة مثلاً إلى ثماني شبكات كل شبكة منها تحوي (30 IPs)، لأنها ببساطة تكسر القاعدة العامة التي زود بها الـ IPv4، وبالتالي تكون قد وفرنا على أنفسنا الكثير من الـ IPs، كما أنها تتيح تقسيم الشبكة إلى الرقم الذي تريده بحيث يكون أحد أضعاف الرقم ثمانية يعني شبكتان، أربع شبكات، 16، 32، 64، 128، وطبعاً لا تفكر بالـ VLSM على مستوى الشبكات الداخلية فقط، بل فكر فيها أيضاً بالشبكات الخارجية وأهميتها هناك في توفير الـ IPs.

CIDR

أو Classless Inter-Domain Routing لهذه الخاصية أكثر من إسم فهناك من يطلق عليها Super-netting وهناك من يطلق عليها Route Aggregation أو Summarization كل هذه المصطلحات تشير إلى نفس الخاصية وأعود إلى أول مصطلح لها وهو الـ Super-netting ماذا يعني لك ؟ هذا التعريف ببساطة يشير إلى عكس عملية الـ Subnetting وبالتالي نستنتج شيئاً في غاية الأهمية وهو الـ CIDR يقوم بعكس عملية الـ VLSM فعوضاً عن تقسيم الشبكة إلى أجزاء صغيرة يقوم الـ CIDR بتجميع الشبكات الصغيرة إلى شبكة واحدة، ونستنتج أيضاً أن الـ CIDR يستخدم الـ VLSM (أي أن الـ

CIDR يستخدم في حالة إذا ما طبقنا الـ VLSM ليقوم بتجميع هذا العدد من الـ Subnets التي نتجت عن الـ VLSM في One Route Entry ليسهل عملية إرسالها في الـ Routing Update) وهو إستنتاج مهم للتعريف بهذه الخاصية وحتى تزيل بعض الغموض عنها أيضاً وحتى تبتعد عن موضوع المقارنة بينهم.

طيب ما الفائدة من الـ CIDR؟ الفائدة يجب أن تكتشفها بنفسك وهي بسيطة، لو فكرت لماذا نقوم بتجميع الشبكات تحت شبكة واحدة ؟ وأطلب منك أن تفكر بشيء مهم أيضاً فنحن قد استفدنا كثيراً من خاصية الـ VLSM لكن على ماذا حصلنا أيضاً ؟ الجواب: حصلنا على عدد كبير جداً من عناوين الشبكات فلو عدنا إلى مثالنا السابق سوف نجد أن الروتر عوضاً عن إرسال شبكة واحدة إلى جيرانه يتوجب عليه إرسال ثماني عناوين ولو فرضنا أن الشبكة مقسمة إلى 128 شبكة عندها يتوجب عليه أن يرسل 128 شبكة إلى كل جيرانه، وتستطيع أن تصل إلى العدد المهول الذي سوف يحصل عليه كل روتر موجود على الشبكة أو على الإنترنت تحديداً، لأن استخدام هذه الخاصية موجود فقط عند مقدمي خدمة الإنترنت، وقليلاً ما استخدمها في الشبكات الداخلية لذلك أرح نفسك من عناء التفكير بها كثيراً.

أتمنى أن أكون قد أوصلت لك جواباً مقنعاً لسؤال حير الكثيرين، وأنا كنت من بينهم وقبل أن أنهي مقالتى أحب أن أشير إلى أنني لم أدخل في تفاصيل عمل كل واحدة منها لأنني أعتقد أن الأمر واضح عند الجميع وخصوصاً الـ Summarization وعلى فكرة هذا السؤال قد يصعب تفسيره على أشخاص يحملون شهادة الـ CCIE، لذلك أستخدم هذا السؤال البسيط لإختبار أحدهم وإحراجة أحياناً.

أيمن النعيمي

Cryptography – PART I

Security Principles

عندما بدأت أفكر في الموضوع الجديد لهذا العدد فكرت قليلا ما الفائدة مما أفعله؟ معظم المواضيع من الممكن للمهتم بها أن يبحث عنها على شبكة الإنترنت و سيجد العديد من الشروحات ربما بالإنجليزية و أحيانا قليلة قد يجد بالعربية، لماذا أتعب نفسي في كتابة شيء مكرر؟ هل لزيادة المحتوى العربي؟ ربما ولكني أرى الكثيرون يحاولون زيادة المحتوى العربي كما يقولون فيحاولون ترجمة عشرة مقالات مثلا مرة واحدة عن طريق أي برنامج ترجمة و النتيجة طبعاً تكون كارثية، فهذه الطريقة تستفزني جداً، عموماً لا داعي للكلام الكثير و لنبدأ.

عندما حاولت أن أبحث عن موضوع جديد بعض الشيء أحاول أن أتكلم عنه، موضوع قد يفيد حقيقةً، وقتها تذكرت موضوع أثناء دراستي كنت قد وجدت صعوبة في فهمه، فقممت ببعض البحث على الإنترنت و وجدت بعض الشروحات لكن كانت صعبة الفهم، على الأقل بالنسبة لي و لكن بعد الكثير من القراءة بدأت أفهم بعض الشيء.

حتى لا يشعر القارئ بالملل فأنا أتكلم عن مجال و علم واسع يسمى بالـ Cryptography أو Cryptology، ويعرف بالتشفير أو علم التعمية باللغة العربية- و سنعرف لاحقاً الفرق بين المصطلحين.

لهجة تاريخية :-

أولا نعود للوراء بعض الشيء لنعرف أساس هذا العلم و أشهر العلماء الذين برعوا فيه، لاحظ هنا أن ما نتكلم عنه ليس له علاقة بالـ Computers أو الـ Internet فهو يعتبر علم منفصل من أفرع الرياضيات و تم استخدامه في الحوسبة و الإتصالات الحديثة بعد ذلك.

يعتبر العلماء المسلمين هم أول من أسسوا هذا العلم و برعوا فيه وذلك لبراعتهم في علم الرياضيات مما أعطاهم ما يحتاجون لفهم و كتابة الخوارزميات المختلفة و أيضاً كسرهما، من أشهر هؤلاء " يعقوب بن إسحق الكندي " و أيضاً " بن دريهم " الذي إذا وقعت عيناه على نص مشفر فكاه في الحال، كما استخدم يوليس قيصر علم التعمية أو التشفير قديماً ليتواصل مع قادته بطريقة سرية، وهناك خوارزميه تسمى (خوارزميه قيصر) سنتعرف عليها لاحقاً.

تعريف الـ Cryptography :-

هو علم إخفاء البيانات و تغيير شكلها إلى شكل آخر تماماً ليصعب فهمها و تحويلها من شكلها المعروف للجميع إلى شكل يتعذر على الجميع معرفة معناه إلا إذا كانت لديك معرفه سرية للطريقة التي تم استخدامها في هذه العملية، فحينها تستطيع إرجاع هذه البيانات إلى حالتها الأولى. كان هذا العلم يستخدم قديماً في الحروب و التراسل، أما الآن فحدث ولا حرج عن المجالات الكثيرة التي تطبق هذا العلم سواء كانت مجالات دبلوماسية أو عسكرية أو إقتصادية أو إعلامية أو تجارية أو معلوماتية. فأنت عندما تسجل دخولك إلى حسابك في موقع أو بريد إلكتروني، فهذه العملية تستخدم هذا العلم الواسع لتأمين بياناتك من السرقة.

ما فكرت فيه هو سلسلة من المقالات تتحدث عن هذا العلم، فإن إكتفيت بمقال واحد فهذا أشبه بأخذ قطرة مياه من محيط واسع، سأحاول بقدر الإمكان في هذه السلسلة إلقاء الضوء على أهم النقاط و المفاهيم التي قد تساعدك في البداية بهذا الفرع و دراسته، فهي ستكون بمثابة الخطوط العريضة أو المفاهيم الأساسية التي تؤهلك للبداية و التعمق أكثر، و للأسف الشديد لن تجد إلا الكتب الإنجليزية لدراسة هذا المجال، و لن تجد

أي شيء بالعربية إلا كتاب واحد فقط يشرح الطرق الكلاسيكية أو القديمة في التشفير و لم يتم تطويره منذ فترة طويلة لذلك سألتزم بالمصطلحات الإنجليزية.

لم أضع خارطة طريق لهذه السلسلة بعد لكنها لن تكون قصيرة و ستشمل على ثلاثة أشياء أساسية وهي:-

- 1- أساسيات الـ Cryptography.
- 2- إرتباط الـ Cryptography بالـ Network security.
- 3- بعض الرياضيات (مجرد أشياء طفيفة).

أي سأدمج الإثنين معا و سيمر بنا بعض القوانين الرياضية التي سأحاول شرحها ببساطه لنستطيع فهم الـ Cryptography جيداً، سألتزم بالمفاهيم الإنجليزية كما قلت في كل شيء، لكي يتمكن الشخص الذي يريد التعمق في هذا المجال أكثر أن يكون عنده خلفية يستطيع بها فهم المزيد.

أبدأ هذه السلسلة بـ "بسم الله الرحمن الرحيم" و من هنا يبدأ الجزء الأول منها بعنوان "Security Principles"

في هذا الجزء سوف نبدأ ببعض الأساسيات و المفاهيم العامة في مجال أمن و حماية

المعلومات.

-: Security Attacks

ببساطة هي أى فعل غير مسموح أو مصرح به قد يهدد سلامة البيانات بأى شكل من الأشكال، و قد تم عمل Classification للهجمات المختلفة فى (Internet Security Glossary RFC 2828)، وحسب هذا التصنيف أصبح لدينا نوعان

يقع تحتها أى هجوم وهما :-

1-Passive Attacks

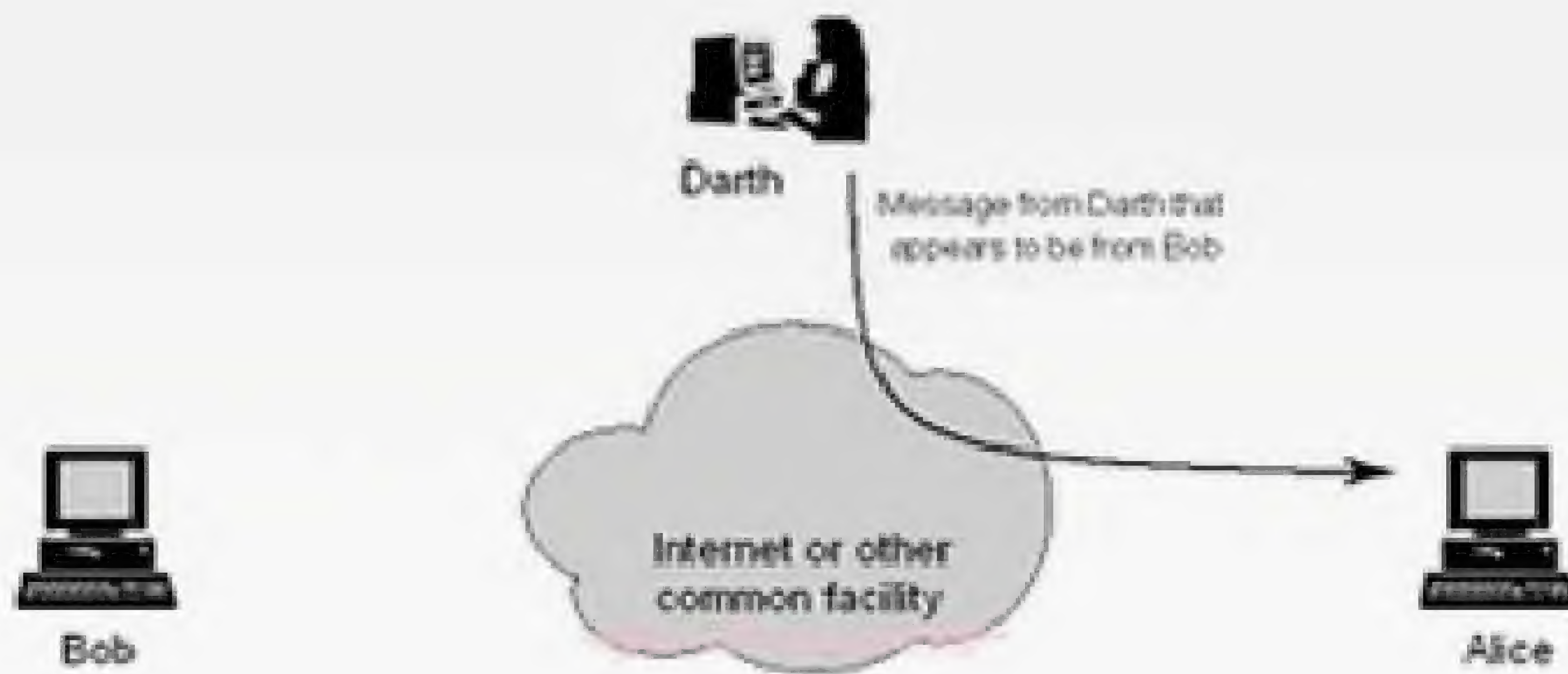
2-Active Attacks

أى هجوم يقع ضمن النوع الأول هو ببساطة هجوم سلبى لا يؤثر على تدفق البيانات و لا يغير شىء فيها، بل هو نوع من التنصت (Eavesdropping) و يستخدم فى جمع معلومات معينة حسب الغرض من هذا الهجوم.



مثال على هذا النوع هو شخص يرسل بريد الكترونى إلى شخص آخر، و يوجد بينهم شخص ثالث يتصنت عليهم. أيضا هذا النوع من الهجمات يستخدم لتخمين نوعية الـ

Traffic إذا تم استخدام طريقة لتشفيرها أو إخفائها، فمثلا عن طريق معرفة طول الـ PACKET يمكن تخمين نوع البيانات (Traffic pattern) التى يتم تناقلها حتى إذا كانت مشفرة. هذا النوع من الهجمات فى العادة يصعب كشفه لأنه لا يتدخل نهائيا فى أى شىء و الحل الأمثل لتقليل الضرر هو تشفير البيانات فى هذه الحالة قمنا باستخدام طريقة لمنع (Prevention) و ليس للكشف (Detection).



Masquerade (Active Attacks)

أما الـ Active Attacks فهو العكس تماما، فهو يشمل أى هجوم يقوم بالتعرض للبيانات أو منعها أو تغييرها أو محاولة إرسال بيانات مزيفة، تم تقسيم الـ Active Attacks إلى ٤ تصنيفات

أخرى هم :-

١- Masquerade - التتكر

يقوم المهاجم بالتظاهر بأنه شخص آخر وذلك للحصول على صلاحيات أعلى (Gain Extra-Access) و الوصول إلى أشياء غير مصرح له بالوصول إليها، مثال على هذا هو شخص يقوم بعمل CAPTURE لعملية الـ Authentication بين شخصين

وفى وقت لاحق يقوم بعمل Reply لما قام بالحصول عليه و إرساله إلى نفس الجهة و بهذا تنكر على أنه الشخص الأسمى و إمتلك كل صلاحياته.

٢- Modification of messages

يقوم المهاجم بتعديل رسالة معينة يتم تناقلها بين شخصين، مثلا يرسل A إلى B هذه الرسالة «إسمح لـ C بقراءة الوثائق السرية»، يتدخل المهاجم ويغير الرسالة إلى «إسمح لـ X بقراءة الوثائق السرية»

التصنت على بعض البيانات و إرسالها في وقت لاحق للوصول إلى هدف معين، ويمكن استخدام هذا النوع لتحقيق النوع الأول Masquerade.

٤- Denial of services

هجوم مشهور يعتمد على إغراق الهدف بالطلبات وذلك لمنع الأشخاص المصرح لهم بالوصول إلى ما يريدون أو تعطيل العمل بهذه الأجهزة.

بهذا نصل إلى نتيجة و هي كالآتي: ال Active attacks هي عكس ال Passive attack تماما، فالأولى يصعب التصدي لها لكثرة الثغرات الأمنية في أنظمة الشبكات و تطبيقاتها و لكن يمكن كشفها بسهولة، و الثانية يصعب كشفها و لكن يمكن منعها بسهولة.

- Security services

بعد أن فهمنا ال Security attacks نبدأ في مصطلح آخر مهم و هو ال Security services و يتلخص تعريف هذا المصطلح في الآتي «القيام بعملية أو إتصال لجهة معينة مع ضمان عامل الأمان في هذه العملية و الحفاظ على أمن البيانات المتناقلة من أي تهديد (Threat) قد يشكل خطر على هذه البيانات».

ما معنى هذا الكلام؟ معناه أنه عندما يحدث إتصال بين شخصين نفترض مثلا بين A و B عندما يبدأ A الإتصال فلا بد أولا أن يضمن سلامة هذه البيانات التي يرسلها إلى B، أي أن هذه البيانات لن يتم اعتراضها أو التجسس عليها، و في الجهة الأخرى يجب أن يتأكد B أن الشخص الآخر هو A حقا و ليس شخص يتظاهر بذلك عن طريق هجمة من نوع Masquerade، هنا يأتي دور ال Security service أي خدمة أمنية تقوم بتحقيق هدف معين فمثلا سنحتاج إلى تطبيق Security service تضمن لنا إجراء عملية Authentication و Security service أخرى تضمن لنا ال Data confidentiality أي سرية المعلومات، أعتقد أن المفهوم واضح الآن، نبدأ بأهم ال SECURITY SERVICES التي سنحتاجها لتأمين الشبكة.

أولا ال Authentication - هذه ال Service تضمن لنا أن الشخص الآخر على الطرف الآخر هو فعلا الشخص الذي يتظاهر به، عندما يقوم A بالإتصال مع B تضمن هذه ال Service A أن الشخص الآخر هو فعلا B و ليس شخص آخر يتظاهر بذلك عن طريق هجمة من نوع Masquerade (إعذروني فأنا ممل بطبعي و أحب التكرار) هذا إذا كان الإتصال Interaction مثل Telnet session مثلا أم لو كانت عبارة عن Connectionless transfer مثلا أرسل A رسالة إلى B فهذه ال Security service تضمن له أن هذه الرسالة من A و ليست مزيفة.

ثانيا ال Data Confidentiality - هذه ال Security

service أخرى تضمن لنا سرية هذه البيانات التي يتم تناقلها أي أنه لن يستطيع شخص متصنت على الإتصال أن يفهم ما يحويه هذا الإتصال سواء كان Interaction connection أو Connectionless.

ثالثا ال Data Integrity - تضمن لنا هذه ال Security service أنه لم يتدخل أحد في هذا الإتصال و قام بالتعديل عليه Modification of messages و يمكن تطبيق ال Security service بطريقتين فإما أن تكشف هذا التغيير أو التعديل الذي تم إجرائه بواسطة متطفل على هذا الإتصال و يقوم بمعالجته (Recovery) أو أن يكتشفه فقط.

رابعا ال Non-repudiation - إذا حاولت ترجمة هذا المصطلح فستجد معناها عدم النكران (ما معنى هذا؟ معناه أنه لو قمت بإرسال E-mail إلى صديق لي أطلب منه طلب و عندما قابلته بعدها سأنته عن الطلب، فلا أجد يقول لي «لم يصلني هذا ال E-mail». ببساطة تضمن هذه ال Security service A أنه عندما يرسل رسالة إلى B يضمن وصولها إليه بنسبة ١٠٠٪.

- Security Mechanism

بعد أن فهمنا معنى كلمة Security service أو هذا ما أعتقده أحب أن أسأل سؤال كيف يمكن تطبيق أو تنفيذ Security service بشكل عملي؟ بالطبع لن تدخل على ال Router أو ال Firewall و تكتب:

```
Data service security #router(config)
Confidentiality
```

لا طبعا و إلا كانت الحياة رائعة و إستراح الجميع، إذن كيف نطبقها؟ عندما نريد تطبيق Security service معينة نقوم بتطبيق Security mechanism واحدة أو أكثر، نستطيع أن نقول أن ال Security mechanism هي وحدة بناء ال Security service، حسنا الآن نريد أن ننفذ ال Security service Data Confidentiality على الشبكة ما هي ال Security mechanism التي سنختارها سواء كانت واحدة أو أكثر؟

رقم واحد لسرية البيانات يجب أن نبدأ ب Mechanism يسمى Encipherment هذا المصطلح يساوي Encryption و لكنه أكثر شمولاً من المصطلح الثاني، هذه ال Mechanism تقوم باستخدام خوارزميات رياضية لتغيير شكل البيانات إلى شكل مختلف تماما لا يستطيع من يتصنت عليها أن يفهم معناها نهائيا، و لتطبيق هذا ال Mechanism يمكننا ببساطة أن نقوم بتفعيل أي خوارزمية على الراوتر مثلا ٣des أو aes و بهذا نحن قمنا بتطبيق ال Security mechanism تسمى Encipherment التي بدورها تحقق ال Security service

Relationship between Security Services and Mechanisms

Service	Mechanism							
	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

تدعى Data Confidentiality أعتقد أن الفكرة أكثر وضوحاً الآن.

سوف أعرض الآن سريعاً أهم ال Security mechanism التي نحتاجها كثيراً في عملية تأمين الشبكة :-

Encipherment - Digital Signature - Access Control - Data Integrity - Authentication Exchange - Traffic Padding

لن أتكلم عن وظيفة كل واحدة حاول أنت الآن أن تقوم بعملية بحث صغيرة إذا كنت مهتماً بالأمر.

هذه الصورة توضح العلاقة بين ال Service وال Mechanism الذي من خلاله يمكننا تطبيق ال Service.

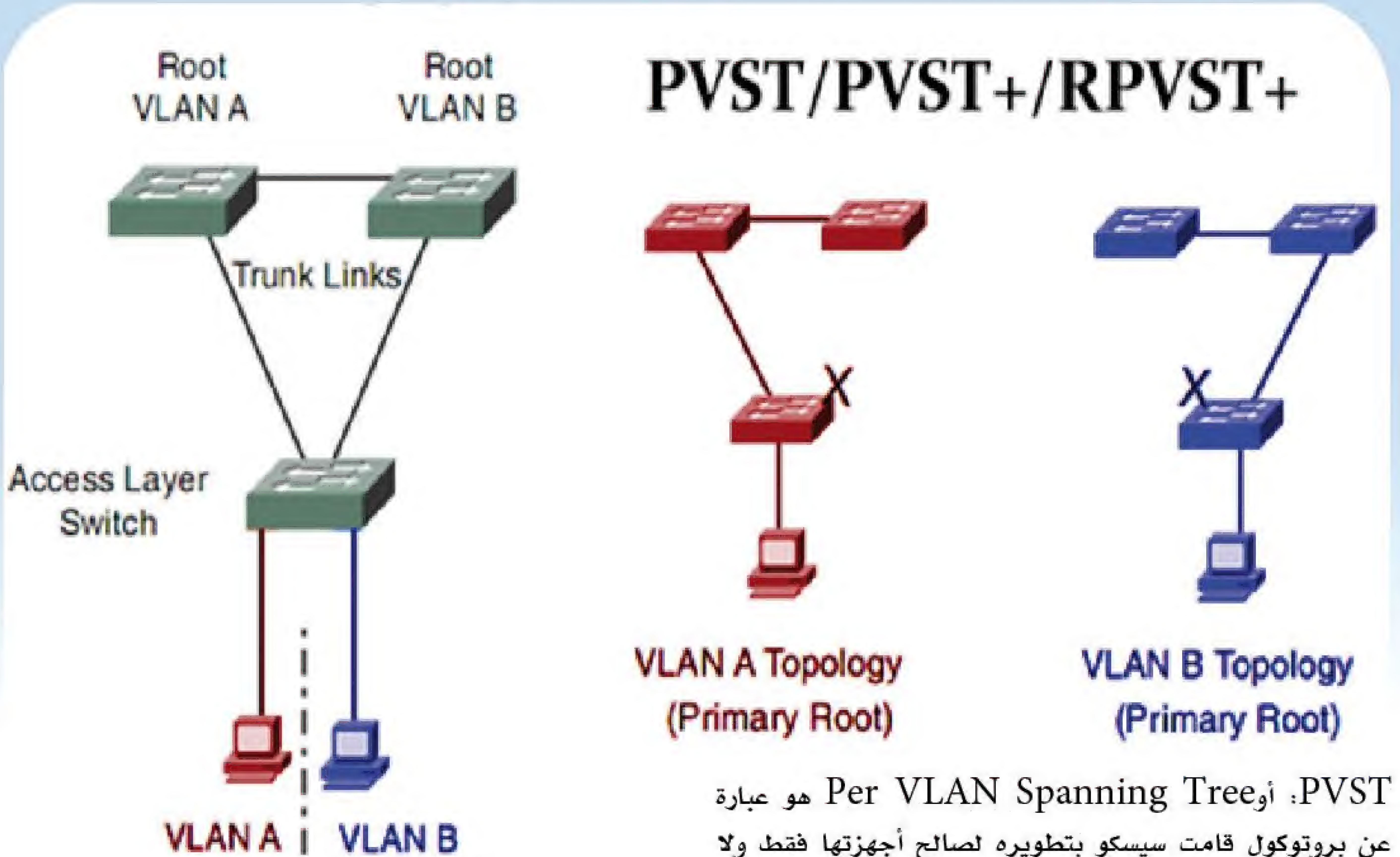
بهذا نكون قد إنتهينا من الجزء الأول من هذه السلسلة و هو مجرد مفاهيم أساسية. إنتظروني في العدد القادم مع الجزء الثاني و الذي

سنتعرف فيه على بعض خوارزميات التشفير البسيطة، إن شاء الله سيكون شيء جديداً بالنسبة للكثير.

إلى اللقاء على أن نلتقي في الجزء الثاني من هذه السلسلة.

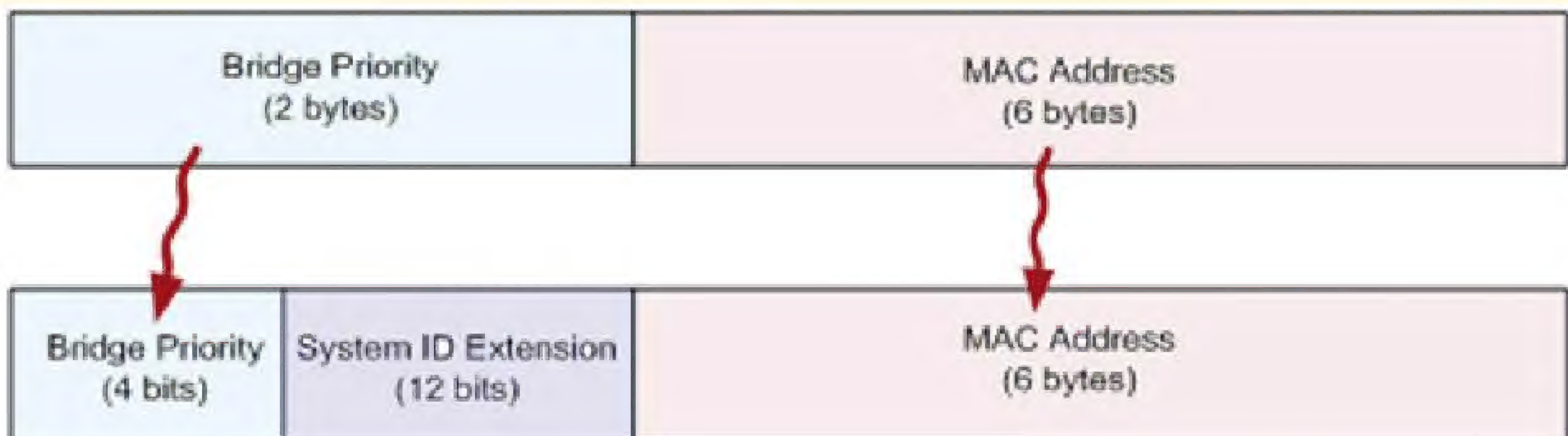
Spanning Tree Protocol

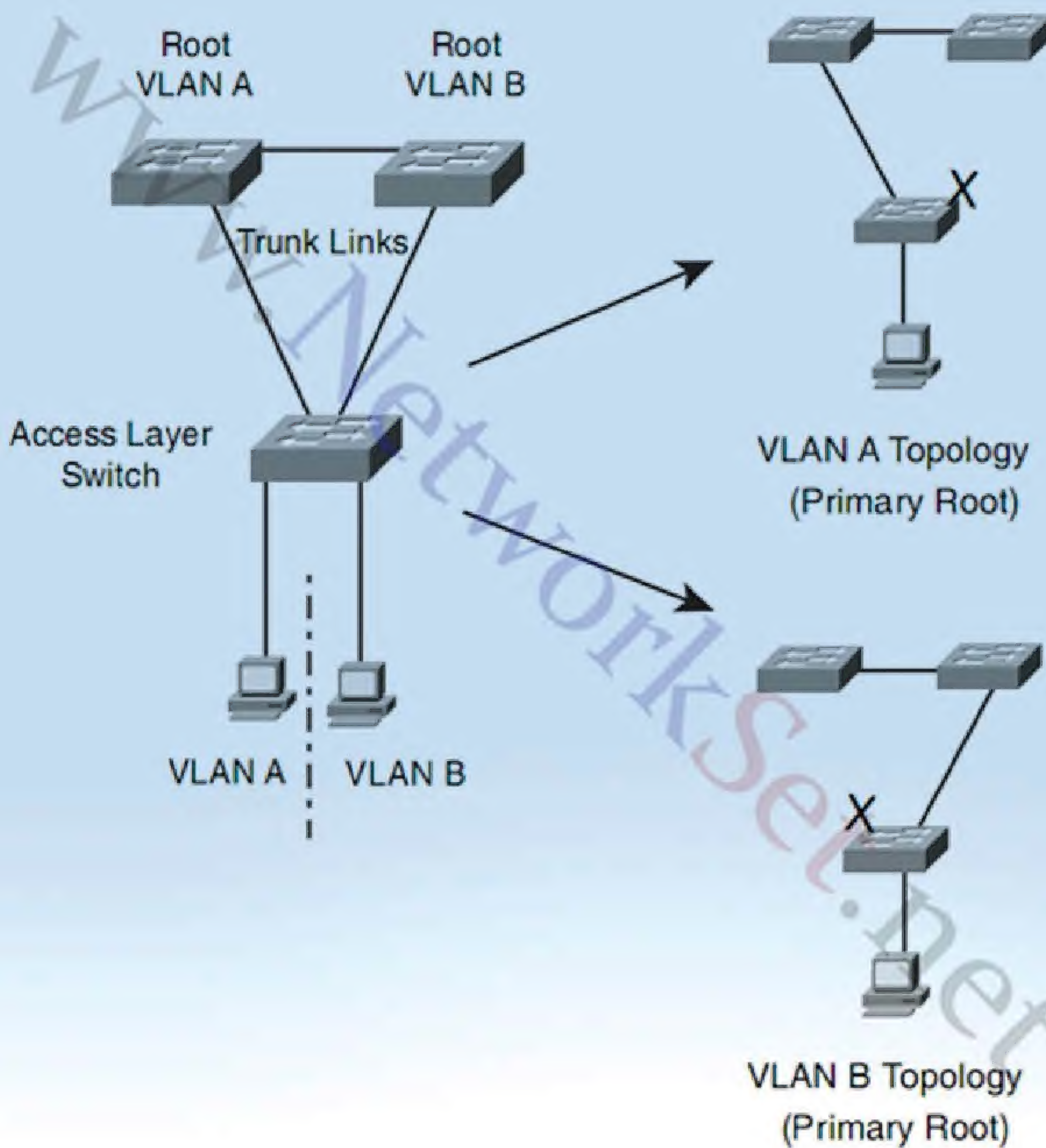
نستكمل في هذا العدد بعون الله القسم الثاني من أنواع الـ Spanning Tree والذي تحدثنا في قسمه الأول عن البروتوكولات الخاصة بي الـ IEEE في العدد السابق أما اليوم فسوف نتحدث عن البروتوكولات التي قامت سيسكو بتطويرها وهي PVST, PVST+, RPVST+ وأهم الاختلافات بينها.



مجموعات ومن عيوب هذا البروتوكول أنه يعمل من خلال الـ Inter Switch Link أو ISL فقط وكما هو معروف عن هذا البروتوكول أنه يعمل على أجهزة سيسكو فقط لذلك أي BPDU تصل إلى سويتشات سيسكو قادمة من أنواع أخرى تستخدم بروتوكول QSTP مثل الـ CST سوف يتم تجاهلها مباشرة ولتتمكن هذا البروتوكول من تخصيص Instance لكل VLAN قامت سيسكو بعمل بعض التغييرات على الـ Header الخاص بي الـ BPDU لكي يتم التعرف أيضا على رقم الـ VLAN فنحن نعلم أن الـ Header

PVST: أو Per VLAN Spanning Tree هو عبارة عن بروتوكول قامت سيسكو بتطويره لصالح أجهزتها فقط ولا يعمل إلا عليها وهو عبارة عن امتداد للبروتوكول المعروف الـ STP ويقوم بنفس الوظائف، وكما ذكرنا في الموضوع السابق أن الـ STP يقوم بعمل Instance واحدة لكل الشبكة وبما فيها الـ VLANs إلا أن سيسكو فكرت بطريقة أخرى وهي لماذا لا نتيج Instance لكل VLAN التي سوف تتيح بدورها Load Balancing بين السويتشات وتحديدًا بين الـ VLANs وعلى نفس فكرة الـ MSTP لكن هنا الوضع مختلف قليلا لأن العزل هنا سوف يكون على مستوى VLAN واحدة، بينما هناك العزل كان على شكل





خلاصة هذا الموضوع أن الـ STP موضوع له تفرعات كثيرة ومهم جدا أن تكون فاهم المادة النظرية فيه بشكل جيد ومتقن للأوامر الخاصة بكل بروتوكول، ولاتنس أن تصميم الشبكة إستنادا إلى موضوع الـ STP يحتاج بعض الدراسات وخصوصا عدد الأجهزة وتوزيع الـ VLANs وكيفية الربط بينها وبين الأجهزة المستخدمة، والكثير من التفاصيل الدقيقة حتى تكون نظرة شاملة تستطيع من خلالها تحديد البروتوكولات التي يجب إستخدامها وكيف سوف يتم الربط فيما بينها.

والصورة المجاورة توضح فكرة عمل هذا البروتوكول بشكل عام ويتضح من خلال الصورة كيف أصبح لدينا Instance لكل VLAN وكيف تم إغلاق بعض المنافذ في VLAN A بينما نفس المنفذ مفتوح بالنسبة لـ VLAN B.

: PVST+ نفس فكرة البروتوكول السابق لكن هنا أتاحت سيسكو إمكانية الربط بين الـ PVST والـ CST والـ MSTP وذلك من خلال PVST+ الذي يدعم بروتوكول الـ Q، 1، 802، 1Q والـ ISL وللقيام بهذه العملية يلعب السويتش الذي يعمل من خلال الـ PVST+ دور المترجم بين الـ PVST الذي يتصل معه من خلال الـ ISL وبين الـ CST الذي يتصل معه من خلال الـ Q، 1، 802.

ملاحظة هامة : الـ PVST و الـ PVST+ ليستا وضعيتان مختلفتان ويمكن تطبيقهما متى نشاء لأن موديل السويتش ونظام التشغيل الخاص به هو الذي يحدد أي الوضعيات مدعومة وهي إما الأولى أو الثانية وليس الإثنان مع بعضهما لأن فكرة الإثنان واحدة والفرق الوحيد دعم الـ Q، 1، 802.

RPVST+: لن أضيف شيء جديدا بالنسبة لهذا البروتوكول لأن الفكرة نفسها، لكن هنا تم الإعتماد على خصائص ومميزات الـ RSTP التي تحدثنا عنها في العدد السابق.

Cisco Certified Systems Instructor

كلامنا اليوم سيكون عن شهادة من شهادات سيسكو قلها يتكلم فيها الناس سواء في المواقع و المنتديات العربية أو الأجنبية و ذلك راجع لعدة أمور من بينها أنها شهادة خاصة بالمعهد المرخصة من سيسكو لتدريس تكنولوجياتها و منتجاتها و لذلك ارتأيت أن أشرح متطلباتها و كيفية الوصول إليها ألا و هي شهادة الإنستركتور

CCSI

بالطبع مع علم سيسكو.

تلاحظ أخي القارئ أن سيسكو أعطت ال CLSP الكثير من الصلاحيات و هذا ما سبب مشاكل مع ال CLP و CLPA و نتيجة الشكاوي فإن آخر عهد لسيسكو مع هذا التنظيم لمراكز التدريس المعتمدة سيكون يوليو ٢٠١١.

أين سيبدأ تطبيق المشروع الجديد الذي يعتمد على التخصصات أي كل مركز يتخصص في مجال معين و لن يبقى هناك مراكز أساسية و أخرى ثانوية و يمكنكم الحصول على أكثر تفاصيل في هذا اللينك:

<http://www.cisco.com/web/learning/enhanced.html/le٥٣/le٢٧>

لاحظ أخي أن كل المراكز تحتاج لمهندسين معتمدين من طرف سيسكو لتقديم الكورسات و لذلك لا يختلف إثنان على ضرورة و أهمية هذه الشهادة. و بناء على هذا سنذكر كل من متطلباتها، إمتحانها و كذلك إستعمالها و كيفية الحفاظ عليها.

متطلبات شهادة ال CCSI:

الشرطان الرئيسيان لهذه الشهادة هما ال CCNA و ال Learning Partner.

الشرط الأول: يجب الحصول على ال CCNA و بنتيجة أكثر من ١٠٠٠/٩٢٠ إضافة إلى ضرورة حضور كورس ال ICND ٢ في مركز معتمد من سيسكو.

الشرط الثاني: يجب أن يكون المترشح مدعوم من طرف مركز معتمد بطريقة أخرى قلنا من قبل أن الجهة الوحيدة التي يمكنها إعطاء شهادة أنستركتور هي ال CLSP إذن المسؤول في المركز الذي ينتمي إليه المترشح يقوم بالتواصل مع ال CLSP

من أجل حجز

مكان للإمتحان
لمترشحه.

أولا يجب أن تعلم أخي أنه حتى الآن يوجد ثلاث أنواع من الشراكة مع سيسكو (نتكلم عن التدريس و ليس عن الموزعين للهاردوير):

أول هذا الأنواع مراكز ال CLPA Cisco Learning Partner Associate

يعتبر مركز تدريس للمبتدئين فصلاحياته لا تتعدى تدريس الكورسات الأولى من مناهج سيسكو و أعني بذلك ال CCNA و ما صاحبها من Security و Voice و Wireless و كذلك ال CCDA.

ثاني هذه الأنواع وهو حال أغلب مراكز التدريس و هو ما يسمى بال CLP Cisco Learning Partner

و هذه المراكز تقوم بتدريس معظم مناهج سيسكو (مناهج المبتدئين مثل ال CCNA و ما تابعها من السكويريتي، الفويس، الوايرلس و أيضا المحترفين كال CCNP و CCNP Security... إلخ)، و مما تطلبه سيسكو منها توفر الإنستركتورز المعترف بهم من طرف سيسكو، كذلك بعض الأشخاص المتخصصين في مجال البيع و هو ما تسميهم سيسكو بال Sales Staff و يشترط فيهم على سبيل المثال شهادة ال CSE Cisco Sales Expert كبداية. هذه المراكز مرتبطة بالمراكز الآتي ذكرها من عدة جوانب كما سيوضح المقال.

أما النوع الثالث من الشراكة مع سيسكو فيسمى بال CLSP Cisco Learning Solutions Partner

و هذا النوع هو أعلى مستوى للشراكة مع سيسكو فيما يخص التدريس. هذه المراكز لها الحق في تدريس أي كورس من كورسات سيسكو من دون استثناء، كذلك هي التي تقوم بتقييم المهندسين حتى يصبحون إنستركتور معترف بهم، و هي المسؤولة عن بيع كتب سيسكو المستعملة في التدريس Student guides حتى إن لها الحق في الدخول على مكتبة سيسكو الداخلية و أبعد من ذلك فهي تحوز على الملكية الفكرية لسيسكو أي يمكنها التغيير في الكتب و السلايدات



إمتحان شهادة ال CCSI:

يجري الإمتحان خلال يومين. اليوم الأول مخصص للتطبيق أي ال LAB وهو يشبه كثيرا إمتحان ال CCIE لكن من ناحية الشكل لا المضمون. و اليوم الثاني يقوم فيه المترشح بتقديم فصل من فصول ال CCNA أي يعمل Presentation أمام ال Proctor.

اليوم الأول:

التطبيق هو أهم شيء فإذا نجح المترشح فيه فلا يمكن لل Proctor أن يرسبه إذا لم يكن في المستوى المطلوب في اليوم الثاني و هذا بإجماع من مر بهذا الإمتحان.

هو عبارة عن لاب بعيد Remote Access يطلب منك أن تقوم فيه بما يلي:

إكتشاف ال Topology عن طريق بروتوكول ال CDP. إعداد كل ما يخص الطبقة الثانية من ال VLANs، VTP، STP، Port Security...

إعداد ال Frame Relay Switch و هذا من أهم الخطوات لأن كل الذي سيأتي مبني عليه.

إعداد ال IP Addressing Scheme هذه الخطوة كذلك تؤثر على ما سيأتي بعدها، و هنا يجب إعداد ال Routing Between VLANs.

إعداد ال RIP ثم بعده ال EIGRP. إعداد ال passive interfaces and default information originate.

إعداد ال OSPF Multi area redistribution. إعداد ال NAT و ال PAT.

إعداد ال ACL. استعمال ال TFTP سيرفر.

الصيانة Troubleshooting و هذا الفصل مهم جدا لأنه أصعب شيء و يأتي في نهاية اليوم فيكون المترشح متعب و يفقد التركيز و عموما يتعلق بال Password Recovery و ال exec-timeout و ال IOS recovery.

هذه أهم النقاط و ليست كلها. أود التنبيه على أن المستوى



المطلوب من سيسكو هو ال CCNA لكني أؤكد أنه غير كاف و يتضح ذلك في ال Redistribution and Frame Relay Switch فأصح الإخوان للتطرق لمنهج ال CCNP حتى يسهل اجتياز هذا الإمتحان.

نقطة أخرى مهمة هذا الإمتحان ليس بالصعب من الناحية التقنية لكنه صعب من ناحية الوقت فسبعة ساعات تنقضي بسرعة و يمكن للمترشح أن يضيعها في أتفه الأمور إن لم يعرف كيف يستغل الوقت فخذ مثال: عندك ستة أو سبعة أجهزة و في كل ال active interface يتوجب إعداد ال description شفت يا أخي الوقت أين يضيع و الحل في هذه الحالة استخدام ال Text file و نسخ لصق.

إضافة لكل هذا هناك أسئلة ال Proctor التي يمكن أن تكون في مستوى أعلى من المستوى المطلوب فعلى المترشح أن يكون رزين في إجاباته و دقيق. و من بين أصعب الأسئلة التي يعتمدها ال Proctors هي استعمال كومنند متعددة لرؤية ال IP Address نتيجة ما. مثال استعمال ٣ كومنند لرؤية ال IP Address خاص بإنترفيس معين.

اليوم الثاني:

في هذا اليوم لا يركز ال Proctor على الجانب التقني من ال Presentation و إنما على كيفية إلقاءك للمحاضرة، تحركاتك، إنفعالاتك، ردودك إن كانت واثقة أم لا، طرحك للأسئلة، إستعمالك للسلايدز في السبورة، إحترامك للوقت المعطى لك و ما إلى ذلك من عوامل إلقاء محاضرة في المستوى. بالنسبة للإختيار، فالموضوع الأول من إختيار المترشح و يكون باللغة الأم، أما الثاني فيكون من إختيار ال Proctor و يلقي بالإنجليزية.

إستعمالها و طريقة الحفاظ عليها:

إن وفقت للحصول على هذه الشهادة فسترسل لك سيسكو رقمك و كما قلت يشبه ال CCIE و من ثم يجب عليك أن تضيف نفسك (تربط نفسك) مع مركز معتمد و ذلك دليل على أنك تعمل لصالحه. و من جهته يتوجب عليه أن يشتري ال The Instructor Membership من طرف سيسكو سواء ال Base or Premium.

اعلم أخي أنه إن لم تربط نفسك مع مركز معتمد لمدة ستة أشهر فسيتم نزع الشهادة منك حتى إن ربطت نفسك و لم تعط أي كورس لمدة عام فستنزع منك كذلك.

هذا ما تيسر جمعه سبحانه الله و بحمده أشهد أن لا إله إلا هو أستغفره و أتوب إليه. **عبد الرحمن بن واوو**

طريقة توقيت عمل الأكسس ليست على أجهزة سيسكو

Access-List Time

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1	2	3
4	5	6	7	8	9	10 ACL:1
11	12	13	14 ACL:2	15	16	17
18 ACL:2	19	20 ACL:1	21	22 ACL:1	23	24
25	26	27	28	29	30	

حال استخدامه أحد المخربين أو أحد الموظفين الذين يريدون تنفيذ شيء غير قانوني على الشبكة، أو لنفرض أن هناك برنامج أو فايروس تم إعداده لكي يتصل في وقت يكون الموظفين غير موجودين ويقوم بإرسال معلومات معينة إلى جهات معينة.

المثال الثاني لن يكون من الداخل بل من الخارج وهو مثلا ال VPN نحن لا نريد لأحد الإتصال خارج وقت الدوام مع الشبكة والعبث فيها وطبعا نحن لا نقصد الموظفين أنفسهم بل منالمكن أن يكون شخص ما موجود على جهاز الموظف ويقوم بحذف أو تغيير شيء معين .

قد يكون التعامل مع الأكسس ليست Access-List على أجهزة سيسكو أحد الأساسيات التي يطلب منا معرفتها ومعرفة كيفية تفعيلها على الروترات، لكن ماسوف أقدمه لكم اليوم شيء مختلف قليلا واحترايف وهو يدور حول كيفية تحديد الوقت الذي نرغب به لتطبيق ال Access-List على الروتر، متى تبدأ ومتى تنتهي باليوم والساعة.

وللموضوع أهمية كبيرة فهو يرفع من حجم الحماية على الشبكة ويقدم لنا إمكانيات أكبر للتحكم بالشبكة وبالمستخدمين الموجودين ولنذكر أهمية الوقت في الأكسس ليست لنعطي بعض الأمثلة :

المثال الأول نحن نعلم أن لكل شركة هناك خط إنترنت يسمح للموظفين الموجودين بالعمل

وإستخدام الإنترنت وعادة ما يكون الدوام الوظيفي من الساعة الثامنة

إلى الخامسة وهو الوقت الذي نحتاجه لكي نقوم بفتح الإنترنت وبعد هذا الوقت لن يفيدنا وجود الإنترنت بل سوف يضرنا لو في

```
Router# conf t
Router(config)# time-range Internet-Access
Router(config-time-range)#?
Time range configuration commands:
absolute absolute time and date
default Set a command to its defaults
exit Exit from time-range configuration mode
no Negate a command or set its defaults
periodic periodic time and date
```


ومما لا شك فيه أن الأمثلة كثيرة، بل كثيرة جدا و خصوصا عندما نعلم أن كل هذه الأمور مرتبطة بوجود أكسس ليست تسمح فيه للأشخاص الموجودين في الداخل بالخروج وفي نفس الوقت تسمح للأشخاص الموجودين في الخارج بالدخول، لذا سوف نلجأ اليوم إلى تحديد أيام وساعات معينة نسمح فيها لهذه الأكسس ليست بفرض قيوده على الشبكة وعلى حركة المرور. وسوف يقوم تطبيقنا على المثال الأول وهو السماح للموظفين باستخدام الإنترنت في أيام وساعات معينة .

و التي سوف نبدأها بأول خطوة وهي تحديد الوقت وفق الإعدادات التالية :

نقوم أولاً بإختيار اسم معين لهذا الوقت، وهنا اخترت (Internet-Access)، وبعدها وضعت إشارة الإستفهام لكي أجد الخيارات المتاحة لدينا. والذي يهمنا من كل هذه الأوامر هو أول أمر absolute، وهو من أجل تحديد وقت معين وتاريخ معين وساعة معينة يبدأ تطبيق الأكسس ليست مع التنويه أننا أيضا سوف نختار متى يجب أن تنتهي هذه البولييسي، أو نتركه فارغا للإشارة إلى أننا نريد تفعيل هذه الأكسس ليست و لانريد إيقافها أبدا.

أما الأمر الثاني periodic، فهو من أجل تحديد وقت متكرر يوميا أو أسبوعيا أو شهريا يتم تطبيق هذه الأكسس ليست والتي سوف نعتمد عليها في إعداد الشبكة وسوف تكون الإعدادات على الشكل الآتي :

```
Cisco's
Router(config-time-range)# periodic Sunday Thursday 8:00 to 17:00
Router(config-time-range)# periodic Saturday 8:00 to 13:00
```

ماذا نستنتج من هذه الإعدادات؟ الفكرة بسيطة في الأمر الأول وضعت الراج الخاص بالعمل وهو من الأحد إلى الخميس وهي أيام العمل المعروفة في وطننا العربي وهو يبدأ في الثامنة صباحا وينتهي في الخامسة مساءً، والأمر الثاني أخبر الروتر أو الأكسس ليست بأن هناك يوم إضافي قصير يأتي الموظفين فيه إلى الشركة للعمل وهو يوم السبت و يبدأ الدوام من الساعة الثامنة وينتهي في الواحدة ظهرا.

أما الخطوة الثانية فهي إعداد الأكسس ليست التي تسمح للمستخدمين باستخدام الإنترنت من خلال فتح المنفذ الخاص بالتصفح والمعروف بالمنفذ ثمانين (Port 80).

```
Cisco's
Router(config)#access-list 101 permit tcp any any eq 80 time-range Internet-
Access log
```

أعتقد أن الأمر مفهوم، فقد قمت بالسماح لبروتوكول ال HTTP بالعبور وفق التوقيت الموضح في البولييسي التي قمت بإعدادها منذ قليل (Internet-Access).

وقمت بعدها بإضافة كلمة log لمراقبة محاولات تجاوز هذه الأكسس ليست على سيرفر ال SysLog وأخيرا نقوم بتطبيق الأكسس ليست على المنفذ المتصل مع الشبكة الداخلية ولنفرض أنه FE0/0 وانتهى الأمر.

```
Cisco's
Router(config)# interface fa0/0
Router(config-if)# ip access-group 101 in
```

أبهن النعيهي

٢- VMware vCenter Server

هو مركز إدارة و إعداد مركز البيانات الافتراضى (VirtualizedDataCenter).
تتضح أهميته جليا عند شركة تحوز مثلا ٤٠ سيرفر فيزيائي بكل واحد منها ESX/ESXi، علما أن بكل واحد ٩ أنظمة افتراضية (VMs) - خليك

معي - نتكلم الآن عن ٣٦٠ نظام يجب إدارة راماته، معالجته... وما إلى ذلك من ال devices.

فبالله عليكم كيف يتمكن المسؤول عن هذه الهيكلة من الإعداد من دون خطأ إن لم يكن لديه مركز موحد للإدارة و التحكم. حتى وإن تم الإعداد بشكل جيد من دون vCenter Server فكيف سيقوم بمراقبة التطورات و احتياجات كل VMs لاحقاً (How to Supervise and Provision the Datacenter without vCenter Server)
أما من الناحية التقنية فال vCenter Server عبارة عن سيرفر له متطلباته الخاصة من رام و معالج و تخزين... و لنا الاختيار في تسطيبه على الهارد مباشرة أو جعله كسيرفر افتراضى داخل النظام الذي يديره هو بالذات. سنشرح عمل ال vCenter في مواضيع لاحقة إن شاء الله.

٣- VMware vSphere Client
هو برنامج يمكننا الحصول عليه من خلال برنامج تسطيب ال vCenter Server أو تحميله من موقع VMware. و هو عبارة عن واجهة رسومية تمكنا من الدخول على ال vCenter Server أو ال ESX/ESXi إنطلاقاً من أي جهاز ويندوز.

٤- VMware vSphere Web Access
وهي عبارة عن واجهة وab تسمح لنا بإدارة ال VMs عن بعد أي يتم إستعمال ال web browsers للدخول و التحكم في ال VMs.

٥- VMware vStorage VMFS
و هذا يعتبر نظام الملفات المطور من طرف VMware (Virtual Machine File System). يستعمله ال ESX/ESXi عند تعامله مع مختلف وسائط التخزين (...local hard disks, SAN LUN)

٦- VMware Virtual SMP
(Virtual Symmetric Multi-Processing) تمكن ال VMs الحساسة كال Oracle Database مثلا و غيرها من إستعمال عدة بروسيسورات فيزيائية في نفس الوقت. و لها علاقة مباشرة مع نوع ليسانس ال ESX/ESXi الذي تم شراؤه (تحب التكنولوجيا >== تدفع)
هذه كانت أهم المكونات إلا أنها لا تحصر جميع ما تقدمه

الحلقة الثالثة من تقنية

Virtualisation

مع ال VMware

ما هية ال vSphere

66929

66929

دائماً مع تقنية ال virtualisation و شركة VMware نستكمل ما كنا بدأناه في المواضيع السابقة. و بدايتنا اليوم ستكون من آخر ما قلناه و كان ذلك حول النظامين الأساسيين ال ESX و ال ESXi الفرق بينهما و مبدأ عملهما بشكل مختصر.

لكن في رأيكم هل هذان النظامان كافيان لضمان عمل جيد للهاردوير و تقسيم العبء على كل السيرفرات؟ و هل هما قادران لوحدهما على ضمان شبك جيد للأنظمة الافتراضية (Virtual Machines - VMs)؟ و هل هما قادران على تسيير جيد لأنظمة التخزين (Storage) و حماية جيدة لمركز البيانات؟

بالطبع لا، فهذا جواب من لديه أدنى فكرة عن ال ESX و ال ESXi. فيا ترى ما هي الخطوات التي إتخذتها شركة VMware حتى تبقى رائدة مجالها، و ما الذي أضافته لتتفوق على منافسيها؟ هذا هو موضوعنا لهذا العدد.

أصدرت VMware منتجها الأخير و الذي يسمى ال vSphere و هو عبارة عن مجموعة من التطبيقات و الأنظمة التي إعتمدتها VMware لضمان إستقرار جيد لمركز بيانات شركة ما.

ال vSphere مصطلح أطلق على عدة تطبيقات تتكامل فيما بينها من حيث عملها و هدفها فهذا مسؤول عن تسيير الهارد و تطبيق آخر مسؤول عن التحديثات و آخر مسؤول عن الحماية و كلها تهدف لغاية واحدة و هي الحصول على نظام بيانات لا يتوقف عن العمل مهما كانت الأسباب مع إستغلال ذكي للهاردوير و حمايته من أي تهديد.

مكونات ال vSphere عديدة و كثيرة منها ما هو أساسي ضرورى و منها ما يمكن التخلي عنه بالنسبة للشركات ذوات مراكز البيانات الصغيرة و لذلك سنذكر أهمها:

١- ال VMware ESX/ESXi

و هذا كان موضوعنا السابق و هي الطبقة الافتراضية (Virtualisation Layer) الذي توفره VMware و يتم تسطيبه مباشرة على الهاردوير مثله مثل أى نظام تشغيل. و هو المسؤول عن توزيع الهارد على الأنظمة الافتراضية (VMs).

VMware و إنما هي ذكر لأهمها. يقسم الـ vSphere من حيث عمل مكوناته و مهمة كل جزء منه إلى عدة أقسام تتضح من خلال الصورة و الشرح الذي يليها.



القسم الأول: Infrastructure Services

و هي الخدمات التي تتعلق بتسيير النظام مباشرة سواء كان السيرفرات، وسائط التخزين أو الشبكة، و هي تنقسم بدورها إلى ٣ أقسام:

vCompute؛ و هو يتمثل في نظامي الـ ESX و الـ ESXi إضافة إلى خاصية الـ vSMP، و هنا يمكنك أخي ملاحظة أن كل ما له علاقة بالهارد يدرج في خانة الـ vCompute. و منه أيضا الـ DRS Distributed resource Scheduler و هي خاصية تمكن من توزيع عبء إستعمال الـ رام و المعالج على مجموعة من السيرفرات الفيزيائية بشكل أوتوماتيكي و هنا تظهر فكرة الـ clusters.

vStorage؛ و هنا نتكلم عن وسائط التخزين و كيف يتم التعامل معها بإستعمال نظام الملفات VMFS و كذلك كيف يتم إتخاذ الحبيطة و تقدير إستعمال الأنظمة الوهمية لوسائط التخزين و هو ما يعرف بالـ Provisioning.

vNetwork؛ تعلمون أن في العالم الملموس أي الأجهزة الحقيقية يتم إستعمال سويتشات لربط الأجهزة فيما بينها و تكوين شبكة، و لا يخفى عليكم أنه عند التحول من أنظمة البيانات الحقيقية إلى الافتراضية يتوجب علينا أن نوفر

HA... و غيرهما. و كذلك بعض التطبيقات المرافقة له و الموجودة مبدئيا في ال vCenter Server installer package. إلا أن هناك بعض التطبيقات التي يلزم شراؤها على حدة.

التطبيقات الأولية (by default) :

vCenter Converter : يمكننا من تحويل الأجهزة الحقيقية و الأجهزة الوهمية الأخرى (Workstation VMs مثلا) و صور الأنظمة (Third party images مثل Ghost) إلى أجهزة وهمية قابلة للإشتغال على ال ESX/ESXi.

vCenter Update Manager : يصلح لتحديث

ال ESX/ESXi (hosts) وكذلك ال VMs مقارنة

بمرجعية يتم تحديدها من طرف المسؤول عن النظام.

vCenter Guided Consolidation : يستعمل

لاكتشاف و تحليل و برمجة تحويل الأجهزة الحقيقية إلى

أجهزة وهمية. فهو يمكننا من معرفة ما إذا كان نظامنا

الافتراضي سيتحمل ال VM الجديد أم لا.

إعلم أخي أنك لن تدفع و لا دولار مقابل استعمال الثلاث

تطبيقات السابقة فهي متوفرة مع ال vCenter Server

Installer، و هاك باقي الحزمة التي لا يتسع المجال لشرح كل تطبيق منها

vCenter Server Heartbeat، vCenter

Operations، vCenter Orchestrator،

vCenter Capacity IQ، vCenter Site

Recovery Manager ، vCenter Lab

Manager، vCenter Configuration

manager، vCenter Chargeback، vCenter

Application Discovery و كثيرة هي تطبيقات ال

vCenter و ال Plug-ins التي يمكن إضافتها.

هذا مجمل ما وسعني جمعه لهذا العدد من معلومات بسيطة

حول ال vSphere الذي مكن VMware من التربع

على عرش ال Virtualisation، و الجميل في هذا كله

أن VMware من خلال هذه الحزمة توفر حل كامل و

شامل لأي شركة تريد الانتقال من الأنظمة الفيزيائية إلى

الأنظمة الوهمية. و لهذا ذكرنا في أول موضوع أننا سنتطرق

لهذه التكنولوجيا المقدمة من VMware ليس حبا فيها و لا

دعاية لها و إنما لأنها رقم واحد على الأقل لحد الآن.

أرجو أن تكونوا قد استفدتم و لوقليلا و موعدا في

العدد القادم إن شاء الله مع مزيد من المعلومات عن ال

Virtualisation.

خاصية الشبك لل VMs و هذا ما قامت به VMware من خلال ال vNetwork Distributed Switches

. و هي عبارة عن سويتشات يتم إنشاؤها افتراضيا

(virtually) و ربط الأجهزة الوهمية بها مع إمكانية

التحكم كما في الهارد من vlans و ما شابهها، حتى أن

VMware ذهبت إلى أبعد من ذلك و هو إمكانية دمج

سويتش سيسكو قامت هذه الأخيرة من تطويره خصيصا

للعالم الافتراضي ألا و هو ال vNexus 1000.

القسم الثاني : ال Application Services

و هذه يمكن اعتبارها سوفت لأنها لا تتعامل مباشرة مع

الهاردوير و إنما تساعد على التحكم في ال VMs و أداؤها. و

يمكن تقسيمها أيضا على حسب ال application المتوفرة

كما يلي :

Availability : و هي application تساعد على توفير

ال resources في أي لحظة و كذلك تضمن الإستمرارية

للنظام يعني downtime و منها ال vMotion

التي تتمكن من خلالها من نقل تشغيل ال VMs من سيرفر

إلى آخر، و ال Storage vMotion الذي يضمن عملية

نقل ملفات ال VMs من وسيط تخزين إلى آخر (أود

التنويه على أن ال VMs عبارة عن ملفات عديدة يمكن نقلها

من مكان إلى آخر و منها ال .vmx و ال .vmdk و غيرهما).

و كذلك ال HA High Availability التي تمكن من

إقلاع VM معين في سيرفر ثان عندما يحصل عطب في

السيرفر الذي يحمله و هنا سيكون التوقف حوالي 5

دقائق، أما إن أردنا إعادة الإقلاع من دون توقف فيجب

استعمال ال FT Fault Tolerance.

Security : ال application التي تصنف هنا تساعد

على ضمان حماية عالية و منها ال vShield Zone و ال

VMsafe و هي تمكن من تقسيم ال VMs و التحقق من

أنها تحترم القواعد و المتطلبات التي تم تحديدها من إدارة

النظام مع عزل كل مجموعة VMs عن الأخرى. كذلك

يمكن لمصنعي و مطوري برامج الحماية و تحليل الترافيك من

إدماج منتوجاتهم مع ال hypervisor.

Scalability : و أهم خاصية هنا هي ال hot Add

أي إضافة ال رام و المعالج و التخزين ل VM معين أثناء

إشتغاله من دون التأثير على عمله.

إعلم أخي أن ال application services لا يمكن

الإستفادة منها في غياب ال vCenter Server.

القسم الثالث : vCenter Suite

عند تثبيت ال vCenter Server الأولى تجدون معه

بعض ال functionality مثل ال vMotion و ال

عبد الرحمن بن داود

معايير معهد مهندسي الإلكترونيات والكهرباء للشبكات اللاسلكية



IEEE 802.11™ WIRELESS LOCAL AREA NETWORKS

The Working Group for WLAN Standards

تكلّمنا في الحلقة السابقة عن معهد مهندسي الإلكترونيات والكهرباء بصفة عامة و عرفنا أن ما يخصنا كمهندسي شبكات في مقاييس هذا المعهد هي المقاييس التي تبدأ بتلك الصيغة IEEE 802.X وتستطيع ان تضع مكان حرف X اي رقم يتراوح بين 1 و 22 وكل رقم له تفرعات وفي مجموعها تشرح وتؤصل للشبكات السلكية واللاسلكية وانواع الكابلات وقيم الترددات وغيرها وهذا مخطط لما يدعمه هذا المقياس

802.1 HILI Overview	802.2 Logical Link Control IEEE Std 802.2, ISO 8802-2: 1989										802.10 SILS	OSI- Layer 2
	802.1 MAC Bridging IEEE Std 802.1 D: 1990											
Architecture Management	802.3 CSMA/CD	802.4 Token Bus	802.5 Token Ring	802.6 MAN	ISLAN	802.11 WLAN	802.12 Demand Priority	802.14 CATV	802.15 WPAN	802.16 BWA	802.17 RPR	OSI- Layer 1
	IEEE Std ISO 8802-3 1990	IEEE Std ISO 8802-4 1990	IEEE Std ISO 8802-5 1990	IEEE Std 802.6	IEEE Std	IEEE Std	IEEE Std					
802.7		Broadband TAG (BBTAG)				IEEE 802.7-1989						
802.8		Fiber Optic TAG (FOTAG)				IEEE 802.8-1987						
802.18		Radio Regularity TAG (RRTAG)										

وسنتكلم الآن عن ما يخصنا من المقاييس التي يدعمها هذا المعهد لتكنولوجيا الشبكات اللاسلكية المحلية WLAN أو مقياس IEEE 802.11 وهو عبارة عن عدة مقاييس لضبط التعامل مع الشبكات اللاسلكية المحلية WLAN وذلك في المدى الترددي

802.11 network standards							
802.11 protocol	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate (Mbit/s)	Modulation	Indoor rang	outdoor range
—	Jun 1997	2.4	20	1, 2	DSSS, FHSS	20	100
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
		3.7				—	5,000
b	Sep 1999	2.4	20	5.5, 11	DSSS	38	140
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM, DSSS	38	140
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150		70	250

2 و 4 و 3,6 و 5 جيجا هرتز و تم اطلاقه في 2007 و لذلك فإنه يسمى أحيانا 802.11a و المعايير التي أطلقت من خلال المقياس 802.11g بينها هذا الجدول

لقد أطلق هذا المعيار كمحدد بدائي للشبكات اللاسلكية المحلية في العام ١٩٩٧ متشابهاً مع شبكات الإيثرنت في طريقة التواصل وهي CSMA/CD والتي يتحسس فيها الوسط قبل الإرسال لكشف التصادم وهي نقطة ضعف في هذا المعيار وفي أي تقنية تعتمد على بروتوكول CSMA/CD نتيجة تضحيته بقسط كبير من المدى الترددي في سبيل ضمان وصول البيانات.

يحدد معيار IEEE 802.11 أيضاً سرعتين أساسيتين لنقل البيانات: ١ و ٢ ميغابت في الثانية للإرسال عبر الأشعة تحت الحمراء (Infrared (IR) أو موجات الراديو التي تعمل على التردد ٢,٤ غيغاهرتز.

ظهرت في الأسواق عدة منتجات صممت وفقاً للمواصفات الأصلية لمعيار IEEE 802.11 لكنها سرعان ما استبدلت بمنتجات متوافقة مع معيار IEEE 802.11b بعد إقرار التعديل b على المعيار الأساسي في العام ١٩٩٩ ولم يظهر وجود أي تطبيق عملي حتى الآن للإرسال عبر الأشعة تحت الحمراء، إلا أنها مازالت جزءاً من المعيار الأصلي 802.11b

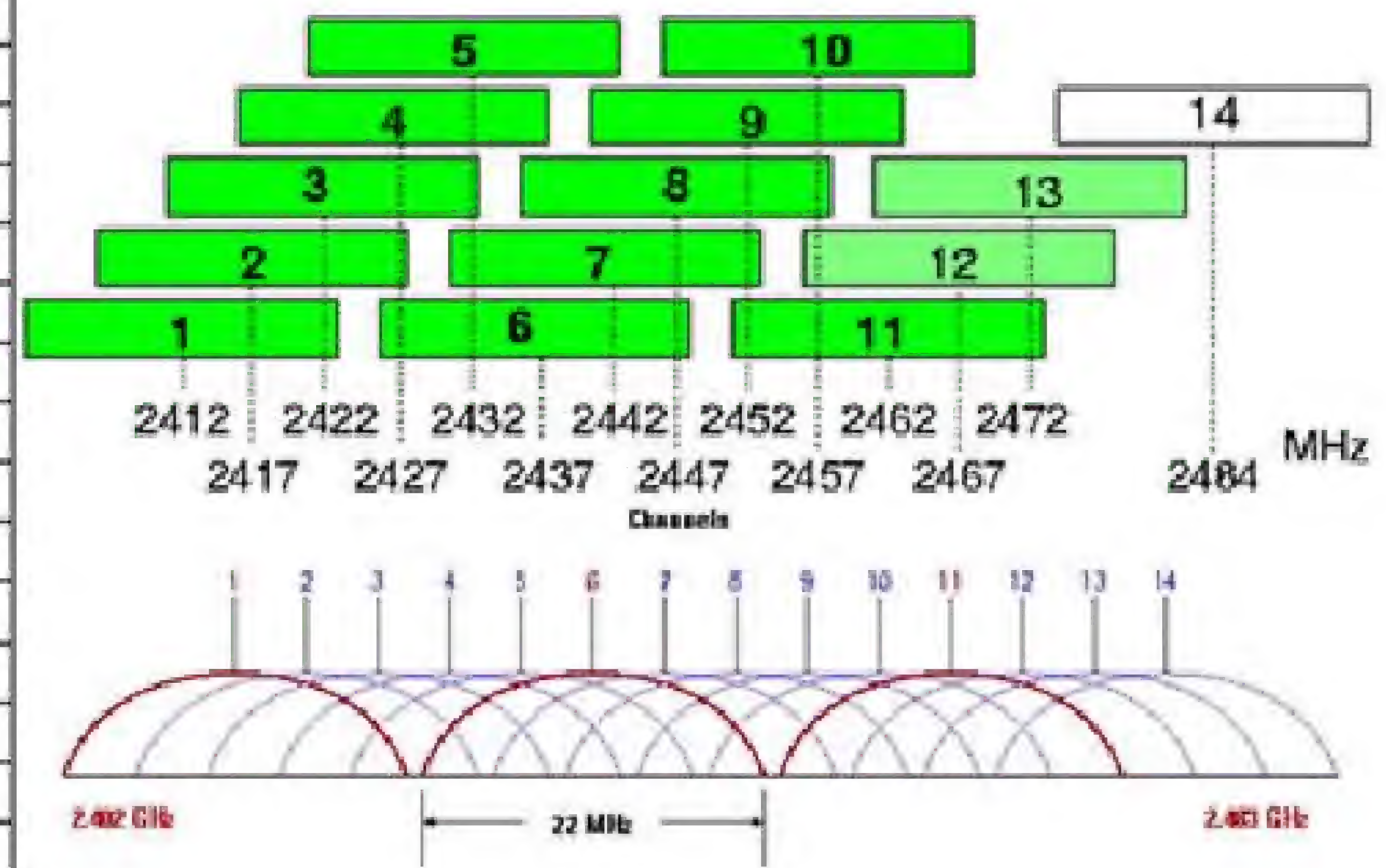
صادق المعهد الدولي لمهندسي الكهرباء والإلكترونيات IEEE على هذا البروتوكول ١٩٩٩ وهو يعتبر أكثر بروتوكولات الشبكات اللاسلكية انتشاراً في يومنا الحالي.

ويتضمن معيار IEEE 802.11b تحسينات عن المعيار الأصلي 802.11 لدعم نقل البيانات بسرعات ٥,٥ و ١١ ميغابت في الثانية

يستخدم هذا البروتوكول تقنية Direct Sequence Spread Spectrum – DSSS ويعمل ضمن المدى الترددي ٢,٤١٢ و ٢,٤٨٢ جيجا هرتز

وهذه هي الترددات والقنوات الترددية المستخدمة مع هذا النوع

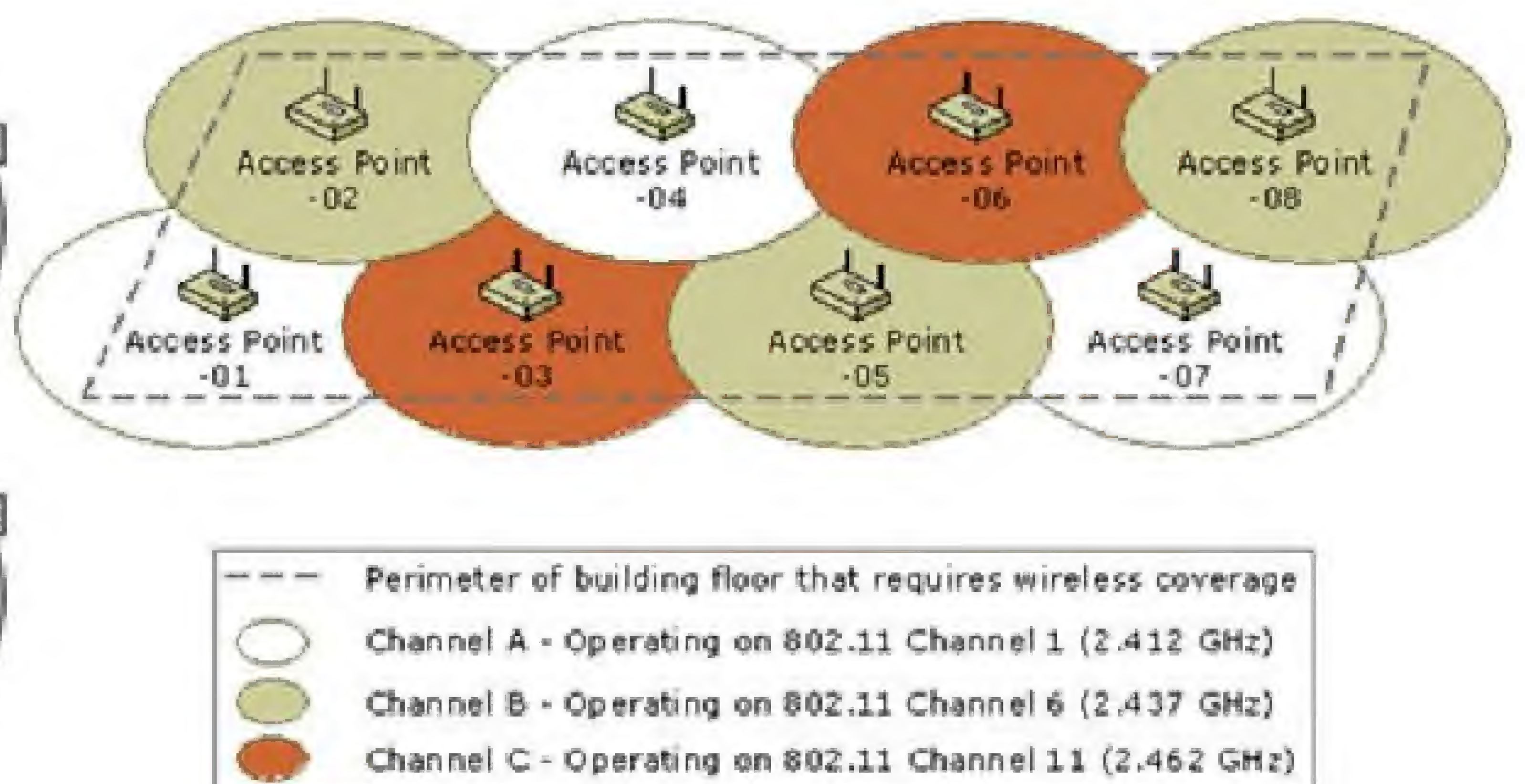
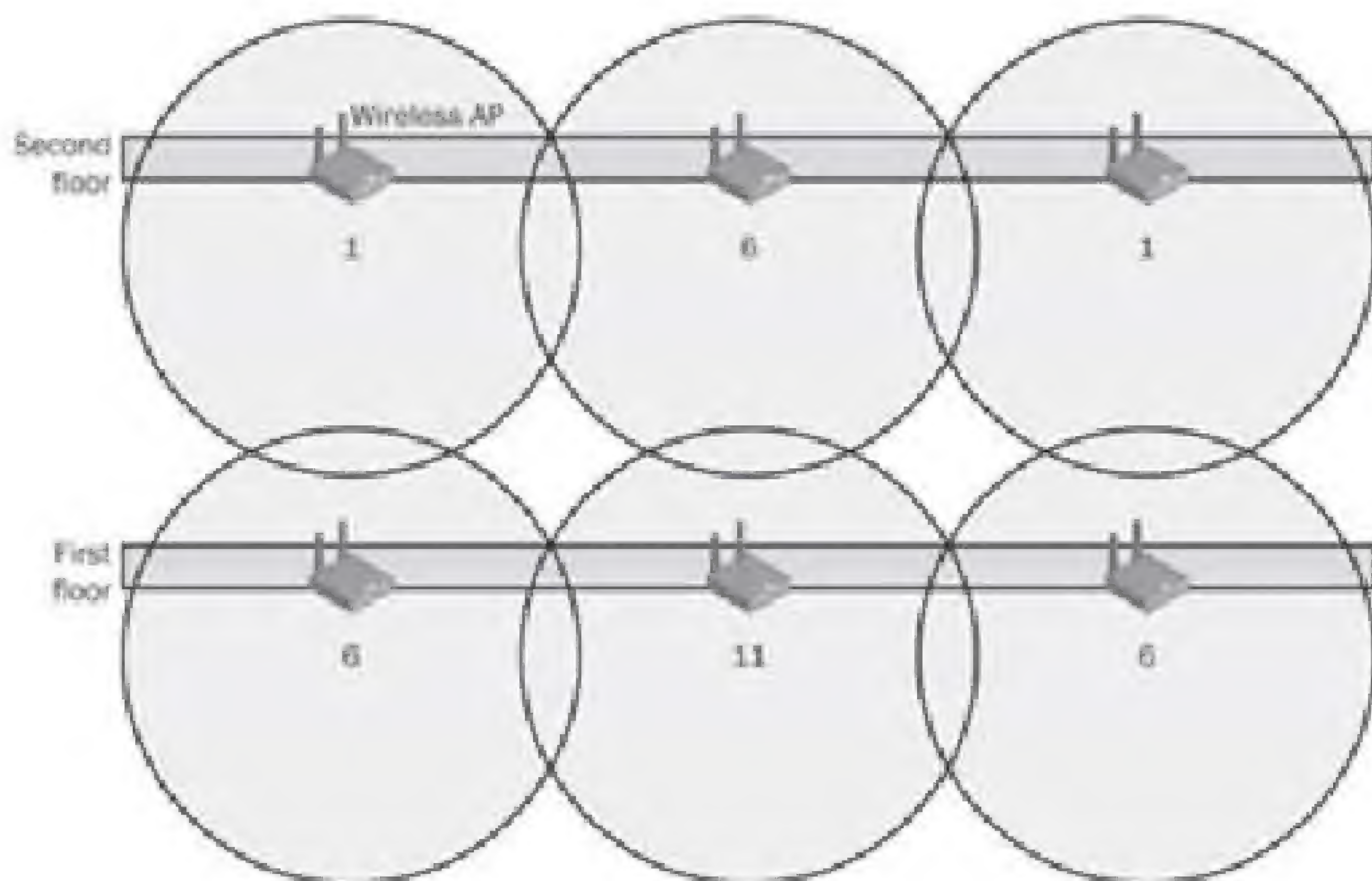
Channel	Frequency (GHz)	Range	Channel Range
1	2.412	2.401 - 2.423	1 - 3
2	2.417	2.406 - 2.428	1 - 4
3	2.422	2.411 - 2.433	1 - 5
4	2.427	2.416 - 2.438	2 - 6
5	2.432	2.421 - 2.443	3 - 7
6	2.437	2.426 - 2.448	4 - 8
7	2.442	2.431 - 2.453	5 - 9
8	2.447	2.436 - 2.458	6 - 10
9	2.452	2.441 - 2.463	7 - 11
10	2.457	2.446 - 2.468	8 - 11
11	2.462	2.451 - 2.473	9 - 11
12	2.467	2.456 - 2.478	Not US
13	2.472	2.461 - 2.483	Not US
14	2.484	2.473 - 2.495	Not US



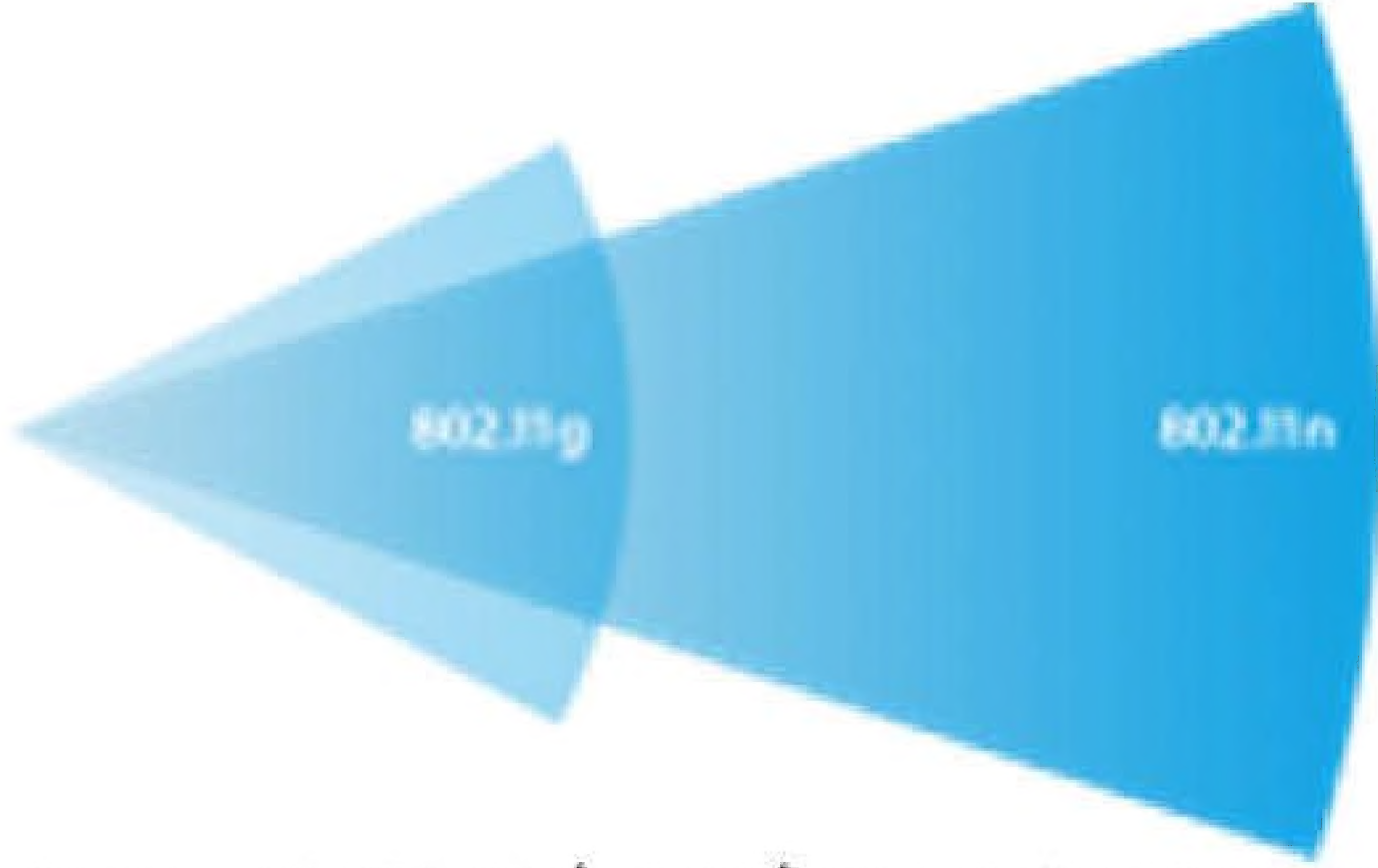
و ستجد بالطبع أن هذه القنوات تتداخل فيما بينها لتعكير التواصل بين خلايا الشبكة و لذلك فإننا نستخدم منها ثلاث

نطاقات فقط غير متداخلة وهي من ١ الي ٣ و ٤ الي ٨ و ٩ الي ١١

لذلك فعند اعداد شبكة لاسلكية بها العديد من أجهزة الأक्सس بوينت فلا بد أن تراعي ان يكون كل جهازين متجاورين من نطاقين مختلفين لمنع التداخل هكذا



لزيادة سرعة نقل البيانات ونطاق الإرسال.
التوافقية بين المعايير



إذا كنت تنوي شراء مودم أو راوتر أو كارت لاسلكي مع ميزة الوايرلس من نوع "N" أو بالأصح "802.11n" للحصول على بث أقوى ومدى أبعد تأكد من أن باقي أجهزة الشبكة اللاسلكية تدعم هذا النوع حتى يمكنك الاستفادة من أقصى إمكانيات الجهاز الجديد .

و أغلب أجهزة الكمبيوتر المستخدمة حالياً تدعم استقبال الإشارة من نوع 802.11b/g فإن كان كرت الشبكة اللاسلكي لديك من هذا النوع وجهاز البث من نوع "802.11n" فلن يمكنك الاستفادة من المدى البعيد الذي يوفره أبداً وكأنك تستخدم جهاز بث عادي. وإذا كنت تنوي شراء كمبيوتر أو كرت وايرلس تأكد من أنه يحمل هذه العلامة 802.11n أو 802.11b/g/n.

ففي الصورة التي علي يمينك تري ان الخلايا المتشابهة اللون هي غير المتداخلة ، و الصورة علي يسارك تطبيق عملي علي اختيار الخلايا

وعادة ما يقدم لهذا المعيار وجود إشارة واضحة بما فيه الكفاية لجعلها فعالة لنحو ٥٠ متراً و تتغير المسافة تبعاً لمتغيرات كثيرة، مثل الأحوال الجوية والعوائق المادية و وجود مشوشات الكترونية و كهربية علي الإشارة مثل فرن الميكروويف أو الهاتف اللاسلكي.

802.11a

يعمل معيار IEEE 802.11a ضمن نطاق التردد ٥ غيغاهرتز ويستخدم تقنية OFDM و سرعة قصوى لنقل البيانات تعادل ٥٤ ميغابت في الثانية.

لم يبلغ معيار IEEE 802.11a حتى يومنا هذا الانتشار الواسع الذي حققه نظيره IEEE 802.11b .

802.11g

لقد تم اعتماد هذا المعيار في عام ٢٠٠٣ وأعطى الاسم IEEE 802.11g. يعمل هذا المعيار شأنه شأن نظيره IEEE 802.11b ضمن النطاق الترددي ٢,٤ غيغاهرتز.

يستخدم معيار 802.11g تقنية OFDM (802.11a)

و سرعة قصوى لنقل البيانات تصل حتى ٥٤ ميغابت في الثانية. لضمان التوافقية مع المنتجات العاملة وفق معيار

802.11b فإن هذا المعيار يستخدم تقنيات CCK+DSSS

مثل تلك المستخدمة في 802.11b عند سرعات نقل

البيانات ١١ و ٥,٥ ميغابت في الثانية في حين يستخدم تقنية

DBPSK/DQPSK+DSSS عند سرعات ١ و ٢

ميغابت في الثانية.

يعود الفضل إلى القبول الواسع الذي حظي به معيار IEEE

802.11g بالدرجة الأولى إلى توافقيته مع التجهيزات

العاملة وفق معيار 802.11b

802.11n

بعد مخاض عسير زاد عن سبع سنوات، اعتمد المعهد الدولي

لمهندسي الكهرباء والإلكترونيات IEEE المعيار اللاسلكي

«802.11n». وذلك بعد فترة اختبارية طويلة مع نسخة

منه تسمى 802.11n draft محاولة إقناع المستهلكين بأن

أجهزتهم ستتوافق في العمل مع الإصدار الأخير للمعيار

ويهدف هذا المعيار إلى الوصول إلى سرعة نظرية قصوى

لنقل البيانات تعادل ٥٤٠ ميغابت في الثانية مما يجعله أسرع

٤٠ مرة من معيار 802.11b و ١٠ مرات من معيار 802.11a.

ويعتمد المعيار الجديد على نفس التعديلات السابقة

لمعيار 802.11 مع فارق أساسي يكمن في استخدام تقنية

(Multiple-Input Multiple-Output MIMO)

والتي تتطلب استخدام عدة مرسلات وعدة مستقبلات

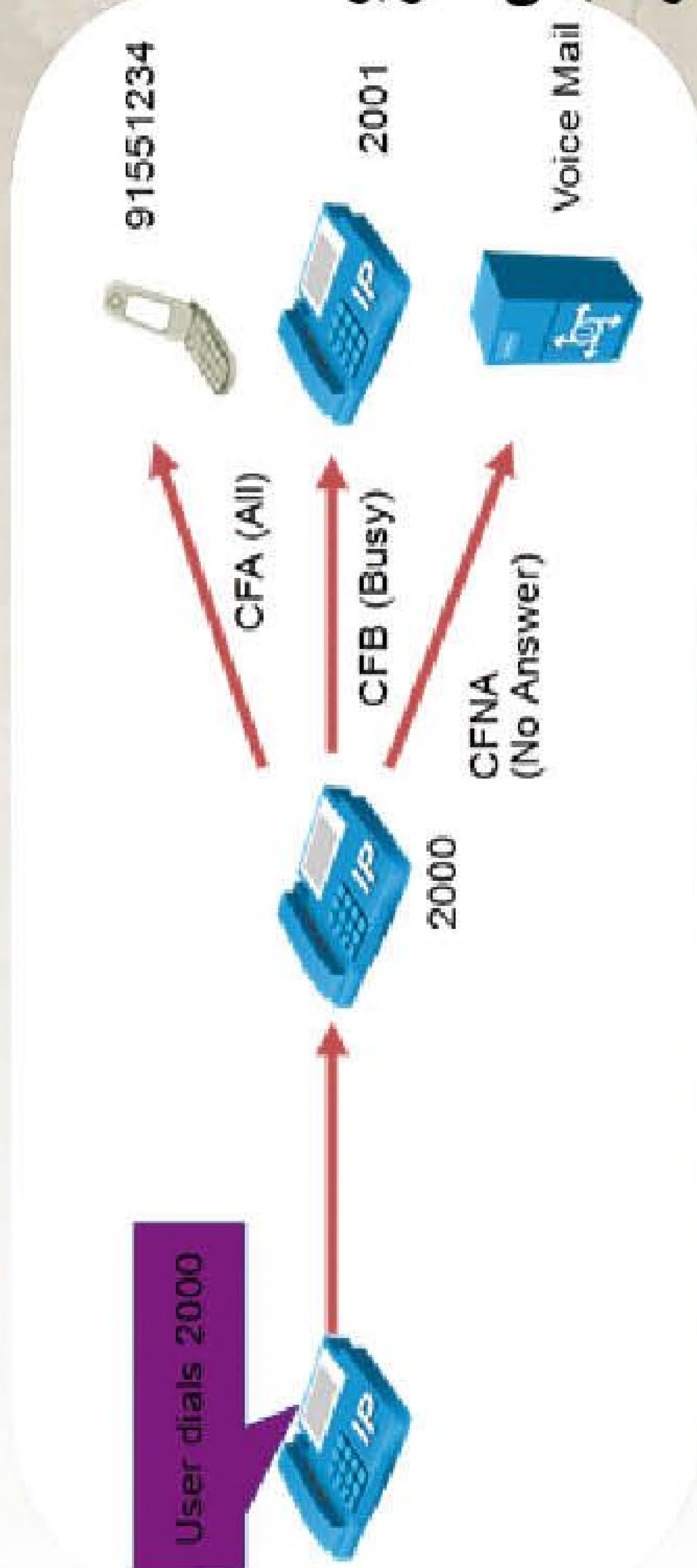
Call Coverage

ويمكن برمجة هذه الخاصية من User web page أو من التليفون نفسه بواسطة مستخدم التليفون أو CUCM Administrator.

(Call Forward NO Answer (CFNA) معناه تحويل المكالمات في حالة عدم إجابة المستخدم خلال وقت معين يتم تحديده بواسطة مستخدم التليفون من user web page أو بواسطة CUCM Administrator.

Call Forward Busy معناه تحويل المكالمات في حالة إنشغال التليفون المطلوب بمكالمة أخرى، ويمكن برمجة هذه الخاصية بواسطة مستخدم التليفون من user web page أو بواسطة CUCM Administrator.

ملحوظة : يمكن لمدير النظام أن يقوم بعمل Calling search space منفصلة لكل نوع من أنواع التحويل السابقة (CFNA & CFB) ويمكن أيضا وضع CSS مختلفة للمكالمات الداخلة ON-NET والمكالمات الخارجية Off Net، وفيما يلي شكل توضيحي لتمرير المكالمات:



في مقالتي لهذا العدد سوف أتطرق للحديث عن أحد أقوى ميزات أجهزة التليفون الخاصة بسيسكو وهي ال Call coverage التي تضمن لنا عدم فقدان أى مكالمات ترد إلى أحد العملاء وهي جزء من ال Dial Plan وله مظاهر عديدة منها:

Call forwarding ومعناه أن الرقم المطلوب لو لم يجب سيتم تمرير المكالمات إلى رقم آخر أو إلى ال Voice mail.

Shared Lines ومعناه وضع DN رقم تليفون واحد على أكثر من جهاز لكي يرد أحد الأجهزة في حالة عدم رد الجهاز الأول.

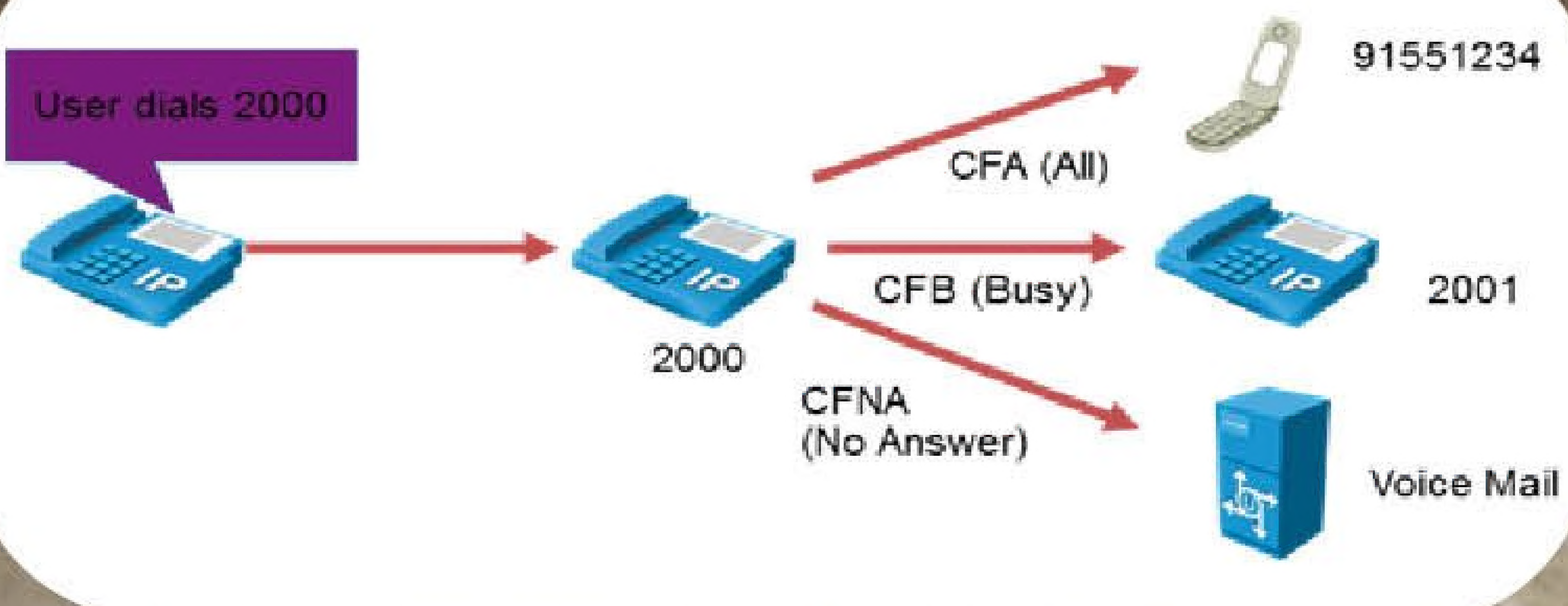
Call pickup ومعناه سحب المكالمات التي ترن على أحد التليفونات إلى تليفون آخر، بمعنى أنك و صديق لك على مكتبين في نفس الغرفة وسمعت تليفونه يرن ولكنه غير موجود، فليس من الضروري أن تقوم من على مكتبك وتذهب إلى مكتبه للإجابة على هذه المكالمات، ولكن تستطيع الإجابة عليها من خلال تليفونك أنت بواسطة ضغط الزر Pick up ولكن يجب تفعيله أولا فهو لا يعمل تلقائيا.

Call hunting هي مظهر آخر من مظاهر ال Call coverage ولكنه أفضل وأبعد قليلا وأكثر مرونة من المظاهر الأخرى التي رأيناها وهي محور حديثنا في هذا الدرس، وخلصتها أن التليفون الذي يرن الآن إذا لم يجب صاحبه خلال وقت معين - نقوم بتحديدده - سيتوقف عن الرنين ويبدأ تليفون آخر في الرنين بدلا منه في مكان آخر، وإذا لم يجب الثاني وهكذا سيرن في مكان آخر حتى يجد من يرد عليه. كما ذكرنا في البند رقم واحد Call forwarding وكما هو مفهوم من اسمه هو تحويل المكالمات.

سؤال : ولكن كيف ستمرر هذه المكالمات وما شروط تمريرها؟

الإجابة: هناك ثلاث أنواع من Call forwarding:

(Call forward All (CFA) معناه تحويل جميع المكالمات الواردة إلى هذا التليفون بدون شروط والتليفون المطلوب لن يرن أصلا بل سيرن التليفون المحولة له المكالمات،



في هذه الحالة عند الاتصال ب الرقم ٢٠٠٠ سترن جميع التليفونات التي تحمل نفس الرقم، وعند إجابة أحد التلفونات ستتوقف التليفونات الأخرى عن الرنين، أما بخصوص ال PICK UP التي تحدثنا عنها في مقال سابق تقوم على مبدأ بسيط وهو قيام CUCM بالسماح بتجميع خطوط عديدة داخل Call-pickup groups وكل مجموعة من مجموعات Pickup تكون معرفة برقم وحيد لا يتكرر لمجموعة أخرى.

ملحوظة مهمة :

التليفون يكون داخل مجموعة واحدة من مجموعات Pickup

سؤال: إذا كان التليفون الذي يرن ليس في نفس المجموعة التي أنت فيها ولا تستطيع عمل Pickup له هل ستضيع المكالمات؟ الإجابة : بالطبع لا هناك وسيلة أخرى وهي ال Group Pickup، تضغط على زر GPickupsoftkey وتدخل رقم المجموعة التي يرن فيه التليفون المراد إلتقاطه وتسحب الخط.

CALL HUNTING

عرفنا فيما سبق معنى Call hunting ولا داعي لتكراره ولكن ما سنتكلم عنه الآن هو:

مكونات Call hunting

رقم التليفون phone dn أو البريد الصوتي voice mail يتم تخصيصهم إلى line groups .

Line groups تخصص إلى HUNT LIST .

و ال hunt list يمكن أن تحتوى على واحدة أو أكثر من ال line group .

خصائص ال Line group hunt و distribution algorithm يمكن تحديدهم لكي نحدد كيف ستتم عملية ال hunting لأعضاء ال line group

تخصيص HUNT LIST إلى ال HUNT PILOT .

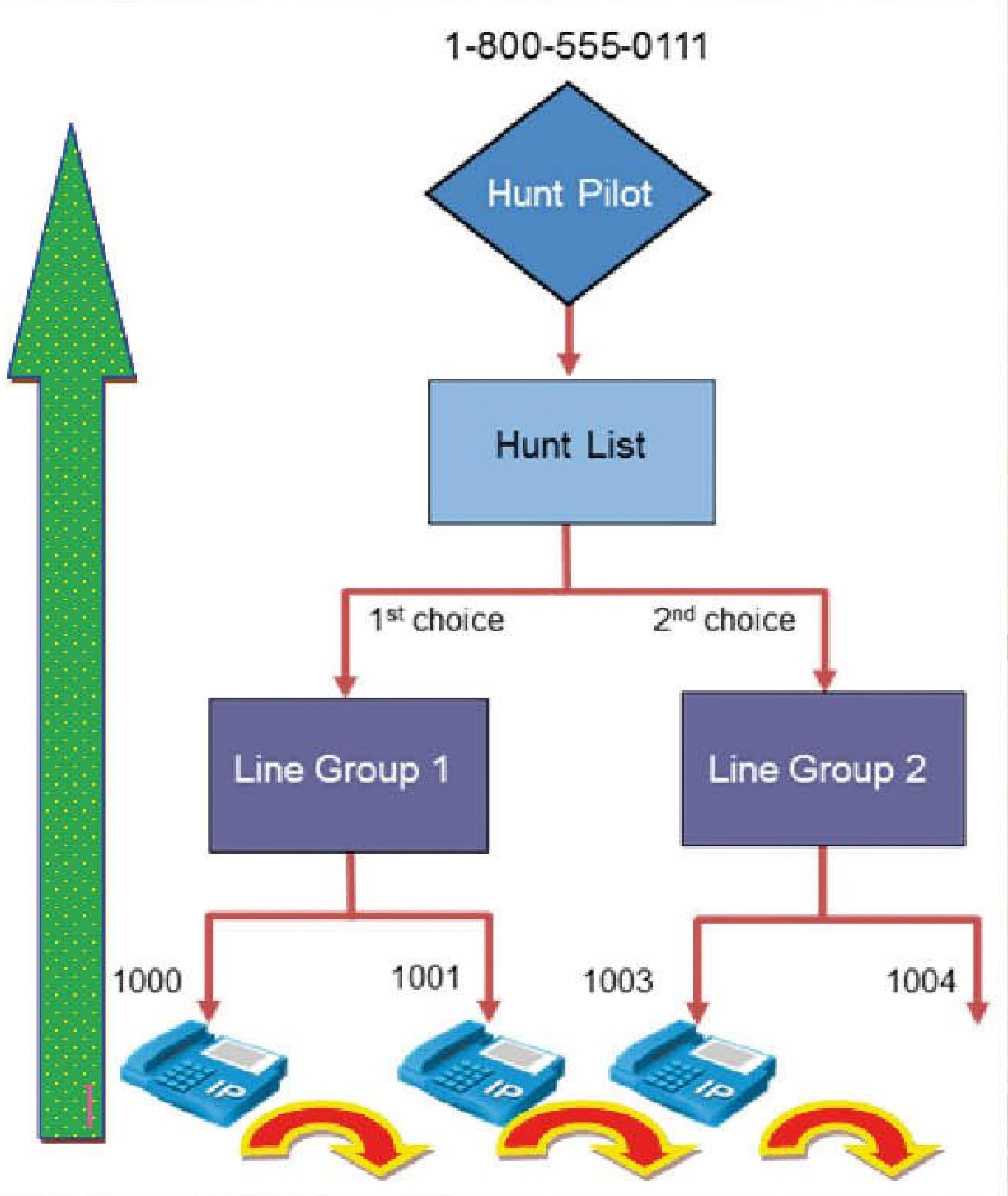
وكما علمنا أن ال hunt list هي مجموعة من ال line groups .

pilot هي أعداد سوف تطابق الأرقام المطلوبة لكي تنفذ عملية ال hunting .

Hunt pilot ممكن أن تطلب مباشرة أو يتم تمرير المكالمات لها من أي تليفون تلقى المكالمات وكان قد تم برمجته لكي يمرر المكالمات إلى ال hunt pilot .

أثناء عملية ال hunting فإن البرمجة التي تم عملها لتمرير المكالمات لأعضاء ال line

group لن تستخدم، فمثلا لو التليفون في حالة ال hunting ولم يتم الرد على المكالمات فإن إعدادات CFNA (call forward not answer) لن تطبق وسيجاهلها cucm وسيطبق ال hunting algorithm وستذهب المكالمات إلى العضو التالي في ال line group .

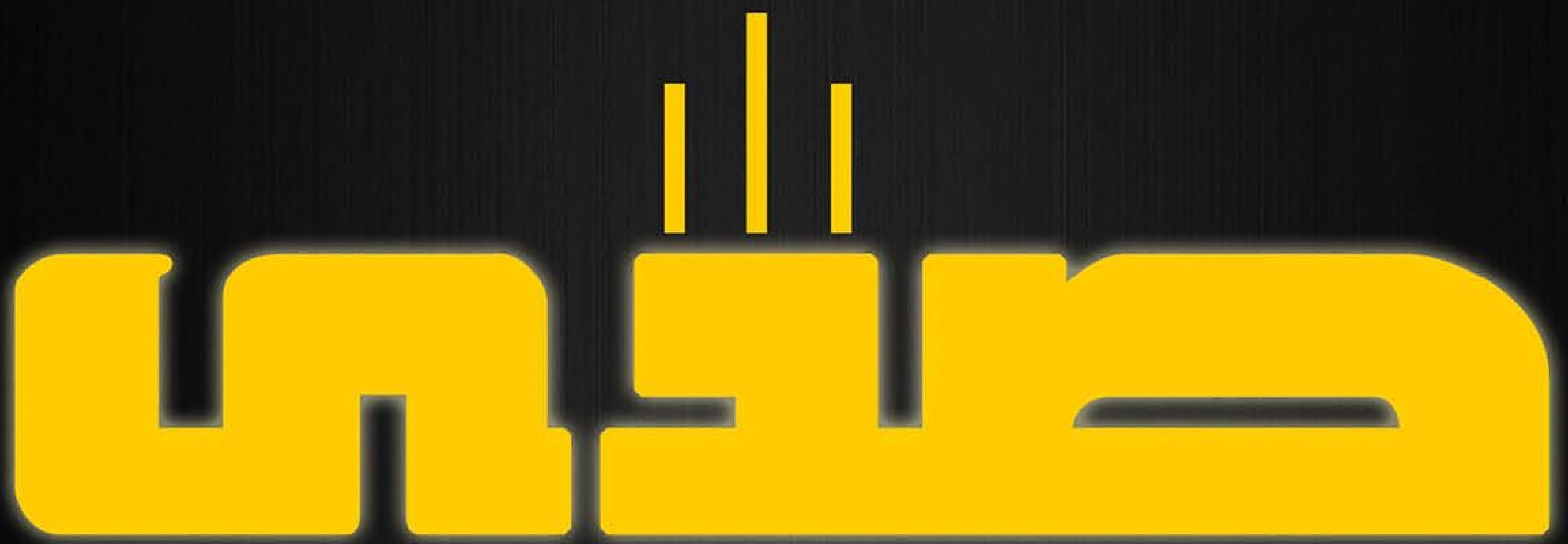


كما نلاحظ من السهم سيتم عمل الشكل من أسفل إلى أعلى، أي أننا سنعمل line group أولا ثم hunt list ثم hunt pilot

المفروض ببساطة أن يرد رقم ١٠٠٠ فإن لم يرد، يرن التليفون عند ١٠٠١، إن لم يرد تذهب المكالمات إلى line group ٢ ويرد ١٠٠٣ فإن لم يرد تذهب المكالمات إلى ١٠٠٤ .

إلى هنا نكون قد إنتهينا من القسم الأول من المقال وسوف نعود لنتابع معكم كيفية عمل ال Call Hunting في العدد القادم.

المهندس : أحمد الشحات



Echo Technology

Integratoin Technical Solution

Network - Web Design

Training & Development

Programing - Design & Printing

Electronic System - Control System

**Whole Technical
One Supplire**

Study and implementation of engineering projects

Syria - DeirEzzor - Telefax: 051 218452 - Mob: 0967 96265 - 0955 478942

Website:WWW.EchoTechno.com - E-mail:Info@EchoTechno.com (Soon)