



*spanning tree protocol*

*ESX and ESXi*

*Auto-secure*

*REGEX*

*ieee*



clearBOX™



ClearBOX Hardware

*March 2011*

# NetworkSet



# NetworkSet Magazine

أول مجلة عربية مجانية تختص بأمور الشبكات  
www.Networkset.net

مؤسس ورئيس تحرير المجلة : م.أيمن النعيمي

## المحررون

المهندس أيمن النعيمي  
المهندس أنس الأحمد  
المهندس أحمد الشحات  
المهندس عمرو يحيى  
المهندس عبدالجليل الوكيل  
المهندس عبد الرحمن بن داود  
المهندس شريف مجدي  
المهندس نادر المنسي  
المهندس علاء مازن عدي

## المراجعة اللغوية

المهندس أسامة الشرقاوي

التصميم والإخراج الفني

**صدى**  
**Echo Technology**

Integratoin Technical Solution

eng.Anas kh Al-Ahmad

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



# المحتويات

المحتويات	2
المبادرة	3
الرخص وطريقة إعدادها على أجهزة سيسكو	4
AAA	9
Auto-secure	12
Cisco Configuration Professional&GNS	14
ClearOS	16
ESX and ESXi	20
REGEX	23
spanning tree protocol	27
Wireless Network technologies	30
IEEE	30



# البحوث العلمية أم المحتوى العربي

قد لا يخفى على الجميع أن المحتوى العربي على الأنترنت والمراجع العلمية بشكل عام تشكل عشرة بالمئة فقط من المراجع الموجودة بلغات أخرى وتشير بعض الدراسات أن المحتوى العربي على الأنترنت يشكل ثلاثة بالمئة فقط؟؟؟...

نعم أخي العزيز هذا هو حالنا العربي على الأنترنت آلاف المواقع العربية والمدونات والمنتديات وفي الآخر ثلاثة بالمئة فقط وما زال اغلبنا نائم ينتظر اليوم الذي يستيقظ فيه ويجد كل ما يطلبه من علوم متوفر على الأنترنت وأكد أن هذا اليوم لن يأتي طالما مازال تفكيرنا وهدفنا هو إيجاد العمل والفرصة المناسبة وطالما هناك زر في أجهزة التشغيل يدعى (نسخ <sup>سرقة</sup> لصق) فمن خلال متابعتي لأحد أشهر المنتديات العربية في مجال الشبكات أجد آلاف الأعضاء الذين يمرون على المنتدى ويستفيدوا من وجود بعض الأعضاء الذين يعملون بدون مقابل ويبدأ أستهلاك كل ما هو موجود ومفيد ويأخذوا هذه الشهادات الورقية ليضعوها في سيرتهم الذاتية ليخففوا بعدها من دون رجعة فهذه فهم قد تحقق وهو سيرة ذاتية وعمل يحقق لهم غاية الأستهلاك الوقائي. ومن ناحية أخرى نجد بعض المؤسسات والحكومات العربية التي تنفق ملايين الدولارات لبناء مراكز أبحاث مجهزة بأفضل الوسائل العلمية لكي يبدوا أكتشاف أبحاثهم العلمية المزعومة ومن هنا أطرح سؤال في غاية الأهمية، ياترى من سوف يعمل في هذه المراكز وعلى أي المراجع سوف يعتمدوا؟ المراجع محلولة فلقد أتفقنا أن المراجع العربية شبه معدومة وسوف تكون المراجع الأنكليزية هي المكان الوحيد لهم وبالتالي سوف نستنتج شيء في غاية الأهمية وهو ضرورة وجود باحثين ومطورين يجيدون اللغة الانكليزية كلغة أم بينما الشخص الذي لايجيد اللغة الأنكليزية بطلاقة فمكانه عمل إداري ممل محصور في أربع جدران لأنه ببساطة ليس من الأقلية التي يمكنها أن تستفيد من هذه المراكز.

بالنسبة لي أعتبر هذا الشيء في غاية \*\*\*\* لأن التفكير الحقيقي الآن يجب أن ينصب في أستهداف الاكثريّة وهي التي تتحدث اللغة العربية لأن صعود درج العلم يجب أن يكون درجة درجة وليس عشر درجات فأنتم تحاولوا القفز إلى مراكز لن تصلوها أبدا لأنكم تستهدفوا الأقليات وهذه الاقليات مهما كان درجة ذكائها ومستواها العلمي سوف تبقى أقلية بينما تركتم الأكثرية لتجلس وتنتظر.....لذلك أنا أتوجه إليكم ومن خلال منبري الصغير هذا توقفوا عن دعم الأبحاث العلمية قليلا وفكروا في دعم المحتوى العلمي فهو البوابة التي وصلت لها جميع الأمم إلى ما هي عليه الآن وليس في صرف الملايين على أستيراد معدات نحتاج فيها فنيين من عندهم لكي نتعلم كيف نستخدمها!!! إلى متى هذا الأستهتار؟ وإلى متى سوف نبني دراسات فاشلة؟ وأستحلفكم بالله أليس صرف مبلغ عشرة ملايين دولار يمكن أن يحول المحتوى العربي من ثلاثة بالمئة إلى ثلاثين بالمئة في فترة أقل من عام؟!!!! أليس صرف مبلغ عشرة ملايين على دعم المناهج العلمية في الجامعات العربية سوف يخرج لنا آلاف الباحثين والمفكرين؟!...

أخي العزيز أختي العزيزة أتركوا سوء بناء الدراسات من قبل المؤسسات والحكومات العربية وساهموا في بناء عزة عالمنا العربي فنحن الاكثريّة ونحن من سوف يبني هذا التاريخ وحاولوا ان توجهوا تفكيركم نحو حلم عربي واحد وكبير وثقوا بأن شخص واحد يمكنه أن يغيرا العالم ويمكن ان يكون هذا الشخص هو أنت!... لكن إذا تعلمت كيف تستفيد من قدراتك ووقتك بشكل صحيح في صالح بناء محتوى عربي نورثه للأجيال التي من بعدنا وخصوصا أن عجلة العلم كل يوم تصعد مئات الدرجات ونحن مازلنا نحاول صعود الدرجة الأولى منها وهو بناء المحتوى..... ودمتم بود



هذا المقال هو الجزء الثاني من مقالة نشرت في  
المجلة في العدد قبل السابق (أى فى عدد يناير  
2011) بعنوان - الرخصة و طريقة إعدادها على  
أجهزة سيسكو - ، وتكملة لما بدأتها فى  
ملاحظة :

## الرخص وطريقة إعدادها على أجهزة سيسكو

أحمد الشحات

كل node تكون لها رخصة واحدة node license unit تأتي معها، وكما قلنا سابقا أن ال Node هو cucm ، أما  
كل جهاز فيكون له عدد ثابت من ال Licenses units تختلف باختلاف نوع الجهاز، وكما قلنا سابقا أن الجهاز 7970  
يحتاج 5 رخص و الجهاز 7961 يحتاج أربعة وهكذا.

Cucm يحتوى على starter license تأتي مع الجهاز الجديد التي يمكن إستخدامها للبدء فى عملية التحميل  
للبرنامج على Cucm . النظام يقوم بعملية الكتابة على ال starter licenses عندما نحصل على الرخصة  
الدائمة permanent license ونقوم برفعها لل cucm .

للحصول على الرخصة الدائمة permanent license نستخدم (Product Authorization Key) (PAK) الذي  
يأتي مع المنتج، ندخل (Product Authorization Key) (PAK) الذي تم الحصول عليه مع المنتج أو بواسطة  
التليفون فى License Registration web tool الموجود فى الرابط التالي  
<http://www.cisco.com/go/license>، ونضغط Submit  
ونتبع التعليمات.

و يجب أن ندخل ال MAC Address الخاص بال NIC ه Ethernet الخاص بأول node من cucm فى  
CLUSTER وعدد الأجهزة وعدد ال nodes أيضا، وأيضا ندخل عنوان البريد الإلكتروني لكي نتلقى الرخص عليه  
. Licenses

Workwide | Change | Logged in | Account | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

HOME Support

Product License Registration

Product License Registration

Enter a PAK Number Step 2 Validate Features Validate Features Step 3 Designate Licensee Designate Licensee Step 4 Finish and Submit Finish and Submit

Licenses Not Requiring a PAK

If you do not have a Product Authorization Key (PAK), please click [here for available licenses](#).

Available licenses include Evaluation/Demo Licenses, Cisco ASA 3DES/AES, PIX Firewall 3DES/AES and DES Encryption, Cisco Services for IPS, and Cisco Unified Communications Manager Version Upgrade licenses.

Product Authorization Key (PAK)

Enter the Product Authorization Key (PAK) below exactly as it appears on the label that accompanied the Cisco Information Packet.

Product Authorization Key (PAK): \*

Enter one value at a time including dashes.  
Example 1: 4XDD88V8888  
Example 2: UNTY-2X-SJ-000000X  
Example 3: CRS-3X-CO-000000X

Go Back SUBMIT

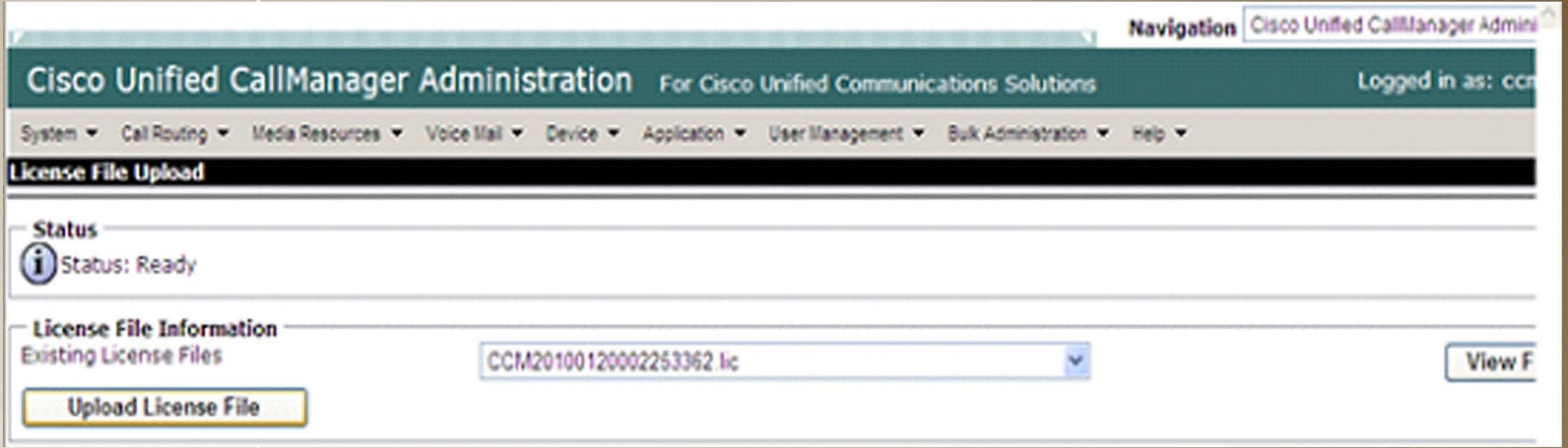
RMA License Transfer



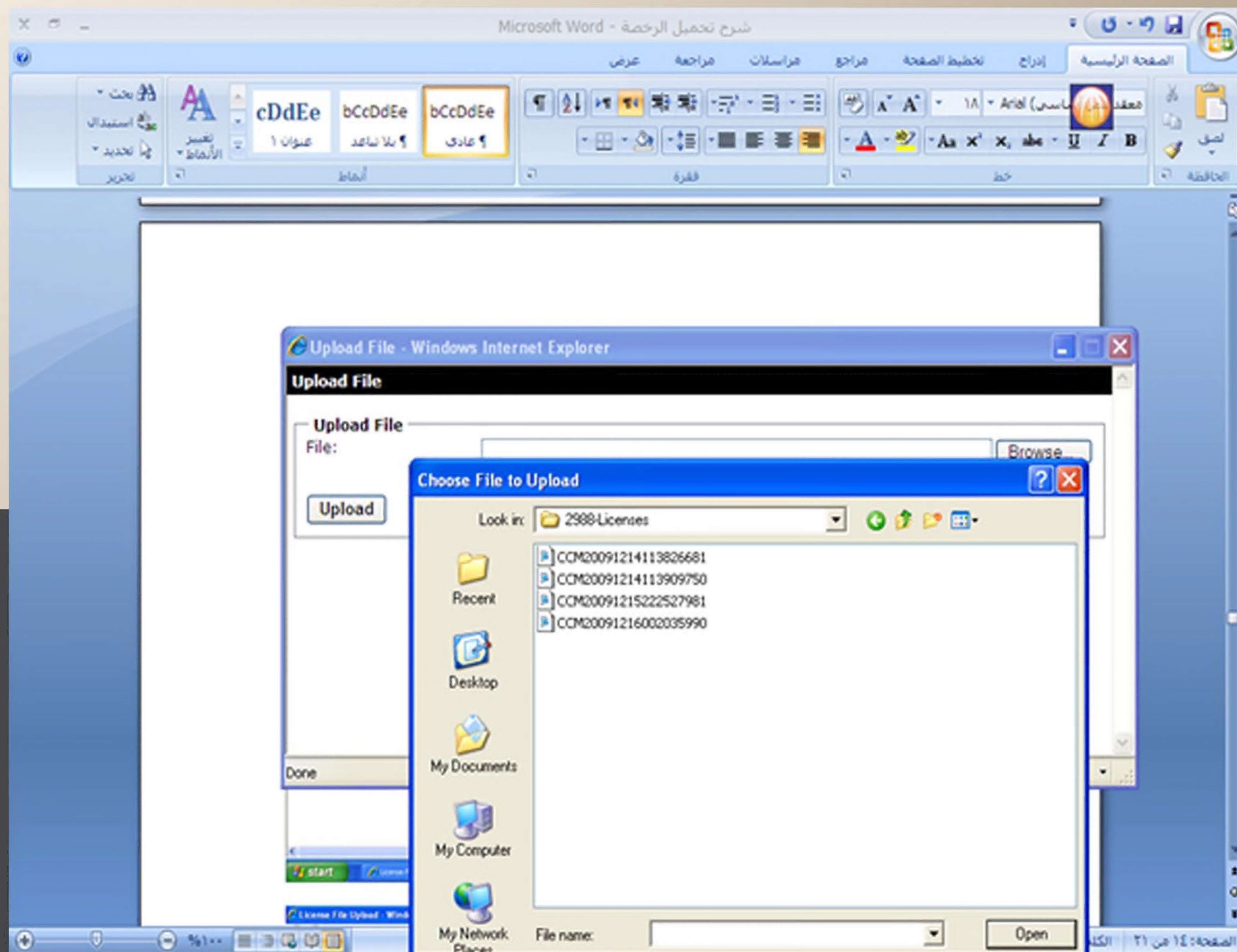
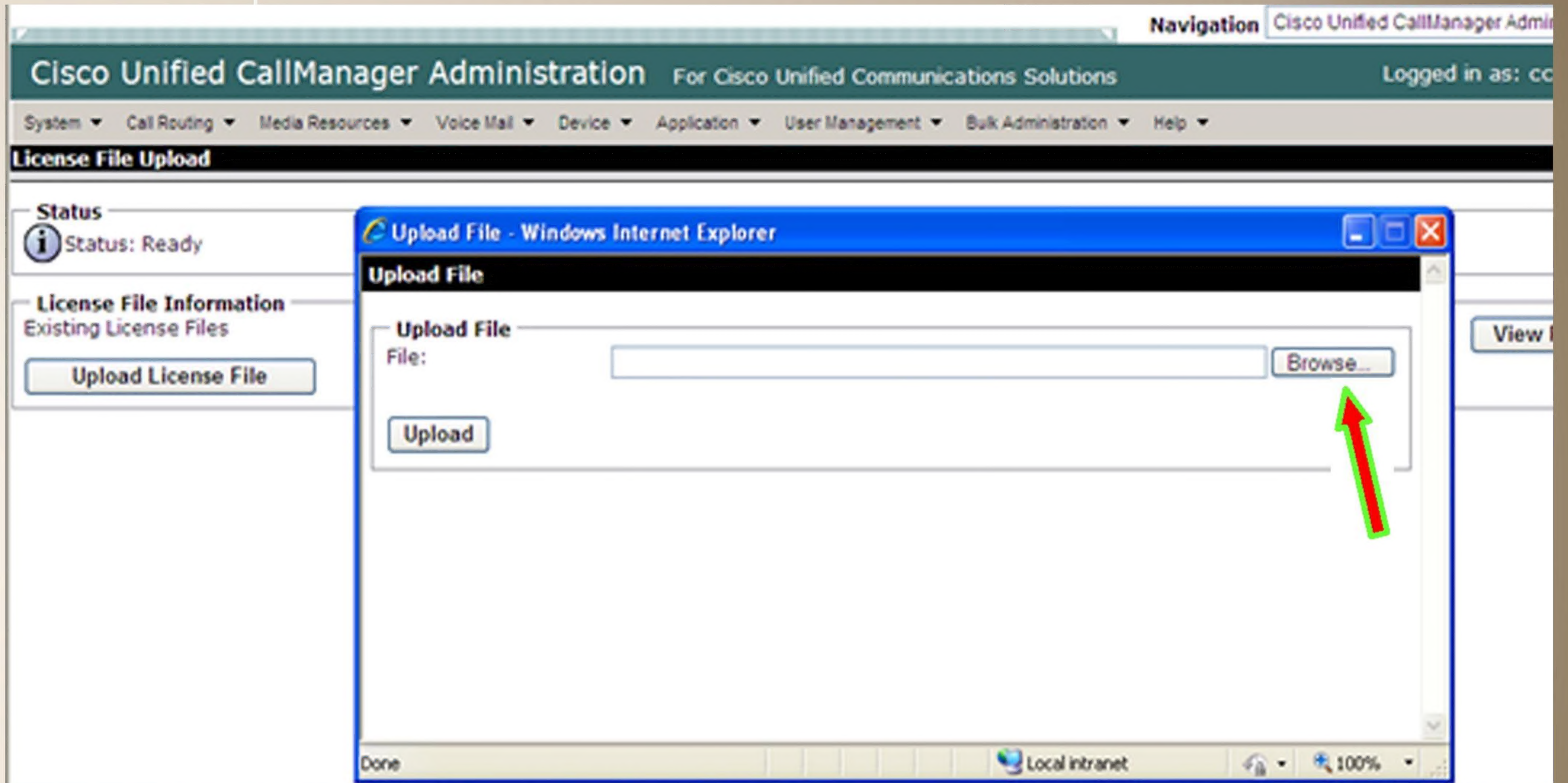




طبعاً License موجودة لأنني لن أقوم بحذفها من أجل التجربة، أما في الواقع ستجد هذا المربع فارغ و تضغط على Upload License file لتحميل الرخصة الجديدة.



ولرؤية محتويات الرخصة نضغط على View file، و لتنزيل رخصة جديدة نختار BROWS ثم نحدد المسار.



نحدد الرخصة المطلوبة ثم نختار Upload .



Navigation Cisco Unified CallManager Administration  
 Cisco Unified CallManager Administration For Cisco Unified Communications Solutions Logged in as: ccm  
 System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help  
**License File Upload**  
 Status  
 Status: Ready  
 License File Information  
 Existing License Files  
 Upload License File  
 CCM20100120002253362.lic  
 CCM20100120002253362.lic  
 CCM20100120002336862.lic  
 CCM20100120002409427.lic  
 CCM20100120002444155.lic  
 View File

بعد أن إنتهينا من تحميل الرخصة سنتكلم عن محتويات الرخصة، و فيما يلي محتويات الرخصة:

سأضع نموذج لرخصة CUCM ونموذج لرخصة IP PHONE

\*1 نموذج رخصة الـ NODE

\ INCREMENT CCM\_NODE cisco 6.1 permanent uncounted

VENDOR\_STRING = <Count>1</Count><OrigMacId>00215ABBFD92</OrigMacId>

\ <<LicFileVersion>1.0</LicFileVersion

\ HOSTID = 002655ad4de0

\ <NOTICE = "<LicFileID>20091214113826681</LicFileID><LicLineID>1</LicLineID

\ PAK>1156J5028D9</PAK>" SIGN = "0618 88F6 653B 8136 985E 503E>

\ A1A8 97BF 9FBD D196 2629 E598 C90B 9621 9F06 1357 2310 E040

"14D4 A29F C50B A5E7 6589 3D64 6668 4C8B 03CD 947C 0552 E2CD

\ INCREMENT SW\_FEATURE cisco 6.1 permanent uncounted

VENDOR\_STRING = <Count>1</Count><OrigMacId>00215ABBFD92</OrigMacId>

\ <<LicFileVersion>1.0</LicFileVersion

\ HOSTID = 002655ad4de0

\ <NOTICE = "<LicFileID>20091214113826681</LicFileID><LicLineID>2</LicLineID

\ PAK>1156J5028D9</PAK>" SIGN = "1DE2 CD17 6102 C277 341A 2A29>

\ 26B4 CB2F 14A1 57C6 4ABB C55D B19C 67F2 506D 0CF8 79DD 8D5B

"9F1F BDC6 D0F1 42BC 7BF2 70C1 E708 ABF2 9005A86B 66B2 53EF

معنى الجملة INCREMENT CCM\_NODE cisco 6.1 permanent uncounted انها رخصة غير منتهية

معنى الجملة VENDOR\_STRING = <Count>1 انها رخصة واحدة فقط، لجهاز واحد

معنى الجملة HOSTID = 002655ad4de0 هذا هو الـ MACADD



2\* شكل رخصة IP PHONE

INCREMENT PHONE\_UNIT cisco 6.0

\ permanent uncounted

VENDOR\_STRING = <Count>1000</Count><OrigMacId>000BCD4EE59D</OrigMacId>

<d

\ <LicFileVersion>1.0</LicFileVersion>

HOSTID = 000bcd4ee59d

NOTICE = "<LicFileID>20050826140539162</LicFileID><LicLineID>2

\ <LicLineID/>

\ PAK></PAK>" SIGN = "112D 17E4 A755 5EDC F616 0F2B B820 AA9C>

\ A36F B317 F359 1E08 5E15 E524 191566EA BC9F A82B CBC8 0313

"4CAF 2930 017F D594 3E44 EBA3 04CD 01BF 38BA BF1B

هذه رخصة ل 1000 تليفون

أتمنى أن أكون قد وفقت في توصيل المبادئ إليكم

والله ولي التوفيق



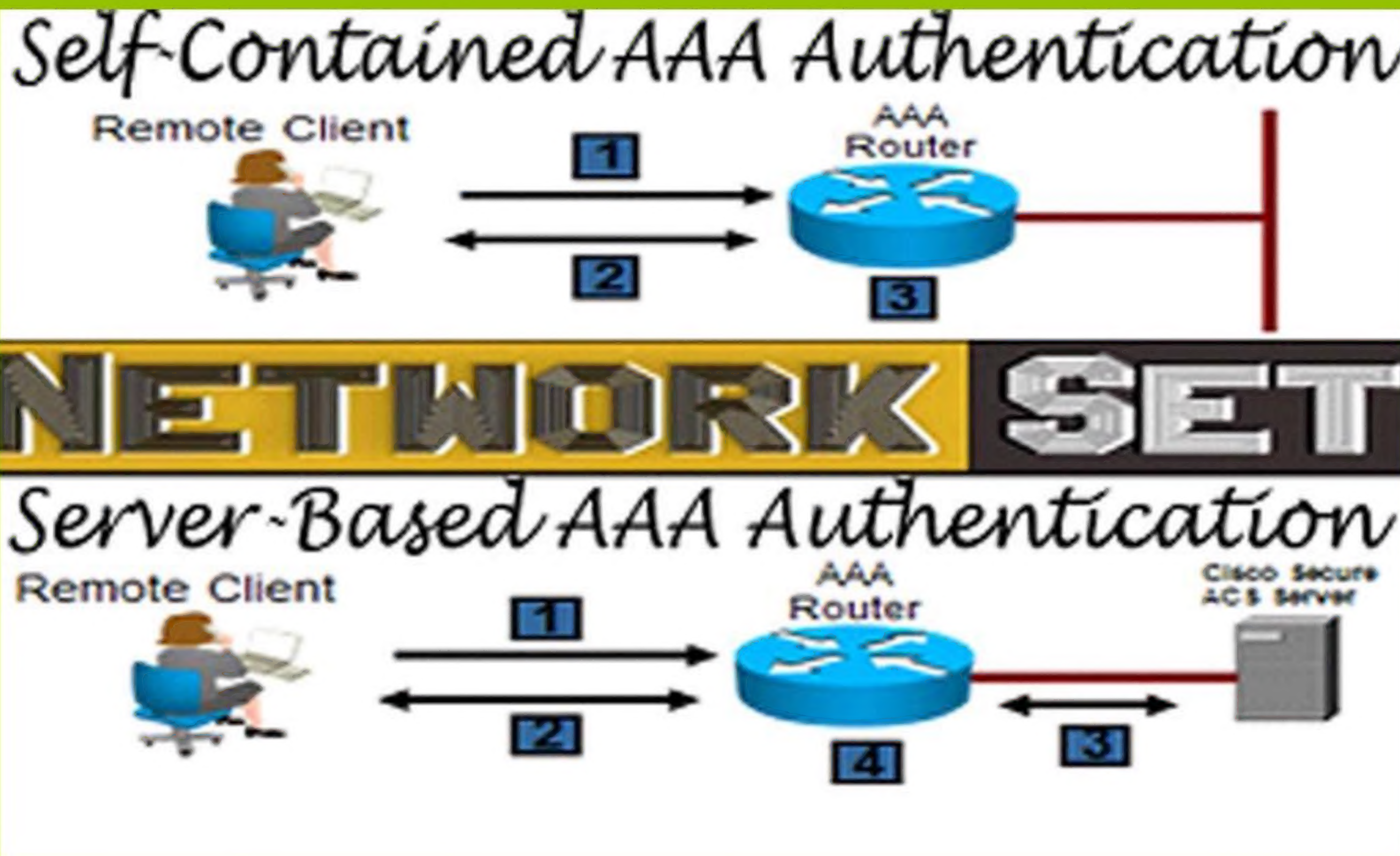


## Accounting

هي المرحلة الثالثة وهذه العملية تسجل الأفعال وما قام المستخدم أو المدير بعمله خلال استخدام الأجهزة أو الدخول على الشبكة كل حسب صلاحياته فهي تراقب المستخدم للشبكة وأيضا تسجل فترة دخوله ومعلومات أخرى تفيد في الحماية ومنها Security Audit والتي عن طريقها يتم معرفة الإختراقات في الشبكة وعلاجها، وهذه الخاصية مهمة جدا حيث تستخدم في عملية التفتيش عند إختراق الشبكة حيث يتم تتبع كل مستخدم وما قام بفعله خلال الفترة التي حدث بها الإختراق ومن ثم يتم معرفة الثغرة أو الشخص الذي قام بالإختراق.

لكن قبل التعمق في ال (AAA) هناك سؤال يتبادر إلى الأذهان، وهو لماذا إتجهنا إلى ال (AAA)؟ وما المرحلة التي سبقتها؟

الإجابة باختصار أنه قبل استخدام ال (AAA) تم الإعتماد على ال (Local Database) حيث يخزن على كل جهاز جميع المستخدمين وكلمات السر الخاصة بهم، ومع زيادة الأجهزة وكبر حجم الشبكات أصبح من الصعب الإعتماد على ال (Local Database) وتم التوجه إلى ال (AAA) حيث سيقوم سيرفر بإدارة هذه العملية.



## أنواع سيرفرات ال (AAA)

### • RADIUS

سنتحدث عنه بنظره عامة كبروتوكول ثم نظرة عن كثب كسيرفر

أهلا بالقراء الأعزاء وأسف لعدم كتابتي لمقالات خلال الفترة الماضية نظرا لإمتحاناتي، وللظروف التي مرت بها مصر الحبيبة حفظها الله وحفظ كل البلدان العربية وحدة واحدة وأمة واحدة.

## موضوع ال AAA

هي عملية هامة جدا في عملية الحماية للشبكات حيث أنها توفر ثلاث مزايا غاية في الروعة لحماية الشبكات وهذه المزايا الثلاث هي المكونة لإختصار ال AAA أو Triple A .  
Authentication, Authorization, and Accounting

## Authentication

هي المرحلة الأولى حيث أنها العملية التي يتم من خلالها إثبات أن المستخدم أو المدير هو الشخص الصحيح أو المفترض به

أن يكون. والغرض من هذه العملية هي التأكد من عدم دخول أشخاص غير مسموح لهم بالدخول وتتم هذه العملية باستخدام أوراق الإعتماد (Credentials). وتشبيها لهذه العملية هي شرطة المطار حيث تسمح بالدخول حسب أوراق الإعتماد وتمنع الأشخاص الضارين وأمثلة أوراق الإعتماد كثيرة منها: (Passwords, one-time tokens, digital certificates).

## Authorization

هي المرحلة الثانية حيث أن كل مستخدم مسموح له بالدخول يمتلك صلاحيات محددة لا يستطيع أن يتعداها و يقوم بالتعامل مع الأجهزة من خلال هذه الصلاحيات فتحدد الأماكن التي يمكن الدخول عليها وصلاحيات التعامل مع البيانات، ومثال لها المنظومة العسكرية حيث كل رتبة لها الصلاحيات المحددة لها.



ولن أتطرق إلى عمليات ال (Authentication) و (Accounting) و (Roaming) فقد تم التحدث عنها بشكل أعمق في عدد سابق، فالهدف من هذا المقال الحديث بشكل عام على ال (AAA).

## • TACACS

هذا إختصار ل Terminal Access Controller Access-control System ((TACACS

هذا السيرفر من نوع (Remote Access Server (RAS)) ليحدد إذا كان المستخدم له حق الدخول على الشبكة أو لا، فقد قدم (TACACS) في البداية يستخدم أى من (TCP) أو (UDP). ثم قامت شركة سيسكو بتطويره فقدمت عام 1990 (Extended TACACS (XTACACS)).

وقد أتاح ال (TACACS) السماح للمستخدم (Client) عن طريق الباسورد و إرسال ال (Query) إلى (TACACS Server)، وقد إستبدلته (CISCO) ب (+TACACS) المستخدم حاليا بكثرة والمكافئ لل (RADIUS) ولكنه و على العكس منه يستخدم (TCP) و (UDP).

وهذه مقارنة بين (TACACS+ & RADIUS)

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client.
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis.	Has no option to authorize router commands on a per-user or per-group basis
Confidentiality	Limited	Extensive

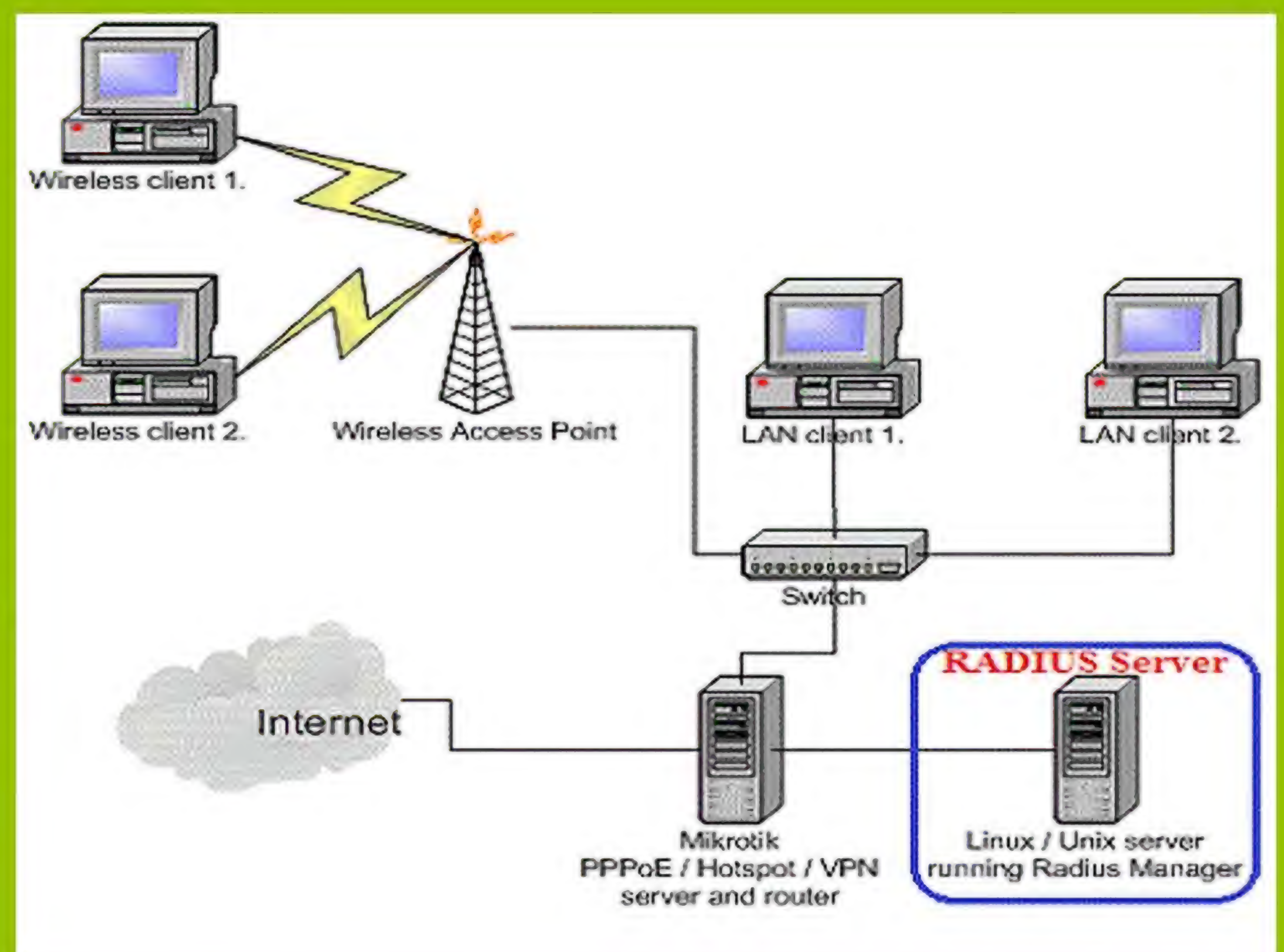
AAA using SDM (Security Device Manager) برنامج ((SDM)) و هو خاص بسيسكو وله مزايا عديدة منها الخاصية الأكثر من رائعة (Security Edit)، ومنها أيضا تطبيق ال (AAA) بكل سهولة.

هذا البروتوكول قد تم تطويره بواسطة شركة ليفينغستون (Livingston Enterprises Inc.) وأصبح بعد ذلك (One of IETF Standards). وبسبب طبيعة تكوينه الواسع، ظهرت له إستخدامات جديدة وعديدة منها الإنترنت، والشبكات الداخلية، واللاسلكية، وخدمات الإيميلات المتكاملة. ولكثرة أنواع الشبكات التي يتعامل معها ظهرت في إستخداماته قاعدة كبيرة من الأجهزة والخدمات منها Modems, DSL, Access points, VPNs, Network ports, Web servers

يعتمد هذا البروتوكول في تكوينه على (Client/Server) من الطبقة السابعة (Application Layer) بإستخدام ال (UDP Transport Layer) ولذلك يستوجب ذلك وجود كل من: RADIUS client component

RADIUS server

(RADIUS) وهي إختصار ل Remote Authentication Dial in User Service (Linux, UNIX, Windows NT) غالبا يعمل كسيرفر في بيئة الأنظمة ويتم الإتصال بين جميع المستخدمين أو ال (Clients) مع ال (Remote Access Server (RAS) وهو ال (RADIUS Server) للسماح لهم بالدخول للشبكة.





Select Configure > Additional Tasks > Router Access > User Accounts/View

2. Click Add

3. Enter username and password

4. Choose 15

5. Check the box and select a view

6. Click OK

وهذه قائمة بأنواعه ومزاياه

Cisco Secure ACS

	<p><b>Cisco Secure ACS for Windows</b> can be installed on:</p> <ul style="list-style-type: none"> <li>- Windows 2000 Server with Service Pack 4</li> <li>- Windows 2000 Advanced Server with Service Pack 4</li> <li>- Windows Server 2003 Standard Edition</li> <li>- Windows Server 2003 Enterprise Edition</li> </ul>
	<p><b>Cisco Secure ACS Solution Engine</b></p> <ul style="list-style-type: none"> <li>- A highly scalable dedicated platform that serves as a high-performance ACS</li> <li>- 1RU, rack-mountable</li> <li>- Preinstalled with a security-hardened Windows software, Cisco Secure ACS software</li> <li>- Support for more than 350 users</li> </ul>
	<p><b>Cisco Secure ACS Express 5.0</b></p> <ul style="list-style-type: none"> <li>- Entry-level ACS with simplified feature set</li> <li>- Support for up to 50 AAA device and up to 350 unique user ID logins in a 24-hour period</li> </ul>

Cisco Secure Access Control System



إختصار لـ (Access Control System):

هو أحد منتجات سيسكو قد يكون عبارة عن سوفت وير يعمل على أنظمة تشغيل مختلفة أو هاردوير قائم بذاته يوفر تحكم وإدارة للدخول لموارد الشبكة مع المجموعات المتنوعة من الأجهزة ومجموعات المستخدمين، وطرق أخرى للدخول عن بعد لفرض الحماية الكافية للشبكة، ويقلل من الـ VPN، ويسمح بالتحكم عن بعد، ويتيح التعامل مع جهود الإدارة والتحكم على مديري الشبكات.

TACACS+ & RADIUS ويستقبل البيانات من بروتوكولين مختلفين هما:

- (Easy-to-use) ويزود دخول سهل بواسطة troubleshooting يوفر مراقبة تامة للشبكة وتقارير عنها.

- وأيضا (Web-based GUI)

لا أعتقد أنه يسعني الوقت لذكرها قد أتمكن من عرضها في (AAA) وهناك تطبيقات وخفايا كثيرة يمكن تطبيقها على موضوعات قادمة بإذن الله وأتمنى أن أكون قد وفقت في عرض الموضوع بنظرة شاملة تمكن القارئ من معرفة (AAA) وأيضا لا أود أن أطيل عليكم حتى لا يشعر القارئ بالملل.



# AUTO-SECURE

ميزة من سيسكو تضعك  
مع محترفي الأمن والحماية

أيمن النعيمي



قد يتطلب منك حماية روتر على الشبكة بشكل جيد القيام بتنفيذ أكثر من أمر وهذا يشمل تفعيل وتعطيل بعض الخدمات الموجودة على الروتر من أجل رفع مستوى الأمن على الروتر وطبعا هذا يتطلب خبرة جيدة مع نظام التشغيل وأوامره، لذا قامت سيسكو بأضافة ميزة لهذا الأمر ويتم تفعيلها من خلال أمر يقوم بتنفيذ كل خيارات الأمن المتاحة على أجهزتها وهو الأمر Auto secure

فمنذ الإصدار 12.3 تم أضافة ميزة لأجهزة سيسكو تسمح لرفع مستوى الأمن والحماية على أجهزتها وبسرعة كبيرة جدا ومن خلال أمر واحد تقوم بكتابته في الـ Privileged Mode وبعد هذا الأمر مدعوم في عدة أجهزة ومن بينها الأجهزة التالية 800, 1700, 2600, 3600, 3700, 7200, 7500 ومن ناحية أخرى

أتاحت سيسكو هذا الأمر من أجل الأشخاص المبتدئين في مجال سيسكو ولاتوجد لديهم خبرة في التعامل مع أجهزتها ومع نظام التشغيل IOS الخاص بها وذلك من خلال عمل Dialog بسيط يسألك فيه بعض الأسئلة أي أن الأمر شبيه بالـ initial configuration dialog الذي نراه عند تشغيلنا للروتر أول مرة لكن هنا الأسئلة سوف تكون متعلقة بالأمن والحماية فقط لذا لنشاهد بعض الأمثلة الواقعية وقبل أن أبدا لنكتب الأمر ونضع بعدها إشارة أستفهام لكي نرى ماهي إمكانيات هذا الأمر وماهي الـ Plan المتاحة :

Cisco's IOS

```
Router#auto secure ?
forwarding   Secure Forwarding Plane
full         Interactive full session of AutoSecure
login        AutoSecure Login
management   Secure Management Plane
no-interact   Non-interactive session of AutoSecure
ntp          AutoSecure NTP
ssh          AutoSecure SSH
tcp-intercept AutoSecure TCP Intercept
<<cr
```



وكما يتضح لكم هناك ثمانية خطط أو Plans ولكن Plan هناك شرح بسيط عنها يحدد نوعية الأسئلة التي سوف يتم سؤالك عنها ولو لم تختار أي واحد منها وقمت بكتابة الأمر فقط فسوف يتم تفعيل خيار ال Full كخيار Default لا AutoSecure لتأخذ هذا المثال البسيط وهو خاص بي ال Login ولنشاهد الأسئلة المطروحة :

## Cisco's IOS

```
Router>en
Router#auto secure login
— AutoSecure Configuration —
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]: no
Enable secret is either not configured or
is the same as enable password
Enter the new enable secret*****:
Confirm the enable secret***** :
Enter the new enable password*****
Confirm the enable password*****:
Enter the username: networkset
Enter the password*****:
Confirm the password*****:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters
Blocking Period when Login Attack detected: 200
Maximum Login failures with the device: 3
Maximum time period for crossing the failed login attempts: 180
!
end
Apply this configuration to running-config? [yes]: yes
Applying the config generated to running-config
#Router
```

كما تشاهدون معي أن السؤال الأول كان حول معرفة هل هذا الروتر متصل مع الأنترنت أم لا وقد أجابت بلا ولو أجبت بنعم كان طلب مني تحديد أي المنافذ متصل مع الأنترنت وبعدها تم سؤالني حول كلمات السر واسم المستخدم الخاص فيني وعدد مرات التي سوف أسمح فيها بتسجيل خاطئ لكلمة السر والفترة الزمنية التي سوف أسمح فيها بكتابة كلمة السر مرة رابعة والخ.... وطبعا آخر سؤال سوف يكون حول إضافة هذه الأوامر وتطبيقها على الروتر.

وطبعا نفس الشيء لو تم اختيار خطة أخرى فلو مثلا اخترنا خيار ال Full فسوف تكون الأسئلة مختلفة بعض الشيء ومن بينها وضع ال Banner واسم المستخدم وكلمة السر واسم الدومين والخ.....

كلمة لآخيرة هناك أمر مشابه لهذا الأمر لكن مع ال Voice وهو خاص بي ال QoS.



هل إنتهي عصر الـ SDM؟

وهل إحتل الـ CCP عرش الـ GUI كلية؟

وهل بدأت سيسكو عهداً جديداً في التضييق علي برامج المحاكاة؟

هذا وغيره من الأسئلة ما سنتناوله في هذه المقالة بإذن الله.

توقفت سيسكو عن تحديث برنامج الـ SDM (Cisco Security Device Manager) منذ عام 2008، وتوقف البرنامج عند الإصدار V2.5. ثم في عام 2010 أصدرت سيسكو النسخة الأولى من برنامج Cisco Configuration Professional أو إختصاراً CCP.

البرنامج لا يختلف كثيراً عن الـ SDM في واجهته الرسومية، ولكن عملية الـ Configuration أصبحت أفضل وأكثر مرونة، ولكنه يختلف عن الـ SDM في الآتي:

**\* متطلبات التشغيل أصبحت أكبر من الـ SDM وهذه يمكن تلخيصها في الآتي:**

System Component	Requirement
Processor	2 GHz processor or faster
Random Access Memory	1 GB DRAM minimum; 2 GB recommended
Hard disk available memory	400 MB
Operating System	Any of the following: <ul style="list-style-type: none"> <li>• Microsoft Windows 7-32 and 64 bit</li> <li>• Microsoft Windows Vista Business Edition</li> <li>• Microsoft Windows Vista Ultimate Edition</li> <li>• Microsoft Windows XP with Service Pack 3-32 bit</li> <li>• Mac OSX 10.5.6 running Windows XP using VMWare 2.0</li> </ul>
Browser	Internet Explorer 6.0 or above
Screen Resolution	1024 X 768
Java Runtime Environment	JRE versions 1.6.0_11 up to 1.6.0_21 supported
Adobe Flash Player	Version 10.0 or later, with Debug set to "No"

أنا مازلنا نحتاج إلي الـ SDM لعمل الإعدادات Configurations اللازمة لبعض الموديلات، وأن الـ CCP لم يتربع كلية على عرش الـ GUI Configuration.

**\*3 وعن الاختلافات أيضاً، أن البرنامج يأتي في صورتين:**

أ\* نسخة Express وهي نسخة صغيرة الحجم للتسطيب علي الروتر.

ب\* نسخة Professional وهي النسخة التي يتم تسطيها علي الـ PC.

علي عكس الـ SDM، حيث كانت النسخة الواحدة يمكن تسطيها علي الروتر والـ PC معاً.

وكما نلاحظ أن قدرة الـ Processor والـ RAM زادت، وهذا أيضاً يزيد تبعاً لنسخة الـ CCP. كما نلاحظ أن سيسكو لا تدعم باقي أنظمة التشغيل مثل الـ LINUX فالبرنامج بنسخته موجود في صورة EXE وهو ما لا تدعمه باقي أنظمة التشغيل، كما نلاحظ أيضاً أن البرنامج ذاته عبارة عن صفحة ويب لا تعمل إلا على الـ Internet Explorer فقط دون باقي المتصفحات.

**\* النقطة الأهم أن البرنامج أصبح لا يدعم كثير من الأجهزة التي كان يدعمها الـ SDM.**

فهو لا يدعم أغلب الأجهزة التي يدعمها برنامج المحاكاة GNS3، اللهم إلا نسخة 7200، وهذا يجيب على التساؤلات التي طرحناها في البداية،



\*3 نتأكد من أن الروتر قادر على الإتصال بال NIC عن طريق عمل PING

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.1.30

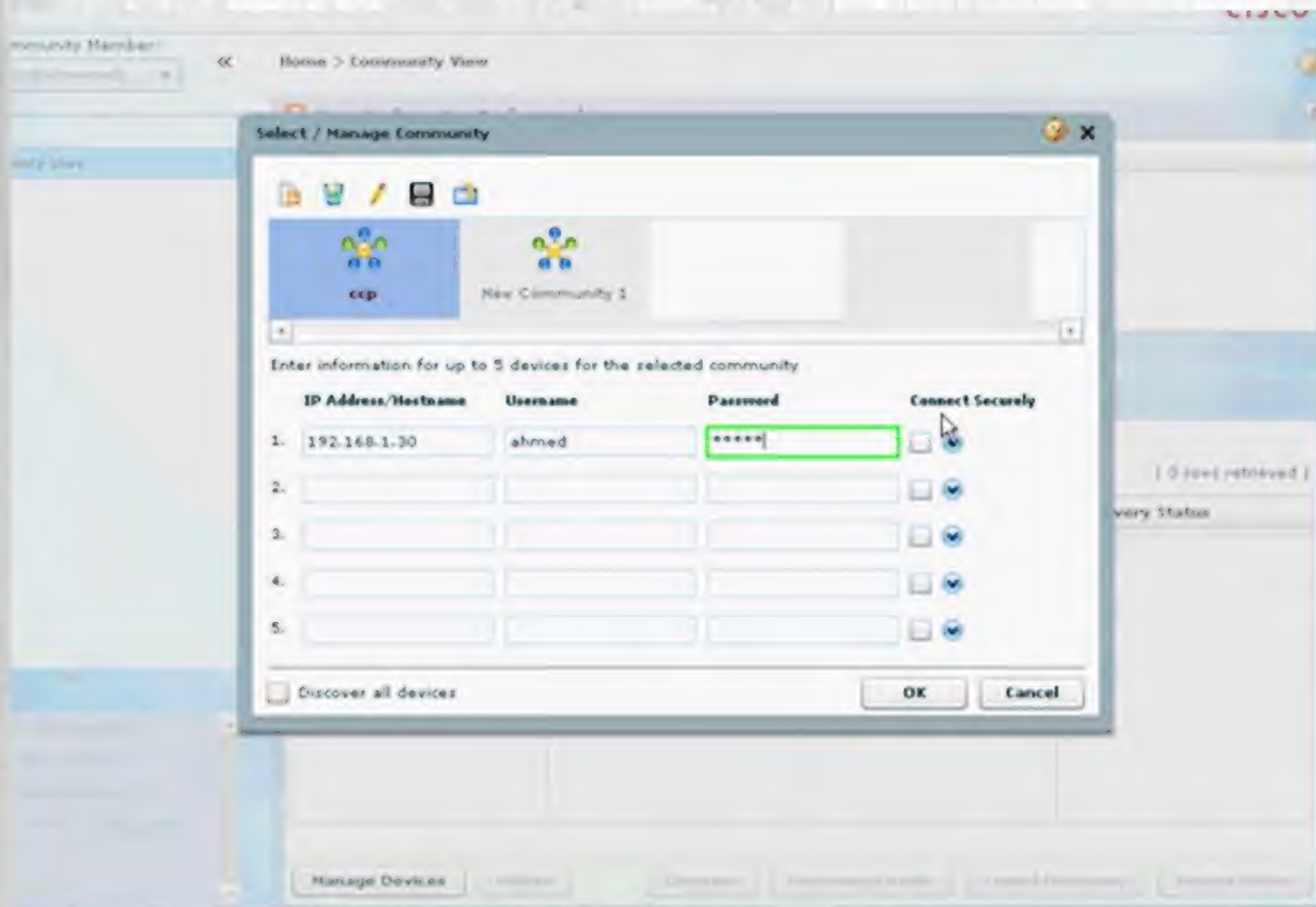
Pinging 192.168.1.30 with 32 bytes of data:

Reply from 192.168.1.30: bytes=32 time=84ms TTL=255
Reply from 192.168.1.30: bytes=32 time=31ms TTL=255
Reply from 192.168.1.30: bytes=32 time=37ms TTL=255
Reply from 192.168.1.30: bytes=32 time=38ms TTL=255

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 84ms, Average = 47ms

C:\Documents and Settings\Administrator>
```

\*4 نقوم بفتح ال CCP وإدخال عنوان الروتر وإسم المستخدم وكلمة السر:

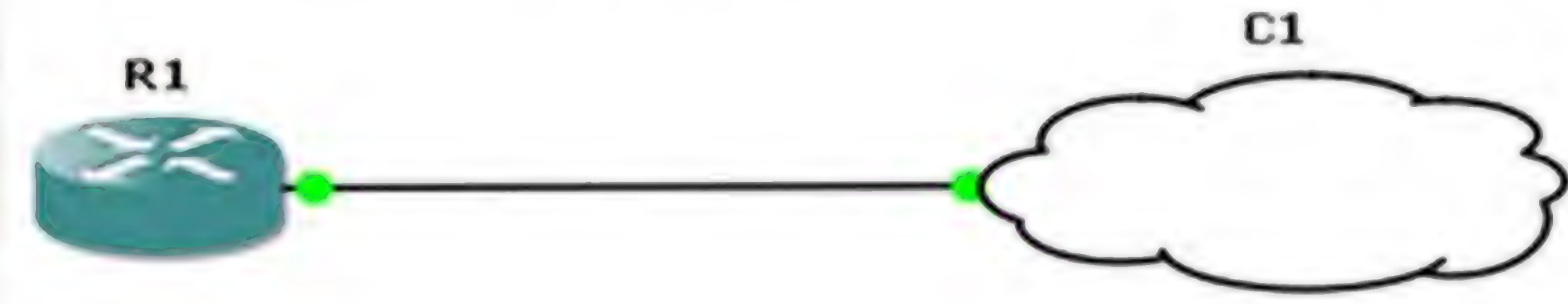


ثم نضغط على Discover ليبدأ البرنامج في إستكشاف الروتر وتجهيزه للعمل. وفي الختام أسأل الله عز وجل أن ينفعني وإياكم بهذا العلم.

\*4 يوفر البرنامج أيضاً نسخة Demo. وهي نسخة تجريبية تعطيك الحرية للتدريب علي البرنامج في بيئة محاكاة، بدون التطبيق علي ال Production Network تفادياً لحدوث أي مشاكل.

ونأتي للغرض الأساسي من هذا المقال وهو كيفية تطبيق البرنامج علي ال GNS3، ولندع الصور تتكلم:

\*1 نقوم بتوصيل الروتر مع الجهاز عن طريق عمل Loopback، أو عن طريق التوصيل مباشرة مع كارت ال NIC



\*2 إعداد الروتر كالاتي:

```
R1#conf t
R1(config)#inter f00/
R1(config-if)#ip add 192.168.1.30
255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip http server
R1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Mar 11 01:50:57.423: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Mar 11 01:50:58.743:
%PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save new certificate
R1(config)#ip http authentication local
R1(config)#user ahmedprivillige 15 secret cisco
R1(config)#username ahmed privilege 15 secret cisco
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#login local
R1(config-line)#transport input all
```





# CLEAROS

## عبد الجليل الوكيل

سأبدأ حديثي عن أحد البرامج أو الأنظمة المفتوحة المصدر المبنية على Linux. و بدأ هذا النظام تقريبا منذ عام 2000م، و بدأ إنتشاره بشكل واسع. و كان في بدايته يسمى ClarkConnect، و تم تغيير هذا الإسم في منتصف عام 2009م إلى ClearOS. و يعتبر هذا النظام أحد الأنظمة أو كأحد أفضل التوزيعات على Linux، و قد صمم هذا النظام لإدارة الشبكات و خصيصا ليكون ك Gateway للشبكة لقوة تحمله و لكونه يتمتع بقائمة واسعة من الخدمات و المميزات بالإضافة إلى واجهة رسومية لسهولة الإعدادات GUI.

أولا أحب أن أشكر الله سبحانه و تعالى، ثم أشكر المجلة و أخص المهندس أيمن النعيمي لإتاحة الفرصة لي للكتابة بهذه المجلة الرائعة التي بدأ إنتشارها في أوساط المنتديات و المدونات العربية بفضل الله سبحانه و تعالى.

و بما أن هذا أول مقال لي في هذه المجلة أحببت أن أبدأ بموضوع يعتبر من المواضيع المهمة و المناسبة لمختلف بيئات العمل سواءً في ال Small, Medium, Enterprise أو حتى في الشبكات المنزلية.

## أنواع أنظمة ClearOS

تم تقسيم الأنظمة في ال ClearOS إلى:

Software: وهو عبارة عن ال Operating System الخاص بال ClearOS و يمكن تثبيته على أي جهاز شخصي بمواصفات معينة و ذلك بناء على عدد المستخدمين، و الجدول أدناه يبين متطلبات الجهاز لتثبيت النظام:

RAM and CPU	5 users	5-10 users	10-50 users	50-200 users
Processor/CPU	500 MHz	1 GHz	2 GHz	3 GHz
Memory/RAM	512 MB	1 GB	1.5 GB	2 GB
<b>Hard Disk</b>				
Hard Disk	Installation and logs require 1 GB - optional storage is up to you			
RAID	Recommended for mission critical systems			

و تم إصدار ال ClearOS Operating System من Version و ذلك بناء على بيئة العمل و متطلبات العمل. و الجدول أدناه يبين هذه الإصدارات و سعر كل إصدار، والفروق بين هذه الإصدارات

	Free	Good	Better	Best
				
Subscription Type	ClearOS Basic	ClearOS Basic Plus	ClearOS Standard	Premium Enterprise
Recommended Environment	Small	Small	Medium	Enterprise Unlimited
Number of Users	Unlimited	Unlimited	Unlimited	Unlimited
ClearOS Version	5.x	5.x	5.x	5.x
Dynamic DNS	✓	✓	✓	✓
ClearCenter Marketplace Access*	✓	✓	✓	✓
ClearOS Remote Configuration Backup	✓	✓	✓	✓
ClearSDN Services Access*	✓	✓	✓	✓
Dedicated SDN Servers	-	✓	✓	✓
ClearBOX Hardware Access*	-	✓	✓	✓
ClearCARE Support Access*	-	✓	✓	✓
ClearOS Verified Security Updates	-	✓	✓	✓
ClearOS Verified Software Updates	-	-	✓	✓
ClearOS Quality Assurance	-	-	✓	✓
Dynamic VPN	-	-	✓	✓
30-Day Basic Installation Support	-	-	✓	✓
Priority Bug Resolution	-	-	-	✓
Continual Performance Optimization	-	-	-	✓
ClearOS Central Management	-	-	-	✓
Q2-2011				
Priced From/Year	\$0	\$60	\$80	\$160





clearBOX™

ClearBOX Hardware

	Free	Good	Better	Best
CPU	Use	Intel Celeron 440, 2.0GHz	Intel Pentium E5300, 2.6GHz	Intel Core2Duo E8400, 3.0GHz
Memory	Your Own	1GB (1 x 1GB)	2GB (1 x 2GB)	4GB (2 x 2GB)
Hard Drive	Hardware	500GB: 1 x 500GB SATA @ 7200-rpm, LFF	500GB: 2 x 500GB SATA @ 7200-rpm, SFF, SW Raid	160GB: 2 x 160GB SSD, SW Raid
Warranty		2 year	3 year	5 year
Priced From	\$0	\$1199	\$1549	\$2799

و تم إصدار ال ClearOS Operating System بأكثر من Version و ذلك بناء على بيئة العمل و متطلبات العمل. و الجدول على اليسار يبين هذه الإصدارات و سعر كل إصدار، والفروق بين هذه الاصدارات و بعد مشاهدة النوعين من منتجات Clear، راح نتعمق أكثر في معرفة أهم مميزات ال Software لأنه مناسب تقريبا في أغلب بيئات العمل لخصه و لإحتوائه على أغلب متطلبات ال Security

## مميزات النظام ( ClearOS Software ):

و نظام التشغيل من ClearOS عبارة عن دمج مجموعة كبيرة من البرامج المهمة في إدارة الشبكات غير الخدمات الأساسية. و راح نبدأ بشي من التفصيل لأهم المميزات لهذا النظام:

• Domain Name System DNS: أي بمعنى بإمكانك وضع ال ClearOS كـ DNS سيرفر الخاص بشبكتك في حال كان لديك Domain.

• Domain Controller DC: بإمكانك عمل مجال أو Domain خاص بشبكتك بدلا عن استخدام Windows (و هذه الميزات من المميزات الجميلة في هذا البرنامج)، و بكل المميزات التي توجد في Windows Domain مثل ال Group Policy و ال ADS و غيرها من مميزات ال Windows Domain.

• Stateful Firewall: ويعتبر من أقوى أنظمة الجدار الناري لأنه عبارة عن Packet Filtering و يراقب تدفق البيانات من ال Source إلى ال Destination بخلاف ال Stateless Firewall الذي يعتبر بسيطا جداً مثل Windows Firewall.

• Load Balancing: و هو عمل موازنة أو استخدام أكثر من مزود خدمة لموازنة استخدام الإنترنت، فبإمكانك استخدام إلى ستة مزودين خدمة (و هذا غير موجود في أي إصدار من إصدارات ال ISA أو ال TMG). على سبيل المثال لدي خطين دي إس إل، الأول 2 ميجا والثاني 4 ميجا، وأريد الفئة الذين يستخدمون التصفح وفتح الإيميل أن يستخدموا الخط ال 2 ميجا، أما الذين يستخدمون التحميل والداونلود أن يستخدموا الخط ال 4 ميجا.

• VPN: الشبكات الافتراضية و التي تمكنك من الولوج أو دخول شبكتك الخاصة من أي مكان عن طريق الإنترنت Virtual Privet Network.

• Bandwidth Management: و هذه ميزة أخرى تفتقر لها منتجات مايكروسوفت مثل ال ISA أو ال TMG.

• Demilitarized Zone DMZ: وهو السيرفر أو مجموعة السيرفرات التي يتم وضعها خارج الشبكة الداخلية ليتمكن المستخدم من الدخول عليها من الإنترنت دون استخدام صلاحيات الشبكة المحلية مثل ال Username أو ال Password الخاص بالشبكة المحلية.

• Mail Server: و هذه ميزة أخرى، و هي تمكنك من استخدام ال ClearOS كـ Mail Server بدلا من استخدامك ال Exchange Server و هذا يفيدك في تقليص التكاليف التي تدفع سنويا لميكروسوفت كـ License سواءاً لـ Exchange Server نفسه أو للكلابنت CAL.



## إعدادات و تحميل البرنامج:

بالضغط على الرابط التالي ISO يمكنك تحميل ملف الـ  
<http://download.clearfoundation.com/clearos/enterprise/5.2/iso/clearos-enterprise-5.2-service-pack-1.iso>

(حجمه 700 ميغا ) و طبعا هناك إصدارين 5,1 و 5,2 و يفضل تحميل الإصدار الأخير لإحتواؤه بعض المميزات الجديدة عن الإصدار القديم و الرابط الموجود في الشرح للإصدار الجديد.

طبعا هناك طريقتين لإقلاع البرنامج أو الـ Booting :

\*1 عن طريق الـ CD : و يتم بعمل عمل حرق أو burn لملف الـ ISO على الـ CD.

\*2 الثانية عن طريق Bootable USB : و يمكنك تحميل البرنامج بالضغط على الرابط التالي:

<http://download.clearfoundation.com/clearos/enterprise/5.2/images/diskboot.img>  
( لعمل الـ Bootable USB )

و تثبيت البرنامج سهل جداً، و يمكنكم مشاهدة الفيديو الخاص بكيفية تثبيت البرنامج من الرابط التالي:

<http://jalooo.wordpress.com/201124/02//>  
مجاني-تشغيل-نظام-clear-os

و من الأشياء الجميلة التي قدمتها الشركة المنتجة لهذا البرنامج هو عمل Online Demo لمعرفة مميزات البرنامج و الخدمات التي يشملها البرنامج و يمكنك مشاهدة الـ Demo بالضغط على الرابط التالي:

<https://demo1.clearos.com:81/admin/users.php>

إسم المستخدم هو get و كلمة المرور هي clear .

و لمزيد من المعلومات يمكنك الإطلاع على البرنامج من الموقع الرسمي

<http://www.clearfoundation.com>

• Built in Antivirus

• IDS and IPS: و قد تم شرح هذين النظامين في

عدد سابق للمجلة ( عدد نوفمبر )

• Publishing: يمكنك عمل نشر لموقعك أو

سيرفرائك الخاصة عن طريق الـ publishing من خلال

نظام الـ ClearOS.

• و غيرها الكثير من الخدمات الأساسية مثل الـ FTP

Server, DFS Server, Print Server and Built in

MySQL.

• بالإضافة إلى الريبورتات التي يمكن الحصول عليها

من النظام مثل:

Network Status

Network Traffic

Web proxy report

Resource Reports

و غيرها من الريبورتات التي يمكن الحصول عليها من

الـ ClearOS .

## متطلبات و كيفية إعداد الـ Operating System

متطلبات النظام هو كما أسلفنا سابقا بالجدول المبين أعلاه و المتطلبات بناء على بيئة العمل و عدد المستخدمين و يفضل عمل الـ RAID لحماية و تأمين السيرفر من الأعطال المفاجئة و عمل الـ Backup.

و بخصوص كرت الشبكة أو الـ NIC ، فيفضل تركيب كرتين شبكة إذا تم إستخدامه كـ Gateway ، أو كرت شبكة واحد في حال إستخدام الجهاز كـ Web Cashing.

و الـ System يتضمن تعريفات لجميع أنواع كروت الشبكة، ماعدا الـ Wireless NIC فيفضل إستخدام كرت شبكة عادي Fast or Giga Ethernet ، و أيضا إمكانية عمل إعدادات الـ PPOE بمعنى عمل إعدادات الـ DSL من البرنامج نفسه بدلا من إستخدام المودم.

و أود التنويه أن هناك بعض الـ Services تحتاج إلى معالج قوي و ذاكرة إضافية مثل:

• Intrusion Detection and Prevention

• Content Filtering

• Webmail

• Antispam

• Antivirus



The logo for Echo Technology features the letters 'E', 'C', 'H', 'O' in a large, bold, yellow, stylized font. Above the letter 'H', there are three vertical yellow bars of varying heights, resembling a bar chart or a signal waveform.

# **Echo Technology**

**Integratoin Technical Solution**

**Network - Web Design**

**Training & Development**

**Programing - Design & Printing**

**Electronic System - Control System**

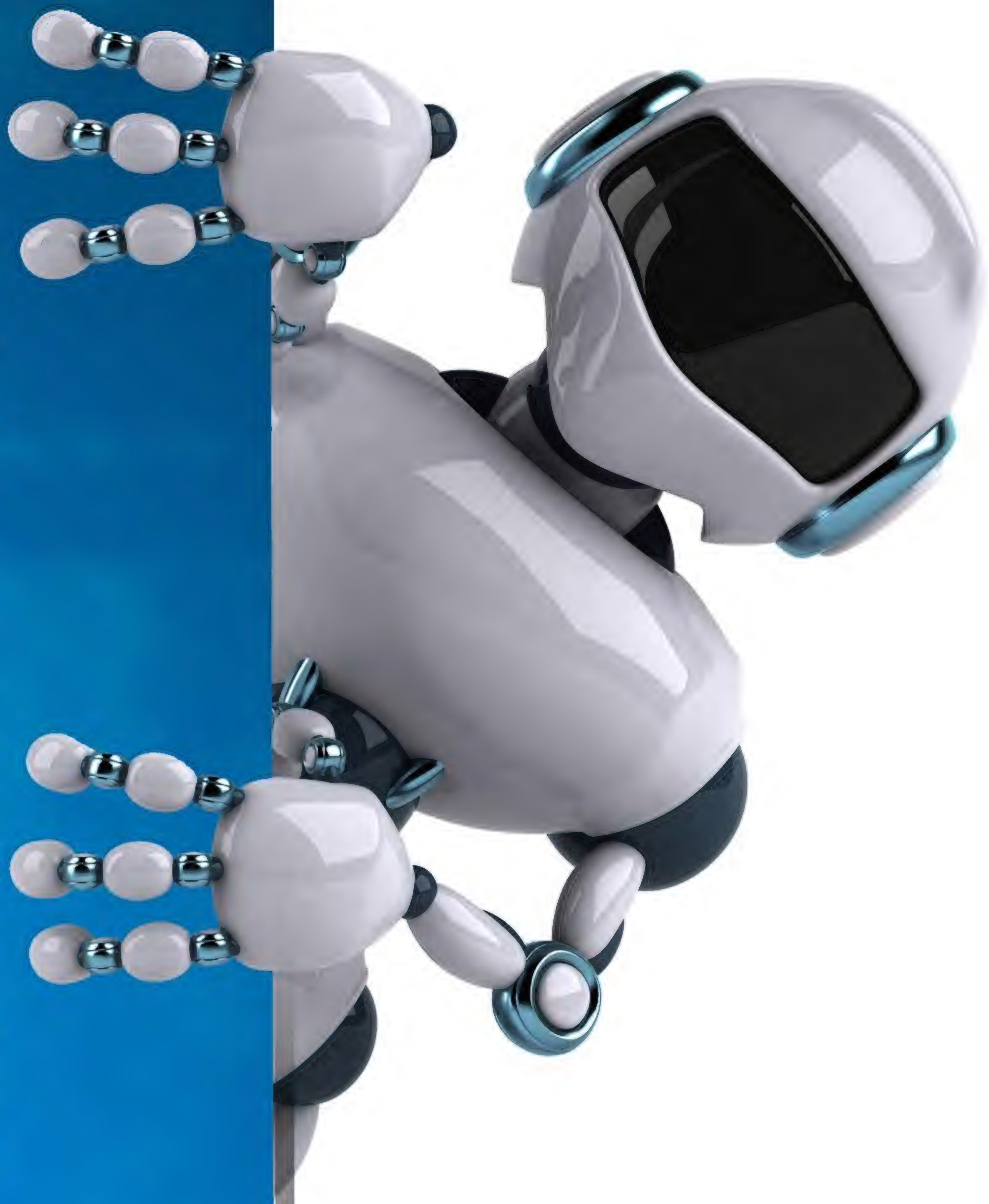
**Whole Technical  
One Supplire**

**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)**





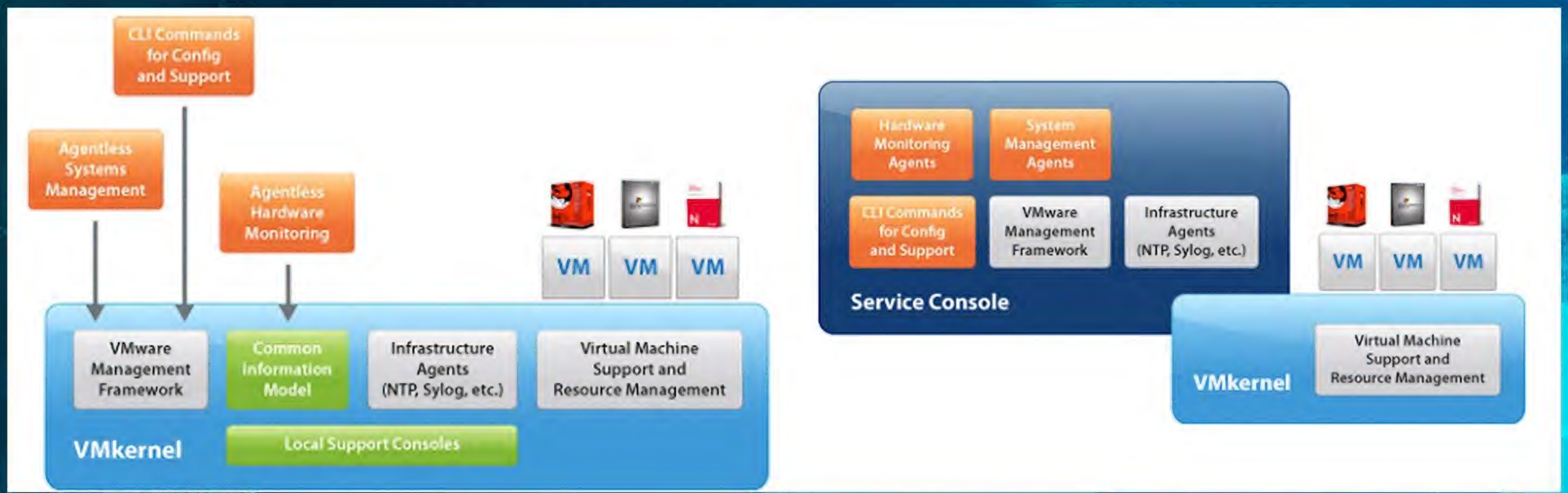
# الفرق بين الـ ESX و الـ ESXi

## الحلقة الثانية من تقنية VIRTUALIZATION مع الـ VMWARE

عبد الرحمن بن داود

كنا قد تكلمنا في الموضوع السابق عن أنواع الـ Virtualization والتي هي نوعين:  
\*1 Bare-Metal  
\*2 Host-Based  
وقلنا أن النوع الأول (أي الـ Bare Metal) هو الذي يهمنا في سلسلة شروحاتنا لمنتجات VMWare، لأنه الحل المخصص للشركات ذات أنظمة المعلومات الضخمة (حيث تكثر فيها السيرفرات).  
تعرض VMWare منتجين أساسيين تحت مظلة الـ Bare-Metal وهما الـ ESX و الـ ESXi أو ما أصبح يعرف اليوم بالـ vSphere.  
فما الفرق بينهما؟ وأي واحد يختاره المسؤول عن نظام المعلومات؟ وأي منهما يمثل الحل الأنسب لشركتي؟ هذا ما سنجيب عنه في هذا الموضوع المختصر.  
يعتبر الـ ESX الحل القديم والأكثر متانة إذا ما قورن بالـ ESXi الذي أثبت خفته وأمنه العالي، ولكن إذا لاحظنا التطور الحاصل فإننا سنجزم بأن أيامه معدودة، وهذا ما صرحت به شركة VMWare، فنهاية 2011 ستكون نهاية الـ ESX و لذلك تعمدت الشركة إصدار النسختين معا لمدة تزيد عن السنتين حتى يتسنى للشركات ترقية الـ ESX إلى ESXi أي عمل (upgrade).  
يمكن إحصاء الكثير من الاختلافات بين الإصدارين إلا أنه يمكن حصرها فيما يلي علما بأن أغلبها تقنية :  
1 <sup>مصدره نسبي</sup> أول اختلاف بينهما وهو الاختلاف الأساسي : يكمن في الهندسة أو التصميم. فالـ ESX يعتمد على ما يسمى بالـ Service console وهي عبارة عن نظام تشغيل افتراضي (Virtual Machine) RedHat، يتم تسطيه تلقائيا مع عملية التنصيب الأولية للـ ESX ويتم من خلاله التعامل مع الـ VMKernel (الذي يربط بين الـ Hardware و الـ VMs) وإدارته و التحكم فيه.  
تستعمل أيضا الـ SC للربط بين الـ VMKernel والتطبيقات (البرامج) التي توفرها شركات أخرى وبالخصوص برامج المراقبة (Monitoring) والحماية (Security).  
أما على مستوى الـ ESXi فقد تم حذف الـ SC ولذلك يلاحظ فرق كبير بينهما من حيث سرعة التحميل (Loading)، و إستعمال أقل للهاردوير (Performance).  
و إليكما مخططان يسهلان فهم الفرق بين الإشتغال بوجود الـ SC (Service Console) و في غيابها:





إلا أنه يمكن التعامل مع ال ESXi في البداية من خلال واجهة تمكنا من تعيين كلمة السر لل root و كذلك المعلومات المبدئية للشبكة كال ip address و ال default gateway و ال DNS ، و هي ما يسمى بال Direct Console User Interface (DCUI) وهذه صورة توضح شكلها.



لو قارنا حجم القرص الذي يشغله ال ESXi لوجدنا أنه على الأقل يأخذ 2GB (لوجود ال SC على هيئة Virtual Machine لا تظهر)، أما ال ESXi فيتطلب 32Mb وهذا ما يسهل عملية تنصيبه (SD flash or USB key تكفي). هناك طريقة وحيدة لتنصيب و إقلاع ال ESXi وهي عن طريق ال CD/DVD أو باستعمال الإقلاع عن طريق شبكة تخزين مركزية (SAN). أما ال ESXi فزيادة على ذلك يمكن أن يشتري شبه منصب في الهاردوير باستعمال رقائف فلاش وهذا يتم على مستوى الشركات المتعاقدة مع VMware مثل DELL وهو ما يسمى بال EMBEDDED وما يسهل هذه العملية هو صغر الحجم الذي يستهلكه ال ESXi مقارنة بال ESX.

يتميز ال ESXi بسرعة الإقلاع وإستغلال جيد للهاردوير مقارنة بال ESX فمثلا ال SC يمكنها أن تصل إلى 800Mb إستهلاك من ال RAM، في حين أن هذا تم اجتنابه مع ال ESXi.

بما أن ال ESXi يحتوي على إصدار (RedHat(SC updates and patches الخاصة فقط بال VMKernel، بل يبحث عن تحديثات وتصحيحات ال Service Console أيضا، أما ال ESXi فيختزل كل هذا في ال VMKernel فقط.

كل هذا يساعد على ضمان الإستقرار للنظام لأنه معلوم أن مع كل تحديث أو تصحيح يجب إعادة تشغيل النظام، فال ESXi يضمن إستقرار أفضل من ال ESX.



يعتبر ال ESXi أمن من ال ESX، لأن معظم البورتات و الخدمات موقفة تلقائيا، عكس الثاني الذي يتتيم عليه فتح بعض البورتات للتوفيق بين عمل ال VMKernel و ال SC. أما بخصوص إدارة ال ESXi فهو يفتقر لل Console التي إعتاد مستخدمو ال ESX إدارته من خلالها ولذلك يمكن حصر إدارة المنتجين كما يلي:

### ESX Management :

- \* vCenter Server.
- \* vSphere Client.
- \* Built-in Web Service.
- \* CLI (SSH) to Console.

### ESXi Management :

- \* vCenter Server (for licenced ESXi)
  - \* vSphere Client (for free ESXi)
  - \* vCLI and PowerCLI vMA (remote execution of scripts and commands من أجل إصدار أوامر عن بعد)
- إعلم أخي أنه يمكنك إستعمال ال ESXi بدون مقابل، و هذا غير موجود مع ال ESX مع محدودية طبعاً، و من جملة ذلك أن ال vCLI و ال PowerCLI سيكون read only علماً أنه لا يمكن استخدام ال SNMP ، و لا يمكن إستخدام عدد كبير من الخواص التي تميز VMware عن باقي المنتجين و الجدول الآتي يوضح ما أنا بصدد قوله:

	ESXi – Free License (ESX not available without VI)	VI Foundation (with ESX or ESXi)	VI Standard (with ESX or ESXi)	VI Enterprise (with ESX or ESXi)
Core hypervisor functionality	Yes	Yes	Yes	Yes
Virtual SMP	Yes	Yes	Yes	Yes
VMFS	Yes	Yes	Yes	Yes
VirtualCenter Agent		Yes	Yes	Yes
Update Manager		Yes	Yes	Yes
Consolidated Backup		Yes	Yes	Yes
High Availability			Yes	Yes
VMotion				Yes
Storage VMotion				Yes
DRS				Yes
DPM				Yes

هناك إختلاف أيضا في الصيانة فال ESX تتم صيانتها عن طريق ال SC أما ال ESXi فعن طريق ال PowerCLI أو ال vCLI أما الصيانة المتقدمة فتتم بواسطة Tech Support Mode الذي يمكن الدخول عليه بطريقتين:

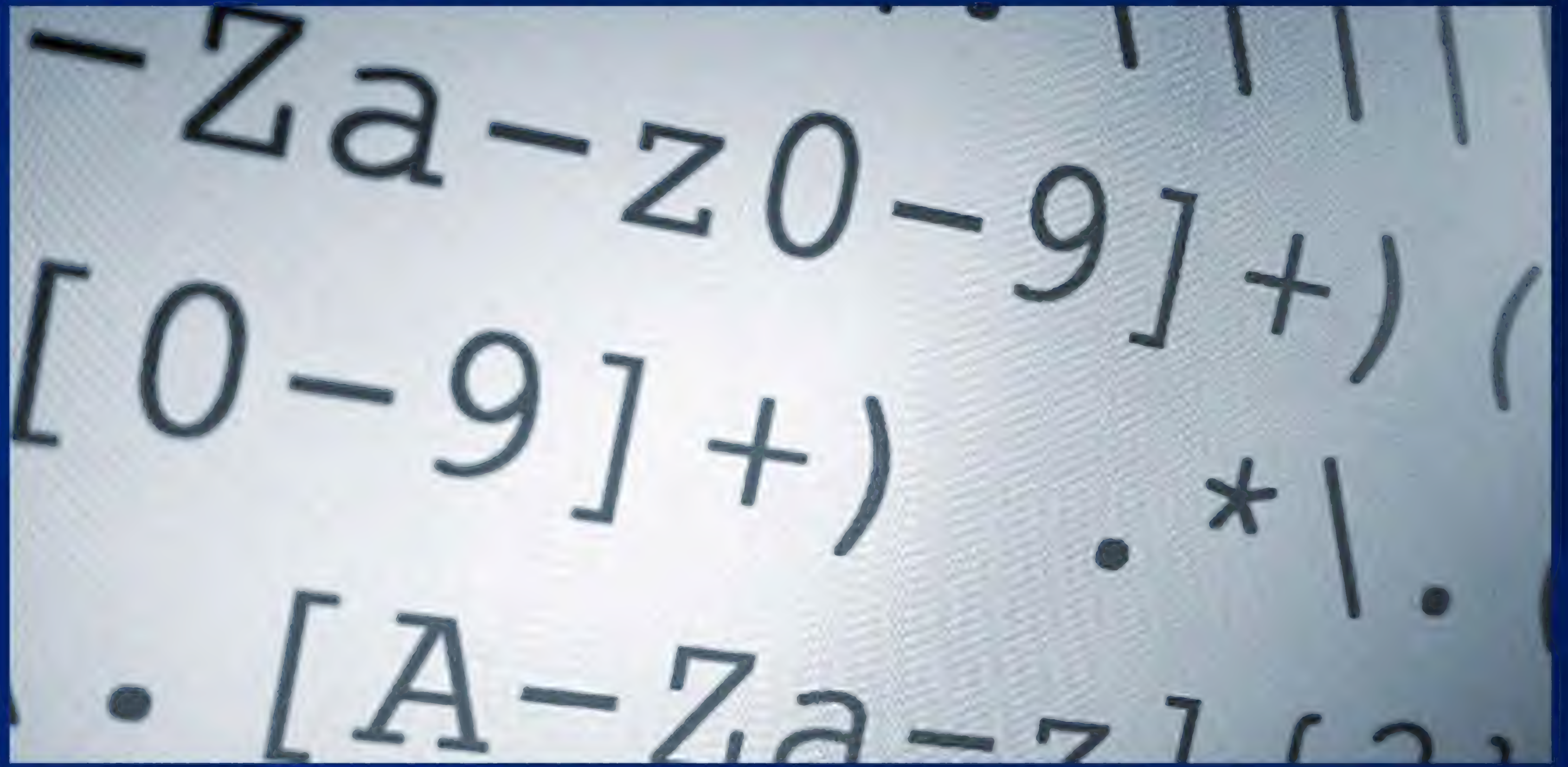
- \* إما الدخول على الواجهة المباشرة المتاحة تلقائيا DCUI
- \* أو ال SSH

تنبيه: هنا تجدر الإشارة أنه يتم الدخول على الواجهة DCUI التي تتعامل مباشرة مع ال VMKernel من دون وجود وسيط كما في حالة ال ESX و هو SC. و في الأخير أود أن أخص ما سبق ذكره، و التنويه بأن أكبر فرق بين الإصدارين هو ال Service Console، و هذا الذي يجب تذكره. أما باقي الفروق فتبقى سطحية و لا يتسع المجال لذكرها كلها لأن الهدف من هذا الموضوع هو إعطاء نبذة عن ال ESX و ال ESXi. أما فيما يتعلق بالإختبار بينهما فالأولى بالمهتم بهذه التقنية مراجعة متطلبات نظامه، فإن كان يعتمد على تطبيقات و برامج سيتم إدماجها مع ال VMware فالأفضل إستعمال ال ESX كاملاً، أما من أراد الحصول على تقنية ال virtualization و كفى فليستعمل ال ESXi الذي يعتبر أرخص من الناحية المادية و أسرع و أمن من سابقه.



# Regular Expression (REGEX)

## ودورها في تأمين الشبكة



تعريف ال Regular Expression :

تبسيطا لفكره ال Regular Expression سأستعين

بمثال بسيط لشرح الفكرة:

مثال 1: <sup>بدر</sup>بدرنا لدينا شبكة يوجد بها FTP server غايه في الأهميه، وتأميننا له وضعناه خلف جهاز IPS sensor ليقوم بفحص ال Traffic المرسله إليه، في أحد الأيام تم إكتشاف ثغره تستهدف ال FTP servers، الآن يجب علينا أن نقوم بتأمين ال server لدينا، ولكن كيف؟؟ Cisco لم تطرح بعد أي signature تقوم بكشف الهجوم، إذن لا يوجد أماننا الآن إلا تصميم signature لهذا الهجوم.

أولا قمنا بعمل بحث حول هذا الهجوم ووجدنا الأتي - هذا الهجوم يحتوى على هذه ال string التي تقوم بتنفيذ شيء خبيث في ال server ولتكن هذه الكلمه هي ATTACK، الآن قمنا بعمل ال configuration اللازم لل IPS ليقوم بكشف الهجوم والذي يتعرف عليه عن طريق البحث داخل ال packet عن الكلمه ATTACK، ولكن هل هذا كافي؟

تابعوا معي لتعرفوا أن ال HACKER الذكي لايعتمد على طريقة واحدة في تنفيذ هجوم ما، بل يقوم بتغيير طريقته ليتفادى الكشف، فإذا قام مخترق بمحاوله تنفيذ هجوم على ال FTP server الذي تتولى عمليه تأمينه الآن، و تفاعاً هذا المخترق بأن الهجوم لم ينجح، لذلك فسوف يفكر في طريقه لخداع جهاز ال IPS الذي يؤمن شبكتنا، فمن الممكن أن يقوم هذا الشخص بتعديل بسيط في الهجوم وهو كالأتي، فبدلاً من أن يحتوى الهجوم على كلمه ATTACK قام بتغييرهذه ال string إلى ATTacK، مجرد تغيير حرفين من

مقدمة :

إستكمالا للموضوع السابق حول أجهزة ال IPS & IDS & تطرقت إلى موضوع ال regular expression هذا ولكن لم أتكلم عنه بالتفصيل، مما دفعني إلى تخصيص مقال لهذا الموضوع، فالكثير لايعلم شيء حول هذا الموضوع بالرغم من أن له بعض التطبيقات في أجهزة Cisco المختلفه سواء كانت IPS & IDS OR ASA firewall OR Router، وإن كان يستخدم كثيرا جدا في البرمجيه ومن لديه خلفيه برمجيه سيجد الموضوع بسيط جدا.

CASE إلى LOWER-CASE ولكن النتيجة قد لا تسرنا، أولا عندما مر هذا الهجوم على ال ips قام هذا الأخير بعرضه على مجموعه من ال signatures التي تقوم بفحص البيانات ومن بينها ال sig التي قمنا بتصميمها، عندما بدأت هذه ال sig فحص الهجوم لم تكتشفه لأنها تعتمد على شكل واحد للكلمة ATTACK الموجودة في الهجوم للتعرف عليه، والآن هذا الهجوم تجاوز ال IPS، ووصل إلى ال server ونجح في تنفيذ أعمال تخريبية في ال server.

الآن ما الحل لمثل هذه المشكله؟ أسمع من يقول بذكاء "بسيطة يمكننا أن نقوم بعمل sig أخرى لتقوم بمنع أي packet تحتوى على أي string من الأتي ATTACK أو ATTack أو ATTack أو attack أو attack إلخ ... ممتاز ولكن ماهي الطريقة التي نستطيع بها تحديد أي شكل ما لهذه الكلمه؟ غير معقول طبعاً أن نصمم signature واحده لكل شكل من هذه الكلمه، فمثلاً sig 1 تقوم بكشف attack و sig 2 تقوم بكشف ATTack إلخ ...

طبعاً هذا مستحيل لأنه في الهجوم الحقيقي لن تكون مجرد كلمه من ستة أحرف فقط! هنا يأتي دور Regular Expression لتساعدنا في تحديد هذه الكلمه بأي شكل لها، فال Regular Expression عبارة عن notational language أو لغة ترميزية تساعدنا لعمل وصف ال text pattern، فمثلاً لنقوم بعمل وصف للكلمة ATTACK بكل أشكالها بمساعده ال regular expression سنفعل الأتي "(Aa)(Tt)(Aa)(Cc)(Kk)" هل رأيتم السهوله التي إستطعنا بها عمل match للكلمه بكل أشكالها



الآن نضع هذا النص "(Aa)(Tt)(Aa)(Cc)(Kk)" في ال signature وستقوم ال signature بمنع أي packet تحتوي على أي شكل من هذه الكلمة.

تستخدم ال regular expression مجموعة من الرموز تسمى Metacharacters تعطى مرونة لوصف أي نص نريده ، فمثلا إستخدمنا هذه الاقواس ( ) وهي تدل على كلمة attack بجميع أشكالها عن طريق إستخدام حرف واحد من كل قوس، نأخذ مثال آخر لنفهم اكثر

نريد ال regular expression التي تمثل الكلمتين hacker أو Hacker الحل هو (Hh)acker  
 نريد ال regular expression التي تمثل الكلمتين hacker أو Hacker الحل هو (Hh)ack(Ee)r  
 نريد ال regular expression التي تمثل الكلمتين hat أو hot الحل هو h(oa)t  
 أعتقد أن الأمر أصبح واضحا الآن ، ولكن هناك رموز أخرى كثيرة تساعدنا في هذه العملية تعالوا نتعرف على أهمها

## ال Regular Expression Metacharacters :

Symbol	Meaning
?	Repeat 0 or 1 times
*	Repeat 0 or more times
+	Repeat 1 or more times
{x}	Repeat exactly X times
.	Any one character except \n or \t
[abc]	Any character listed
[^abc]	Any character not listed
[a-z]	Any character listed inclusively in range
()	Used to limit the scope of other metacharacters
^	The position at the start of the line
\char	Literal character match, including metacharacters
char	Matches character literally, not including metacharacters
	OR of two regular expressions
\n	Line feed
\t	Tab

### علامة الإستفهام ؟

تعنى هذه العلامة إحتمايه وجود الحرف الذي يسبقها أو قد لا يوجد

مثال - he?llo تقوم بعمل match لـ hello أو hlllo

مثال - pl?ay تقوم بعمل match لـ play أو pay

### النجمه \* asterisk

تعنى إحتمايه تكرار الحرف الذي يسبقها أكثر من مرة أو قد لا يوجد نهائيا

مثال - lo?se تقوم بعمل match لـ lse أو lose أو loose أو loose أو loose أو إلخ ...

### علامة +

تعنى إحتمايه تكرار الحرف الذي يسبقها أكثر من مرة أو

على الأقل وجوده مرة واحدة

مثال - lo+se تقوم بعمل match لـ lose أو loose أو loose أو looooooose أو إلخ .. (لاتقوم بعمل match لـ lse لأنها تشترط وجود الحرف مرة واحدة على الأقل)

### زوج الاقواس {}

يستخدم هذا النوع لتحديد عدد تكرار حرف معين، وذلك بإدخال رقم داخله ، وهذا الرقم يشير إلى عدد مرات التكرار للحرف الذي يسبق القوس

مثال - l{3}ose تقوم بعمل match لـ lllose

### زوج الاقواس ()

يقوم بتجميع عدد من الأحرف بداخله ليتم معاملتهم كأنهم حرف واحد فقط



مثال -  $\{4\}(xyz)$  تقوم بعمل match ل xyzxyzxyzxyz (تم معاملتها داخل الأقواس كأنه كيان واحد) **النقطة .**

تشير النقطة إلى أنه من الممكن أن يكون مكانها أى حرف فيتم تجاهل أى شيء مكانها  
مثال <sup>بزر</sup> h.t تقوم بعمل match ل hat أو hot أو hit أو إلخ ...

## زوج الاقواس [ ]

تحديد عدد من الخيارات المتوقعه بداخله

مثال - (Aa) تقوم بعمل match ل A أو a

مثال - (Hh)(Ee)(Ll)(Ll)(Oo) تقوم بعمل match لكلمه hello بجميع حالاتها سواء كانت capital or small

## العلامة ^

مع زوج الاقواس ( ) - تساوى هذه العلامة كلمه NOT

مثال - (^abc) تقوم بعمل match لأى حرف غير a أو b أو c

## العلامة ^ منفردة

تستخدم إذا أردنا عمل match لجمله أو أى text يبدأ بكلمه معينه

مثال - ^hello تقوم بعمل match لأى سطر يبدأ بكلمه hello مثل hello sherif أو hello ali أو hello إلخ ....

## علامة \$

تستخدم إذا أردنا عمل match لجمله أو أى نص ينتهى بكلمة معينه

مثال - xyz\$ تقوم بعمل match لأى سطر ينتهى ب xyz مثل aaaaaxyz أو ggggxyz إلخ ..  
الشرطة " - "

تقوم بتحديد range معين

مثال - بدلا من كتابة (abcdef) يمكننا كتابه <sup>بزر</sup> (a-f)

تقوم بعمل match لأى حرف فى هذا ال range

مثال <sup>بزر</sup> (9) <sup>بزر</sup> (1) تقوم بعمل match لأى رقم فى

هذا ال range

## علامة |

هذه العلامة تساوى كلمة OR

مثال - (sherif)|(magdy) تقوم بعمل match

لكلمة sherif أو magdy (لاحظ استخدام الأقواس)  
مثال - (G-Z)|(a-f) تقوم بعمل match لأى حرف small من a إلى f أو حرف capital من G إلى Z (لاحظ الفرق بين هذا النوع من الأقواس والنوع السابق)

## العلامة \

هذه لها مدلول مختلف فهى تسمى "escape character"، حتى أستطيع شرح هذه العلامة تابعوا هذا المثال

مثال - نريد أن تقوم بعمل match ل IP address معين لنفترض مثلا 192.168.10.10، المشكله هنا هو أن هذا string يحتوى على علامة مميزة بالنسبه لل REG EXP وهى النقطة

لذلك لكى نزيل معنى هذه النقطة ونجعلها مثل أى حرف أخر نفعّل الأتى 192\168\10\10 حيث قامت ال \ بجعل النقطة مثل أى حرف أخر، ويمكننا استخدام هذه العلامة مع أى metacharacter أخرى لعمل match لأى نص يحتوى على أحد هذه العلامات.

## مثال مفصل :

الآن سأقوم بشرح REGEX تقوم بعمل match لأى E-mail للتحكم بمدخلات المستخدم

<sup>بزر</sup> 9a+(Nn)(Ee)(Tt)(Ww)(Oo)(-A-Z0)(Rr)(Ss)(Ee)(Tt)\.(com)|(net  
نبدأ بالجزء الأول من ال REGEX  
+ (\_9a-z-A-Z0)

الأقواس من النوع ( ) تخبرنا أنه يمكن إختيار أى شيء من داخلها مثلا

أى حرف من ال range الأول و هو من A الى Z ((Upper-case  
أو

أى رقم من ال range الثانى و هو من 0 إلى 9

أو

أى حرف من ال range الثالث و هو من a إلى z ((Lower-case  
أو

أو

علامة ال \_

بعد ذلك تأتى علامة ال + تقول لنا أنه يمكننا تكرار ما سبق على الأقل وجوده مرة واحدة أو أكثر وذلك لمنع



المستخدم من ترك هذا الجزء فارغ

بعد ذلك يجب وجود علامة @ ثم كلمة networkset بجميع حالاتها ثم النقطة بعد ذلك وتم استخدام الـ \ ليتم معاملة النقطة كأنها حرف عادى.

أخيرا نترك خيارين فى النهايه وهو أن ينتهى بـ com أو net باستخدام | التى تساوى OR

تطبيقات ال Regular Expression فى أجهزة Cisco

يوجد العديد من التطبيقات على أجهزة Cisco يستخدم فيها ال Regular Expression وسأحاول تلخيص أهمها الآن:

أولا: Cisco router تستخدم ال Regular Expression فى ال BGP ومن يدرس شهادته CCIE R & S أعتقد أن يعرف هذا الموضوع ويجب أن يكون ملم بال Regular Expression جيدا.

ثانيا: ASA Firewall تستخدم ال Regular Expression فى ال (Modular Policy Framework)MPF أو مايسمى بـ MQC إذا تم تطبيقه على Router.

ثالثا: IPS & IDS راجع مثال 1

رابعا: فى الأمر show run على أى جهاز Cisco شاهد

مثال 2 : أثناء القيام بـ troubleshooting or verifying للإعدادات أو ال configuration على router أو switch أو firewall نحتاج إلى تحديد مخرجات معينة للتركيز عليها، فبدلا من مشاهدة ملف ال configuration كاملا، يمكننا تحديد جزء معين لنراه

```
NetworkSet#show running-config | include ?
LINE Regular Expression

NetworkSet#show running-config | include h[ao]t
username hot
username hat
NetworkSet#
```

وكما نرى يمكننا استخدام Regular Expression لتحديد مخرجات معينة، وهذا مثال آخر:

```
NetworkSet#show running-config | include magdy$
username sherif-magdy
NetworkSet#
```

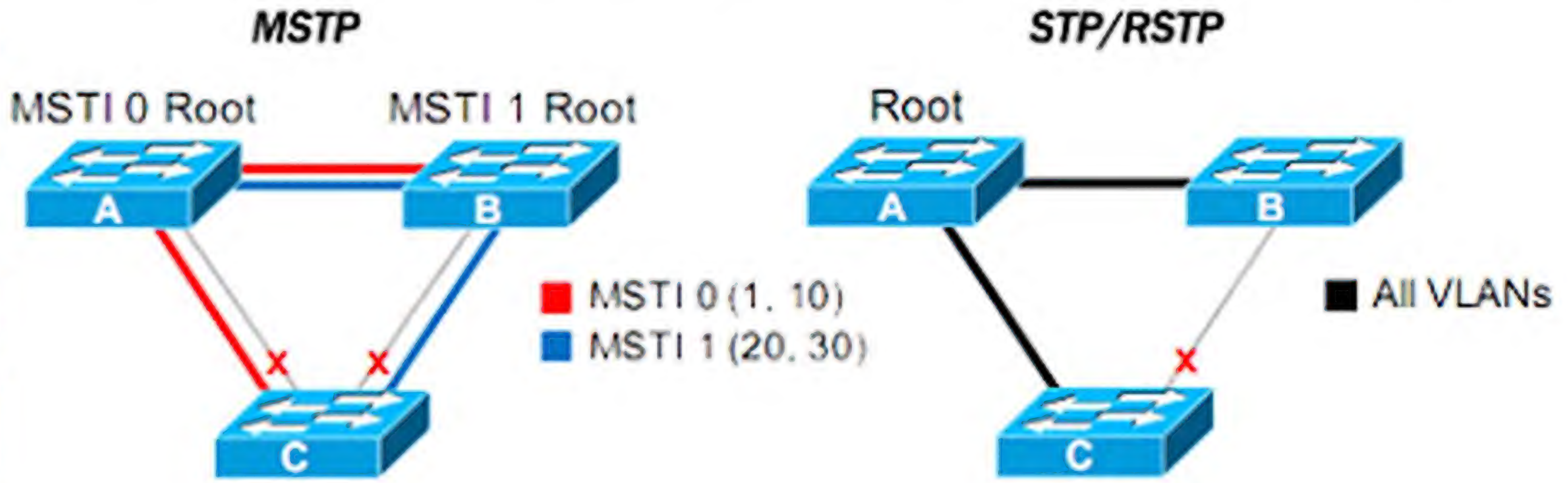
أترككم لتجربوا هذه الطريقة بأنفسكم ، فهى تسهل العمل إذا كان ال configuration file كبيرا الحجم.  
خاتمة :

هذه مجرد نظرة موجزة للموضوع فهو له تطبيقات كثيرة فى غاية التعقيد، و أجد بعض التشابه بينه و بين ال subnetting عندما بدأت تدرسه فى CCNA و كنت ترى أنه معقد و صعب الفهم و لكن بعد فهمه جيدا تجده فى منتهى السهولة، هذا هو الحال مع ال Regular expression و هناك الكثير من الكتب تشرحه بالتفصيل .

شريف مجدي



# IEEE

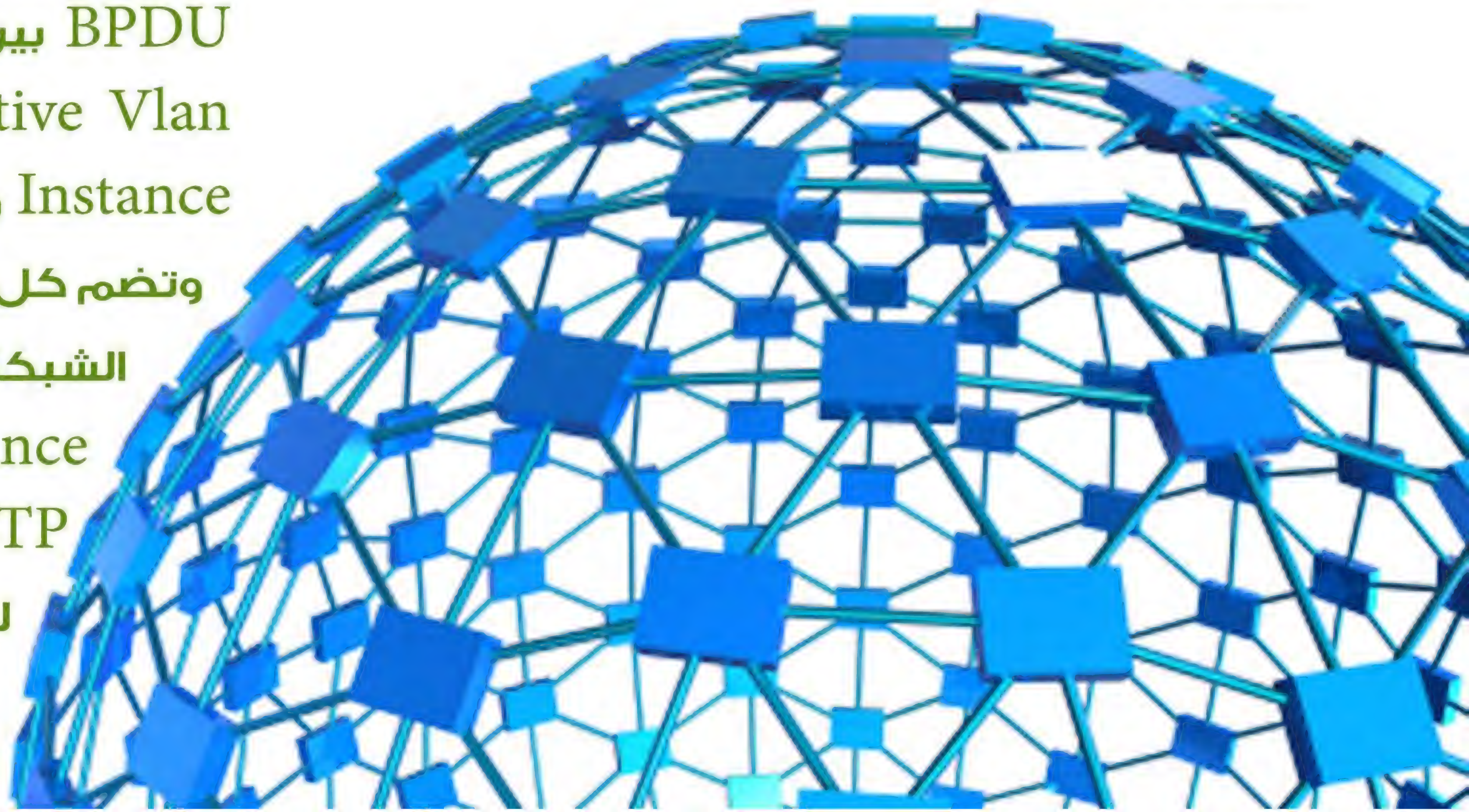


بالإضافة إلى أن الموضوع لن يكون حول آلية عمل كل واحد منها لأنها بحسب إعتقادي معروفة عند الجميع، بل فقط عن الاختلافات بينها ولنبدأ ب البروتوكولات الخاصة ب IEEE:

CST: أو Common Spanning Tree أو الـ STP الذي نسمع عنه والذي يعرف من خلال منظمة IEEE بأنه 802.1D يتصف هذا البروتوكول بأنه يعمل على كل أنواع الأجهزة سيسكو كانت أم جونيبر وبدون تفريق. وما يميزه هو وجود نسخة Spanning Tree واحدة أو One Instance تضم جميع الـ Vans ويتم تبادل الـ BPDUs بين السويتشات من خلال الـ Native Vlan، وهو يعمل من خلال Instance واحدة تضم كل البورتات وتضم كل الـ Vans الموجودة في الشبكة (سوف نفهم فكرة الـ Instance أكثر عندما نصل إلى MSTP) وهذه صورة توضيحية للـ CST.

أغلبنا وإن لم يكن جميعنا قد مر أثناء دراسته على بروتوكول الـ STP وعلى الأغلب أن هناك من وجد صعوبات وتعقيدات كثيرة في أنواعه المتوفرة فمن خلال إحصائية صغيرة قمت بها أحصيت على الأقل ستة أنواع لهذا البروتوكول وهي CST, RSTP, MSTP, PVST, PVST+, RPVST.

لنتعرف اليوم في القسم الأول من هذا المقال على أهم الاختلافات الموجودة بين STP, RSTP, MSTP والخاصة بـ IEEE. وقبل أن أبدا أحب أن أتوه أن هذه البروتوكولات لها وظيفة واحدة وهي منع حدوث ما يعرف ب اللوب (Loop) على مستوى الطبقة الثانية Data Link.

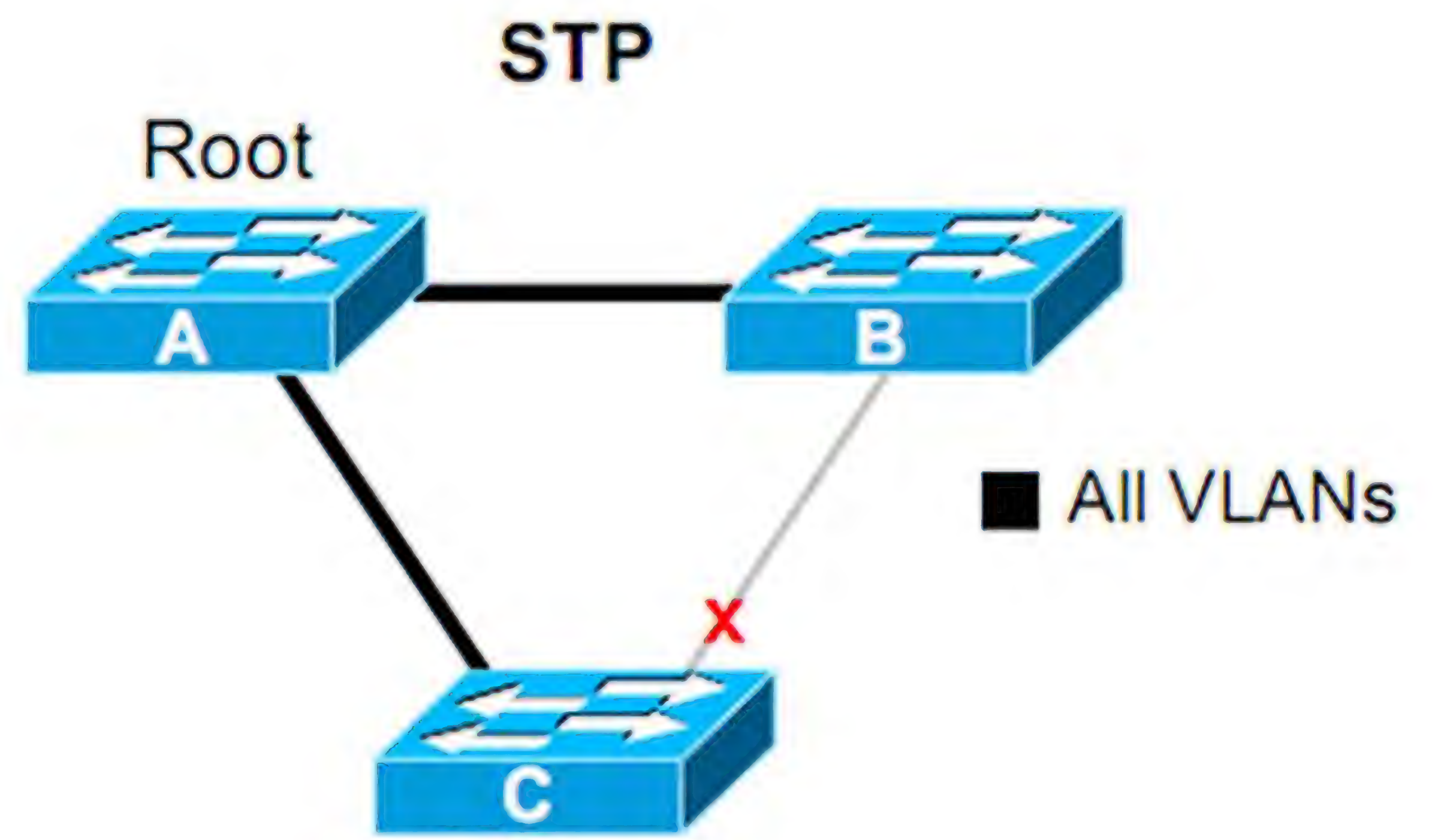




\*5 في الـ STP كان الروت بريدج هو الوحيد الذي يقوم بإرسال BPDU، وبعدها تتناوب باقى السويتشات على الإرسال. أما مع الـ RSTP فكل السويتشات الموجودة يمكنها أن تقوم بإرسال BPDU، فلو كان لدينا سويتشان موجودان ضمن شبكة كبيرة وأصبح أحد البورتات فى حالة Down، فإن السويتش سوف يرسل BPDU إلى السويتش الأخر لكي يقوم بتفعيل البورت الإحتياطي بشكل مباشر.

\*6 إستحداث مسميات جديدة خاصة بأنواع المنافذ الموجودة على السويتش مثل Edge Port وهي تعني أنه تم تفعيل خاصية الـ Port Fast على هذا البورت، والتي تقوم بتحويل البورت بشكل مباشر من الـ Discarding إلى الـ Forwarding. وهي تستخدم عادة في البورتات التي لاتحوي سويتشات ممكن أن تؤدي إلى حدوث لوب في الشبكة أو مع أجهزة الكمبيوتر. بالإضافة إلى مسمى آخر وهو Shared Port، وهو يعني أن هذا البورت متصل مع الـ HUP. وأخيرا مسمى جديد وهو Point-to-Point Port ويدل على أن البورت متصل مع سويتش آخر.

ملاحظة أخيرة وهي منذ عام 2004 تم اعتماد الـ RSTP لكي يكون هو الـ Default للـ STP وتم تعريفه بـ الـ 802.1D وإحالة الـ STP للتقاعد، لذا عندما نسمع الـ STP فمفكر بأنه الـ RSTP.



Protocol وهو نموذج مطور من الـ STP ويعرف بـ الـ 802.1W ومن خلال إسمه نستطيع أن نستنتج أن هذا البروتوكول هو أسرع من البروتوكول العادي والأسباب كثيرة:

\*1 تم دمج حالتا الـ Blocking و Listening إلى حالة واحدة وهي الـ Discarding وكما هو معروف أن الوصول إلى حالة الـ Listening كان يستغرق 15 ثانية.

\*2 الزمن الذي يلزم لإنتقال البورت من الـ Discarding إلى الـ Learning هو 6 ثواني، وهي تعني عدم إستلام BPDU لـ 3 مرات متعاقبة لأن الـ BPDU ترسل كل ثانيتين وهذا يعطينا 6 ثواني فقط، بينما نجد أن الـ STP يحتاج منك 20 ثانية للدخول في مرحلة الـ Listening، أي يجب أن ينتظر البروتوكول توقف إستلام الـ BPDU لعشر مرات.

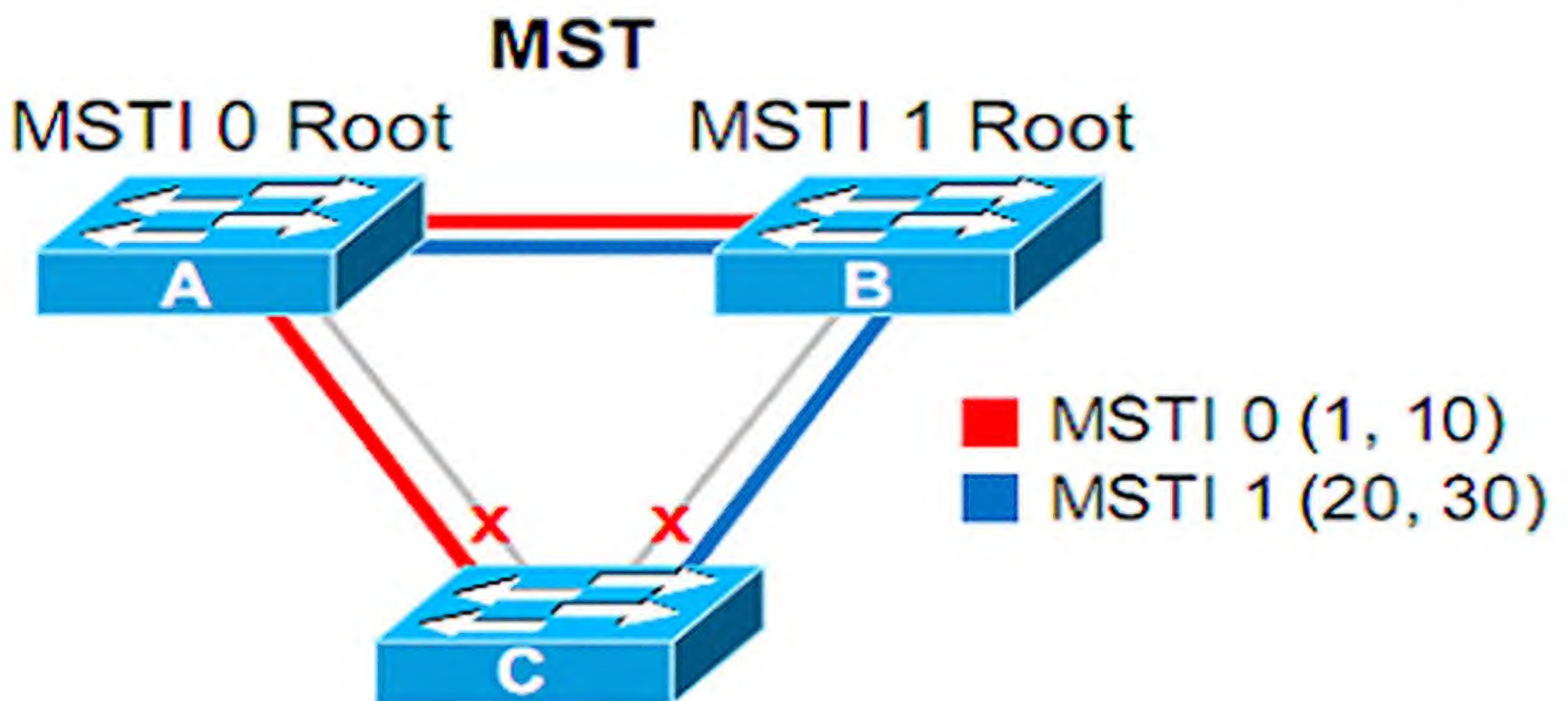
(فكرة الإنتقال تعتمد على عدد مرات إستلام الـ BPDU وليس على زمن معين، أي أن البروتوكول يحسب عدد مرات عدم إستلام الـ BPDU، ونستطيع نحن من خلال ذلك أن نستنتج الوقت اللازم).

\*3 من خلال هذه المقارنة نجد أن الـ STP يستغرق حوالي 50 ثانية لكي يتحول من حالة الـ Block إلى حالة الـ Forward بينما الـ RSTP يستغرق حوالي 21 ثانية.

\*4 تسميتان جديدتان حلتا مكان الـ Blocking Port وهي الـ Alternate Port & Backup Port الأول هو بورت إحتياطي لكل الـ segment موجودة في الشبكة، والثاني هو بورت بديل للـ Root Port.



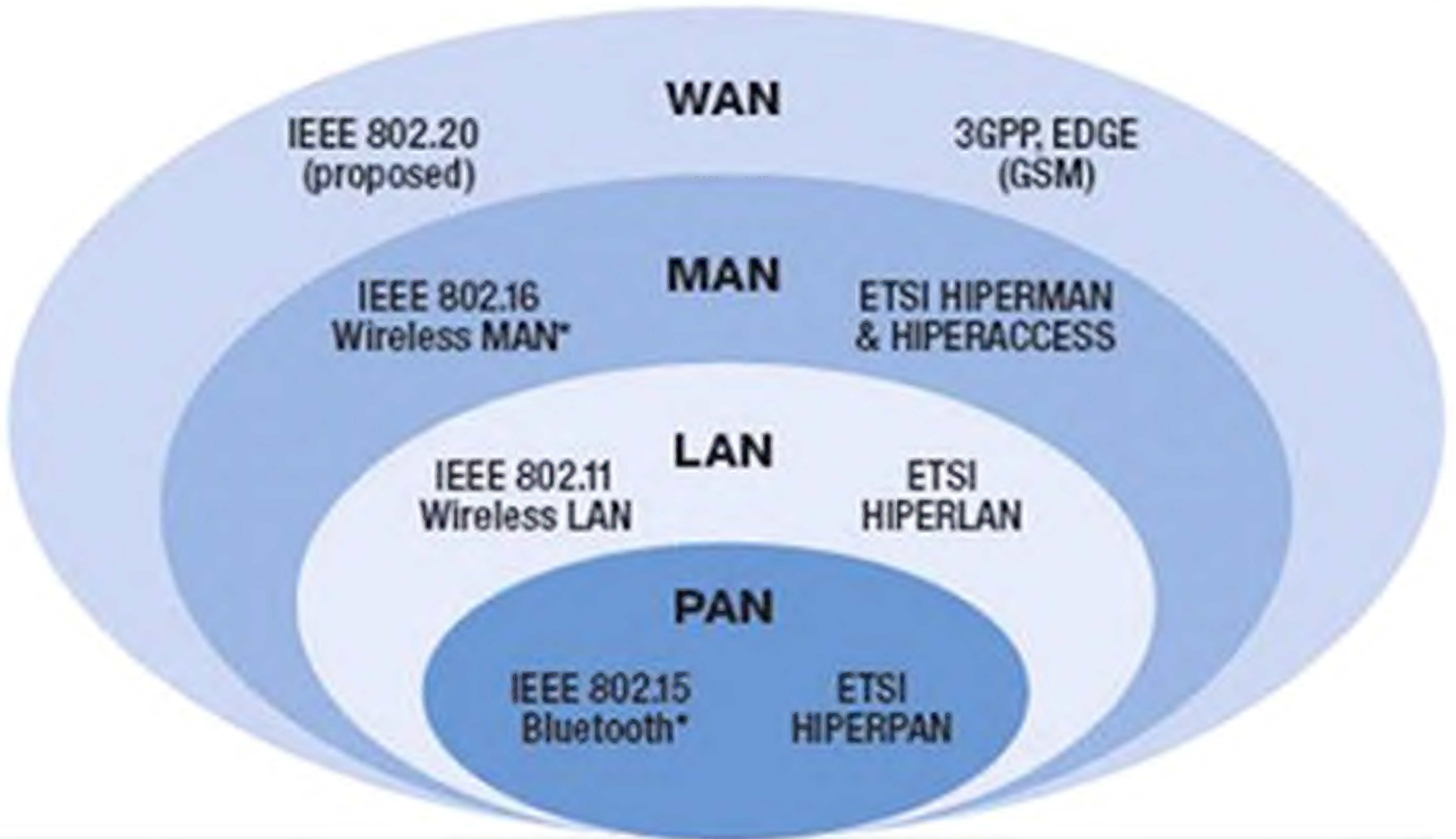
**MSTP**: أو **Multi Spanning Tree Protocol** وهو معروف من قبل ال **IEEE** ب **802.1S**. فكرة هذا البروتوكول تهدف إلى تقليل عدد ال **Instances** الموجودة بحيث نستطيع أن نضم أكثر من **Vlan** في **Instance** واحدة فكما ذكرت أن ال **STP** سوف يقوم بعمل **Instance** لكل **Vlan** موجودة في الشبكة. ومما لا شك فيه أن هذه العملية تخفف الضغط على المعالج كمنحى إيجابي لكنها سوف تمنع الشبكة من عمل **Load Balancing** بين ال **Vlans** كمنحى سلبي. ومن هذا المنطلق وجد ال **MSTP** الذي أتاح لنا تقسيم ال **Vlans** على مجموعات تعمل كل منها بشكل مستقل عن الأخرى ومن خلال **Instance** منعزلة. وكمثال صغير حول هذه العملية لنفرض أن لدينا **40 Vlan** في الشبكة وطبعا كل هذه ال **Vlans** سوف تعمل على شكل **Instance** واحدة كما ذكرنا في ال **STP**، لكن مع ال **MSTP** الموضوع مختلف قليلا لأنه ببساطة سوف يسمح لنا بإنشاء **Instance** منفصلة لكل مجموعة منها. ولنفرض أن أول **10 Vlan** موجودة في **One Instance**، بينما باقي ال **Vlans** في **Instance** أخرى وبهذه الطريقة سوف يتم إغلاق منافذ معينة لكل مجموعة من ال **Vlans**، بينما سوف تكون هذه المنافذ مفتوحة في المجموعة الأخرى. لاحظ معي الصورة القادمة لكي تفهم العملية بشكل أكبر:



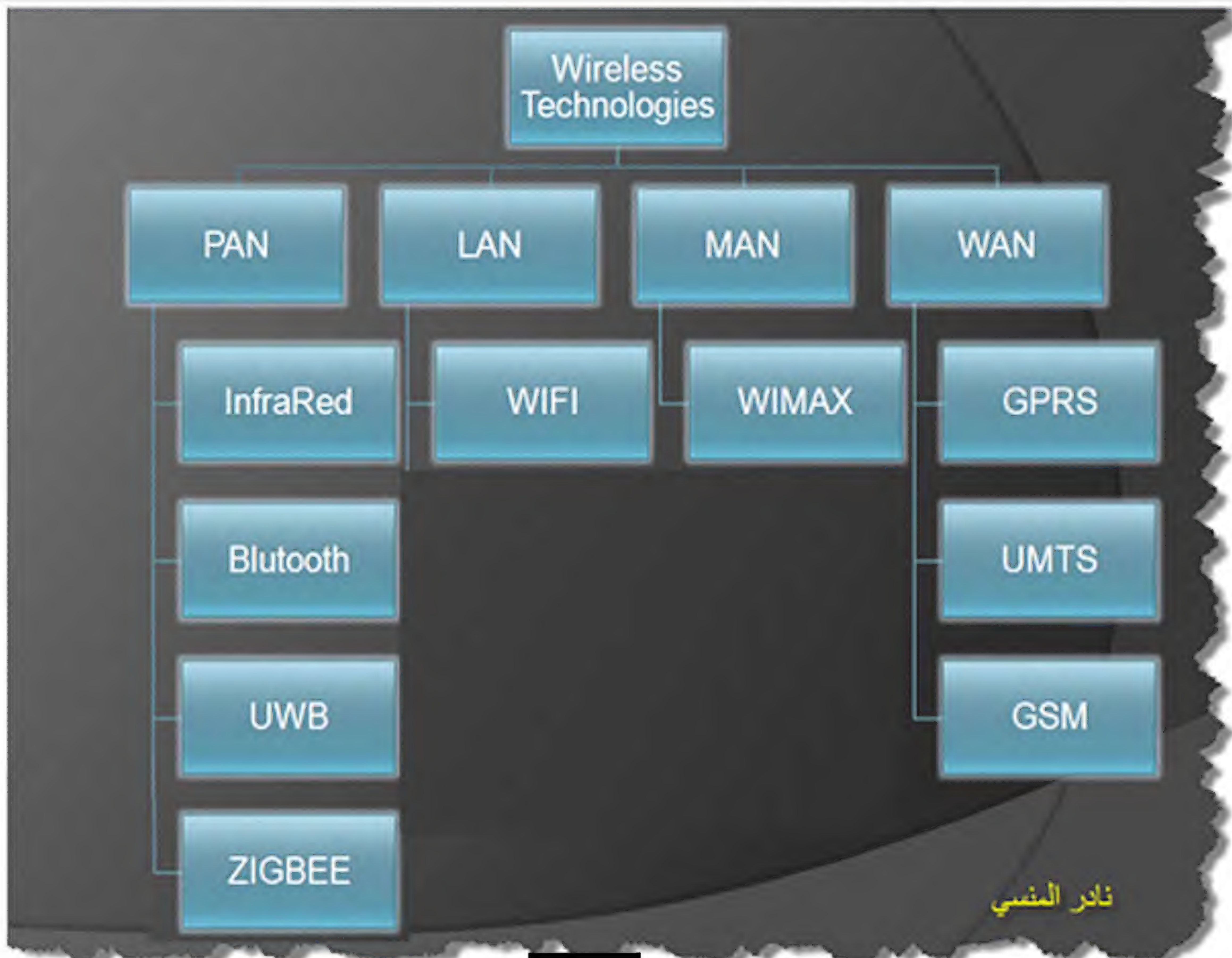
إلى هنا يكون الموضوع قد إنتهى على أمل أن نستكمل فيما بعد البروتوكولات الخاصة بـ **RPVST**, **PVST+**, **PVST** والتي سوف أطرحتها في العدد القادم إن شاء الله.

أيمن النعيمي





يتم تقسيم الشبكات اللاسلكية بنفس طريقة تقسيم الشبكات السلكية الي أربعة أنواع كل منها يتحدد حسب المساحة التي يغطيها و التي يستخدم في كل منها تقنية لاسلكية تتناسب مع المساحة التي تغطيها الشبكة و الشكل التالي يبين بعضا من التقنيات اللاسلكية المستخدمة مقسمة تحت هذه الأنواع الأربعة





### تقنيات الأشعة تحت الحمراء

Infrared Data Association (IrDA)

يتم استخدام تقنيات الأشعة تحت الحمراء IR Infrared للاتصال المباشر line of sight عندما يكون الجهازان على خط واحد و لا يفصلهما اي عائق مثلما تستخدم أجهزة الريموت كنترول و رغم أن الأشعة تحت الحمراء ليست اشعة مرئية فهو يعتمد على استخدام خواص الضوء المرئي في الإتصال و يتأثر الإتصال بما يتأثر به الضوء العادي

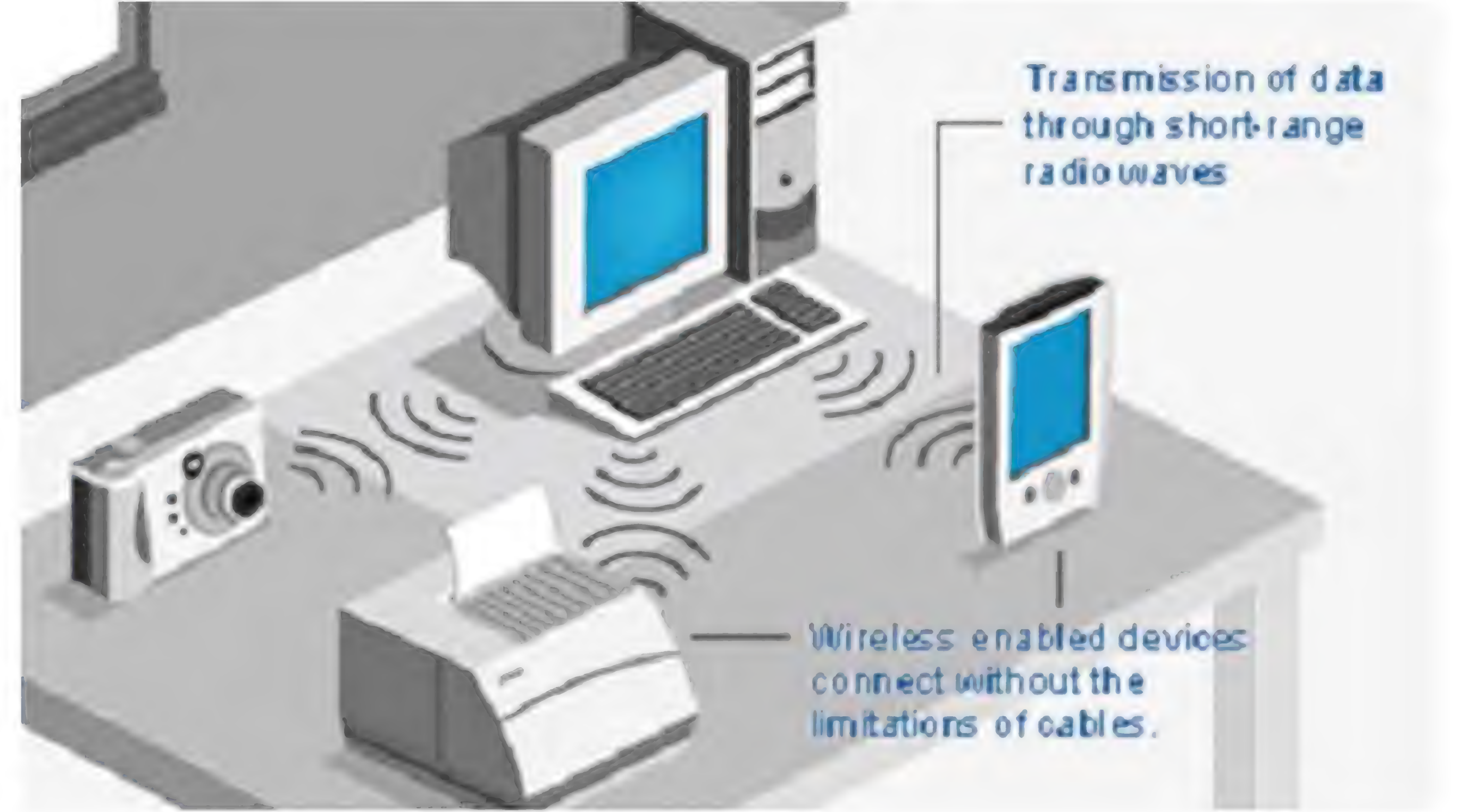


### تقنية الإتصال اللاسلكي بواسطة البلوتوث Bluetooth

عالجت هذه التقنية مشكلة اشتراط تواجد الأجهزة على خط نظر واحد ومشكلة تعدد الإتصال ومشكلة الأمان ومشكلة السرعة حيث تستطيع أن تحقق الإتصال بين أكثر من جهاز في نفس الوقت مع توفر الأمان الشبكي

### الشبكات اللاسلكية الشخصية

(PAN ( Personal Area Network



و هي تختص بالشبكات الشخصية على مستوى متر الي عشرة امتار و تختص بالأساس في اتصال جهاز الكمبيوتر لاسلكيا ببعض الأجهزة الأخرى الخدمية مثل الطابعات و الأكسس بوينت و السكار و الكاميرات و أحيانا الماوس و الكيبورد

و تتميز هذه التقنية باستخدام ارسال لاسلكي بقدرة و طاقة محدودين لحصر حيز الإرسال في مكان صغير يستخدم في هذه الشبكات تقنيات شبك لاسلكي مثل IrDA, Bluetooth, UWB, Z-Wave , ZigBee



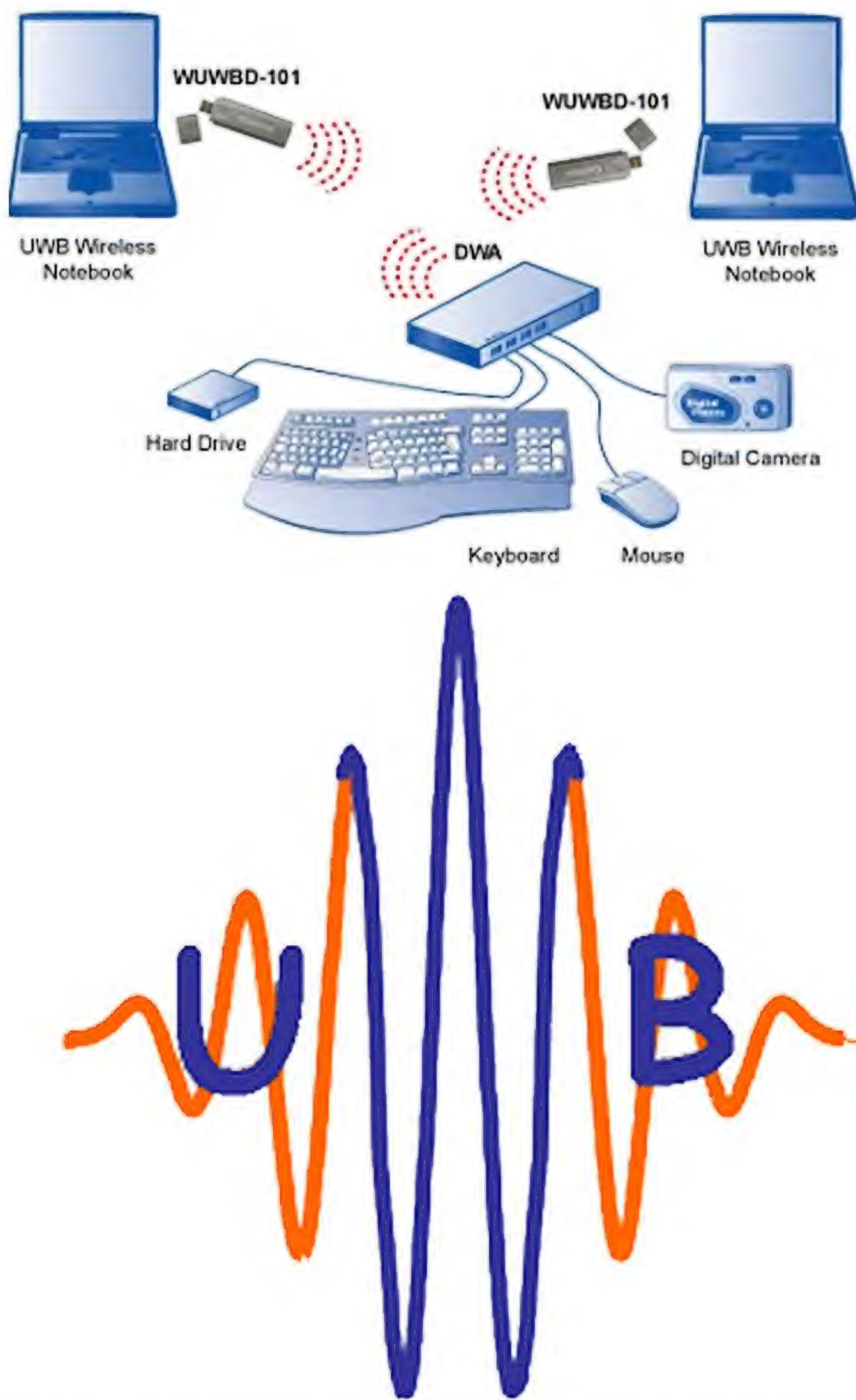
و كذلك ضمان سرعة تدفق للبيانات و يتم استخدام طريقة master / slave لعمل الإتصال و هي طريقة منظمة و عملية و منطقية للغرض الذي أنشئ له هذا النظام

تقنية البلوتوث تستخدم تردد ما بين 2.40 إلى 2.48 جيجاهيرتز و تقوم الأجهزة بتغيير التردد كل مرة اتصال و لذلك فمن الصعب جدا حدوث تداخل في الترددات بين الإتصالات



### تقنية الإتصال اللاسلكي فائقة الإتساع UWB Ultra-wideband

يعتبر الإتصال اللاسلكي فائق الإتساع من التقنيات الأحدث في عالم الإتصالات الشبكية اللاسلكية و الأعجب ايضا فهي تستخدم موجات راديوية واسعة النطاق ذات طاقة منخفضة جدا لإرسال بيانات كبيرة جدا و هذه الميزات قد تزيح جانبا اسماء عملاقة مثل البلوتوث و الواي فاي في الشبكات السالكية الشخصية يبلغ سرعة نقل بيانات لاسلكيا تصل إلى أكثر من 480Mbps و هو هكذا أسرع عشرات المرات من معيار الواي فاي 802.11b و تتميز معداته أيضا بما يتميز به معدت البلوتوث من توافقيته و أيضا قدرته علي العمل بتكنولوجيا التشغيل و التوصيل الآلي PNP و تتميز معداته ايضا بإمكانية ربطها بواسطة جهاز سويتش يعتمد علي تكنولوجيا UWB بما يجعله شبيها بأجهزة الواي فاي

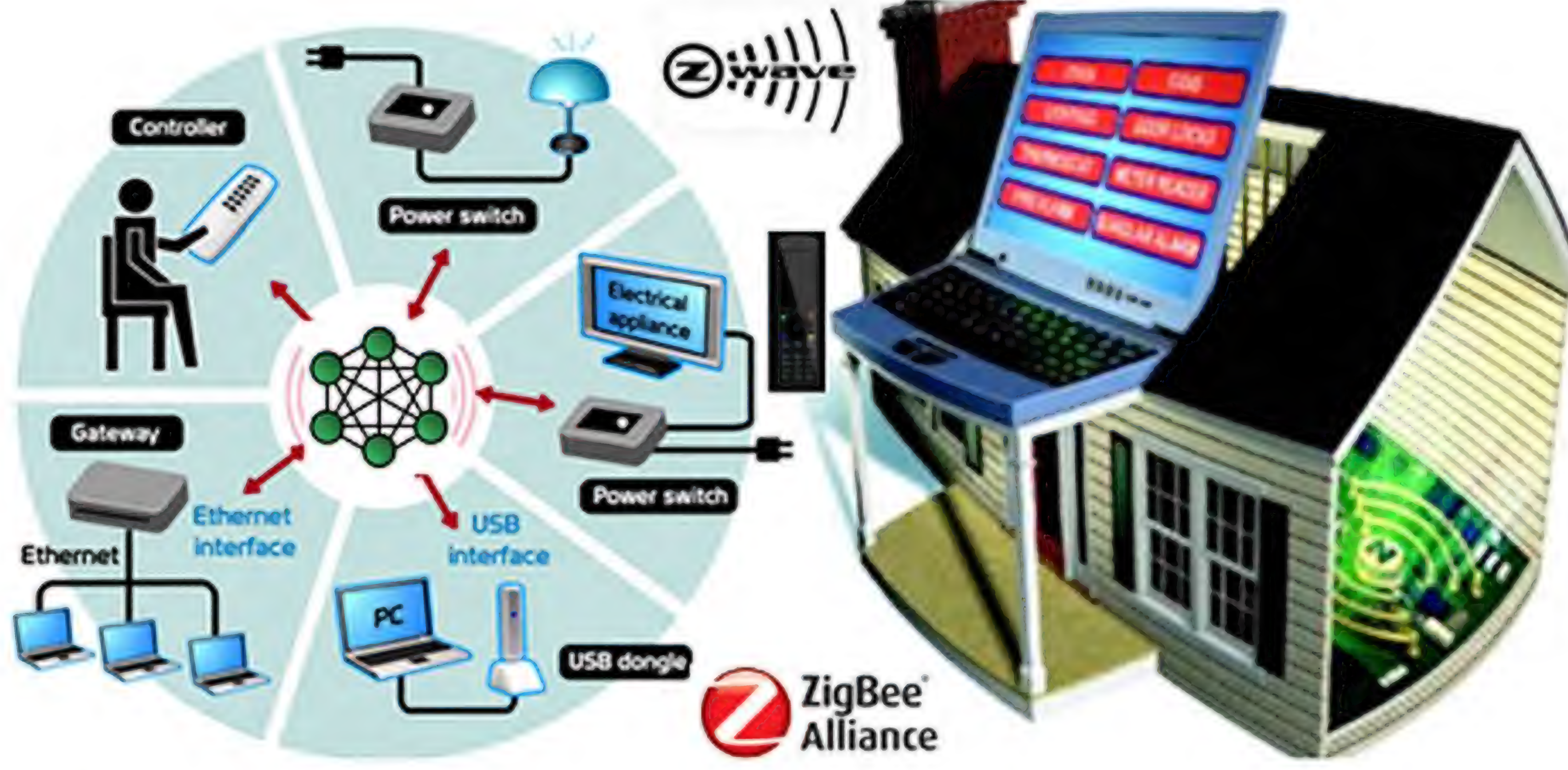


يعتبر الإتصال اللاسلكي فائق الإتساع من التقنيات الأحدث في عالم الإتصالات الشبكية اللاسلكية و الأعجب ايضا فهي تستخدم موجات راديوية واسعة النطاق ذات طاقة منخفضة جدا لإرسال بيانات كبيرة جدا و هذه الميزات قد تزيح جانبا اسماء عملاقة مثل البلوتوث و الواي فاي في الشبكات السالكية الشخصية

يبلغ سرعة نقل بيانات لاسلكيا تصل إلى أكثر من 480Mbps و هو هكذا أسرع عشرات المرات من معيار الواي فاي 802.11b و تتميز معداته أيضا بما يتميز به معدت البلوتوث من توافقيته و أيضا قدرته علي العمل بتكنولوجيا التشغيل و التوصيل الآلي PNP و تتميز معداته ايضا بإمكانية ربطها بواسطة جهاز سويتش يعتمد علي تكنولوجيا UWB بما يجعله شبيها بأجهزة الواي فاي



الإتصال و التحكم اللاسلكي عبر تقنيتي  
Z-Wave / Zigbee



في هاتين التقنيتين سنتخطي حدود الشبكات الكلاسيكية التي تعتمد فقط علي الكمبيوتر و ملحقاته ,, فأنت هنا تستطيع أن تربط كل جهاز كهربى في بيتك بالشبكة ( شبكة الواي فاي -معدات الإنترنت - التلفاز - المصباح - الثلاجة - الأبواب الكهربائية - الغسالة - السخان - التكييف .. الخ ) حيث تمكنك هاتين التقنيتين ومعداتهما من صنع شبكة تقوم بالتحكم بكافة أجهزتك الكهربائية و الإلكترونية و ذلك لاسلكيا بواسطة برنامج تحكم علي الكمبيوتر و أجهزة الريموت كنترول

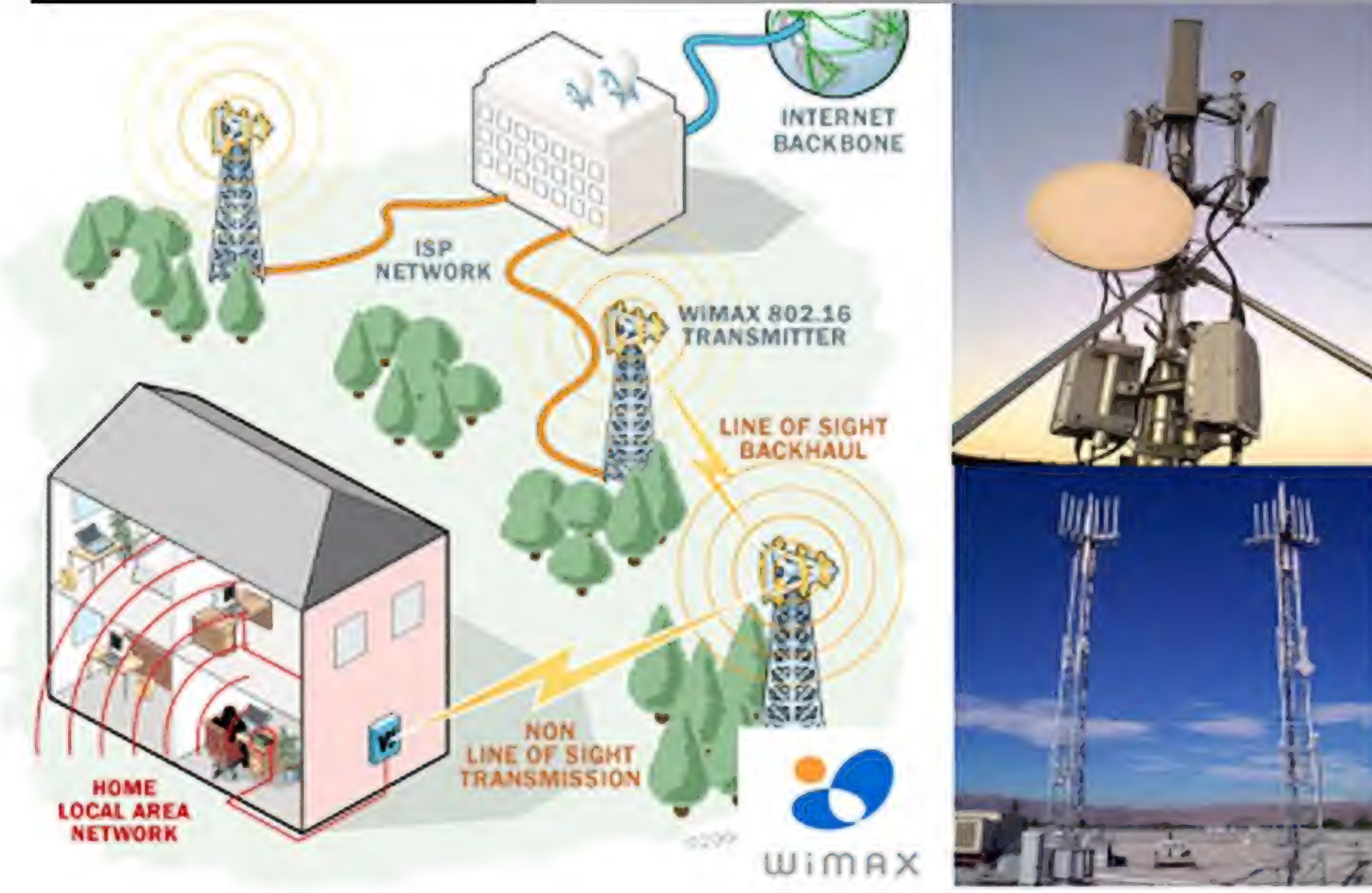
و علي عكس الشبكات العادية التي تحتاج أن يكون الجهاز مصنع مسبقا لينضم للشبكة فإنك هنا تستطيع ان تضم اي جهاز الكتروني او كهربى الي شبكة z-wave بواسطة وضع رقاقة تحكم لاسلكي خارجية لأي جهاز و ذلك بعملية تسمى "pairing" and "adding" وبقاقي الشبكات الشخصية فإنها تستخدم نطاق ترددي مجاني هو industrial, scientific (ISM) and medical) و يستخدم بالأساس في الأجهزة الطبية و الصناعية و هذه الترددات تعمل بموجات ذات طاقة منخفضة علي مسافات قصيرة و علي عكس أجهزة البلوتوث فإن شبكة z-wave او zigbee تستطيع التحكم في ما يقرب من 232 جهاز تتواصل فيما بينها بتكنولوجيا أو طبولوجية طبولوجية source-routed mesh network حيث يكون هناك أكثر من جهة تستطيع التحكم في الشبكة و التخاطب مع أكثر من جهة

الشبكات اللاسلكية المحلية

WLAN (Local Area Network)

و هي أكثر الشبكات اللاسلكية انتشارا و شيوعا و هي تعتبر الشبكات المناظرة للشبكات السلكية الشائعة و تسمى أيضا الواي فاي WIRELESS FIDELITY <sup>مصراته • ليبيا</sup> WI Fi وهي خدمة الإتصال الشبكي لاسلكيا فائقة السرعة والدقة و يتم الدخول اليها عن طريق الكمبيوتر المحمول Notebook PC أو عن طريق الكمبيوتر الجيبى Pocket Pc مثل <sup>مصراته • ليبيا</sup> i mate او PDA أي " المساعد الرقمي الشخصي "





و تقدم غالبا بسرعات وسرعات خدمة الواي ماكس 512 كيلو بايت , 1024 كيلو بايت , 2048 كيلو بايت و يتم بث الإرسال عبر أبراج لاسلكية تشبه أبراج الموبايل تخدم مناطق تزيد مساحتها عن مئات الكيلومترات و يتم استقبال الإرسال عبر هوائيات أطباق استقبال DESH علي ارتفاع ثلاثة امتار



و توجد في المواقع العامة مثل الفنادق والمطارات والجامعات والمطاعم وأصبحت شركات الطيران تقدم هذه الخدمة على متن طائراتها. ومن المتوقع ان يصل مستخدمي هذه الخدمة الي 150 مليون شخص بنهاية عام 2011 م ان لم يصل بعد.

### WMAN (Wireless Metropolitan Area Network)

#### شبكات المدن اللاسلكية

أصبح الغموض يكتنف مستقبل تكنولوجيا الواي ماكس بعد ان قامت عديد من الشركات بوقف خطوط انتاج معداتها و علي رأسها سيسكو و نوكيا , فلقد كانت و لازالت حتي الآن تكنولوجيا الواي ماكس مثال تطبيقي علي شبكات المدن اللاسلكية WMAN و كنا و لازلنا ننظر لها بكثير من الأمل متمنين يوما أن تحل مكان شبكات الواي فاي و نتخيل اننا سنتعامل مع الإنترنت و نتوغل فيه و كأننا نستخدم شبكة الموبايل

الواي ماكس أو Worldwide Interoperability for Microwave Access هي تكنولوجيا لاسلكية تستخدم المعيار IEEE 802.16 لتوصي مقاييسها و تختلف عن سابقتها ان المدي الترددي المستخدم لها مدفوع الأجر و لابد من اصدار تراخيص لها من الجهات المختصة



الشبكات اللاسلكية الموسعة

Wireless WAN (Wide Area Network)

قبل أن أقول أن هذا الأمر واسع جدا أحب أن أركز في ذهنك مبدأ مهم جدا وهو ان أي من التقنيات السابقة قد تتأرجح بين كونها شبكات محلية او مدن او واسعة حسب المنطقة التي تغطيها و لا يعتبر كونها ذات تقنية معينة أن نحكم عليها بهذه التقنية , فنحن نستطيع أن نصنع شبكة مدن بواسطة تقنية الواي فاي بل و وواسعة ايضا بالسنة للشبكة اللاسلكية الموسعة فهي تستخدم غالبا عبر شركات الهواتف المحمولة و التي تستخدم الموجات اللاسلكية و كذلك الأقمار الصناعية و المهم فيها هو طريقة انتقال الأرسال بين عدة شبكات محلية أو مدن أو حتي شبكات فردية او شخصية و لأن الخوض ي هذه الشبكات سينقلنا الي حيز أكبر لتوسعنا به فسنكتفي بذلك و هذا جدول مقارنة بين الشبكات اللاسلكية

	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11 HiperLAN2	802.11 MMDS, LMDS WiMAX (802.16)	GSM, GPRS, CDMA, HSDPA 2.5-3G-3.5G
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps 1.8/3.6 – 7.2Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	E1 replacement, last mile access	Mobile Phones, cellular data



- IEEE 802.1 Bridging (networking) and Network Management
- IEEE 802.2 Logical link control (inactive)
- IEEE 802.3 Ethernet
- IEEE 802.4 Token bus (disbanded)
- IEEE 802.5 Defines the MAC layer for a Token Ring (inactive)
- IEEE 802.6 Metropolitan Area Networks (disbanded)
- IEEE 802.7 Broadband LAN using Coaxial Cable (disbanded)
- IEEE 802.8 Fiber Optic TAG (disbanded)
- IEEE 802.9 Integrated Services LAN (disbanded)
- IEEE 802.10 Interoperable LAN Security (disbanded)
- IEEE 802.11 Wireless LAN & Mesh (Wi-Fi certification)
- IEEE 802.12 demand priority (disbanded)
- IEEE 802.13 Cat.6 — 10Gb lan (new founded)
- IEEE 802.14 Cable modems (disbanded)
- IEEE 802.15 Wireless PAN
- IEEE 802.15.1 (Bluetooth certification)
- IEEE 802.15.4 (ZigBee certification)
- IEEE 802.16 Broadband Wireless Access (WiMAX certification)
- IEEE 802.16e (Mobile) Broadband Wireless Access
- IEEE 802.17 Resilient packet ring
- IEEE 802.18 Radio Regulatory TAG
- IEEE 802.19 Coexistence TAG
- IEEE 802.20 Mobile Broadband Wireless Access
- IEEE 802.21 Media Independent Handoff
- IEEE 802.22 Wireless Regional Area Network

# IEEE 802

# معهد وهندسي الإلكترونيات والكهرباء

## نادر المنسي

عندما تريد الولوج الي مجال وتكون متخصصا فيه فلا بد ان تدرس المقاييس الخاصة به والإتفاقيات التي سطرت لتحديدتها وان تتابع دوما المنظمات والهيئات المختصة به

وفي مجال الشبكات فإن معهد مهندسي الإلكترونيات والكهرباء هو المنوط به وضع تلك المقاييس ودراستها تستطيع ان تتفهم كثيرا من ذلك المجال

فمثلا شبكات الواي فاي جزء من الشبكات اللاسلكية و التي بدورها جزء من الإتصالات و التي تنتمي بدورها الي فرع الإلكترونيات والكهرباء من الهندسة فإنه وجب البحث عن ما يخص الواي فاي في هذا المعهد

وما 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 تفريعات وفي مجموعها تشرح وتؤصل للشبكات السلكية واللاسلكية وانواع الكابلات وقيم الترددات وغيرها

هي بالفعل موسوعة لم اراد ان يفهم الشبكات هندسيا من وجهة نظر مهندسي الإتصالات والإلكترونيات واليكم كل ما يخصنا كمهندسي شبكات في هذا المعهد





اذن فإن معهد المهندسين الكهربائيين والإلكترونيين من كبار مطوري المقاييس الدولية التي تقوم على أساسها الكثير من المنتجات والخدمات اليوم، وخاصة في مجال الاتصالات، وتكنولوجيا المعلومات، وتوليد الطاقة. ويعد معهد المهندسين الكهربائيين والإلكترونيين، بما لديه من مجموعة فعلية تحتوي على ما يقرب من 900 مقياس فعلي وأكثر من 400 مشروع تحت الإنشاء، المصدر الرئيسي للتوحيد القياسي في نطاق واسع من التكنولوجيات الواعدة، وهو يرحب بالمهندسين الفرديين والمؤسسات للمساهمة في أنشطته.

واليوم فإن سرعة تحرك بيئة الأعمال تتطلب التوحيد القياسي لضمان نمو السوق. وتدرك الشركات أنه من أجل تلبية التوقعات المتزايدة للعملاء، ولزيادة الربحية وتوسيع نطاق فرص السوق، من الأمور الهامة لضمان النجاح أن يتم الالتزام بتطوير وتنفيذ مقاييس معهد المهندسين الكهربائيين والإلكترونيين.

مجموعات معهد المهندسين الكهربائيين والإلكترونيين

\* معهد المهندسين الكهربائيين والإلكترونيين – التطبيقات

\* معهد المهندسين الكهربائيين والإلكترونيين – الاتصالات

\* معهد المهندسين الكهربائيين والإلكترونيين – الكمبيوتر والإلكترونيات

\* معهد المهندسين الكهربائيين والإلكترونيين – الأدوات والمصطلحات

\* معهد المهندسين الكهربائيين والإلكترونيين – الطاقة

وهناك مجموعات اخر تستطيع تصفحها من هنا

<http://www.ieee.org/web/societies/home/index.html>

وتستطيع الإشتراك فيها ولكن بقيمة مدفوعة مقدما

\* يحصل المشتركون على إمكانية الوصول الآمن عبر الإنترنت لخدمات البحث ، والاستعراض ، ووضع الإشارات المرجعية، والتتبع، وطباعة المستندات وفقاً لاتفاقية الترخيص. يتم تحديث المستندات يوميا. يمكن لعدة مستخدمين المشاركة في رخصة واحدة. تحصل أيضاً على إمكانية الوصول إلى البيانات البيبلوغرافية لمقاييس IHS – أكثر من 1 مليون مستند.

موقع المعهد

<http://www.ieee.org/web/membership/home/index.html>

جمعية مهندسي الكهرباء و الإلكترونيات المحدودة. Institute of Electrical and Electronics Engineers, Inc. و إختصارها أي تريبل إي IEEE تلفظ (E - triple عسرته و تريبلا Eye) ، و هي جمعية محترفة تقنية لاربحية لما يقرب من نصف مليون عضو موزعين في معظم دول العالم. ، و هي جمعية معروفة و مشهورة جدا في الأوساط العلمية.

تشكلت IEEE في العام 1963 باندماج مؤسستي American Institute of Electrical Engineers التي تأسست عام 1884 ومؤسسة ( Institute of Radio Engineers ) التي تأسست عام 1912.

تسعى IEEE إلى إختراع، تطوير، مشاركة وتطبيق المعارف المتعلقة بالإلكترونيات وتكنولوجيا\*

وفرت IEEE الدخول لملايين الوثائق التقنية مؤتمرات للبحث وتبادل الخبرات وعرض أخر الإختراعات ، فرص عمل بشركات عالمية ، وبعثات دراسية – هذا ما وجدته للآن

هناك 11 فرع إقليمي في 8 دول عربية ، و 40 فرع طلابي في 40 جامعة عربية ”المعلومة منذ سنتين“ و في عام 1999 تم تأسيس أول فرع للجمعية في فلسطين في الجامعة الاسلامية بغزة ، و قد حظى الفرع بالكثير من التأييد و الاهتمام من قبل محاضري و محاضرات كلية الهندية قسم الكهرباء و الحاسوب ، و لا يزال المكتب يقدم العديد من الخدمات للفئة الطلابية و تجدون تفصيل لنشاطات المكتب و خدماته في صفحة ”نشاطاتنا“ على الموقع.

من خلال مساهمة أعضائها، IEEE تمثل الجمعية المرجع الأساسي للكثير من المواضيع التقنية و التي تتراوح من هندسة الحاسوب، التقنية الطبية الحيوية والاتصالات، إلى الطاقة الكهربائية وهندسة الطيران والأجهزة الإلكترونية، و غير ذلك الكثير.

من خلال نشراتها التقنية، المؤتمرات والنشاطات فإن IEEE تنتج ما يقارب 30 بالمائة من النشر العلمي الخاص بالهندسة الكهربائية و الإلكترونية، و علم الحاسبات، كما تقيم سنويا أكثر من 300 مؤتمر رئيسي و لها تقريبا 900 معيار قياسي مستعمل و ما يقارب الـ 500 تحت التطوير.





تحدثت في الجزء الأول من هذه المقالة في العدد الماضي عن الخطوة الأولى في عملية اكتشاف الأخطاء وإصلاحها وكانت عن جمع المعلومات عن طريق التعرف على الأعراض والمشاكل الموجودة . واليوم سأتابع معكم شرح الخطوات التالية من الخطوات التسع لهذه المنهجية .

ولنأخذ مثالاً عملياً لتقريب هذه الفكرة . افترض أنك تقوم بإصلاح مشكلة اتصال جهاز مستخدم بالشبكة ، فأول ما يجب أن تبدأ به هو أن تذهب لجهاز العميل ( client ) وتقوم بعمل PING منه إلى السيرفر ، فإذا فشلت هذه التجربة حاول أن تكرر هذه العملية من الأجهزة الأخرى الموجودة في نفس الشبكة مع هذا الجهاز . إذا كانت عملية الـ PING في جميع الأجهزة غير ناجحة فإن عملية اكتشاف الخطأ ومعالجة المشكلة سوف تنتقل إلى الشيء المشترك بين هذه الأجهزة ، أي السيرفر أو السويتش ( switch ) مثلاً .

المقابلة هي :

### الخطوة (٣): معرفة آخر التغييرات في الشبكة

عندما تحدث مشكلة في اتصال جهاز ما بالشبكة أو قد تكون المشكلة في الشبكة ككل ، يجب أن تضع في الاعتبار أن ما قبل حدوث المشكلة كان كل شيء يعمل بشكل سليم . وكثيراً ما يتلقى قسم الدعم الفني تليغاً بأن "الكمبيوتر توقف عن العمل" ، وهذا الإدعاء غير محبب نوعاً ما لأن من الأفضل القول أن هناك تغييرات حصلت في النظام أو في الشبكة أدت إلى حدوث هذه المشكلة . و بناء على ذلك ، فإن تحديد ومعرفة ما تغير في الشبكة يمكن أن يقودك في الاتجاه الصحيح لحصر وحل المشكلة .

التغييرات يمكن أن تحدث في أجهزة الشبكة ، أو السيرفرات ، أو في أجهزة المستخدمين . وسأوضح الآن هذه النقاط .

### الخطوة (٢): تحديد الأماكن التي بها عطل في الشبكة

بعض المشكلات تكون متعلقة بمستخدم واحد وفي مكان واحد ، وهناك من المشكلات ما يؤثر على المئات أو ربما الآلاف من المستخدمين وتمتد في عدة أماكن . ولذلك فإن تحديد المنطقة المتضررة في الشبكة هي خطوة مهمة في عملية الإصلاح ، وغالباً ما تكون هذه الخطوة هي نقطة الانطلاق لرسم الاستراتيجيات التي ستستخدمها في حل المشكلة .

المشكلات التي تصيب عدد كبير من المستخدمين في وقت واحد هي مشكلات تتعلق بالاتصال غالباً ، ويمكن حصر مواقعها في كبائن الأسلاك ( wiring rooms ) ، أو في أجهزة الشبكة ( network devices ) مثل السويتشات و الراوترات ، أو في غرف السيرفرات ( server rooms ) . أما إذا كانت المشكلة تخص جهاز مستخدم واحد فإن عملية الإصلاح غالباً ما تبدأ و تنتهي بنفس مكان هذا الجهاز .

عندما يحدث عطل في الاتصالات عن مجموعة ما فإن ذلك سيقودك فعلاً إلى التوجه نحو كبينة الأسلاك أو إلى السيرفر ، ولكن ليس بالضرورة أن تبدأ عملية إصلاح المشكلة هناك ، لذا فإن معرفة من تأثر بهذا التعطل أولاً هي المعطيات الأولية عن مكن وجود المشكلة بالضبط .

# منهجية حل مشاكل الشبكة



## بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ التغييرات في أجهزة الشبكة

تإن إضافة أو إزالة أجهزة Hub أو Switch أو Server في الشبكة أو تغيير قيم معلومات الراوتر ، قد يؤدي إلى حدوث خلل في اتصالات الشبكة . ولذلك فإن أي تغيير في هذه الأجهزة سواء أكان فيزيائياً ( physical ) أو منطقياً ( logical ) فعلى مدير الشبكة توثيق ذلك بمستندات مع التفاصيل الشامل . وبهذا ، فعندما تحدث أو يتكرر حدوث مشكلة ما في توبولوجية الشبكة فإنه يمكن الرجوع إلى هذه الوثائق وبالتالي حل المشكلة في أسرع وقت ممكن .

### التغييرات في السيرفات

يعتبر القيام ببعض الترقية والإصلاحات جزء من مهام مدير الشبكة ، وقد تؤدي هذه الترقية والإصلاحات أحياناً بالرغم من لزومها إلى مشكلات عديدة غير مقصودة . حتى أن أبسط الأعمال على السيرفر يمكن أن يكون لها تأثير سلبي على الشبكة .

ومن هذه الأعمال :

1\* تغييرات في حسابات المستخدمين

2\* تغييرات في صلاحيات المستخدمين

3\* الترقية والتحديثات لنظام السيرفر

4\* تثبيت تطبيقات جديدة

5\* تغييرات بـ هاردوير السيرفر

### تغييرات في أجهزة المستخدمين

ليس كل التغييرات التي تتم على أجهزة المستخدمين تكون من تحكّم مدير الشبكة . فكثيراً ما يقوم بعض المستخدمين بتثبيت برمجيات بأنفسهم مثلاً .



ومثل هذه التغييرات يمكن أن ينتج عنها مشاكل تكون صعبة الحل إلى حد ما حيث أن كثيراً من المستخدمين لا يتوقعون نتيجة تلك التغييرات التي قاموا بها على أجهزتهم .

# منهجية حل مشاكل الشبكة

علاء مازن عدوي