Уж по-сигурна безжична връзка:)

Може би сте свикнали с това, че навсякъде вече има изградени безжични мрежи (малко футуристично говоря,но това е бъдещето и така ще е:)
Да, мрежичката си работи и се конектвате,но дали тя е добре защитена и дали искате само вие да си я ползвате със здраве или да е достъпна и за други хора:) Добре е все пак да се понаправят някои настройки чрез браузъра...ще извървим няколко не толкова сложни стъпки :) ще бъда максимално кратък понеже знам,че не ви се чете много,много:) най-вече моите простотии:)
Много важно е да се разбере,че трябва да се осигури висока сигурност на данните,които преминават по безжичната ви мрежичка...
Ако сесиите на доста от приложенията започнат да се разпадат ползвайки маршрутизатора и се дисконектват и рутера все се ресетва,то е добре да се запознаете с технологията QoS(Quality of Service) новите маршрутизатори вече си имат тази технология:)трябва да си обновявате фърмуера и да активирате QoS
Примерно при Linksys в конфигурационната програма на самия маршрутизатор(рутер) отметнете в таба Applications&Gaming (проверете дали WMM Support е разрешен) и си го активирайте...
Изберете вашите QoS приложения:
Включете Internet Accsess Priority за вашите гласови и медийни приложения(скайп,игри и т.н.) ...от падащият списък си изберете...
Изберете приоритет на приложенията си...изберете Hight,Medium,Normal,Low (или висок приоритет,средно,нормален,нисък) и натиснете бутона Add
Може примерно да искате да поставите нисък приоритет на приложение като торент програми от рода на Utorrent,BitTorrent и др. :) поставете на VoIP услугите (скайпа) висок приоритет (задължително е)
Забележете,че не всички маршрутизатори позволяват да се задават такива приоритети на приложенията и устройствата (за жалост) но все пак могат да включат QoS и WMM те ще оптимизират автоматично медийният трафик... всичко това е изключено по подразбиране в маршрутизаторите(повечето) ... активирайте ги!
Следете за „досадници“ във вашата домашна безжична мрежичка:)
Има голяма вероятност в мрежата,която си имате у дома да се спотайват неизвестни за Вас натрапници:) Грешно е да се мисли,че само защото имате кодиране сте защитени...
Кодирането на мрежичката – WEP (има и други,но няма да се впускам в обяснения:) може да бъде разбито с лекота!!! WEP (Wired Equivalent Privacy) краква се за по-малко от 10мин:)
Ако все пак сте решили,че слагайки и филтрация по MAC мрежичката е бетонче,то аз пак ще трябва да ви разочаровам:) С лекота се измамва:)
Тук е и мястото да спомена,че абсолютно задължително е да си поставите парола за достъп до рутера. Вие трябва да си го командвате,а не някои гост:) По подразбиране повечето имат парола
admin за потребителско име
admin паролата
или нямат такива по подразбиране:)
В браузъра напишете или този ай пи адрес 192.168.1.1 или 192.168.2.1 ,за да си потърсите един вид своя рутер:) и да си нанесете настройките... може разбира се да е и с друг вътрешен ip адрес

За да увеличите сигурността на мрежичката си потърсете и си инсталирайте страхотната програма Network Magic (намира се на адрес: http://www.purenetworks.com)
има и безплатна версия :)
Програмата принципно ще покаже карта на всички компютри, медийни сървъри,принтери и др. устройства,свързани към мрежата.Всяко едно устройство,което не можете да определите какво е може да е някой спотайващ се:) Разбира се и със самата операционна система може да се прави проверка,но статийката е за начинаещи:)
Ако ползвате програмата е добре да отметнете възможността тя да детектва за всяко ново включване на устройство (от опциите й се отмята „A new device joins the network“ т.е. Ще алармира, когато ново устройство се присъединява към мрежата)
Ако все пак сте решили да не бъдете егоисти и искате да си споделите безжичната мрежичка с другите,то имате тази възможност...повечето рутери могат да осигурят споделяне на кабелната връзка извън вашата осигурена wi-fi мрежа...
Публичните точки за достъп принципно са манна небесна за „хакерчетата“ :)
Има и обратен вариант: лъжливи точки за достъп,но те именно са създадени от добри в занаята:)
Ако вашата лична безжична мрежичка не е изградена по протокола VPN , PPPOE то всеки може да разбере целият трафик...пароли,съобщения от мейлите и др.
Именно това правят създадените лъжливи accsess points:)))))) бъдете внимателни!
Ако нямате достъп до VPN то е добре да си инсталнете безплатен VPN софт от http://www.hotspotshield.com
натискате Run Hotspot Shield и самото приложение ще си включи защита...
при инстала и завършването му ще се активира в браузъра самото приложение и ще видите вътрешният локал хост със порта по подразбиране:) все пак е някаква защита,когато сърфирате из нета и ако сте попаднали на безжична мрежа капан отсрещният ще го духа:)
Тези мрежи принципно ги наричат ad-hoc
това са злосторници:) ,които създават доста точки на обществени места,където има и други изградени точки за достъп... както знаете всяка мрежа си има така да го наречем именце SSID
и злонамереният може да си я кръсти Free Wi-Fi
и ако е добре подготвен ще разузнае всичко за вас бъдете сигурни!!!
Едно време в началото на wi-fi по-лесно се прониквaше :)
Макар и рядко да се свързват повечето с комп-комп, но си има преодоляване :)
В система уин XP от св-вата на Network Connections ... може и от контрол панела:)
та оттам ще си изключите възможността Computer to computer to non preferred networks
Полето Automatically connect to non-preferred networks трябва да е отмаркирано!
Под Vista не се деактивират Ad-Hoc мрежите,но още в началото може ръчно да се избира дали да се конектвате към такива:)

Навярно вече имате портативен комп. (онова бе малкото телефонче дето си има всичко:)
PDA(Personal Digital Assistant=Личен цифров помощник:) или още наричани джобни компютри pocket computer или palmtop computer:)
и навярно вече знаете,че почти не се налага да ползвате услугите на разните мобилни оператори:)
нека лекинко да разясня все пак:
инсталирате си любимият на всички ни скайп или друг Vo-IP(Voice over IP)клиент и тъй като вашите приятели не са задръстени, и се подразбира,че и те имат такива яки машинки,и си разговаряте от някое кафенце,което има безплатен безжичен нет по скайпа и се уговаряте за кафенцето:)

И тъй като мобилността е в основата на 802.11 (с различните й версии) то е добре да се знае също така,че мобилните устройства, когато ползват безжичната връзка изчерпват много по-бързо батерията си:)затова,когато сте извън обхват от такива мрежи си изключвайте wi-fi , за да си останете по-дълго време мобилни:) също така трябва да се знае,че всичко това си има и своите минуси:
облъчването
всичко става на честота 2,4Ghz а това си е опасно за здравето при много продължително ползване също така и на честотата 5Ghz

Някъде ще срещнете наименование като IEEE 802 или IEEE 802.11 и след точката други цифрички:)
IEEE означава Institute Electrical Electronics Engineers демек развиват ги теа неща там някъде:)

Навсякъде точките за достъп се обозначават принципно с черна табелка, на която е написано Wi-Fi (wireless fidelity)

Отначало 802.11 е прехвърлял данни с 1 – 2 Mbps на 2.4 Ghz
Версията 802.11a става по-бърза и вече е 54Mbps на 5 Ghz
802.11b с 11 Mbps на 2,4Ghz
802.11g от 20 и нагоре Mbps на 2.4Ghz
802.11n (новата версия с много бърз пренос на данни:)

За LAWN (local area wireless network) се ползва технологията FHSS (frequency hopping spread spectrum)
Другата технология,която се ползва е DSSS (direct sequence spread spectrum)
И не на последно място технологията OFDM (orthogonal frequency multiplexing)
миняват дигитално данните е т'ва е:)

Bluetooth е също подобна технология и сте запознати с нея,но вълните са къси там:) все пак става за изграждане на домашна безжична мрежичка с бавен пренос на данни:)
Операционната с-ма Windows XP си поддържа доста WLAN NIC карти по подразбиране...

РАЗБИРА СЕ ТУК ТРЯБВА С ГОЛЕМИ БУКВИ ДА СЕ ОТБЕЛЕЖИ НЕВЕРОЯТНИЯТ УСПЕХ НА МАКИНТОШ (ЯБЪЛКАТА БЕ) С ТЕХНИЯТ СТРАХОТЕН УСПЕХ В ТАЗИ ТЕХНОЛОГИЯ И ТАКА НАРЕЧЕНИЯТ 802..11b „airport“ умно наименование нали :)
мен ме учуди,че няма буквичката i :) малка шегичка за разсейване :)

Както знаете всеки радио сигнал може да бъде чут и естествено подслушан...така е при нашите gsm-и с лекота те биват подлушвани...така беше и с мобилтел едно време:) лично съм слушал много такива разговори!!!
Седят си тъпите куки и си мислят,че само те знаят за подлушването:)))))))))

За да затрудните снифенето(sniffed) записване на трафика ви е добре да си криптирате не на 64bit а на 128bit дължина
WEP е проектиран да осигури криптиране на целият трафик на физическо и канално ниво на самата мрежа...той криптира трафика независимо от мрежовия протокол като TCP/IP или IPX
но както спонемах WEP се краква вече доста лесно:) познават се с лекота криптиращите ключове после вече лесно се разглежда целият трафик...

SSID(Service Set Identifer или идентификатора на набора от услуги) осигурява средства за множество точки за достъп и обслужването на множество мрежи,но отличава пакетите един от друг.
Може да бъде дълъг до 32 символа. Принципно SSID може да се счита за паролка към точката за достъп:)разбира се тя винаги е в явен текст(не криптирана)
Това е така наречената SNMP тайна, за която обаче всеки с мобилно устройство знае:)

Добре е да тествате с лаптопа до колко метра разпръсква сигнал вашият рутер:) за да знаете все пак обсега и докъде стига проследяването на данните ви :) нормално е 50-100метра
Разбира се има мощни маршрутизатори и външни антени и т.н.

Безжичните карти масово използват Prism базирани чипове. Всяка модерна операционна с-ма си има драйверите спокойно:)
Единствено трябва да се отбягват тези с чип Broadcom – те са зле:) и не можете да ползвате доста от програмите:)

Навсякъде пробутват инструмента NETStumbler :)
Той идентифицира безжичните точки за достъп и мрежите. Това си го може и операционната с-ма:) дори софта,които си идва с било то безжичната карта или маршрутизатора:)
Тази програмка не подслушва данните на протокола TCP/IP
С него локализирате мрежичките (военно шофиране са го нарекли кракерчетата:)
Просто програмката предава заявки за връзка към всички подлушващи точки за достъп със SSID Any Повечето SSID си отговарят на заявката:) Програмата не е пасивен снифер! Може да бъде видян в целевите мрежи или жертвите:) Виждаме с програмата MAC адреса на точката за достъп (не че с др.

**инструменти не се вижда:) вижда се статуса на самата мрежа (дали е криптиранка или не)
силата на сигнала (ако имате GPS към компа ще видите и координатите:)
Такива програми има вече много:) Със всяка мрежова карта си идва софт ...
Разбира се може да се търси по зададени критерии(само свободни мрежи да се търсят и т.н.)**

**ESS е идентификатора на разширения набор от услуги или ESSID (Extended Service Set ID)
това е буквеноцифров код,споделян от всички точки за достъп и безжични клиенти,които участват в една и съща безжична мрежа.Позволява на множество точки за достъп да служат на една и съща мрежа,което си е важно за физически и логически големи мрежи.По този начин две точки за достъп могат да ползват един и същ канал и да служат на две уникални мрежи.**

**IBSS (Peer) този филтър представя друга безжична карта в peer-to-peer или ad-hoc режим
нещо като кросовър кабелче дето слагаме м/у два компа:) така две безжични карти ще си комуникират без наличието на точки за достъп:)**

Просто трябва да знаете,че най-добрата защита за сега е включването на филтрация по MAC адреса и задължително комбиниране с VPN изпълнено по протокола IPSEC

**Ако искате все пак да надниквате в данните,то може да се ползва програмата AiroPeek(има я в пакета,който съм дал за даунлоуд в сайта ми)
С този инструмент вече се улавят до някаква степен пакети от трафика:)
Но има една особеност за тази програма и тя е,че е задължително да се сдобиете с безжична карта с подходящият фърмуер,за да се разреши смесен режим!
Програмата си има така наречен кепчър(ще улавяте:)
Може да декриптирате WEP защитен трафик,но трябва да знаете правилният ключ:)
Ключа се задава(с др. инструменти се разбира и ключа:) като изберете Tools ->Options->802.11->WEP Key Set -> Edit Key Sets
С тази програма може лесно да разберете колко инфо изтича от мрежичката :)
Може да си проверите как работи MAC базирания достъп,WEP ключа как е що е:)
Може да разберете дали се предава домейн автентикация...дали се предават хешовете на NT LAN Menager м/у разните файлове:)
Какви протоколи се ползват в явен текст.**

**Друга полезна програма е Wellenreiter
Има си C++ и пърл версии
добра програма за одит на безжичните мрежи!**

**Просто за юникс базираните с-ми изпълнете скрипта под руут права:)
perl Wellenraiter.pl
и ще видите програмката:)**

**програмката записва уловените пакети в двоичен вид в главната директория на потребителя...
принципно файловете са в pcap формат и се разглеждат с tcpdump или Ethereal**

**Друга програма е KISMET
Доста силен инструмет и разбира се с отворен код:)
Разбира се юникс потребителите знаят за какво става дума и навярно сега се усмихват:))))))
Разбира се,че ще ползваме BSD-та ...ние не сме глупави нали така?
Може разбира се да се ползва и bsd-airtools
програмата се компилира на юникс с-те с лекота,а за уин става с cygwin
разбира се нищо няма да можете да направите с уиндоуса :)
имплементацията е излишна понеже,ако сте стигнали до ползване на тази страхотна програма ще знаете и какво правите с отворения код като цяло:) що да ви подценявам:)**

Сега малко за WEP криптирането пак:) значи то се казва,че криптирането е с 40 или 64 битово криптиране,само че секретният ключ е точно 40 битова ст-ст :) другите 24 бита са си само част от инициализиращ вектор(IV) и се променя за всеки пакет
с пасивно наблюдение на пакетите и сме готови:)

Има и нещо друго сега:) може някой да реши да събори мрежичката ви:)
ползва се така наречената denial of service (DoS) атака:) отказ на услугата:)
ще направи някой така,че временно мрежичката да рухне:)
прави се усилвател с мощен предавател и се „наводнява“ трафика:)

Ето няколко други инструмента, които ще ви улеснят в търсенето на точките за безжичен достъп и ще защитят данните ви в мрежата.

Следващите програми,които ще ви представя имат разнообразни функции, сред които търсене и помощ при свързване в Wi-Fi мрежи, създаване на VPN, за да защитите обменяните данни, бързо преминаване от едни мрежи към други.
Хубаво е да си ги тествате:) много от тези програми изискват разрешение от страна на защитната стена, за да могат да си вършат работата, така че не бива да ви учудва, ако евентуално получите запитвания за оторизация на достъп до и от Интернет:) Някои могат да бъдат прихванати от антивирусните като вируси:) споко!
Също така такива програми инсталират доста различни драйвери и могат да съсипят системата:)

http://www.wefi.com
Тази програма е с добрата идея за връзка между безжичните и социалните мрежи...
с WeFi не само можете да откривате точки за достъп, но и да държите връзка с приятелите си и да създавате нови...като инсталирате софтуера, той ще ви покаже не само близките точки за достъп,а и информация дали мрежата е защитена, или не, както и силата на сигнала.

Plug and Browse
http://www.interactive-studios.net/products/plugbrowse.htm
Ако използвате повече от една LAN или безжична мрежа (примерно използвате лаптопа на работа и вкъщи), и заради настройките, които трябва да правите всеки път при смяната на мрежата(служебната мрежа работи с динамичен IP адрес, разпределен от DHCP сървър, домашната LAN е със статичен) Освен това настройките на защитните стени в двете мрежи са различни, във всяка от тях принтера по подразбиране е различен. Свързването със служебната мрежа често става след задействане на скрипт, в нея имате закачени няколко мрежови устройства; вкъщи вероятно нямате и т.н. Когато се свържете към различна мрежа, трябва да променяте настройките ръчно. Това не само е досадно, но и отнеме време. С Plug and Browse се автоматизира процеса. Този инструмент позволява да създавате профили с мрежови настройки и да преминавате между тях само с няколко щраквания. Въвеждате настройките за всеки профил и след това просто щраквате името на този, който ви трябва в момента.

AirDefense Personal Lite
http://airdefense.net/products/adpersonal/trial.php
Винаги внимавайте, когато ползвате безжична мрежа извън къщи или офиса. Опасностите са доста – има безжични мрежи-капанчета, които са замаскирани като точки за публичен достъп, както и мрежи-клонинги на известни и безопасни точки, които се възползват от репутацията на оригиналите, но всъщност едноименните мрежи са инсталирани от частни лица с цел кражба на лична информация Тази програма е направена, за да ви защити. Следи мрежите, към които се свързвате и извежда предупреждения, ако ги счита за потенциално опасни. Алармира ви, когато сте в незащитена безжична мрежа, или мрежа, която позволява криптиране на данните, но вие не сте го включили. Трябва да отидете на сайта на разработчика и да попълните формуляр,след което ще получите линк, от който да свалите програмата на електронната си поща.

Xirrus Wi-Fi Monitor
http://www.xirrus.com/library/wifitools.php
Ако ползвате безжична мрежа под Windows Vista, това е хубав инструмент. Той показва силата на сигнала, името на мрежата, към която сте свързани, както и текущия ви IP адрес. С нагледен интерфейс под формата на радарен екран са показани мрежата, към която сте свързани, както и другите близки мрежи...разбира се всичко това може да си се прави и от операционната с-ма:)

Whisher
http://www.whisher.com
Когато искате да се свържете в безжична мрежа, направете го през Whisher, вместо през вградената програма на Windows XP или приложението, което върви с безжичната ви мрежова карта:)
Един по-различен подход:)

Wi-Fi SiStr
да добиете по-точна представа за силата на безжичния сигнал:)

Hotspot Shield
това безплатно приложение криптира предаваните пакети данни...използването на програмата е просто – инсталирате, стартирате и вече сте защитени:)
откажете предложената ви като „екстра" лента Dealio toolbar – това е ненужна програма:)

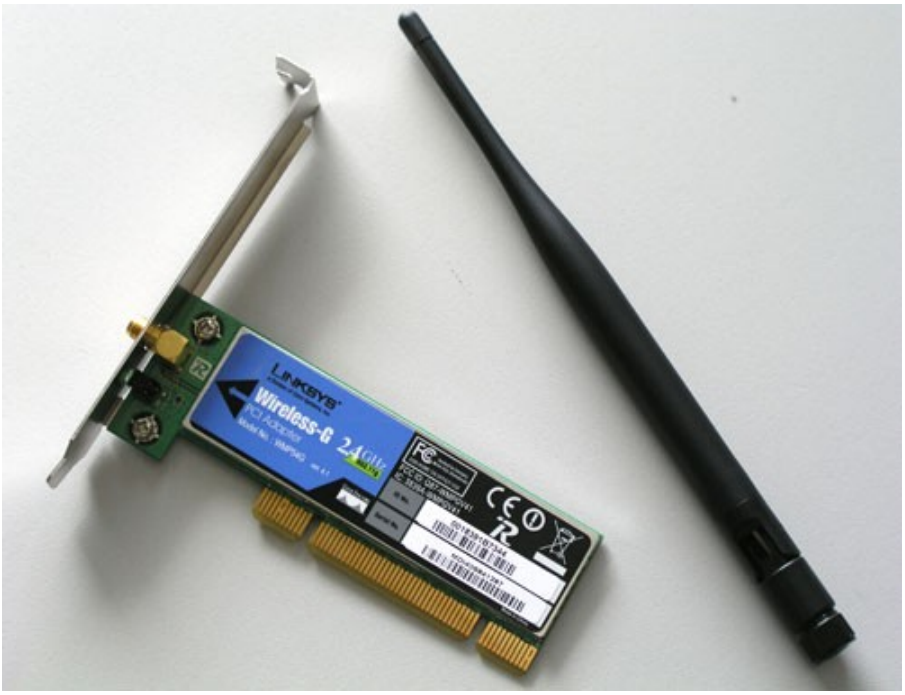
WiFi Guardian
Това е едно приложение, което подобно на Hotspot Shield, инсталира Virtual Private Network (VPN)
Препоръчвам!

WiFi Hopper
Това приложение засича близките мрежи и извежда информация за тях като идеята е да прецените дали и към коя от тях да се свържете. За всяка от засечените безжични мрежи WiFi Hopper показва SSID (името на мрежата), MAC адреса , силата на сигнала, метода на криптиране на връзката (ако мрежата е защитена), честотата, на която работи, и статуса на връзката ви с мрежата...Инструментът също посочва дали мрежата е в infrastructure mode, при който компютрите се свързват към безжичния рутер, или в ad hoc (осъществява се връзка PC-към-PC). Принципно, ad hoc връзките са рискови:)

Loki Toolbar
С тулбара можете ба превърнете мобилния си компютър в навигационно устройство като добавите лентата Loki Toolbar (има версии и за Internet Explorer и за Firefox). Използва метод за триангулация и засича местоположението ви на базата на околните безжични точки за достъп. След това може да ви предостави списъци с кината и магазините наблизо, времето в района и друга информация в отделни „канали", които често се отварят в нови прозорци.

Точките за достъп(AP) позволяват свързване към Интернет, както и към корпоративна компютърна мрежа с помощта на добре защитена VPN връзка,когато се намира на различни места в града.
За да използвате безжични точки за достъп, ще е необходим преносим компютър - лаптоп, ноутбук,нетбук или PDA, или просто GSM с wi-fi т.е. снабдени с безжична мрежова карта...
разбира се и вътрешната безжична мрежова карта на настолният комп. върши работа:)

Ето така изглеждат безж. мреж. карти за настолен комп. нарича се вътрешна...
Слагат се на дъното на компа на PCI слотовете...след това се инсталират драйверите (компакт диска съдържа тези драйвери на производителя и обикновено си има програма,която да управлява всичко)
Може да си закупите удължителче с антенка за малко по-силен сигнал,но принципно тези карти са изчислени и не може да се слага кой знае каква голяма антена,за да усилите приемането на сигнала от маршрутизатора(а и той си има ограничение в метрите за разпръскване на сигнала)



Първи стъпки за свързване към точка за достъп:
Отивате в кафенето, зали на хотел или чакалня на летище и включвате лаптопа:) щракнете с десния бутон на мишката в/у иконата Wireles Zero Configuration (за уиндоус xp), която се намира в областта за известяване.
Щракнете върху View Available Wireless Networks (Показване на достъпните безжични мрежи)
От списъка с достъпните мрежи изберете услугата, към която желаете да се свържете, и натиснете бутона Connect (Свързване). По този начин се установява безжичната връзка.
Стартирайте Интернет браузъра. Заявката за начална уеб страница (home page) може би ще бъде пренасочена към началната страница на фирмата доставчик на услугата. За да бъдат точките за достъп по-лесно достъпни за потребителите, опциите за сигурност като криптиране на данните, които могат да се използват при безжичните компютърни мрежи, обикновено не са активни.
Това означава, че по-голямата част от комуникациите с участието на компютъра ви, например уеб-базирана електронна поща, ще бъдат предадени под формата на ясен, некриптиран текст и ще са незащитени от неправомерна намеса...съществуват някои предпазни мерки, които е добре да имате предвид ,за да сте сигурни, че данните и информационните ви ресурси са максимално добре защитени
Има голям избор от персонални защитни стени (firewalls), които се предлагат.Те могат да осигурят защита на потребителя на безжична мрежа от неправомерни действия на други участници и да предупредят за наличие на опасни приложни програми, търсещи достъп до данните на компютъра ви.
Антивирусните програми предпазват данните на компютъра от действието на вируси и други атакуващи програми, които могат да инфектират компютъра ви от мрежата...този софтуер ще ви спести да заразите без да искате компютърните системи на други потребители, с които поддържате връзка.Може да използвате автоматичната услуга за акуализиране на Windows XP или директно да се свържете към уеб сайта за поддръжка на Microsoft и да изтеглите най-новите обновявания и сервизни пакети (service packs) на операционната система. За целта от браузъра идете на Инструменти(Tools) и кликнете на Windows Update ... ще бъдете пренасочени към сайта за обновяване на с-мата...
За по-голяма сигурност трябва да сте със сервизният пакет 3 (Service Pack 3)
Разбира се трябва и да си актуализирате драйверите на безжичната карта, за да имате най-новото...
Ако се свържете към защитен уеб сайт, данните ви ще бъдат криптирани, като се използва SSL технология.Защитените саптове в Интернет може да разпознаете както по https:// адреса, който се изобразява в адресната лента на браузъра, така и по символа на катинар в областта за известяване в долната дясна част на прозореца му и горе в адрес лентата. Доставчиците на безжични Интернет услуги препоръчват да не се използват уеб-базирани електронни пощенски кутии при изпращане на поверителни данни и по възможност прикачените файлове да бъдат криптирани преди да се изпратят.
Някои оператори на безжични мрежи предлагат услугата VPN (Виртуална частна мрежа), която е свързана с гарантиране на по-голяма сигурност на данните. Ако използвате пароли за достъп до поверителна информация на компютъра, не ги прилагайте при работа с безжичен Интернет, където има вероятност потребителската информация да бъде предадена в некриптиран вид и да стане лесно достъпна за други лица. Деактивирайте безжичния мрежов адаптер, когато не го използвате. Ако използвате лаптоп на открито, без да е свързан към точка за достъп, добре е да деактивирате мрежовата карта...така ще си пестите и от батерията:)

Щракнете с десния бутон на мишката върху иконата Wireless Network Connection (Безжична мрежова връзка) В прозореца Network Connections изберете командата Disable (Деактивиране,Изключване).
За да възстановите отново връзката към мрежата,то от контекстното меню щракнете върху Enable (Активиране,Включване). Избягвайте автоматичното свързване (auto-connect) към непознати мрежи-възможно е кракер да създаде лъжливи точка за достъп, която ще бъде разпозната от компютъра като истинска.
В зависимост от мрежовите настройки в Wireless Zero Configuration, компютърът може автоматично да се свърже с нея и по този начин да се създаде лесен път за достъп до данните.Отворете прозореца Network Connections u щракнете двукратно върху Wireless Network Connection.
В страницата Wireless Networks натиснете бутона Advanced
Премахнете отметката пред полето Automatically connect to non-preferred networks (Автоматично сбързване към мрежи, които не са в списъка с предпочитаните).
Натиснете последователно бутоните Close и OK.

След като сте инсталирали успешно безжичен мрежов адаптер и сте се свързали към точка за достъп, следваща стъпка може би е свързване на два или повече компютъра заедно в обикновена мрежа за споделяне на файлове или други ресурси.

Този тип връзка е известен като равноправна мрежа и представлява една от двете разновидности на безжичната връзка, дефинирани в мрежовите стандарти Wi-Fi или 802.11.
С помощта на равноправна връзка могат да бъдат сбързани няколко компютъра, като например настолни системи, лаптопи, PDA устройства, а защо не и други мрежови и електронни устройства или домашни уреди.Всеки от компютрите в равноправна мрежа комуникира по еднакъв начин с всички останали компютри в нея, без централен концентратор (хъб) или точка за достъп, които да насочват трафика на данни в мрежата.Безжичните мрежови адаптери за настолни системи са два основни типа: вътрешни(горните картинки) и външни.
Предимството на вътрешните адаптери е, че антената често е свързана към мрежовата карта, като се използва подвижна връзка, която позволява поставяне и на външна антена. Това е полезно, в случай че решите да разширите обхбата на мрежата.
Външните мрежови адаптери като Linksys WUSB11 се свързват към компютъра посредством USB порт, USB устройствата могат да се свързват в звездовидни вериги, което означава, че може да поставите безжичния мрежов адаптер във всеки незает USB порт, например в този на монитора, а не непременно в USB порт директно на настолния компютър.

След инсталиране на мрежовия адаптер и софтуера му, в областта за известяване се появява иконата на Zero Configuration на Windows XP.

Може да ползвате и usb безжична мрежова карта ... (те са така наречените външни)

Като е добре да гледате техническите им характеристики:) примерно:
Интерфейс USB 2.0 (по-новата версия...но обикновено си се поддържат и 1.0 и 2.0)
Поддържани стандарти IEEE 802.11b/g/n (забележете,че тази поддържа и новата версия n)
Скорости на трансфер 11/54/135/150Mbps (добре е и тях да гледате)
Вградена антена (може да ви кефи да си има опънатка антенка:)препоръчвам с антенка)
Обхват на действие до 100 метра (обикновено всички са до там някъде)
Честотата е 2.4 GHz (има си облъчване и не е безвредно за вас самите)

Мрежови конфигурации: Ad-Hoc (Peer-to-Peer), Infrastructure се поддържат
Работят си принципно с Windows 2000, XP, Vista, Linux
CD с драйвери си има принципно,но и да нямате може при ъпдейтването на системата ви да бъдат детектнати и да бъдат инсталнати:)

За свързване към съществуваща равноправна мрежа:
Стартирайте един или повече от компютрите в равноправната мрежа и проверете дали безжичните им карти са инсталирани, и работят правилно.
Щракнете с десния бутон на мишката върху иконата Wireless XP Zero Configuration и изберете командата View Available Wireless Networks (Покажи достъпните безжични мрежи). В случай че бъдат показани няколко мрежи, изберете SSID кода на мрежата, към която желаете да се свържете.
Ако WEP механизмът не е активиран за мрежата,поставете отметка за полето Allow me to connect to the selected wireless network, even though it is not secure.(Позволи ми да се свържа към избраната мрежа, въпреки че няма сигурност...)
Ако WEP механизмът е разрешен на останалите компютри в мрежата, въведете мрежовия код и щракнете върху Connect
След като се осъществи връзката, в областта за известяване се появява текстовото балонче за безжичната мрежова връзка (Wireless Network Connection).Състоянието на безжичната връзка може да бъде проверявано по всяко време чрез щракване с мишката върху иконата на Windows XP Zero Connection

Създаване на нова равноправна безж. мрежа:
Изберете Start, Settings, Network Connections (Мрежови връзки) и щракнете двукратно с левия бутон на мишката върху Wireless Network Connection (Безжична мрежова връзка).
В диалоговия прозорец Wireless Network Connection щракнете върху Properties
В диалоговия прозорец Wireless Network Connection Properties изберете страницата Wireless Networks и щракнете върху Advanced.
Изберете Computer-to-computer (ad hoc) networks only (само равноправни мрежи).
Премахнете отметката пред полето Automatically connect to non preferred networks (Автоматично свързване към мрежи, които не са в списъка с предпочитаните) и затворете диалоговия прозорец с бутона Close.
Под полето Preferred networks в диалоговия прозорец Wireless Network Connection Properties изберете Add. В диалоговия прозорец Wireless network propertiesвъведете SSID име за новата равноправна мрежа
Изберете Data encryption (Криптиране на данните) и въведете мрежов код, ако желаете да активирате WEP.
Щракнете върху ОК, при което новата мрежова връзка се появява в списъка Preferred networks. (Предпочитани компютърни мрежи). Червеният знак „x" на иконата показва, че към мрежата не са свързани други компютри.Сега вашата равноправна мрежа ще бъде видима за
всички компютри с разрешен безжичен достъп, които се намират в обхвата й, и те ще могат да се конектнат към нея.
Дори при равноправните мрежи предаваният сигнал може да се разпространи на разстояние от няколкостотин метра в зависимост от типа на местоположението. За да има максимална сигурност на предаваните данни, трябва да осигурите следното: WEP (Wired Equivalent Privacy) да бъде разрешен на всички компютри в равноправната мрежа.
Всеки мрежов адаптер трябва да бъде конфигуриран правилно, като се използва един и същ WEP код.
Ако WEP бъде превключен от неактивно в активно състояние на един компютър в равноправната мрежа, характеристиките на безжичната връзка на останалите компютри трябва да бъдат променени, за да се осигури нормално свързване.
Промяна на статуса на WEP при съществуваща връзка:
Щракнете с десния бутон на мишката върху иконата на Windows XP Zero Configuration и изберете командата View Available Wireless Connections.
В диалоговия прозорец Connect to Wireless Network(Свързване към безжична мрежа), полето за въвеждане на мрежовия код не е активно, въпреки че WEP е разрешен на другите компютри. Изберете Advanced.

В списъка Preferred networks (Предпочитани мрежи) посочете връзката, която желаете да актуализирате, и щракнете с левия бутон на мишката върху Properties.
Щракнете върху Data encryption и след това премахнете отметката пред полето The key is provided for me automatically (Автоматично предоставяне на кода).Въведете мрежовия код в полето и изберете ОК...форматът на кода (Key format) и дължината му (Key length) се избират абтоматично В зависимост от формата на мрежовия код, който сте въвели.
Щракнете отново върху бутона ОК в Wireless Network Properties, при което се показва повторно диалозовият прозорец Connect to Wireless Network с активно поле за въбеждане на мрежов код, показващо, че WEP вече е разрешен за тази връзка.
След това Windows XP осъществява отново връзката към достъпната мрежа с разрешен WEP, като се използва мрежовият код, който сте въвели. Точката за достъп (AP-access point) предоставя връзка или мрежов мост между кабелната и безжичната мрежа. В малък или не толкова малък офис може да има няколко точки за достъп, които да са свързани с кабелната мрежа и така да осигуряват широко покритие за свързване на персонала посредством лаптопи с безжично оборудване Освен осигуряването на безжичен достъп до кабелната мрежа, една точка за достъп може да осъществява и множество други функции, като например:
• Споделяне на Интернет връзка
• DHCP сървър за разпределяне на IP адреси
• Транслиране на мрежови адреси (NAT) за запазване на вътрешните частни адреси
• Контрол и сигурност на безжичния достъп
• Сигурност и филтриране на Интернет връзка (защитна стена)
• Маршрутизиране на мрежовия трафик. Точките за достъп се предлагат във всевъзможни конфигурации - от простия мост между кабелната и безжичната мрежа до многофункционални точки за достъп с вградени превключвател, маршрутизатор, сървър за печат и широколентов модем.
Ако искате просто да осигурите връзка на няколко компютъра с безжични адаптери към съществуваща кабелна мрежа, ще е достатъчна и най-обикновена точка за достъп, като Linksys WAP11 или друг рутер. В повечето случаи споделената Интернет връзка е ключово изискване. Много производители предлагат безжични шлюзове. Например моделът Linksys WRT54G е с вградени 4-портов Ethernet превключвател, маршрутизатор и безжична комуникация по стандарта 802.llg. Маршрутизаторът управлява Интернет трафика от кабелната и безжичната мрежа през широколентовата Интернет връзка. След свързването на маршрутизатора в мрежата ще е необходима проверка на конфигурацията на персоналните компютри и готовността им за работа с маршрутизатора.

Свързване на маршрутизатора към кабелната мрежа:
Преди да започнете конфигурирането и окабеляването на мрежата, изключете захранването на мрежовия хардуер.
СВържете с Ethernet кабел Ethernet порта на Вашия персонален компютър и някои от портовете на задния панел на маршрутизатора.
Свържете с друг Ethernet кабел модема за широко лентовата Интернет връзка и порта WAN или Internet на задния панел на маршрутизатора.Той трябва да светне със светодиодният индикатор за съответния порт, свързан с персоналния компютър, обозначавайки активната Ethernet връзка.
Персоналният компютър трябва да е настроен да получава IP адреса си от маршрутизатора и да има инсталиран протокола TCP/IP. Проверете за това по следния начин:
Отвореме Network Connections от десктопа или като изберете Start, Control Panel, Network Connections.
Щракнете двукратно в/у връзката за локалната мрежа (Local Area Connection) и изберете Properties.
В диалоговия прозорец General проверете дали е поставена отметка пред полето Internet Protocol (TCP/IP)
Щракнете в/у Internet Protocol и след това в/у Properties
В страницата General проверете дали е селектиран радио-бутонът Obtain an IP address automatically Натиснете ОК.
Същите настройки трябва да имат и останалите компютри в мрежата, включително онези, които ще ползват безжична връзка към точката за достъп/маршрутизатора. За да имате работеща точка за достъп/маршрутизатор, ще трябва да промените някои основни настройки на Интернет връзката и на безжичната мрежа.

Влизане в конфигурационното меню:
Точката за достъп/маршрутизатор в ероятно е с уеб базирано приложение за конфигуриране.
Въведете IP адреса му в адресното поле на браузъра.
Промяната на конфигурационни параметри изисква обикновено въвеждане на администраторска парола. Погледнете в документацията на устройството и въведете паролата по подразбиране.
В браузъра ще се появи началният екран на конфигурационното приложение.
Първата стъпка е да изберете часовата зона и да включите автоматичното сверяване на часовника.
Въведете име на хоста (Host Name) и име на домейна (Domain Name), ако такова е изискването на Интернет доставчика.
От падащото меню изберете типа конфигурация за Интернет Връзката.
Ако връзката към Интернет доставчика не ползва DHCP, ще трябва да въведете допълнителни данни.
При статични IP адреси (Static IP) е необходимо да укажете самия IP адрес, подмрежовата маска (Subnet mask), шлюза по подразбиране (Default Gateway) u IP адреса на сървъра за имена на домейни (Domain Name Server-DNS).
За PPPoE ще трябва да зададете потребителското име и паролата.
За PPTP ще са ви необходими IP адрес, подмрежова маска, шлюз по подразбиране, потребителско име и паролата.
Конфигурирайте настройките на точката за достъп за безжичната мрежа. Ако точката за достъп е по стандарта 802.11g , изборът на Mixed mode ще Ви даде възможност за свързване на компютри с адаптери за кой да е от двата стандарта - 802.11g и 802.11b
Можете да изберете канала за безж. комуникация и SSID по същия начин, както при настройката на равноправна безжична мрежа. При инфраструктурния режим допълнителна функция е изключването на разгласяването на SSID (SSID broadcast).
WEP настройката на е същата.

Вероятно вашата точка за достъп/маршрутизатор разполага с множество функции, включително управление на мрежата и на сигурността й...
Сигурност:
В страницата за сигурността (Security) можете да зададете администраторска парола за конфигурационното приложение. Променете паролата ,която си е по подразбиране, за да предотвратите непозволен достъп до мрежовите настройки.
Повечето маршрутизатори поддържат VPN пренос (VPN passthrough), който в офисни условия позволява защитен достъп до офисната мрежа проз Интернет.
Може да конфигурирате един персонален компютър от мрежата да служи за демилитализиран хост (DMZ host), ако ще си хоствате сайтове или др.
Диалоговият прозорец с общите настройки дава възможност за контрол върху някои от основните функции на вашата точка за достъп/маршрутизатор.
Клонирането на MAC адреса дава възможност да подмените този адрес с друг.
Някои Интернет доставчици изискват регистриране на MAC адреса на компютъра, а тази функция позволява маршрутизаторът да ползва вече регистрирания MAC адрес.
Ако се нуждаете от това, следвайте следната последователност:
Открийте MAC адреса на компютъра като в MS-DOS при команд промпт прозореца напишете ipconfig /all
MAC адресът е 12-цифреният „физически адрес" на мрежовия адаптер, който се използва за Интернет връзката.
От падащото меню до опцията MAC cloning изберете Enable. Полето за въвеждане на MAC адреса ще се активира.
Въведете 12-цифрения MAC адрес на мрежовия адаптер в полето.
Натиснете Apply за активиране на променената настройка.
Много маршрутизатори притежават функционалността на DHCP сървър и могат да поемат разпределянето на IP адресите за компютрите в мрежата.
За използване на DHCP сървъра на маршрутизатора натиснете Enable на съответното място.
В повечето случаи не се налага да се променя настройката по подразбиране.
Проверете дали всички компютри в мрежата са конфигурирани да получабат IP адреса си автоматично.
Допълнителна опция в диалоговия прозорец дава възможност да видите списък с IP адресите, присвоени от DHCP сървъра.

Други настройки за безжична мрежа:
Повечето разширени настройки за безжична мрежа могат да се оставят със стойностите си по под-разбиране, но една от опциите, които вероятно ще използвате, е филтрирането на MAC адреси.
Ако сте в обща мрежа със съседите или с друга организация, можете да използвате тази функция за ограничаване на достъпа само за определени потребители.
От падащото меню срещу MAC filtering изберете Enable(т.е. Ще започне филтриране по MAC адрес)
Изберете дали желаете точката за достъп да разреши, или забрани достъпа за MAC адресите във филтриращия списък.
Въведете в списъка за филтъра MAC адресите, които са разрешени или изключени.
Повечето маршрутизатори имат множество филтри, които могат да се конфигурират с цел блокиране или разрешаване на определени видове Интернет достъп.
Въведете име на политиката на достъп и изредете в списъка компютрите, за които тя ще е в сила.
Уточнете филтрите, които ще са в сила за тази политика.
Типични възможности тук са:
филтрирнне no URL адрес, по ключова дума и по време или дата на достъп.
Натиснете Apply за активиране на променената настройка.
Ще имате нужда от тази разширена възможност в случай, че някой от компютрите в мрежата ще изпълнява ролята на уеб сървър, сървър за електронна поща или ftp сървър.
Пренасочването на портове осигурява прехвърлянето на заявките към необходимия компютър в мрежата.
За всяко едно приложение с достъп през външен порт е необходимо въвеждане на диапазона от портове, които то ще използва.
Отбележете кои протоколи ще се пренасочват.
Въведете статичния IP адрес на компютъра, на който ще работи приложението.
В документацията на конкретното сървърно приложение можете да проверите за евентуални други негови специфични изисквания.
Маршрутизиращите функции на хардуера могат да бъдат използвани в два режима:
шлюз към Интернет или маршрутизатор в по-сложна мрежа с други маршрутизатори.
В повечето случаи при домашна или малка офис мрежа ще използвате режима за шлюз.
Изберете желания режим на работа в мрежата:
маршрутизатор (router) или шлюз (gateway).
Разполагате с възможността да изградите статична маршрутизираща таблица с указани маршрути на мрежовия трафик, стига да имате достатъчно опит в конфигурирането на мрежи.
В режима за маршрутизатор е включена опция за използване на динамична маршрутизация (RIP), и то дава възможност на маршрутизатора сам да си изгради маршрутизираща таблица.
Задайте дали RIP да е включен откъм страната на WAN, откъм локалната безжичната мрежа или откъм двете.
Ако предоставеният от Интернет доставчика IP адрес е динамичен, а желаете на някой от компютрите да работи сървър, който да е достъпен откъм Интернет, тогава е необходимо да предоставите начин за посетителите на този сървър да го намерят независимо от промените на неговия IP адрес.
Това се постига с използване на динамична система за имена на домейни (DDNS). Някои шлюзове разполагат и с такава функционалност, но за използването й първо трябва да имате регистрация при някой доставчик на DDNS услуги.
Регистрирайте се за DDNS услуга, като например:
www.tzo.com www.dyndns.com www.dynip.com www.no-ip.com
Включете DDNS в конфигурационната страница на точката за достъп.
Въведете потребителското име, паролата и името на хоста от регистрацията при доставчика на DDNS услугата.Натиснете Apply за активиране на променената настройка.

Без значение дали изграждате нова мрежа с безжична технология, или разширявате съществуващата кабелна мрежа с безжични компоненти, трябва да сте наясно, че голямата сила на безжичните мрежи, а именно — гъвкавостта, е същевременно тяхна потенциална слабост.
За разлика от кабелните мрежи, достъпът до които се осъществява след физическо свързване, безжичният мрежов трафик се излъчва в радио ефира и е достъпен за всеки джобен или настолен компютър, снабден с безжичен адаптер. Този улеснен достъп на свързване е известен още като „военни набези (war driving) ... обикаляне по улиците с лаптоп или джобен комп,които са си с безжичен адаптер като целта е засичане и публикуване на местоположението на безжичните мрежи:)

Уязвимостта на WEP :
Освен модата на дейността по намиране и осъществяване на достъп до незащитени мрежи, твърде скоро след прохождането си методът за криптиране използван в WEP, е обявен за криптографски слаб. Самият факт, че криптографските ключове на WEP остават непроменени, стига да не се сменят ръчно във всяка станция в мрежата, означава, че WEP е уязвим, WEP предава информация за криптиращия ключ като част от всеки пакет с данни и така всеки желаещ кракер, стига да е оборудван с необходимите инструменти, може да събере и анализира изпратените данни и така да извлече криптиращия ключ:)
Това действие изисква прихващане и анализиране на няколко милиона пакети, но при мрежа с натоварен трафик може да се извърши за по-малко от час и дори няколко минутки.
С последната версия на сигурността на 802.11 (WPA) тази слабост е преодоляна обаче чрез въвеждане на автоматична промяна на криптиращия ключ през определени времеви интервали :(хаха
Заплахите към сигурността на безжичните мрежи са много и разнообразни, като тук ще изброя само някои от тях:

Amaku с вмъкване:
Атакуващият успява да се свърже с безжичен клиент към точка за достъп без да има право за това, понеже не му е поискана парола.

Прихващане на сесии:
Атакуващият предава заблуждаващ трафик при връзка и така прихваща TCP сесията на жертвата.

Наблюдение на разпръсквания трафик:
При лошо конфигурирани мрежи, когато точката за достъп е свързана с концентратор (hub) вместо с превключвател (switch), атакуващият може да се добере до пакети с важни данни, които изобщо не са били предназначени за безжичната мрежа.

Подправяне на ARP (ARP spoofing) :
Атакуващият може да излъже мрежата да допусне маршрутизиране на чувствителни данни от кабелната мрежа към Интернет посредством достъп и увреждане на маршрутизиращите таблици.

Прихващане :
Атакуващият използва своя точка за достъп, която привлича безжичните клиенти да се включат и разкрият важни данни, като например пароли, номера на кредитни карти и т.н.

Amaku с отказ на услуга (Denial of service) :
Обикновено са в кабелните мрежи, където атакуващият засипва безжичния клиент с фалшиви пакети:) и маршрутизаторът се рестартира постоянно...

Задръстване:
Атакуващият наводнява диапазона 2,4GHz с радиосмущения и така блокира безжичната комуникация:) Такива устройства, които блокират, смущават мобилните устройства се наричат phone jammer има ги най-различни:) продават се и портативни, а също така има и по-мощни, които са колкото куфар:) разбира се в нета има доста ел. схеми и се обяснява как да се създаде такова устройство и т.н.

Ако познавате марката мобилни апарати Palm трябва да знаете, че те произвеждат и такива продукти разбира се има и много други фирми, които си произвеждат смутители съвсем законно:)
Такива устройства могат с лекота да заглушат сигнала на GSM 850-, 900-, 1,800-, и 1,900-MHz в разстояние 30м т.е. В радиус от 30м никой няма да може да се свърже от gsm-а си с някой друг:)

Тези двете устройства са много мощни смутители :) разбира се могат да смущават и 2.4GHz

Разбира се тези техники са си военни разработки:) в армията си има от край време УКВ радиосмутители ... те са си предназначени за създаване на смущения в тактическите контролни единици на врага работещ в честотна лента 20 - 100 MHz и разни др. честоти и поддиапазони и т.н.
В армията има такива радиосмутители, които се изстрелват от оръдия:) и започват след това да смущават свръзките на врага:) разбира се те са свръх мощни и смущават в радиус 700м и то в продължение на цял час:)
Знаете, че има и така наречените возими радиосмутители...те са предназначен за защита от

дистанционно активирани по радиоканал взривни устройства.Защитава единични и групови подвижни обекти, групи от хора или други цели. Модулите смущават различно широки честотни ленти, намиращи се на различни участъци по честотната ос.Някои от модулите са широколентови и работят в диапазона от 20MHz до 2000MHz ,а др. модули са специализирани и са предназначени за смущаване на най-често използуваните при терористичните актове честотни диапазони, включително и за смущаване работата на клетъчните телефони, на сателитните телефони и на GPS системите. Всеки модул работи с отделна антена.Антените са широколентови и излъчват кръгово.

Но по-вероятно при вас е, че ще разберете от журналния файл за достъпа, че съседа е използвал безплатно широколентовата ви Интернет връзка:) друго едва ли ще разберете:)
В повечето случаи тези видове атаки изискват от кракера висока степен на технически познания, като могат да бъдат възпрепятствани максимално чрез активирането на всички налични мерки за сигурност.
Сменете стойността по подразбиране на SSID и изключете разпространяването на SSID

Повечето точки за достъп разпространяват своите SSID имена по подразбиране, и доста е малък %-та с включена WEP защита. Смяната на стойността по подразбиране и изключването на разпространяването на SSID (ако точката за достъп позволява) са първите стъпки, които ще предпазят мрежата от любопитни безделници като мен примерно хах:)
Използвайте парола за администриране!
Убедете се, че конфигурационната функция на точката за достъп е защитена с парола, така че неоторизирани потребители да не могат да се сдобият с достъп и да променят настройките на защитата.
Включете WEP !
Включването на WEP, използването на трудни за отгатване ключове и редовната им авто смяна са важни мерки за защитата. След ратифицирането на стандарта IEEE 802.11 i,
WEP постепенно се заменя с WPA
Филтриране на MAC адреси!
Филтрирането на MAC адреси дава възможност да защитите безжичната си мрежа, като разрешите достъп само на регистрираните в точката за достъп компютри(те биват прихващани от рутера по своя MAC и рутерът дава нет само към тях)
Използвайте конфигурационното приложение на точката за достъп, за да въведете разрешените MAC адреси в списъка за филтъра. Поддържайте този списък актуален и своевременно изтривайте старите записи!
Използвайте персонална защитна стена!
Инсталирайте и включете защитна стена, която ще изпълнява ролята на защитна бариера. Ако локалната и безжичната мрежа са свързани към Интернет през маршрутизатор, то там е и мястото за инсталиране на защитна стена.
Ако използвате лаптоп с безжичен адаптер за връзка към публична точка за достъп, включете антив. програма на Windows XP за безжичната връзка или инсталирайте друг подобен продукт.
Помислете за варианта с ръчно задаване на IP адресите.
Въпреки че DHCP е по-лесният начин за настройка, ръчното задаване на IP адресите на компютрите в безжичната мрежа ще попречи на неоторизирани компютри да получават адресите си автоматично.
Ако решите да задавате IP адресите ръчно, задаването на различен от подразбиращия се за точката за достъп диапазон от частни адреси би затруднило отгатването им от страна на потенциалните кракери. Например за Linksys диапазонът по подразбиране започва от 192.168.1.100.
Може за други да е 192.168.2.1 и др.
Можете да използвате произволен набор от частните адреси.
Монтирайте точките за достъп далече от прозорци:)
Монтирането на точките за достъп далече от външни стени и прозорци ще намали силата на сигнала, излъчван навън от дома или офиса, и така ще се намали пространството, в което към мрежата могат да се свържат неоторизирани потребители.
Включете журналната функция и редовно преглеждайте записите за достъпа!

Поддържането на журнал на безжичния достъп е една от административните функции на точките за достъп. Активирайте тази функция и редовно проверявайте съдържанието на журнала за неоторизиран достъп.Поддържайте фърмуера актуален(ъпдейтване на програмата и драйверите)
Накрая, ако производителят на мрежовото оборудване предлага актуализации на фърмуера и драйверите, изтеглете ги и ги инсталирайте, за да поддържате системата си в актуално състояние, включително по отношение на сигурността.
Изключвайте безжичните адаптери, когато не ги използвате.
Докато безжичният мрежов адаптер е активен, Windows XP непрекъснато търси точка за достъп или равноправна връзка, която да съвпада с някой от дефинираните мрежови профили.
Възможно е потенциален кракер да включи фалшива точка за достъп, която да съвпада с някой от профилите ви за връзка с обществени точки за достъп. Изключването на бездействащия безжичен адаптер ще предотврати такъв вид атака.
Влезте в менютата на мрежовия адаптер като отворите папката Network Connections от стартовото меню или от иконата на десктопа.
Щракнете с десния бутон на мишката в/у Wireless Connection и изберете Disable(Забранено)
Когато решите да използвате адаптера, повторете тези стъпки и изберете Enable(Разрешено)
Стандартът за защитен безжичен достъп (Wi-Fi Protected Access или WPA) е разработен с цел преодоляване на известните недостатъци на разгледания по-горе WEP.
WPA е дефиниран в стандарти IEEE 802.11 i, който е бил ратифициран през 2003 г. и предоставя нови възможности за защити в пет ключови области.
Протокол за интегритет с временни ключове (Temporal Key Integrity Protocol -TKIP)
Криптирането при WPA е задължително, за разлика от по-ранните стандарти от серията 802.11.
TKIP променя криптиращите ключове и управлява синхронизирането на променените ключове в цялата безжична мрежа.

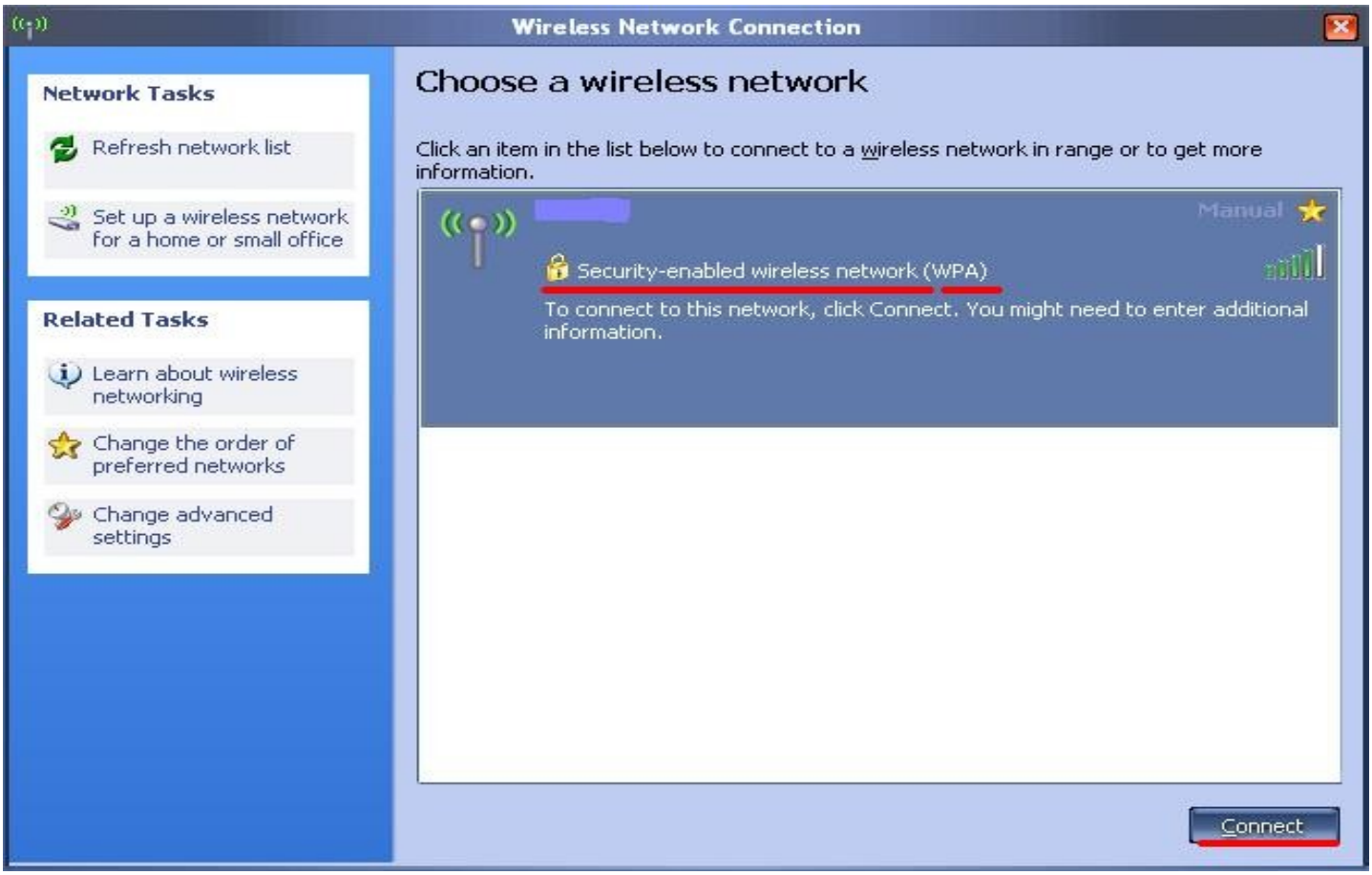
WPA усъвършенства проверките на интегритета с нов 8-байтов код за интегритет (Message Integrity Code - MIC)
Той се използва за потвърждение, че данните в изпратения фрейм не са променени.
Усъвършенстван стандарт за криптиране (Advanced Encryption Standard - AES)
AES подменя криптирането с WEP с нов алгоритъм, който използва 128-, 192- или 256-битови ключове, вместо оригиналните 40-битови на WEP.
В новия стандарт AES е опция. Това е така, понеже WPA трябва да е обратно съвместима с по-ранните устройства по стандарта 802.11, а този нов алгоритъм не може да се реализира като актуализация на фърмуера и изисква нови чипсети.
Удостоверяване на потребителя:
В предишните версии на 802.11 удостоверяването на потребителите беше опция, но във WPA то е задължително. Удостоверяването може да е с предварително договорен общ ключ, а за по-големи мрежи WPA поддържа използването на отделен сървър за удостоверяване.
Инсталиране на WPA
Въпреки че пълната реализация на WPA със сертифицирана съвместимост чака появата на новите хардуерни устройства, много от функциите са достъпни с инсталирането на безплатни актуализации на фърмуера на наличното безжично оборудване.
Може да се наложи да актуализирате и Windows XP:
Актуализацията на Windows XP за активиране на WPA е достъпна за безплатно изтегляне от уебсайта на Microsoft за поддръжка на адреси:
http://support.microsoft.com/?kbid=815485

http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx

http://www.microsoft.com/downloads/details.aspx?familyid=662bb74d-e7c1-48d6-95ee-1459234f4483&displaylang=en

http://www.microsoft.com/downloads/details.aspx?FamilyID=2726f32f-d52b-4f84-ace8-f7fc20195769&DisplayLang=en

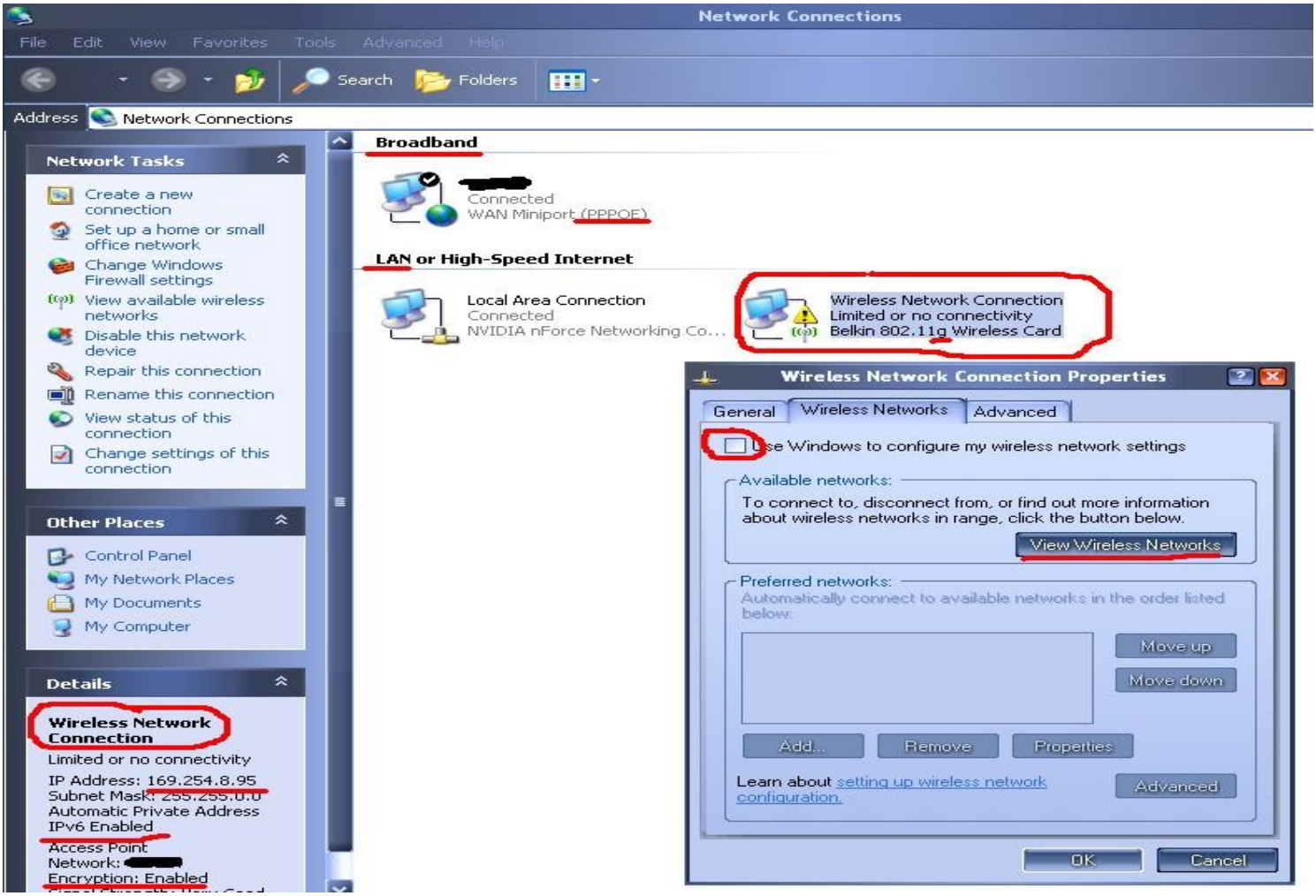
http://www.microsoft.com/downloads/details.aspx?familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en



С включен WPA изглежда така...

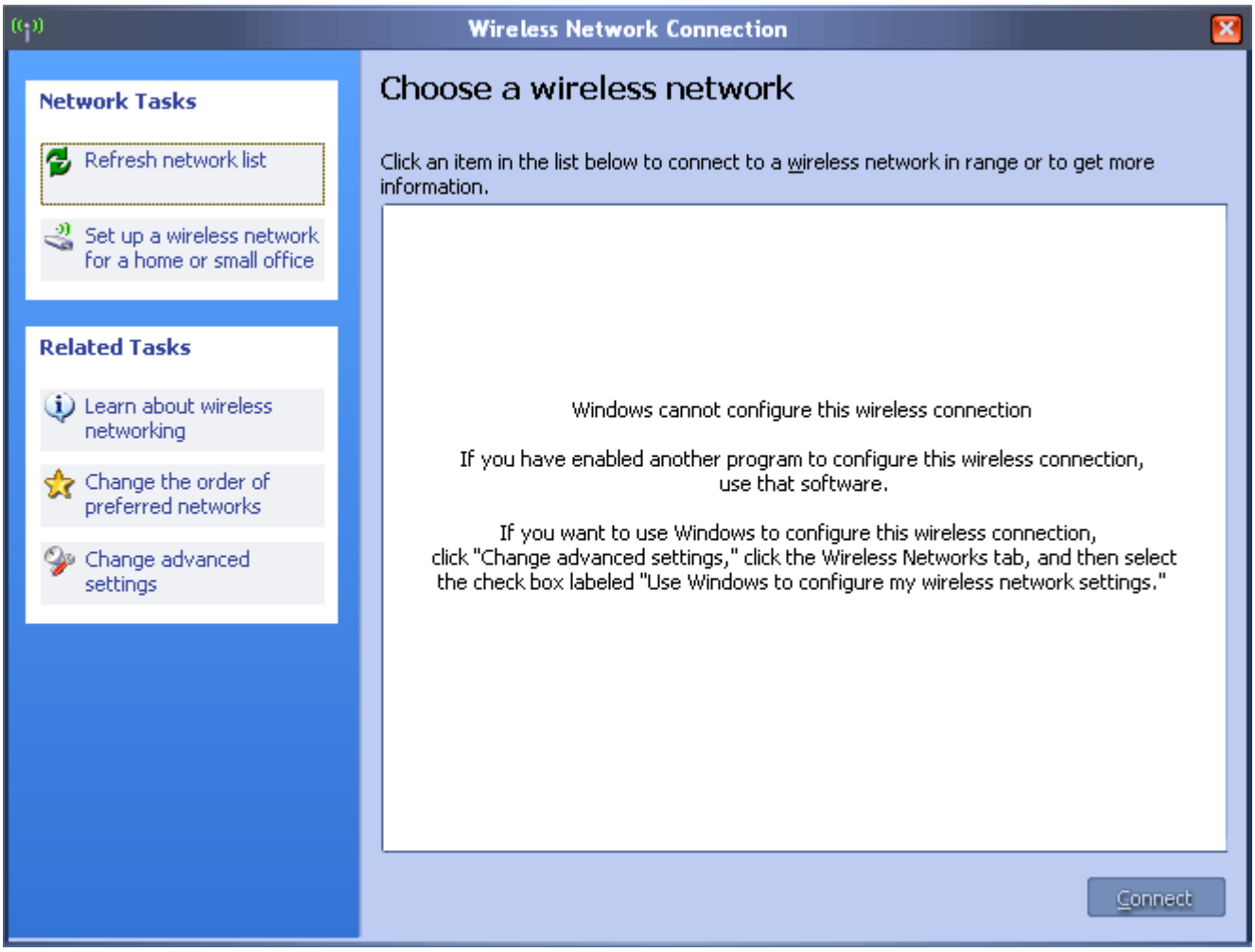
Допълнителна защитна функция на актуализацията SP1/WPA е предупреждението от страна на Windows XP и изискването на потвърждение за свързване към безжична мрежа, за която WEP не е активиран. Изтегляне и инсталиране на актуализацията за WPA:
Стартирайте Internet Explorer и въведете горния URL в адресното поле. Ще се зареди обзорната статия за актуализирането с WPA.Периодичните обновления на Windows се предоставят като сервизни пакети (Service Pack - SP). За обновяване на безжичната сигурност до стандарта WPA версията на Windows XP трябва да е най-малко на нивото на SP 2.
Освен актуализирането с WPA, актуализирането на версията на Windows XP със Service Pack 2 ще обнови и други аспекти на сигурността на Windows XP, ще подобри съвместимостта с различни приложения и ще повиши стабилността на операционната система(разбира се най-добре е със SP 3)

Ето така би трябвало да изглежда системата уиндоус хр с инсталирана безжична мрежова карта на настолен комп (и с протокола PPPoE) :

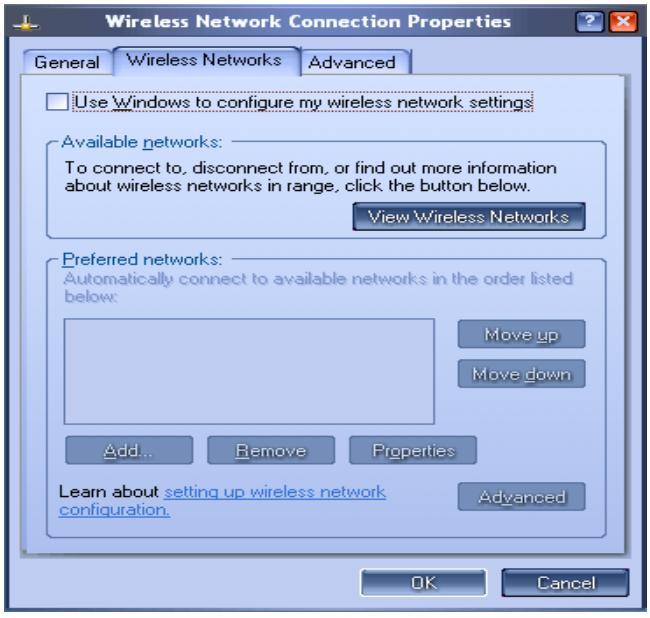


Виждате,че както сме се свързали с ланката и сме се конектнали към нет доставчика ни по протокола PPPoE ние в същото време можем и да се се свържем към някой рутер с нашата безж. мреж. карта,която сме я поставили на PCI слот на дъното...
Сега ние получаваме съобщение,че не сме успели да се конектнем към рутера:) и се показва това жълто триъгълниче:)Всъщност не е точно така...виждате получили сме някакъв адрес 169.254.8.95 (може да е всякакъв)По принцип ни го дава отдалеченият рутер.
За да се конектваме обаче с нашата безжична мрежова карта ние в момента ползваме нейният софтуер (програмата на производителя) и не използваме самата операционна с-ма...
За да направим така,че да си ползваме операционната с-ма,за да се конектваме към даден рутер правим следното:

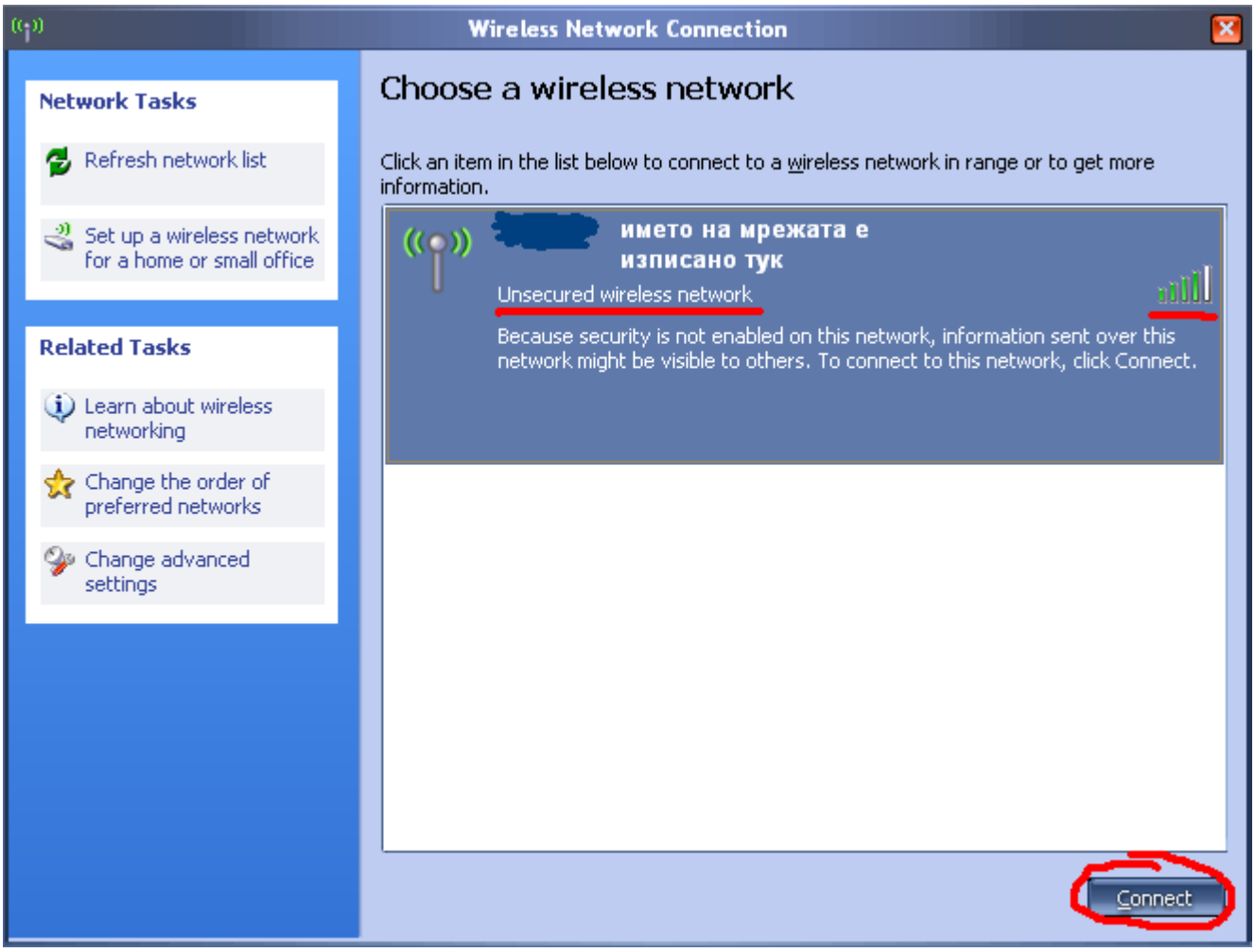
Отмятаме на Use Windows to configure my wireless network settings
Това става като кликнем с десен бутон на мишката в/у иконката Wireless Network Conection и отидем на Своиства (Properties) или кликаме на View Available Wireless Networks ,или просто двойно кликане в/у иконката:)



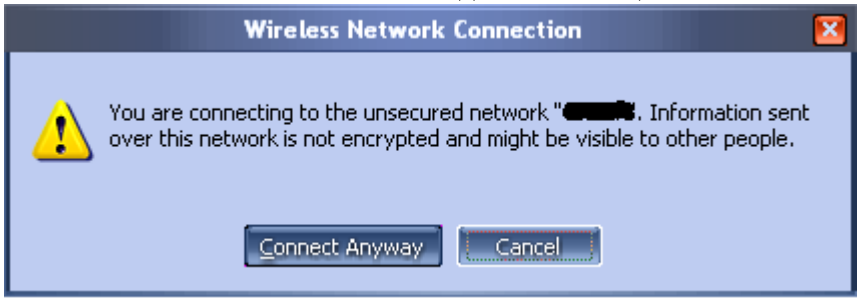
и ето това ще видите:) идете на Change the order of preferred networks и ще видите същият прозорец



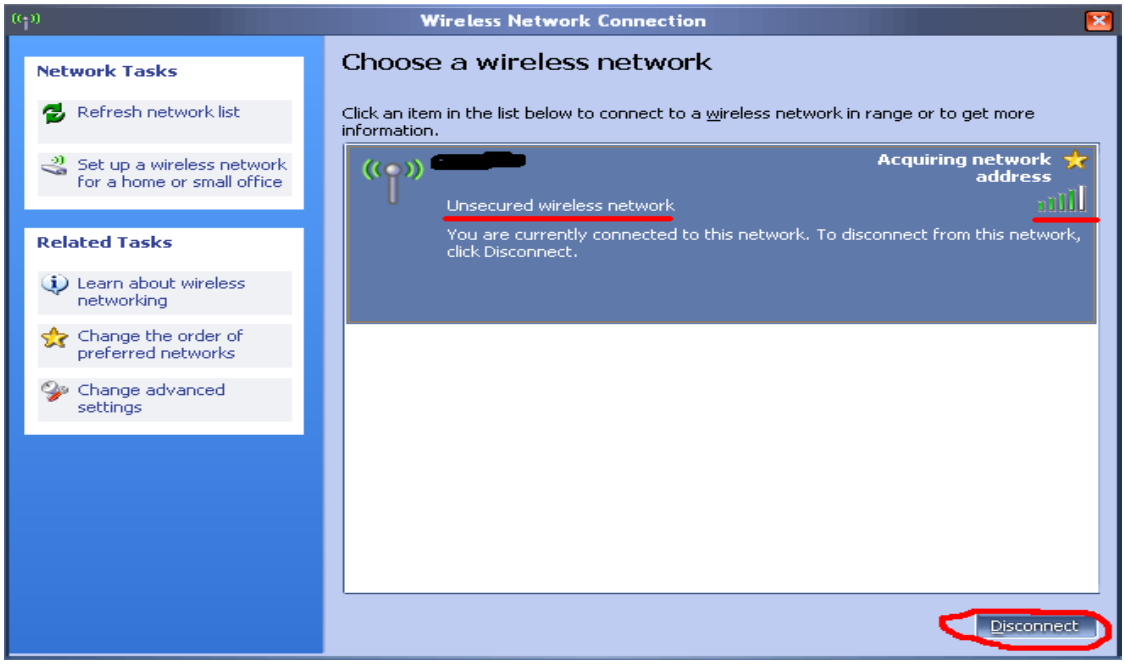
и си отметнете да се конфигурира всичко от самата си система...
Натиснете няколко пъти Refresh network list



На картинката в случая виждате: силата на сигнала и това,че безжичната мрежа не е криптирана и защитена...и се свързваме към нея...но се появява следното съобщение:



То ни съобщава,че се свързваме към незащитена мрежа и че изпращайки данни през нея те няма да са криптирани:)и могат да бъдат уловени...



Разбира се сега сме се свързали към рутера, но сме и с протокола PPPoE а той изисква потребителско име и парола:) през цялото време може и да ви изписва Acquiring network address а после да изпише Limited or no connectivity :)не се тревожете и да си го има това жълто триъгълниче, нет ще си имате:)
Рутерът,който ползваме е конфигуриран да работи по този протокол...и ние трябва да знаем кой е доставчика в случая и да знаем на кой протокол пускат нета:) и да имаме чужди паролки:)
Ето разбрахте,че може да не е защитен кой знае колко този маршрутизатор,но все пак ако е конфигуриран по PPPoE няма да можете да ползвате нета му:)
Затова е добре да имате пароли и потребителски имена за 2-3 големи нет доставчика...те си важат за цялата страна и ще можете да си се свързвате,ако е на този протокол маршрутизатора:)
Разбира се може да са конектнати едновременно и ланката и безжичната то не пречи:)
Разбира се може да изключите:
File and Printer Sharing for Microsoft Networks
и Client for Microsoft Networks
Microsoft TCP/IP version 6 (ако сте си я инсталнали:)
Internet Protokol(TCP/IP)
не за друго,ами да не ви досаждат разни пишман кракерчета:) просто махнете отметките:)
споко нет ще си има и още как:)

Други сканиращи инструменти (scanning tools), за които се сещам са:

Redfang 2.5	**за Bluetooth**
THC-WarDrive	**линукс базиран инструмент за gps**
PrismStumbler	**http://prismstumbler.sourceforge.net**
MacStumber	**http://www.macstumbler.com**
Mognet	**сниферче писано на java и е за линукс ос**
WaveStumbler	**конзолно базирано за линукс**

StumbVerter или Stumbverter
AP Scanner
SSID Sniff

Wavemon	**http://freshmeat.net/projects/wavemon**

Wireless Security Auditor (WSA)

AirTraf	**http://www.elixar.com**

Sniffing инструменти:

AiroPeek
NAI Wireless Sniffer
Ethereal
VPNmonitorl
Aerosol
vxSniffer
EtherPEG
DriftNet
WinDump
ssidsniff
AirMagnet

Ами това е:)