العدد الثاني

صفر 1434

تقريب الشبكات اللاسلكية

تصدر كل شهر عربي عن موقع Wireless4arab.net

ثورة الربيع اللاسلكي WIGIG

الخلايا اللاسلكية و التغطية

دليلك لاختراق الشبكات اللاسلكية

MAC ADDRESS FILTERING

CONTROLLER CODE UPGRADE

SYSTEM OPERATING MARGIN (SOM)

17 سؤال و جواب عن

LIGHTWEIGHT ACCESS POINT

نادر المنسي

مقدمة

مقالة العدد

Wireless solutions, services, technology, products

عندما تتصفح موقع سيسكو و صفحة الشبكات اللاسلكية فسنجد تقسيم الشبكات اللاسلكية الي اربع أشياء Solution – Services – Products – Technolgy و كثير منا يخطئ في التفرقة بينهم فبحثت في صفحات سيسكو الخاصة بها و استنبطت لكم هذه الفروق

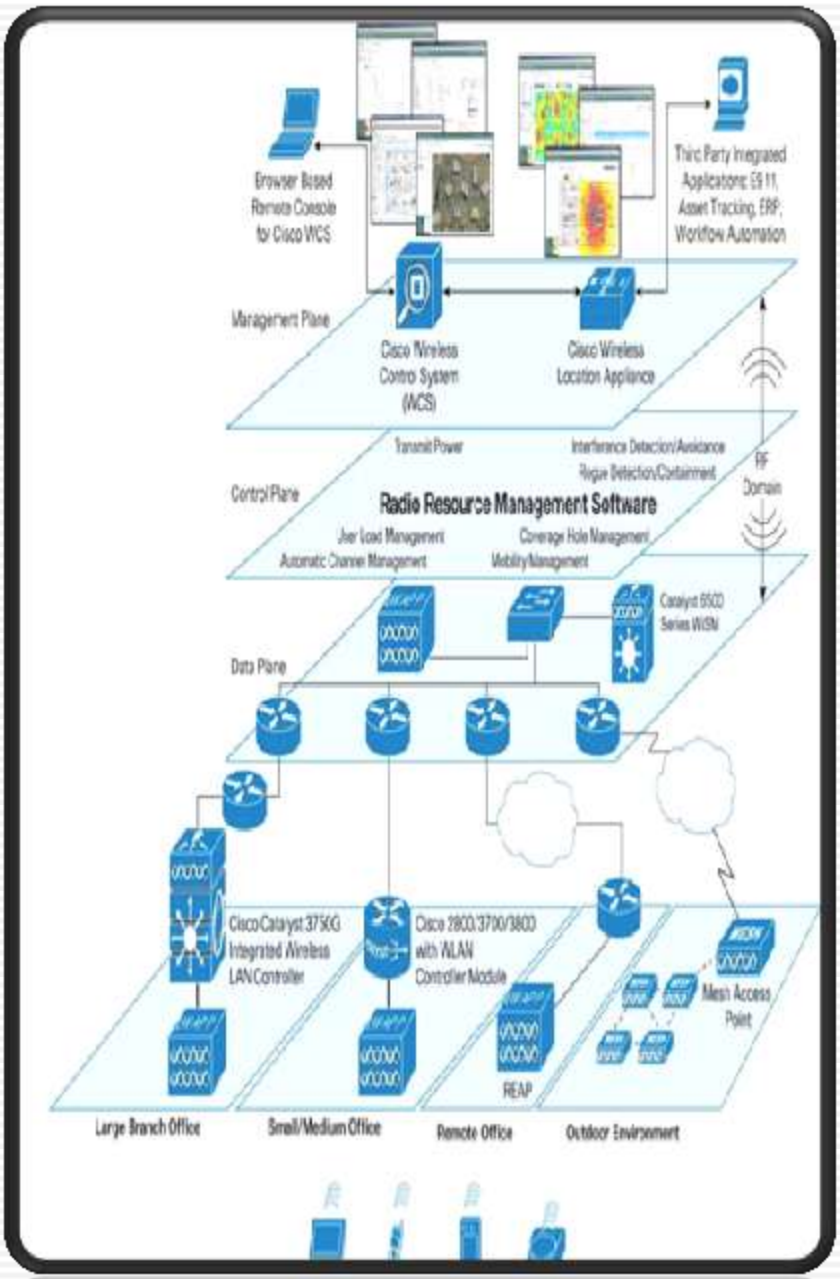
Wireless Product

المنتجات اللاسلكية هي ما نطلقه علي الأجهزة و البرمجيات اللاسلكية و التي تكون أساس عمل الشبكات

أما الأجهزة فتشمل أجهزة الأكسس بوينت Access Point و السويتشات اللاسلكية "الكنترولر" Wireless LAN Controller و أجهزة الحماية اللاسلكية و الهوائيات و الكروت اللاسلكية

أما البرمجيات فتشمل برمجيات المراقبة مثل Cisco Spectrum Intelligence و السيرفر WCS و برنامج الإدارة ADU و CNA

اذن فالمنتجات هي المكونات الملموسة و المرئية للشبكة اللاسلكية

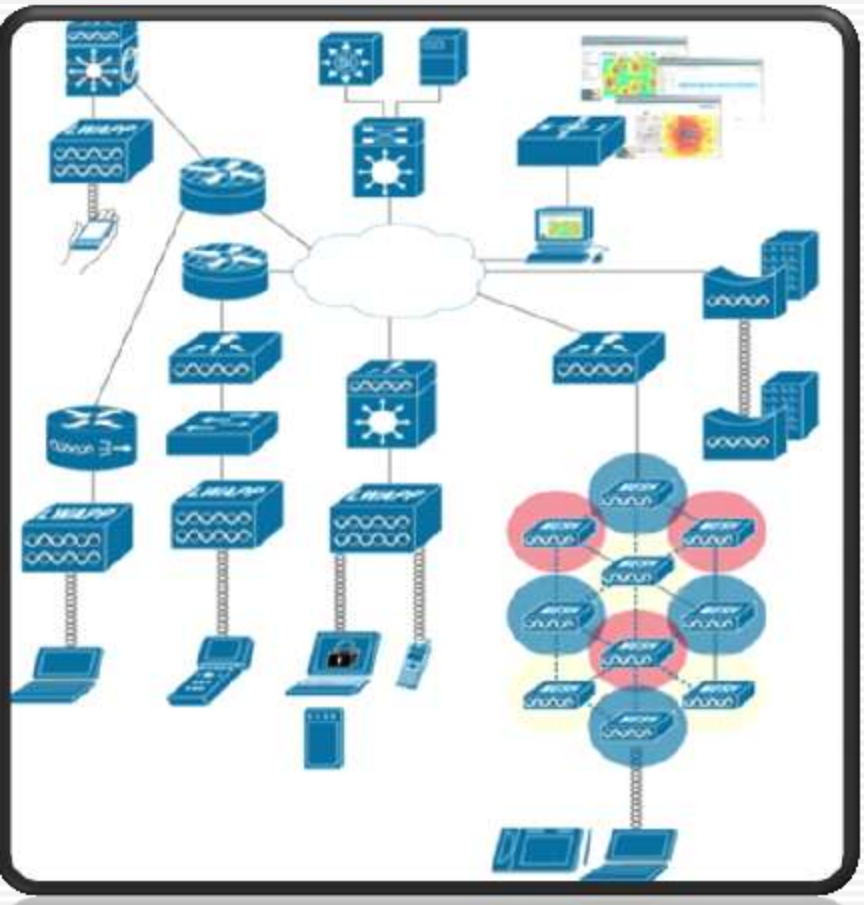


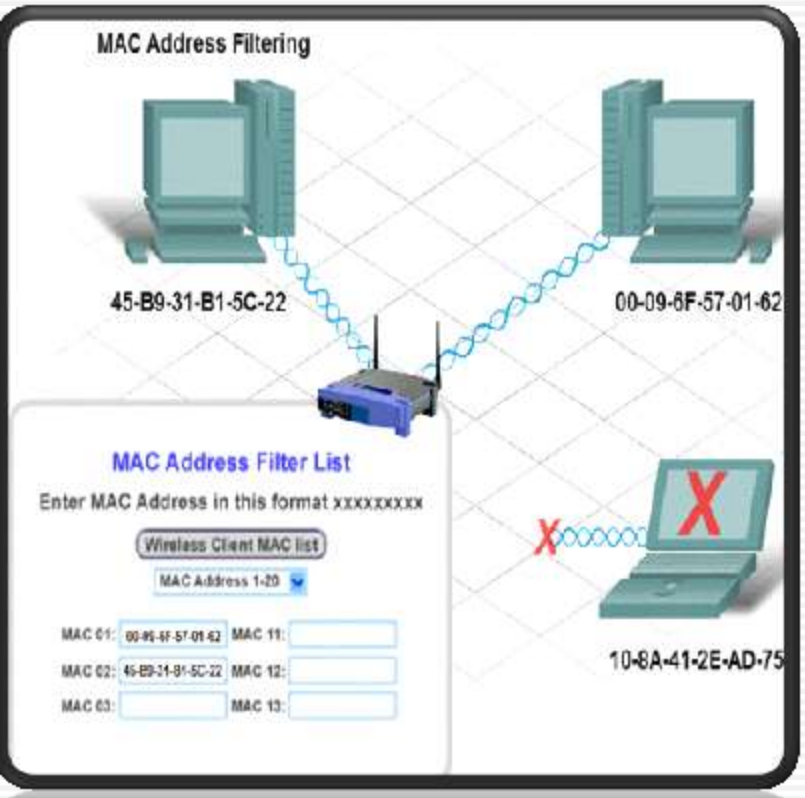
Wireless Services

الخدمات اللاسلكية هي اضافات للشبكات اللاسلكية تستطيع بها تحسين فاعلية الشبكة اللاسلكية مثل خدمات الصوت voice و التنقل Location و خدمات التأمين و خدمات الإنترنت و بالتالي فإن مدي انتاجية و فاعلية الشبكة تعتمد علي عدد الخدمات التي تدعمها

و كل خدمة تضاف في الشبكة تستلزم ايجاد معدات أخري في الشبكة فتستطيع أن تبدأ شبكتك اللاسلكية كشبكة نقل بيانات و تكون الأجهزة الأساسية فيها مثل كنترولر و أكسس بوينت و سيرفر WCSثم تضيف لها فيما بعد خدمة انترنت بإضافة رواتر أو مودم ثم تضيف لها خدمات VOIP بإضافة أجهزة هواتف متنقلة أو soft phone و تستطيع دعم الأمن في الشبكة بعمب سيرفر RADUIS و هكذا

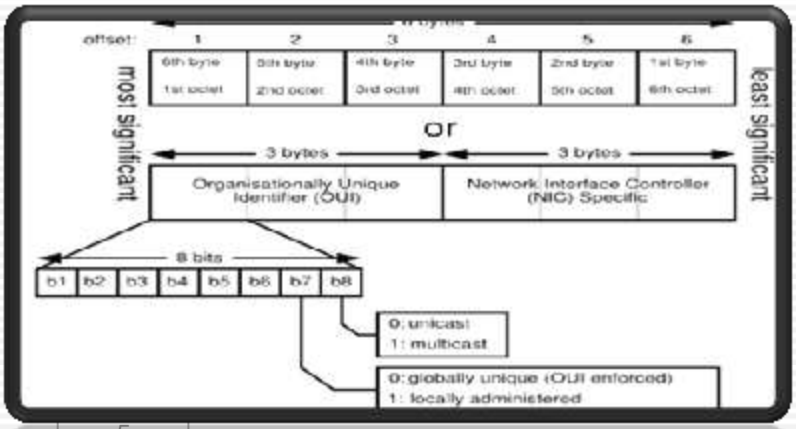
Wirelss Solution





أمن الشبكات اللاسلكية

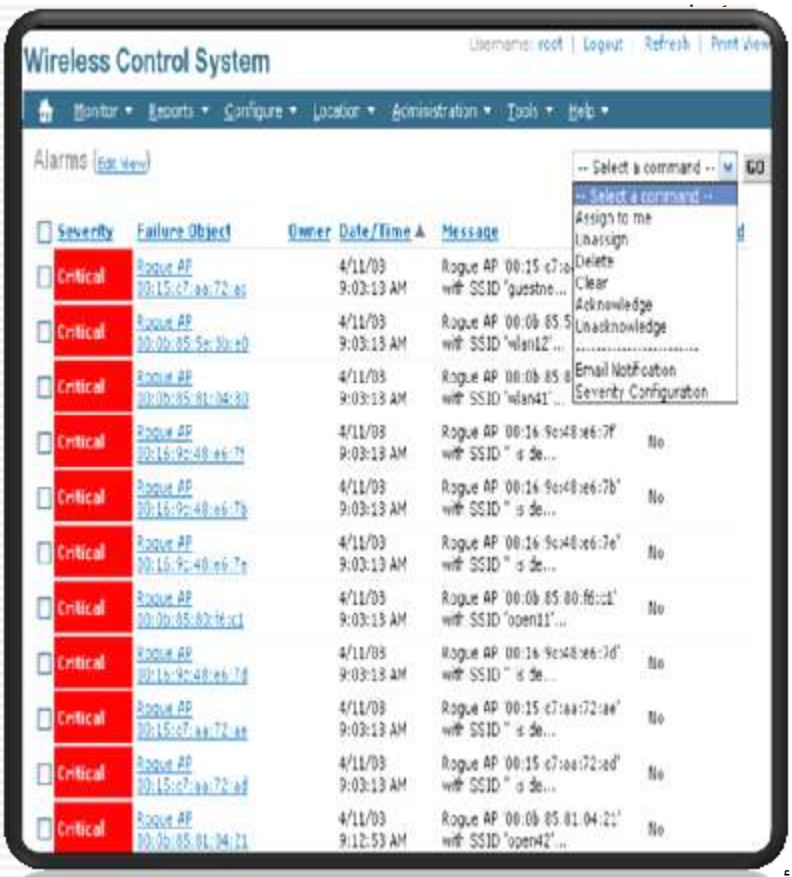
MAC Address Filtering



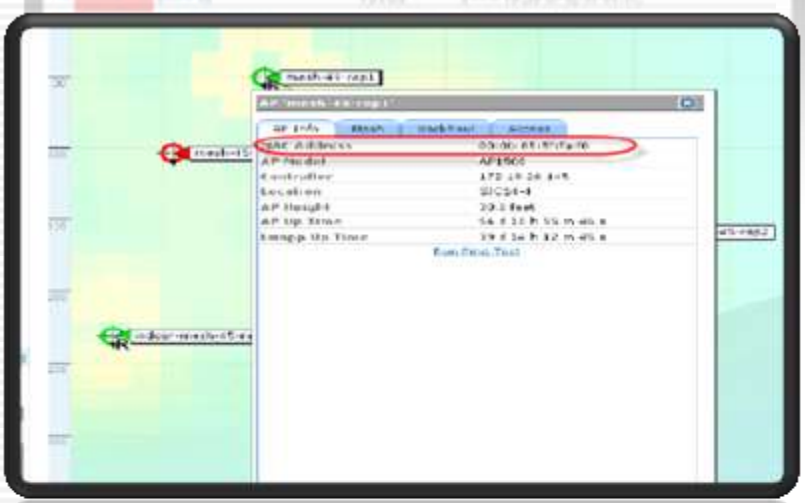
و لأن هذه العناوين فريدة فنستطيع في الشبكات اللاسلكية استخدامها في فلترة الأجهزة التي نسمح أو لا نسمح بدخولها للشبكة و هو ما يطلق عليه MAC Address Filtering و لكن لابد أولا من معرفة هذا العنوان

و لكن كيف تستطيع معرفة هذه العناوين

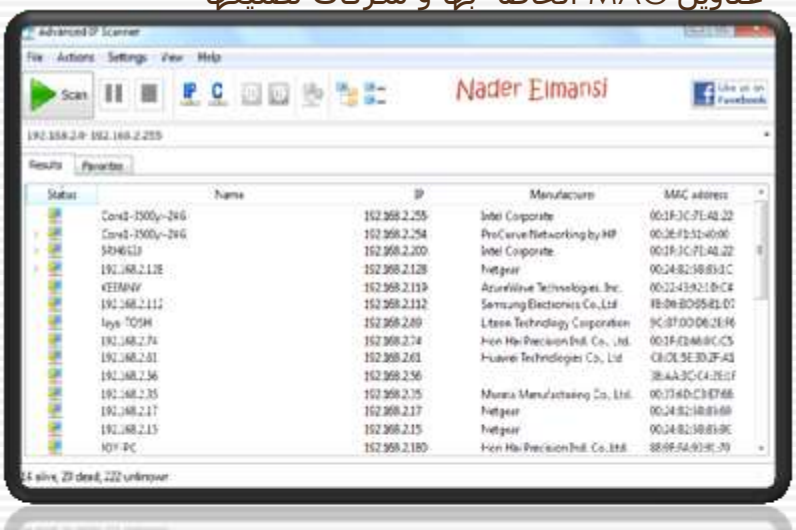
لدينا عدة طرق أولها في حال استخدام شبكات سيسكو اللاسلكية فإن سيرفر WCS يظهر لك الأجهزة الدخيلة Rogue بعناوينها الفيزيائية سواء كانت أكسس بوينت أخري أو كمبيوتر في شاشة الأحداث



أو في شاشة الخرائط هكذا



و هناك طريقة أخري لمعرفة هذه الأجهزة و ذلك باستخدام برمجيات البحث عن عناوين IP في الشبكة مثل Advanced IP Scanner و الذي تظهر الصورة التالية الأجهزة التي تشاركني الإتصال اللاسلكي مع بيان اسمها و عناوين MAC الخاصة بها و شركات تصنيعها

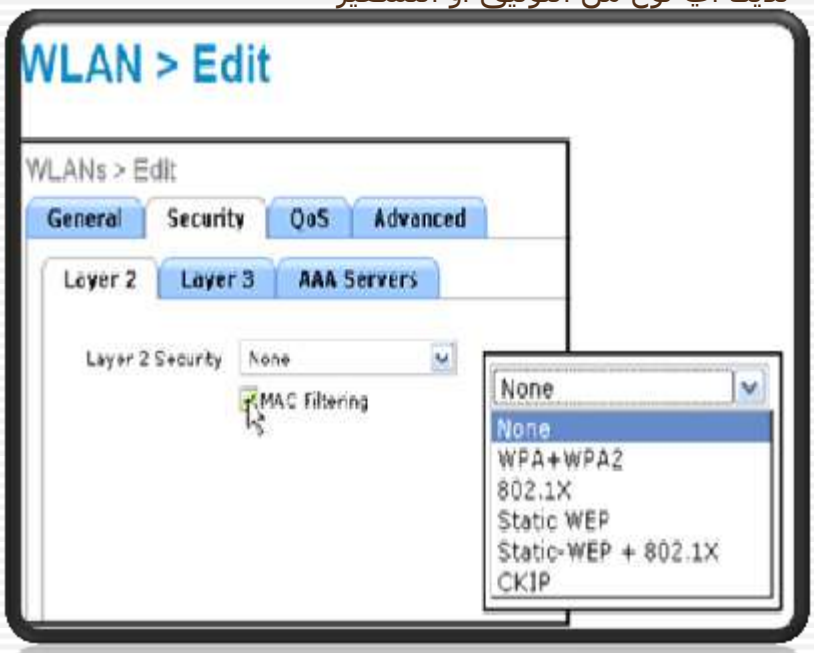


بعد جلبك لرقم الكارت الذي تريد منعه ادخل علي صفحة إدارة الأكسس بوينت الخاص بك ثم قم بإضافة العناوين التي تريد حجبها و هذه طريق عملها علي D-Link Access point

و كما تري فإن الأكسس بوينت منفردا لا يستطيع الا أن يحجب عشرين جهازا و هنا تأتي شبكات سيسكو اللاسلكية بجهاز الكنترولر الذي يستطيع أن يقوم بمركزية حجب 2500 عنوان سواء كان العنوان لجهاز كمبيوتر أو لأكسس بوينت أو أي جهاز لاسلكي يستطيع ولوج الشبكة و له عنوان فيزيائي

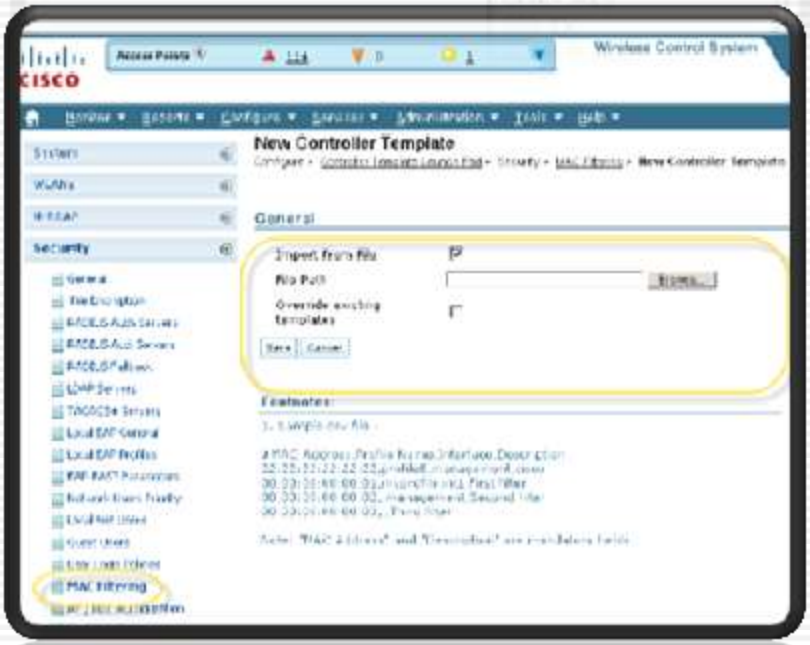
و يعيطك الكنترولر امكانية استخدام سيرفر مركزي لفلترة هذه العناوين باستخدام Raduis فقط ستدخل علي الكنترولر ثم ستتبع الصفحة Security > AAA > MAC Filtering الموجوده في الصورة و ستختار اماكن تواجد هذه العناوين و بالطبع سنجعلها local

بعدها نقوم بتفعيل هذا الأمر بالضغط علي الخيار MAC Filtering و ستضمن منع هذه الأجهزة حتي لو لم يكن لديك أي نوع من التوثيق أو التشفير

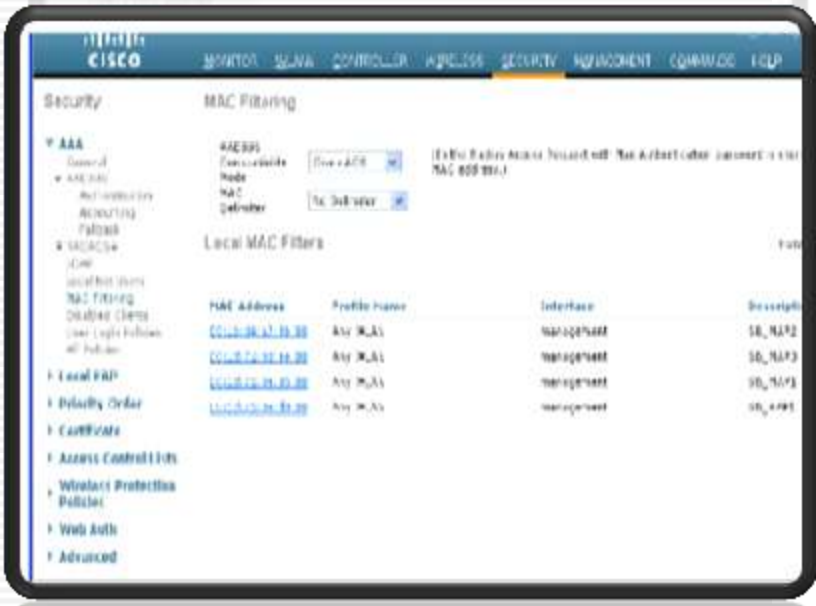


ثم تضغط علي New لإدخال العناوين التي تريدها مع امكانية وضع وصف لكل عنوان كما تري

تستطيع ايضا استخدام سيرفر WCS و تستطيع أن تقوم بتحميل ملف تعريف كامل بهذه العناوين



الآن لدينا قاعدة بيانات للعناوين كما تري



تقنيات و بروتوكولات لاسلكية

ثورة الربيع اللاسلكي

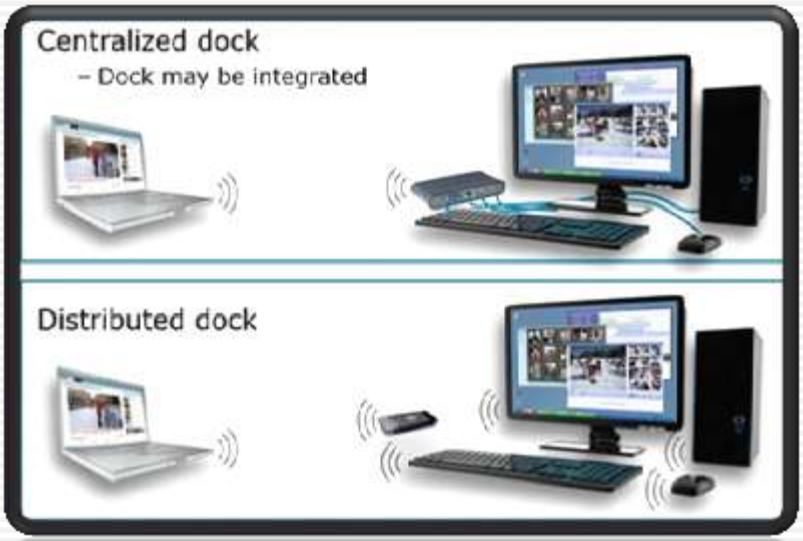
"انها الثورة الحقيقة في عالم الشبكات اللاسلكية "

كانت هذه هي الكلمات التي عبر بها رئيس منظمة WiGig Alliance لقناة BBC معبرا بكل حرفية عن التقنية اللاسلكية الجديدة – التي أسميها ثورة الربيع اللاسلكي" التي تم الإعلان عنها في 2009 و تم اكتمال مواصفاته في 2010 و صدقت مؤسسة WIFI عليه في 2011 ثم اطلق للاختبار في 2012 و اعتمدته الكثير من مصنعي الأجهزة مثل Intel. Dell, NEC, Nokia, Panasonic, Samsung, Toshiba, Nvidia, AMD, Texas Instruments, Atheros,

و بهذا يكون أسرع من المعيار 802.11n بعشر مرات و يعتبر هذا المعيار بهذه المواصفات جاهزا و بقوة لنقل بيانات الصوت و الفيديو بشكل كامل و هذه مقارنة بين عدة معايير حديثة لتستبين الفرق بينها

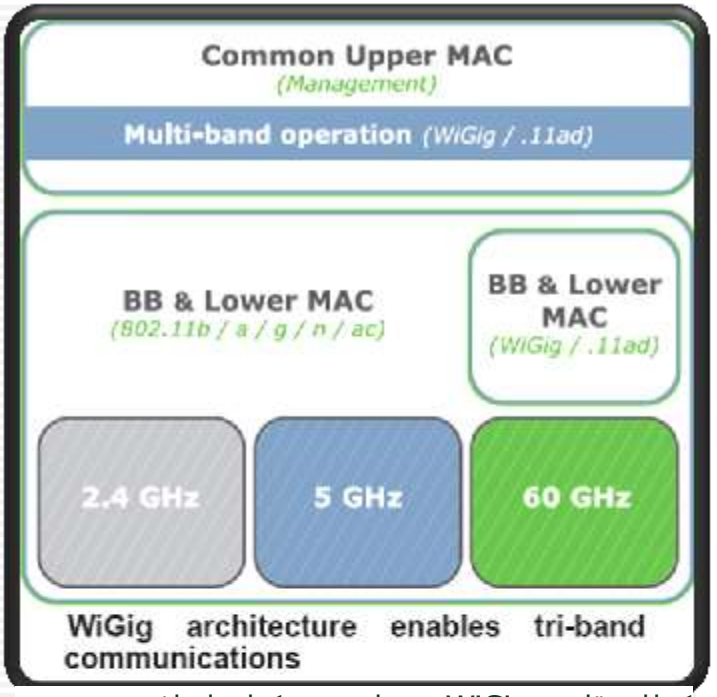
	802.11n	802.11ac	802.11ad
Throughput	600 Mbps	3.2 Gbps	Up to 7 Gbps
Coverage	Home, 70 m	Home, 30 m	Room, <5m
Freq. Band	2.4/5 GHz	5 GHz	2.4/5/60 GHz
Antennas	4 x 4 MIMO	8 x 8 MIMO	>10 x 10 MIMO
Applications	Data, Video	Video	Uncompressed Video

اذن فهو بديل مبهر للبلوتوث و IR و كل أنواع الإتصالات اللاسلكية التي تستخدم في حيز غرفة واحدة بل ان هذه السرعات تمهد للإستغناء عن اتصال بعض الأجهزة ببعض أجزائها و استبدال ذلك بهذا النوع من الإتصال مثل جهاز كمبيوتر تتصل ملحقاته I/O به لاسلكيا عبر هذا المعيار

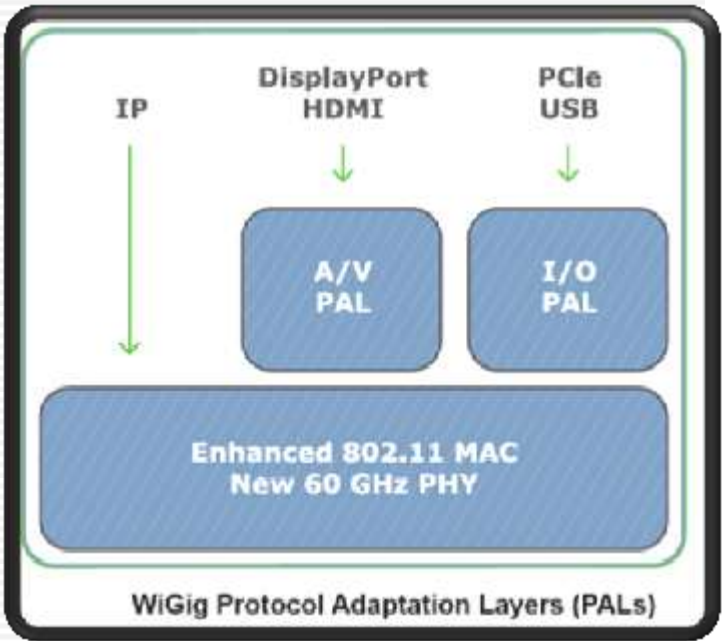


Structure WiGig

تعتمد بنية هذا المعيار علي نفس معايير الواي فاي حيث يتشابهان في Physical (PHY) و Medium Access Control (MAC) layers و هذا هو السبب في قدرة هذا المعيار علي دعم اتصال الأجهزة التي تتعامل بمعايير أخري معه

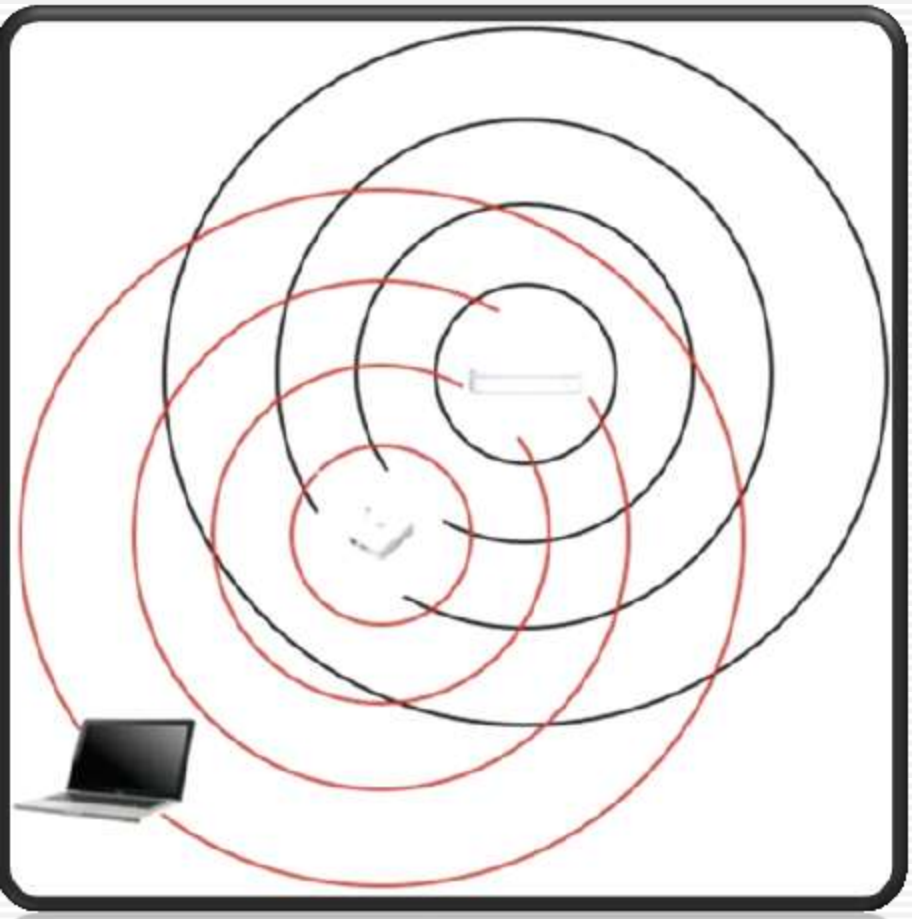


كذلك قام WiGig بعمل بروتوكول اضافي يسمي Protocol Adaptation Layers (PALs) ليسمح للأجهزة التي تستخدم الإتصال المرئي و الصوتي audio-visual (A/V) باستبدال مخارج HDMI و DisplayPort, input-output (I/O), USB , PCIe, التعامل لاسلكيا باستخدام هذا المعيار عبر التردد 60 GHz

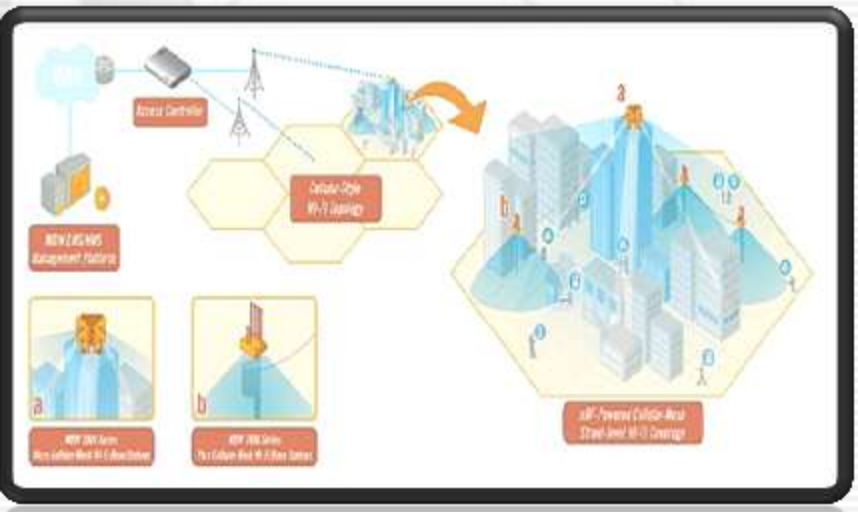


الهندسة اللاسلكية

الخلايا اللاسلكية و التغطية

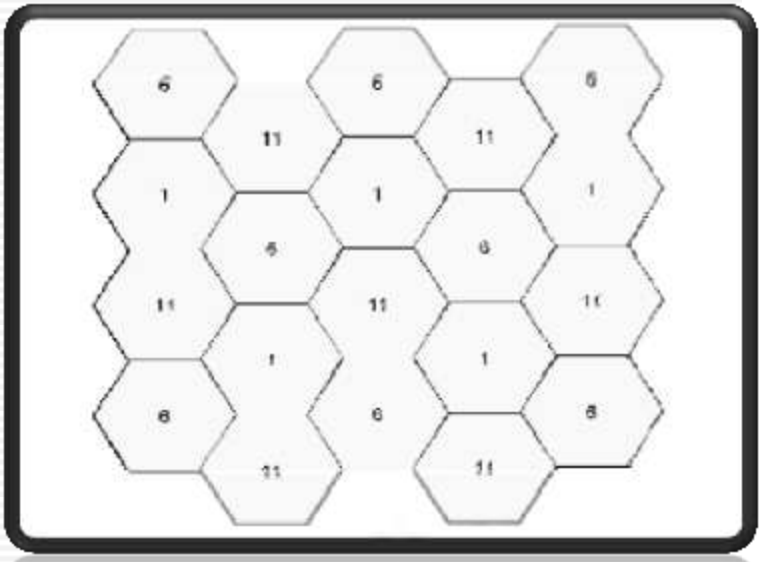


وقد قاموا ايضا بتسمية كل نطاق يستخدم نفس القناة CELL اي خليه واعتمدوا الشكل الدائري أو السداسي ويكون شكل الخلايا متجاورا كما يشبه شكل خلايا النحل

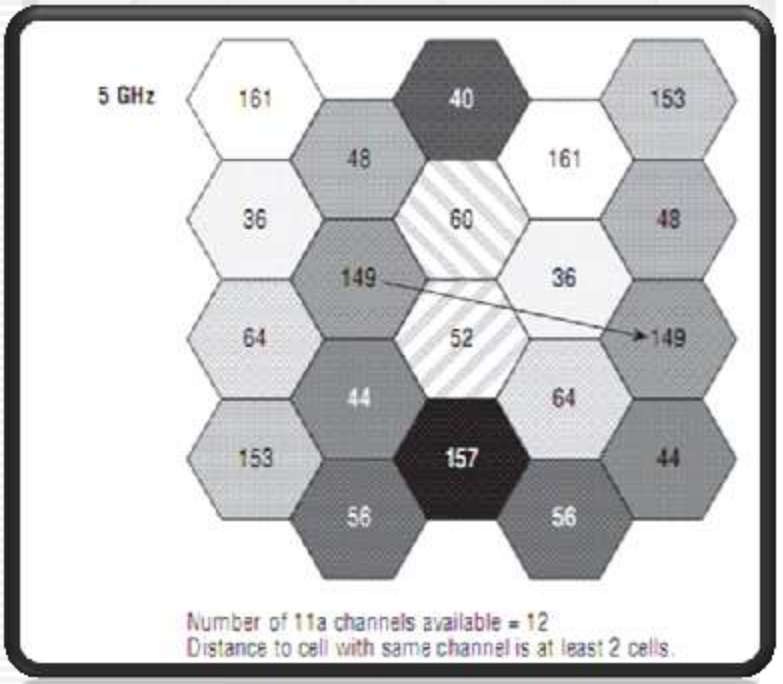


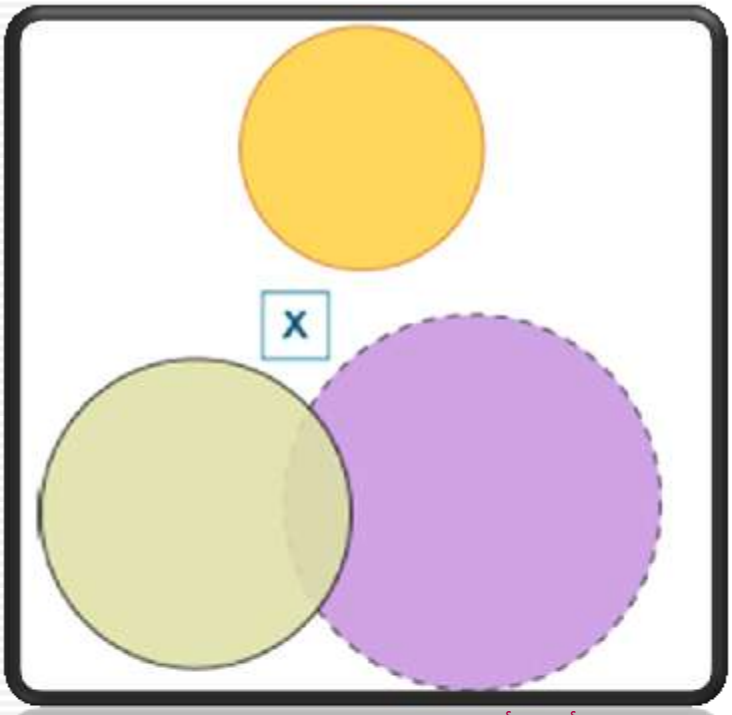
و لكن عندما تريد أن توسع شبكتك ستحتاج بالتالي الي اكثر من اكسس بوينت ولابد ان تكون هذه الأجهزة في نفس الشبكة وتتخاطب فيما بينها بشكل عادي ولكن الحقيقة أنك ستعاني من التداخل في حال لو كان هناك جهازين اكسس بوينت او اكثر يعملان بنفس تردد القناة فمن أكبر الأخطاء عند تصميم شبكتك اللاسلكية هي استخدام نفس القناة channelفي كل الأكسس بوينت هذا سيسبب تداخل

802.11b / g			
رقم القناة	التردد المركزي (غيغاهرتز GHz)	رقم القناة	التردد المركزي (غيغاهرتز GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467
6	2.437	13	2.472
7	2.442	14	2.484

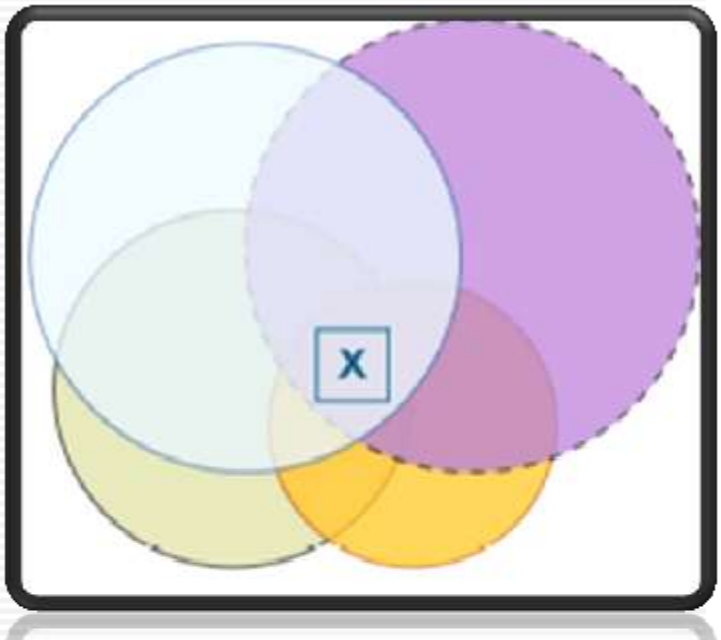


وسيكون ايضا 802.11 a هكذا



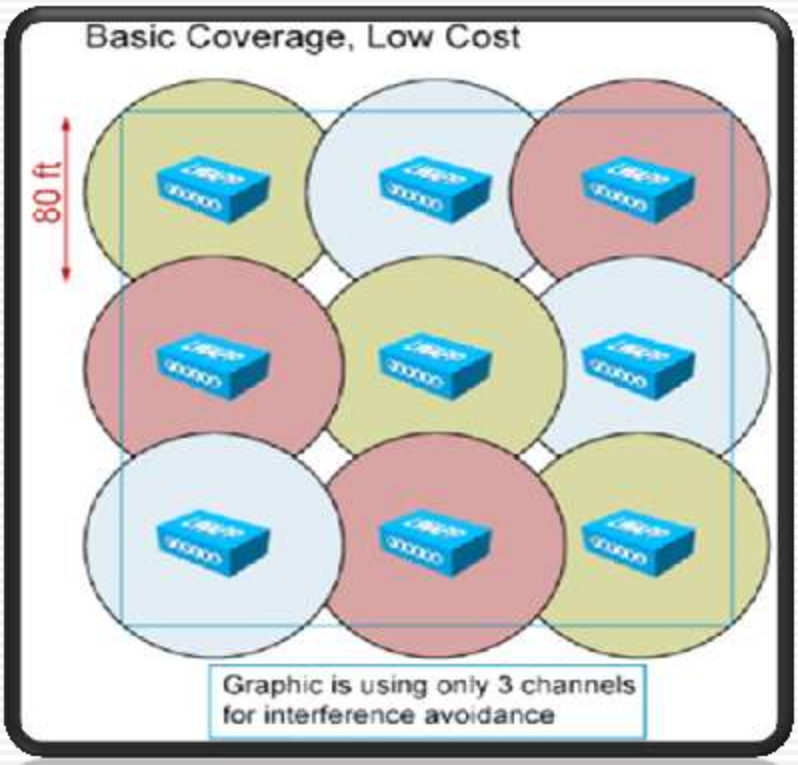


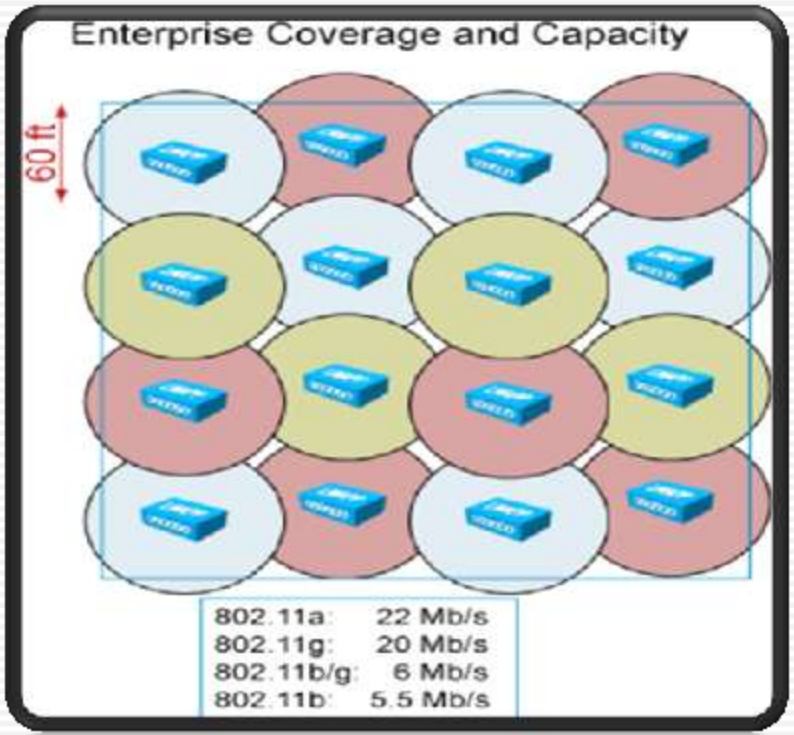
لا تقتصر أيضا أخطاء توزيع الخلايا علي وجود فجوات فالعكس قد يسبب أيضا مشاكل و ذلك عندما يكون التداخل overlap بين الخلايا أكبر مما ينبغي فيحدث اتصال بين خليتين تعملان بنفس التردد و علي نفس القناة و هنا يحدث شوشرة و خطأ في اتصال أي جهاز في الخليتين



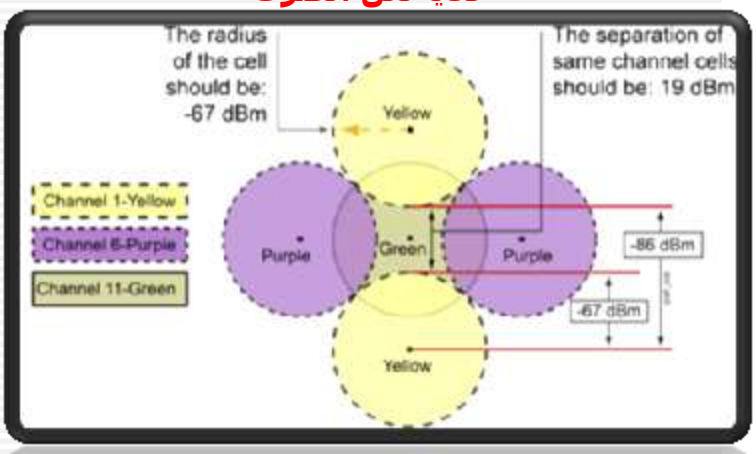
و بناء علي ذلك فعند تصميم شبكة لاسلكية فإن لدينا نموذجين للتصميم أولهما basic coverage و الثاني higher coverage

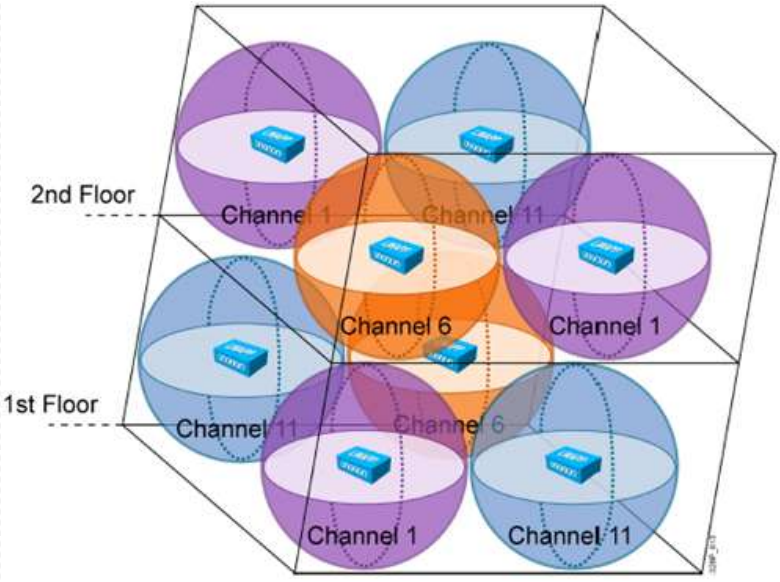
و يعتبر basic coverage قليل التكلفة لاستخدام اقل الأجهزة الممكنة للتغطية إلا أن ذلك يتطلب التأكد من عمل كل الأجهزة لأن فشل أحدها يعني فصل الشبكة في هذه الخلية و وجود فراغ في عملية roaming و ذلك لكبر قطر الخلية كما تري في الشكل التالي

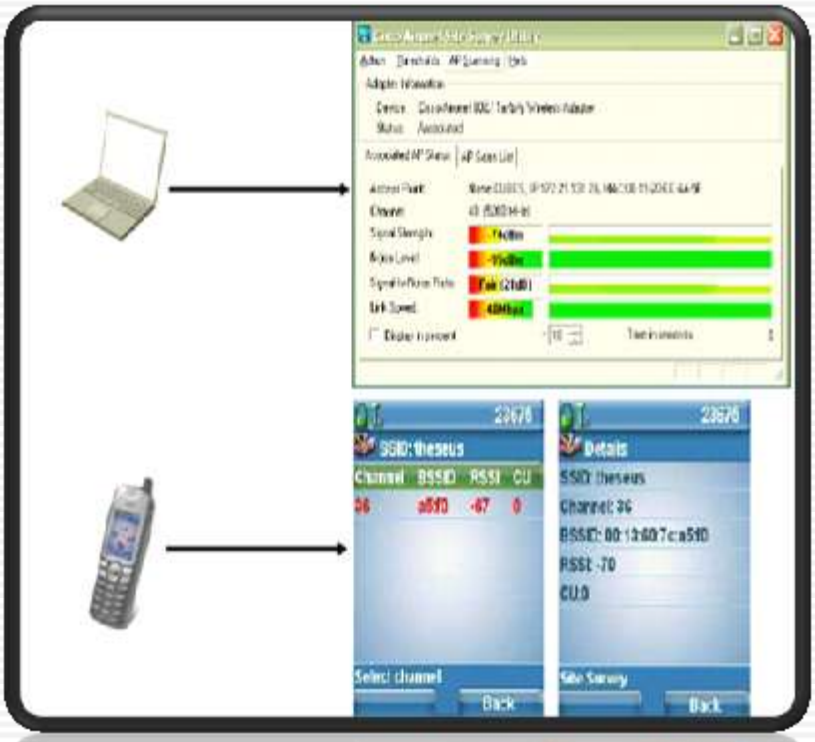




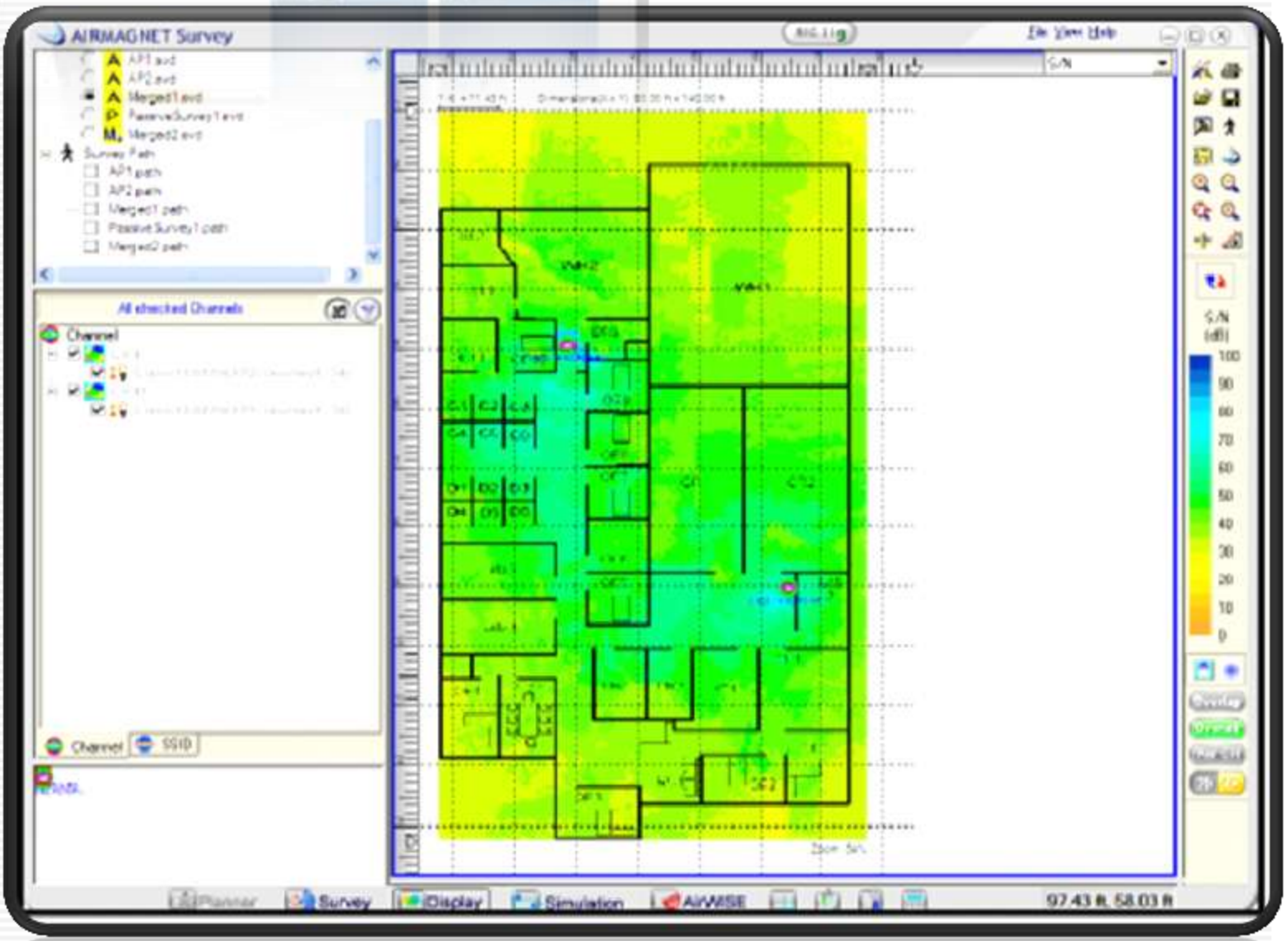
خلايا نقل الصوت

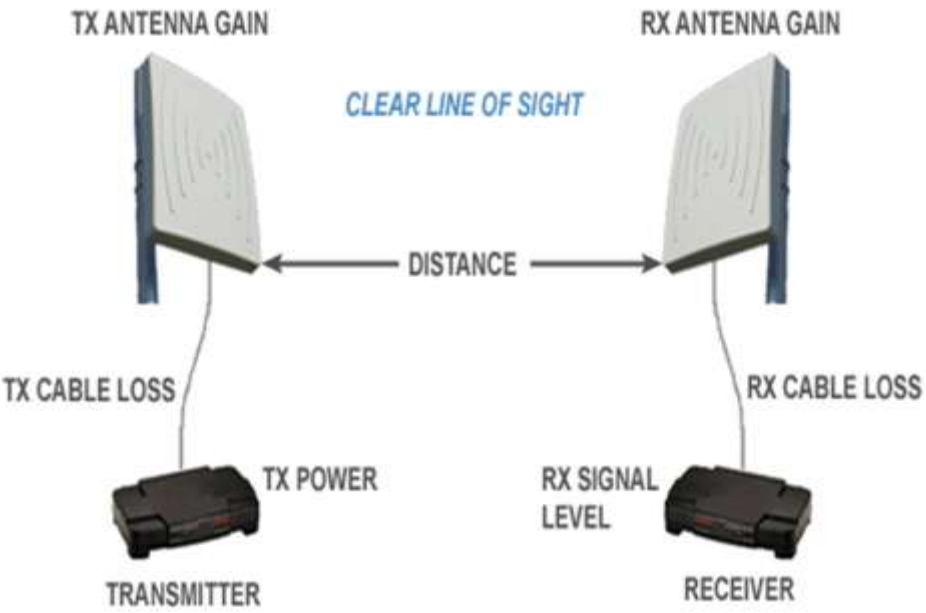






تستطيع أيضا برمجيات مثل cisco ADU ان تقوم بحسابات SNR و RSSI للاشارة و بيان سرعة الإتصال و غيره

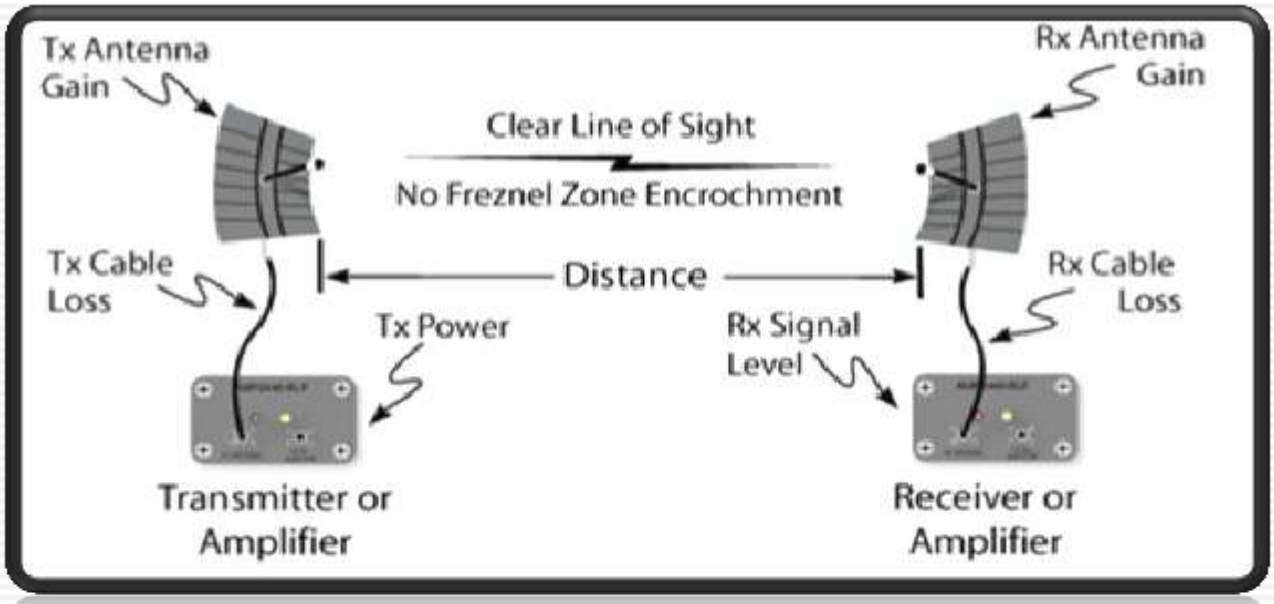




المصطلح budget يعبر بشكل عام عن مدي التحكم في المصادر أو الميزانية مثل ميزانية مشروع أو ميزانية شركة و غيرها و قبل أن تبدأ مشروع ما لابد ان تغطي ميزانيتك تكاليف هذا المشروع و الا فإنك لن تستطيع أن تصل لنهاية المشروع أو تتمه

تعتبر حسابات SOM من الحسابات التي تتم غالبا في الشبكات اللاسلكية الخارجية حيث أنها تعتمد علي الإتصال المباشر direct line of sight علي عكس الشبكات اللاسلكية الداخلية و تستطيع استخدام هذه الصفحة في تلك الحسابات ببساطة جدا "اضغط علي الصورة"

و الشكل التالي يبين اماكن تواجد الفقد و الكسب علي طول مخطط الإشارة



و الشكل التالي يبين اماكن تواجد الفقد و الكسب علي طول مخطط الإشارة

و هذا مثال للحسابات المستخدمة

$$Free\ Space\ Loss = 20Log_{10}(MHz) + 20Log_{10}(Distance\ in\ Miles) + 36.6$$

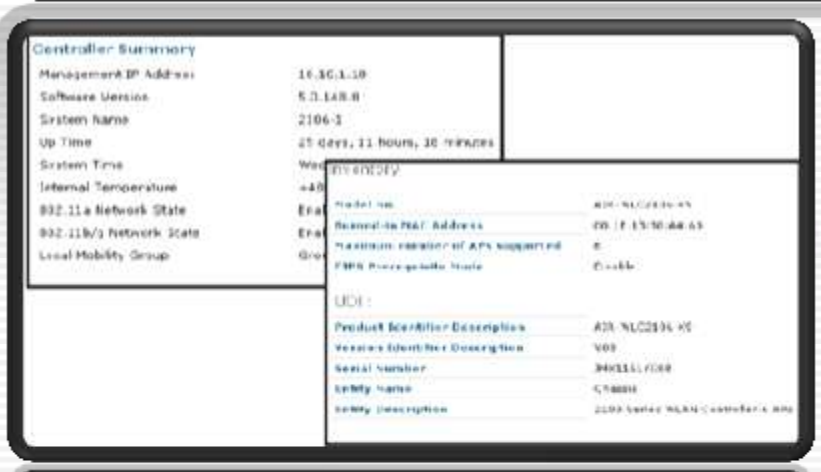
$$Rx\ Signal\ Level = Tx\ Power - Tx\ Cable\ Loss + Tx\ Antenna\ Gain - FSL + Rx\ Antenna\ Gain - Rx\ Cable\ Loss$$

$$SOM = Rx\ Signal\ Level - Rx\ Sensitivity$$

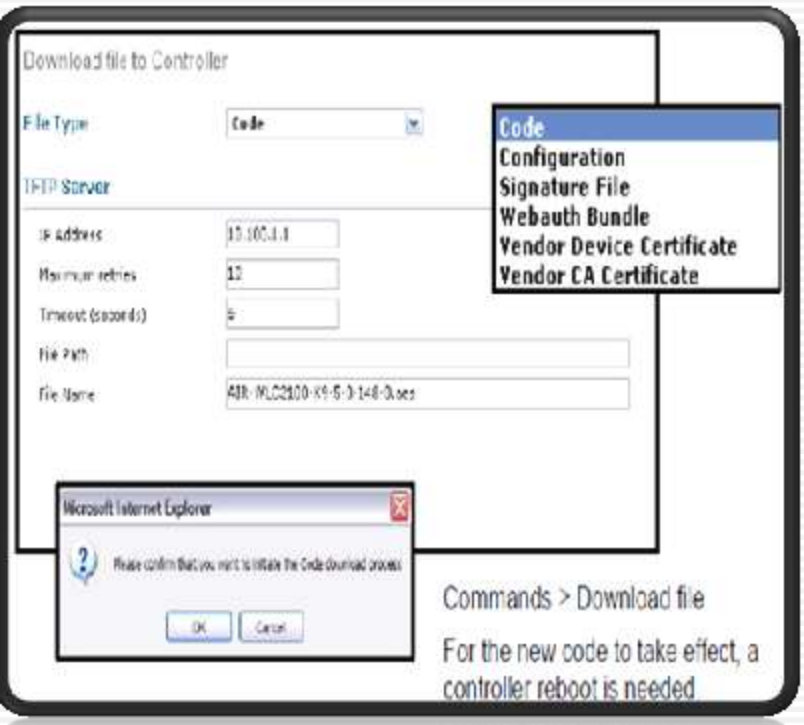
و الشكل التالي يبين اماكن تواجد الفقد و الكسب علي طول مخطط الإشارة


UPGRADE NOW

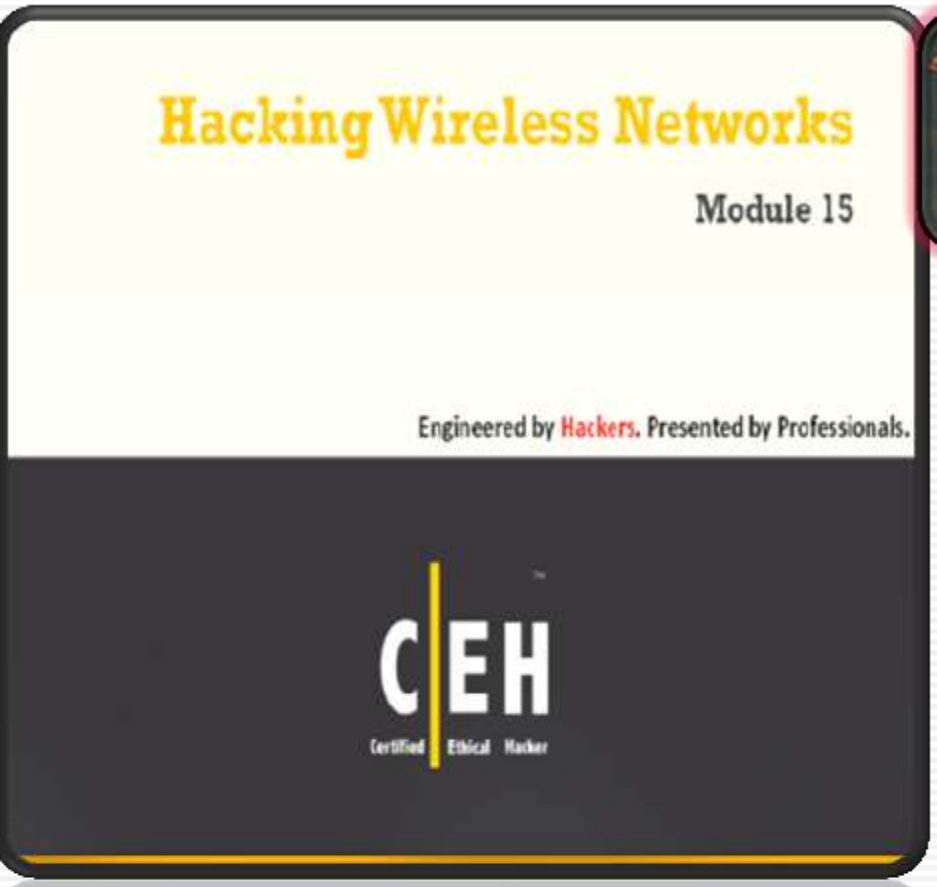

العبادة اللاسلكية
Controller Code Upgrade


Controller Summary
Management IP Address
Software Version
System Name
Up Time
System Time
Internal Temperature
802.11a Network State
802.11b/g Network State
Local Mobility Group
Inventory
UDI :
Product Identifier Description
Version Identifier Description
Serial Number
Entity Name
Entity Description


All APs > Details
General
Inventory
Advanced
Product ID
Version ID
Serial Number
Entity Name
Entity Description
Certificate Type
H-REAP Mode supported
Cisco AP
Cisco Wireless Access Point
Manufacture Installed
Yes
Versions
Software Version
Boot Version
IOS Version
Mini IOS Version
IP Config
IP Address
Static IP

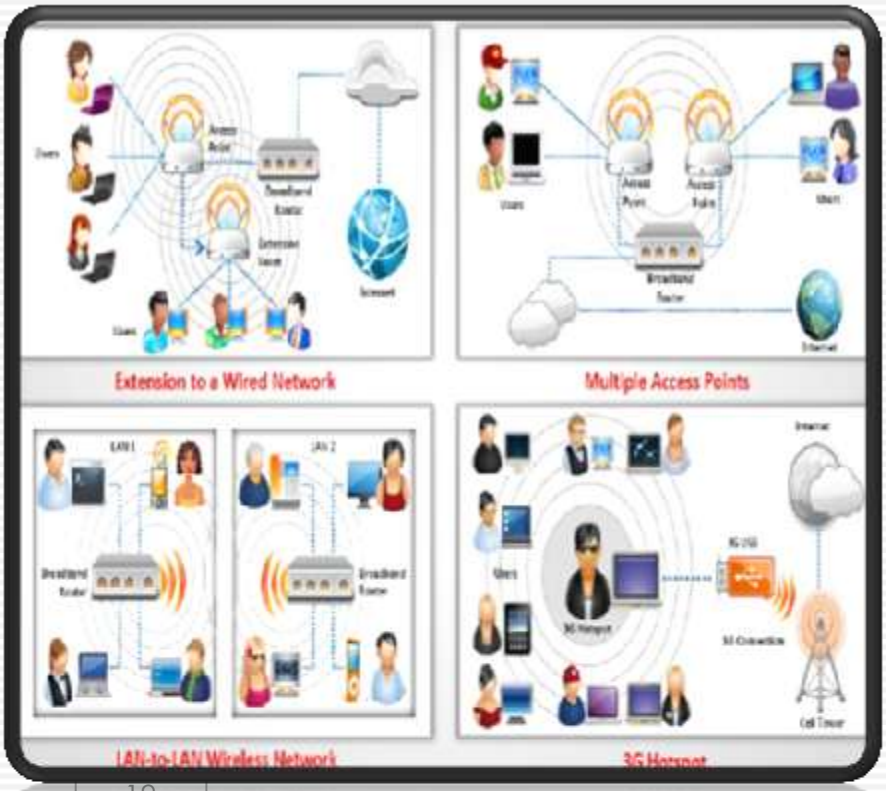

Download file to Controller
File Type
Code
TFTP Server
IP Address
Maximum retries
Timeout (seconds)
File Path
File Name
Code
Configuration
Signature File
Webauth Bundle
Vendor Device Certificate
Vendor CA Certificate
Microsoft Internet Explorer
OK
Cancel
Commands > Download file
For the new code to take effect, a controller reboot is needed

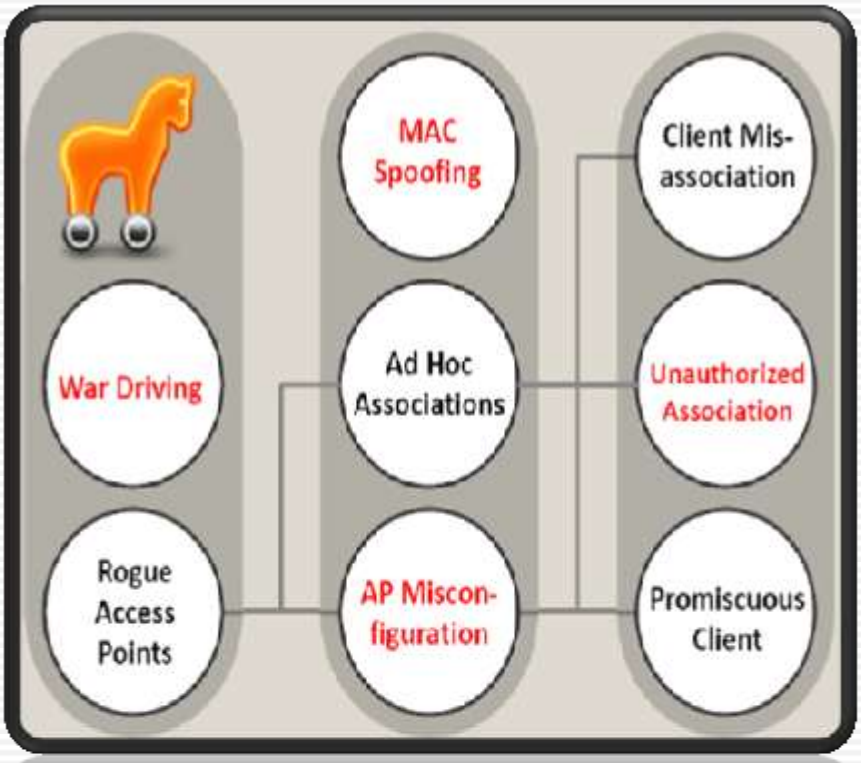

Download file to Controller
File Type
Code
TFTP Server
IP Address
Maximum retries
Timeout (seconds)
File Path
File Name
Code
Configuration
Signature File
Webauth Bundle
Vendor Device Certificate
Vendor CA Certificate
Microsoft Internet Explorer
OK
Cancel
Commands > Download file
For the new code to take effect, a controller reboot is needed.



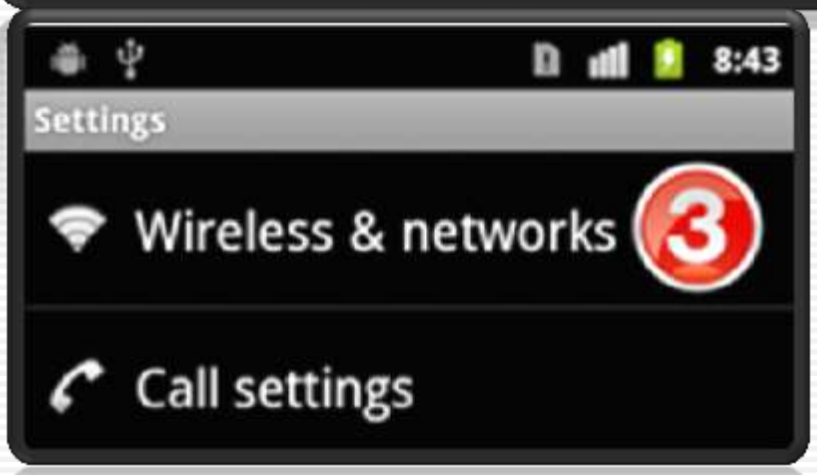
رحلتي مع كتاب
اختراق الشبكات اللاسلكية

يبدأ هذا الفصل بمقدمة سريعة عن الهدف من هذا الفصل و يبين أن ربع الشبكات اللاسلكية تقريبا لا تحتاج اختراق لأنها مفتوحة و الربع الآخر يتم تشفيرها بشكل بسيط و يتكلم الباب عن هذه العناوين

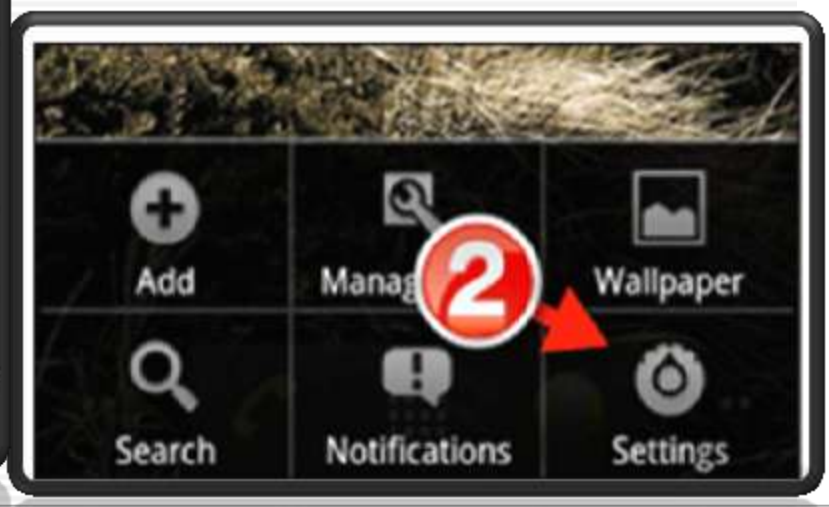



MAC Spoofing
Client Mis-association
War Driving
Ad Hoc Associations
Unauthorized Association
Rogue Access Points
AP Miscon-figuration
Promiscuous Client


WEP
WPA
WPA2
WPA2 Enterprise
TKIP
AES
EAP
LEAP
RADIUS
802.11i
CCMP



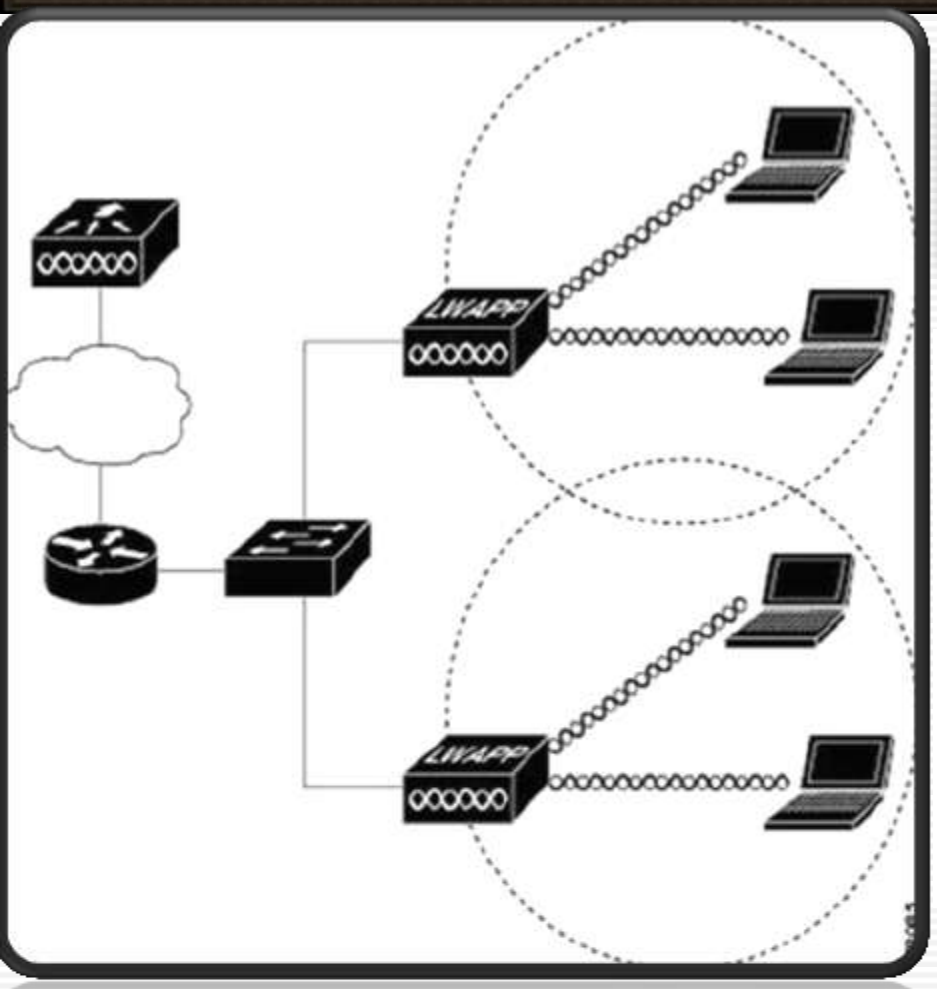
و ستجد العديد من خيارات الإتصال بالإنترنت السلكية و اللاسلكية مثل هذه



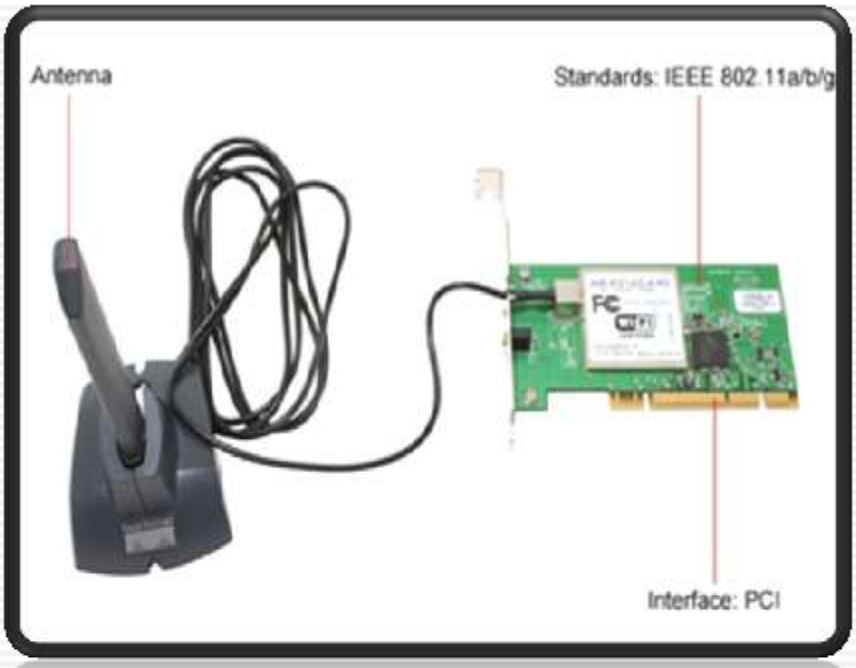
و عند اختيار أحد هذه الشبكات المشفرة لابد من إدخال كلمة تشفير

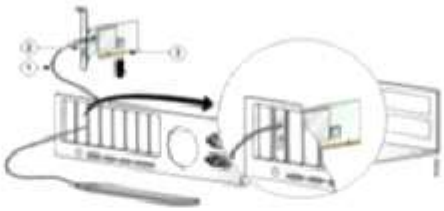
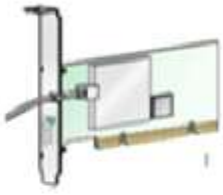
ستظهر الشاشة التالية و في حال كنت تريد أن تجعل جهاز نقطة اتصال لاسلكية لأكثر من شخص فقم باختيار Portable WI-FI hotspot

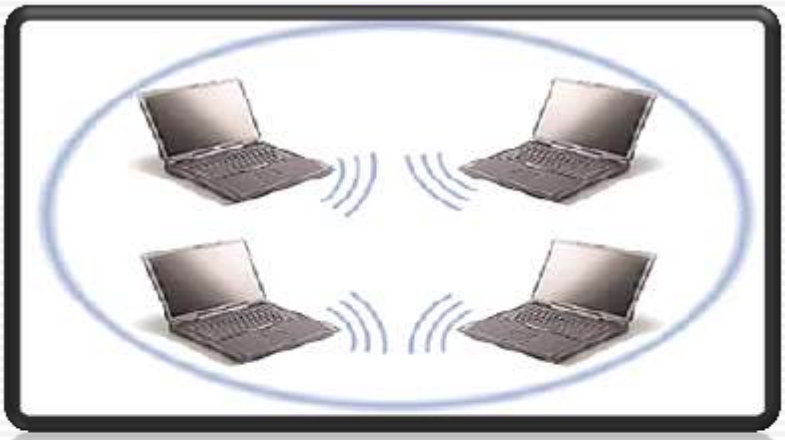
ثم قم بإعداد اسم الشبكة و نوع التأمين مع العلم أن هذه الطريقة تصلح لمشاركة الإنترنت بين ثماني أشخاص فقط

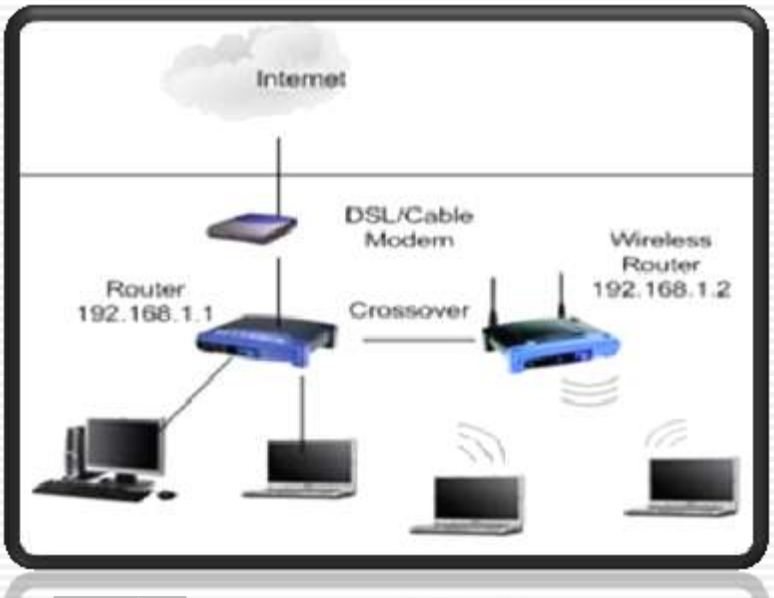


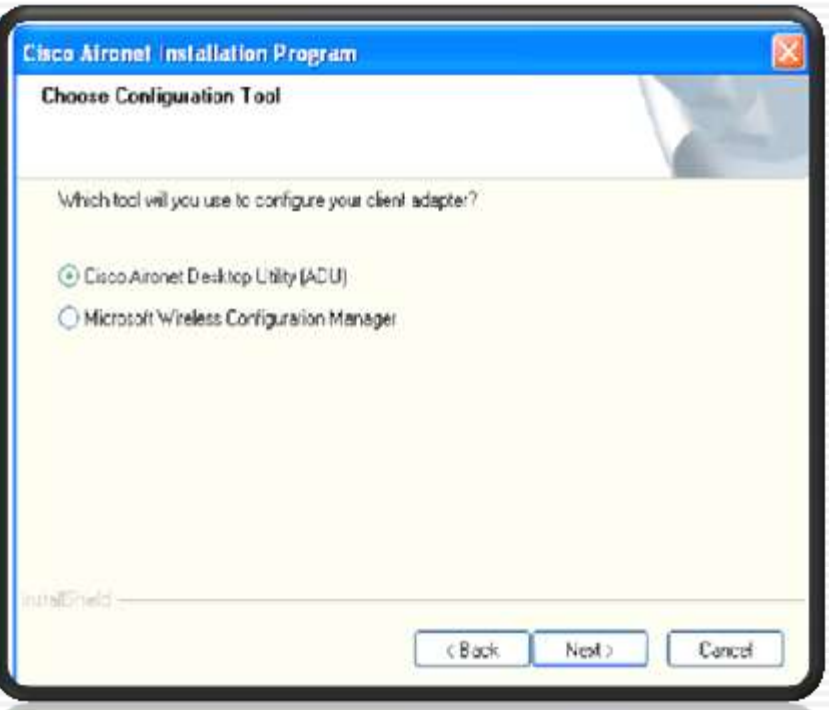
17 سؤال و جواب عن Lightweight Access Point



Client Adapter	Model Number	Description	Illustration
PC-Cardbus card	AIR-CB21AG		
PCI card	AIR-PI21AG		

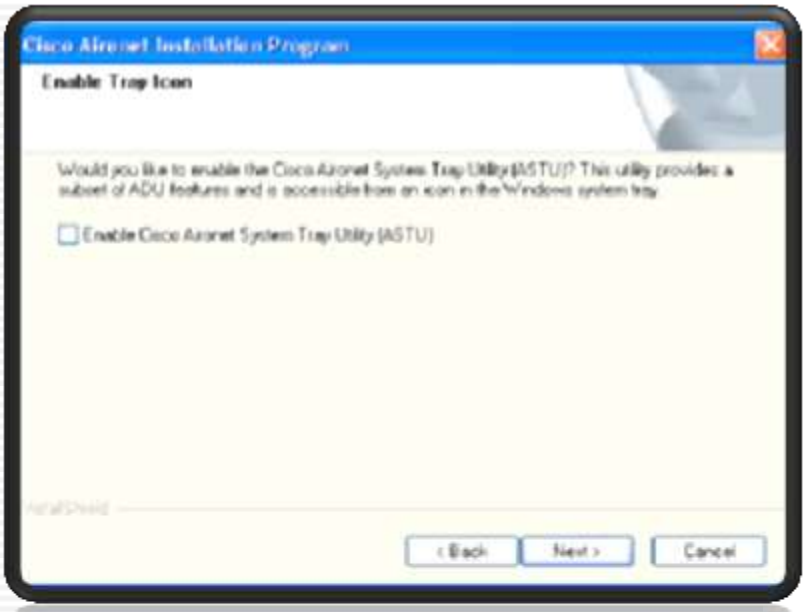



Internet
DSL/Cable
Modem
Wireless
Router
192.168.1.2
Router
192.168.1.1
Crossover

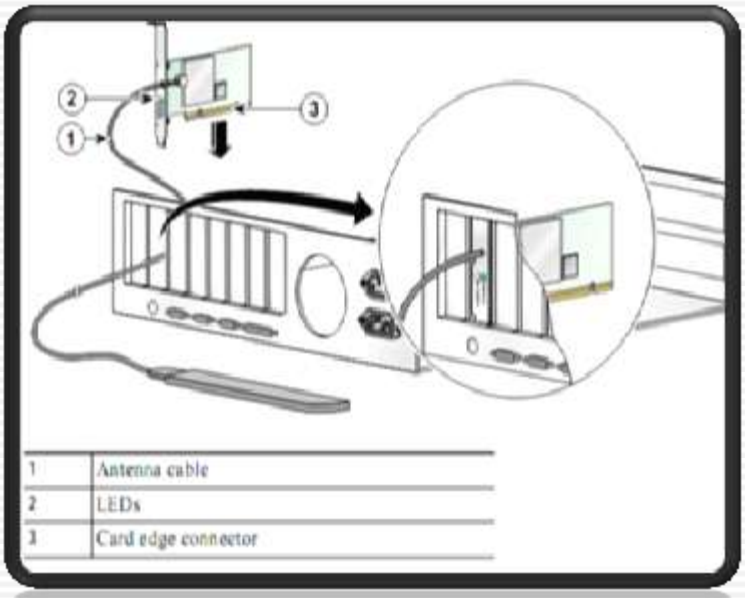


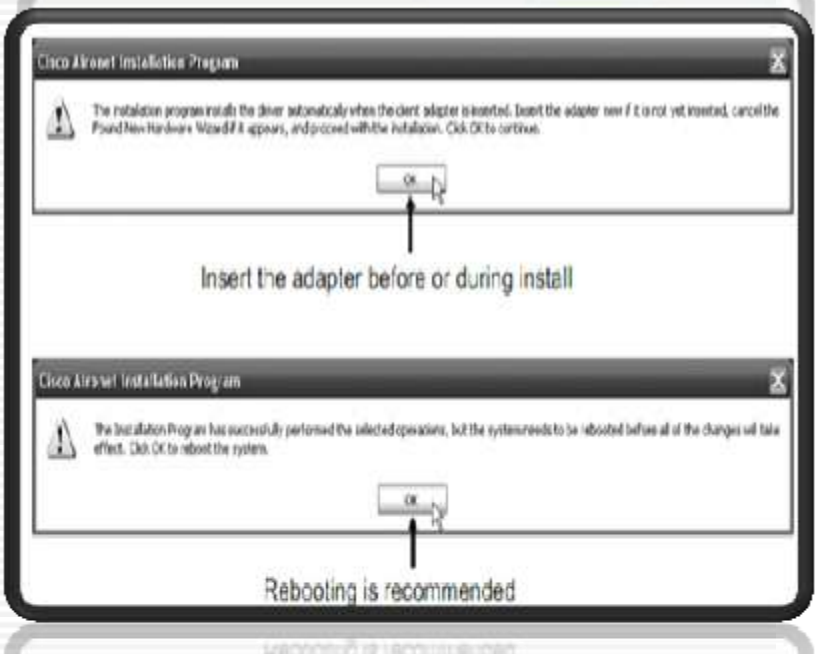
Feature	Windows XP	ADU
Configuration parameters	Limited	Extensive
Capabilities		
Create profiles	Yes	Yes
Enable/disable radio	No	Yes
Security		
Static WEP	Yes	Yes
LEAP authentication with dynamic WEP	No	Yes
EAP-TLS or PEAP authentication	Yes	Yes
Status window	Limited	Extensive
Statistics window (transmit & receive)	No	Yes

اذا اردت أن تباشر عملك من خلال أيقونة علي شريط المهامك فقم بالتأشير علي ASTU و بعد هذه الخطوة سيتم اخبارك بإدخال Cardbus اذا كنت تستعمله بدلا من PCI

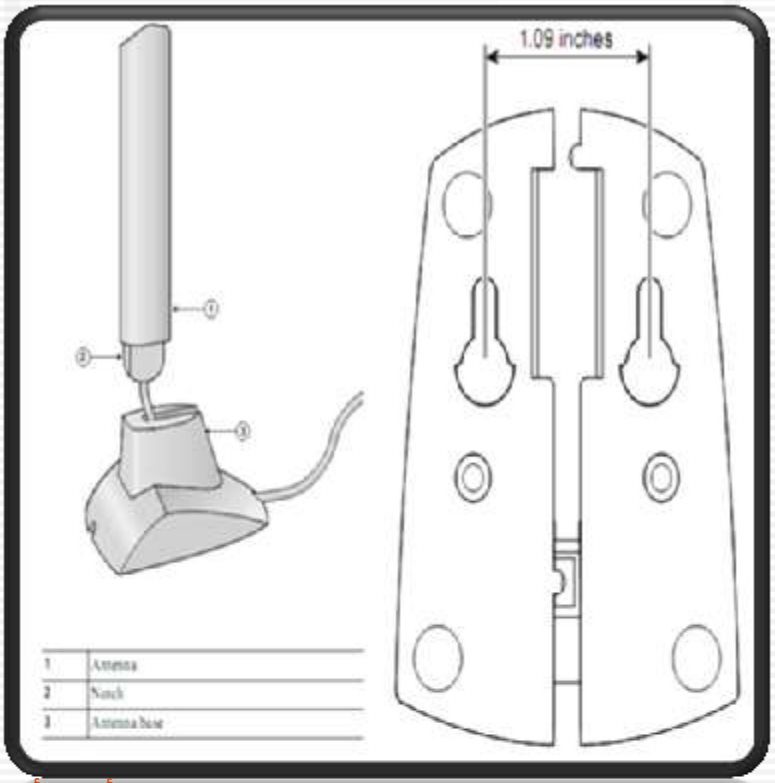


و اذا كنت ستستعمل PCI فانتظر حتي يتم اعادة تشغيل الكمبيوتر لوضعه داخل الجهاز و هذه هي طريقة وضع كارت PCI مع ملاحظة الهوائي و سلكه بالشكل الذي تراه

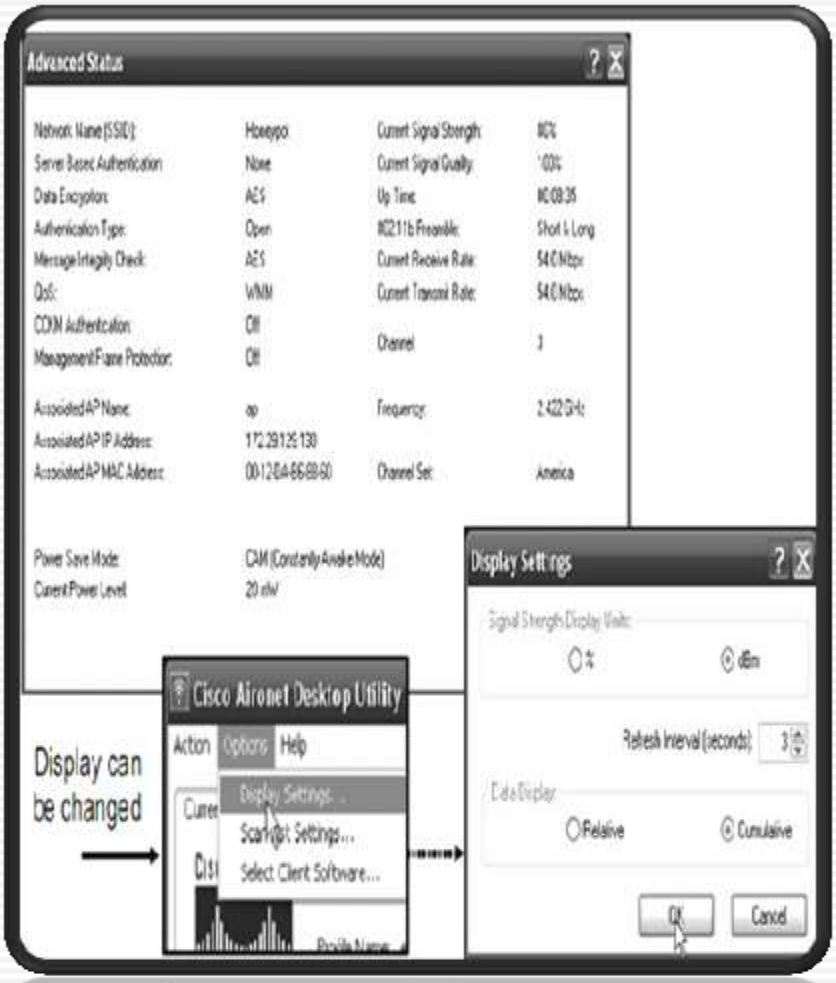


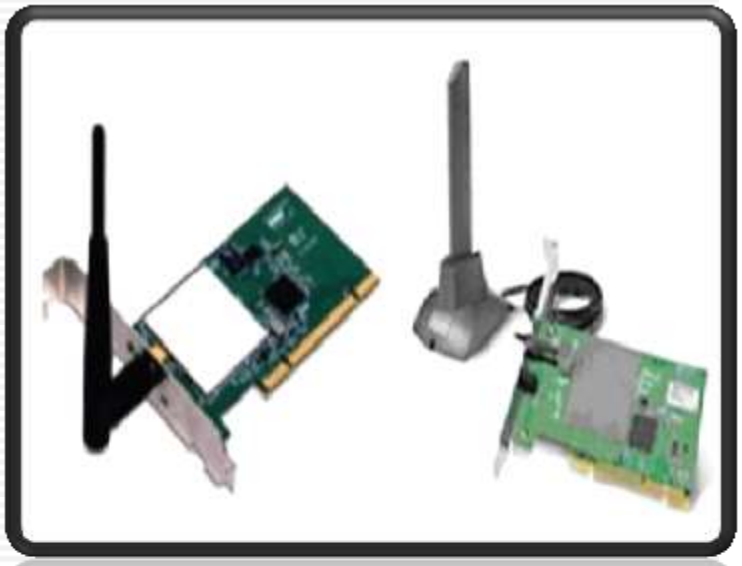


يأتي مع الهوائي قاعدة لتثبيته علي الحوائط أو النضد مع مسمارين و سلك لربط الهوائي بالكارت اللاسلكي

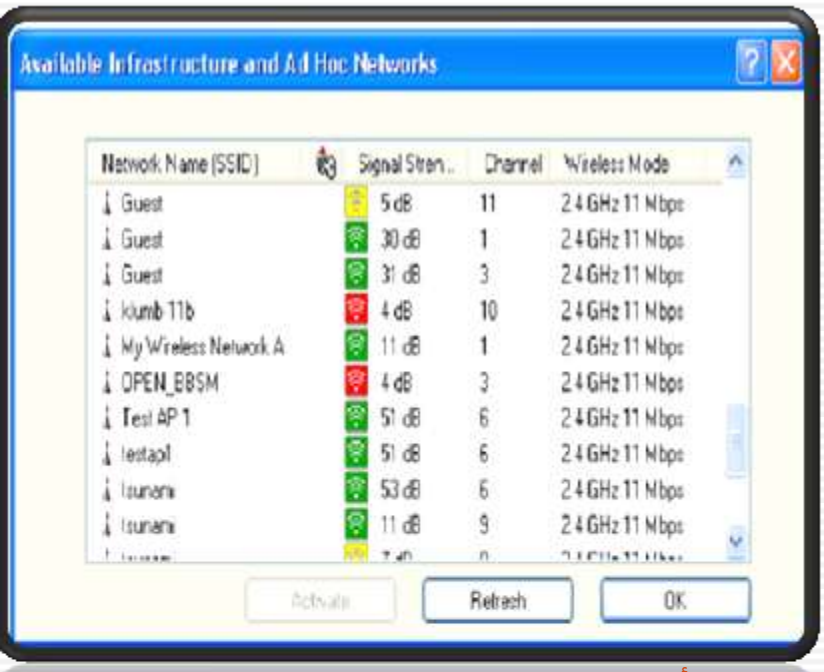


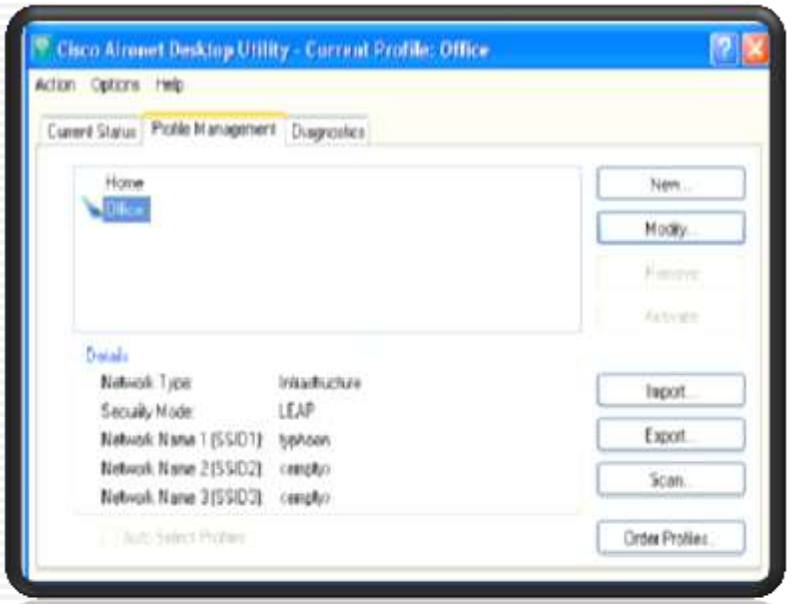
و عند تثبيت الهوائي تستطيع تعديل وضعه أفقيا أو رأسيا كما تري


Advanced Status
Network Name (SSID):
Server Based Authentication:
Data Encryption:
Authentication Type:
Message Integrity Check:
QoS:
CCKM Authentication:
Management Frame Protection:
Associated AP Name:
Associated AP IP Address:
Associated AP MAC Address:
Power Save Mode:
Current Power Level:
Current Signal Strength:
Current Signal Quality:
Up Time:
802.11b Preamble:
Current Receive Rate:
Current Transmit Rate:
Channel:
Frequency:
Channel Set:
America
CAM (Constantly Awake Mode)
Display Settings
Signal Strength Display Units:
dBm
Refresh Interval (seconds):
Data Display:
Relative
Cumulative
OK
Cancel
Cisco Aironet Desktop Utility
Action
Options
Help
Display Settings...
Scanning Settings...
Select Client Software...
Display can be changed



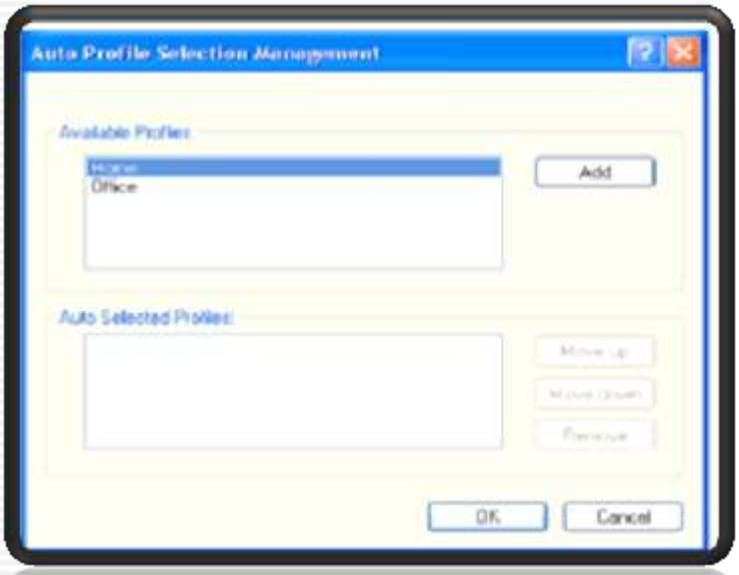

Cisco Aironet Desktop Utility - Current Profile: Globalnet
Action Options Help
Current Status
Profile Management
Diagnostics
Cisco Systems
Profile Name: Globalnet
Link Status: Authenticated
Network Type: Infrastructure
Wireless Mode: 2.4 GHz 54 Mbps
Current Channel: 3
Server Based Authentication: None
Data Encryption: AES
IP Address: 172.29.129.134
Signal Strength:
Good
Advanced
Select to open the ADU GUI
Help
Exit
Open Aironet Desktop Utility
Client Managed Test
Preferences...
Disable Radio
Reauthenticate
Select Profile
Show Connection Status
Local public
Sebastian
Associated
Good
54.0 Mbps, 11g
Cisco Aironet 802.11a/b/g Wireless Adapter #2
The ASTU shows basic information

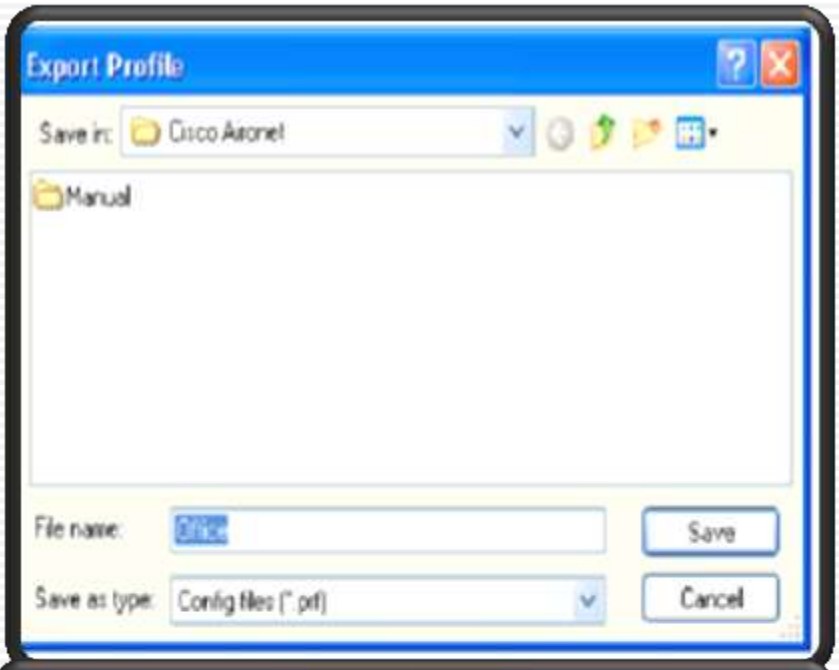


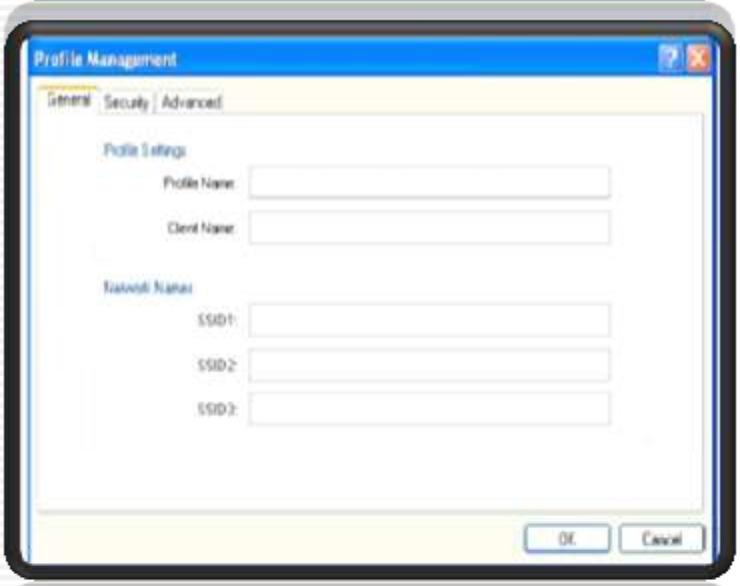


ستجد أيقونة بجوار كل شبكة تمكنك SSIDفي قائمة من معرفة بعض المعلومات عن الشبكة

Icon	Description
	شبكة متاحة
	أنت متصل حاليا بهذه الشبكة
	شبكة Ad Hoc متاحة
	أنت متصل بشبكة Ad Hoc


Auto Profile Selection Management
Available Profiles:
Office
Add
Auto Selected Profiles:
OK
Cancel


Export Profile
Save in:
Cisco Aironet
Manual
File name:
Office
Save
Save as type:
Config files (*.prf)
Cancel


Profile Management
General
Security
Advanced
Profile Settings
Profile Name
Client Name
Network Names
SSID1
SSID2
SSID3
OK
Cancel


Import Profile
Look in:
Cisco Aironet
Manual
File name:
Open
Files of type:
Config files (*.prf)
Cancel


Help
Exit
Open Aironet Desktop Utility...
Troubleshooting
Preferences...
Disable Radio
Manual Login
Reauthenticate
Select Profile
Show Connection Status