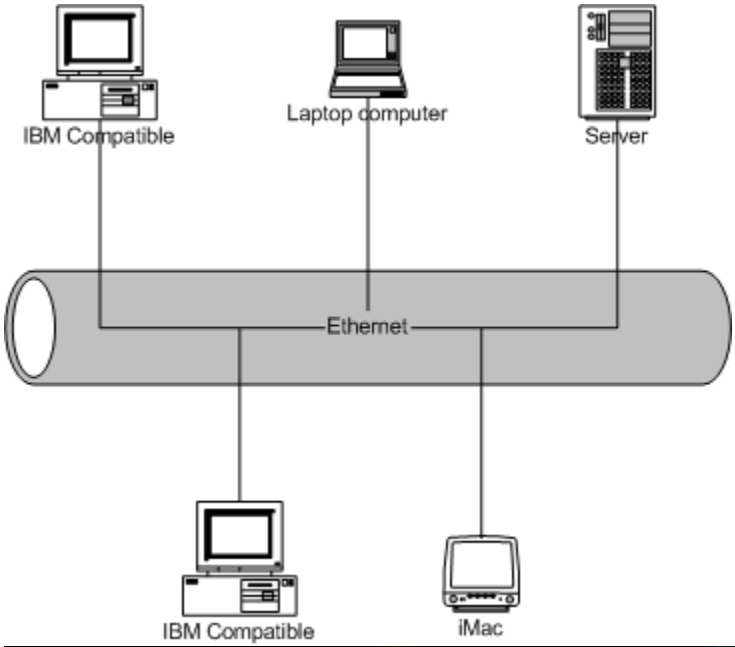
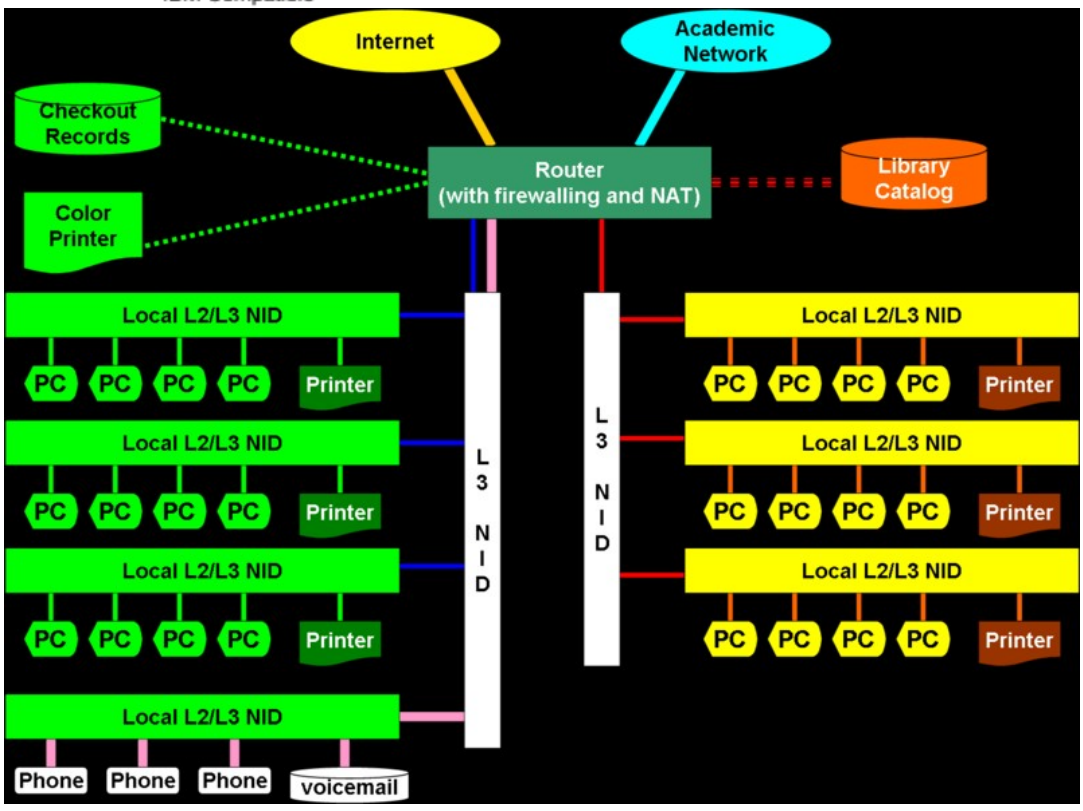
Computer Network

A computer network is a group of interconnected computers. Networks may be classified according to a wide variety of characteristics. This article provides a general overview of some types and categories and also presents the basic components of a network.





Connection method

Computer networks can also be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as Optical fiber, Ethernet, Wireless LAN, HomePNA, or Power line communication.

Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges and/or routers.

Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

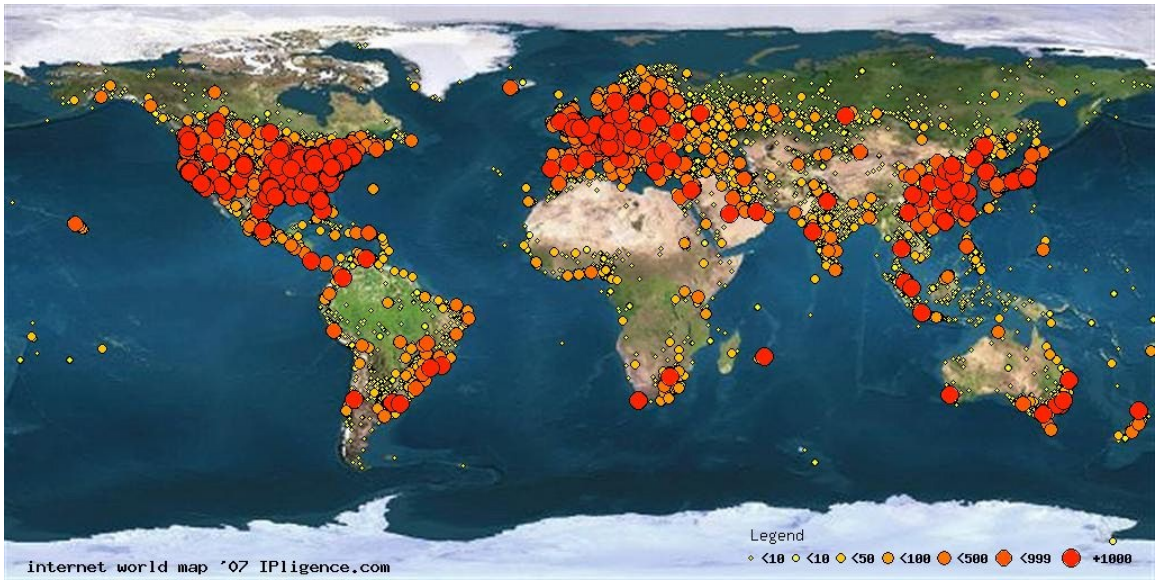
Scale

Based on their scale, networks can be classified as Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Personal Area Network (PAN), Virtual Private Network (VPN), Campus Area Network (CAN), Storage Area Network (SAN), etc.

Intranet
An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

Internet

The Internet is a specific internetwork. It consists of a worldwide interconnection of governmental, academic, public, and private networks based upon the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the U.S. Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW). The 'Internet' is most commonly spelled with a capital 'I' as a proper noun, for historical reasons and to distinguish it from other generic internetworks.



www.ipligence.com/worldmap/

Basic hardware components

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required, usually in the form of galvanic cable (most commonly Category 5 cable). Less common are microwave links (as in IEEE 802.12) or optical cable ("optical fiber"). An ethernet card may also be required.

Network interface cards

A network card, network adapter or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses.

Repeaters
A repeater is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable runs longer than 100 meters.

Hubs
A hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address.

Bridges
A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port.

The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

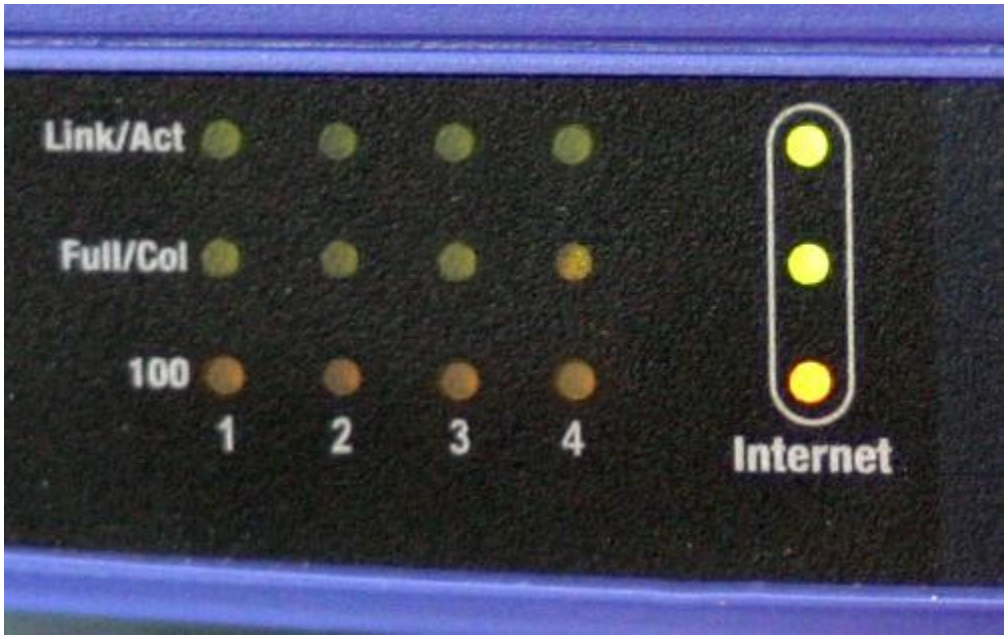
Bridges come in three basic types:
Local bridges: Directly connect local area networks (LANs)
Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced by routers.
Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

Switches
A switch is a device that forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets.[3] This is distinct from a hub in that it only forwards the packets to the ports involved in the communications rather than all ports connected. Strictly speaking, a switch is not capable of routing traffic based on IP address (OSI Layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports, with the intention being that most or all of the network is connected directly to the switch, or another switch that is in turn connected to a switch.

Switch is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier). Switches may operate at one or more OSI model layers, including physical, data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is called a multilayer switch.

Routers

Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. Routers work at the network layer .



Internet Protocol (IP) address

An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes.[1] Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and 2001:db8:0:1234:0:567:1:1 (for IPv6). The role of the IP address has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there." [2]

Static and dynamic IP addresses

When a computer is configured to use the same IP address each time it powers up, this is known as a Static IP address. In contrast, in situations when the computer's IP address is assigned automatically, it is known as a Dynamic IP address.

Setting up an IP address in windows
The dialog you are looking for is here..

Control Panel >> Network Connections >> Local Area Connection >> Properties >> TCP/IP >> Properties

In other words, open the control panel, open Network Connections, right-click the "Local Area Connection" (unless you've renamed it to something else) and chose "Properties", then (in the "general" tab) select "Internet Protocol(TCP/IP)" and click the "Properties" button. Check the "Use the Following IP address" checkbox and enter your desired IP address. If you use 192.168.1.3 as your IP address.

Ping
Ping is a computer network tool used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a speed test. It works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. Ping measures the round-trip time[1] and records any packet loss, and prints when finished a statistical summary of the echo response packets received, the minimum, mean, max and in some versions the standard deviation of the round trip time.

When ping fails, you’ll see one of these error messages:
Request timed out - The IP address is valid, but there’s no reply from it. If the IP address is on a local area network, the most likely cause is a firewall program blocking the ping.

Unknown host <name> or Ping request could not find host <name> - The computer name doesn’t exist on the local area network. Make sure that NetBIOS over TCP/IP is enabled.

Destination host unreachable – The IP address isn’t on a local area network, and the default gateway can’t access it. Either there’s no default gateway, its address is wrong, or it isn’t functioning.

Traceroute
traceroute is a computer network tool used to determine the route taken by packets across an IP network. An IPv6 variant, traceroute6, is also widely available.

The traceroute tool is available on practically all Unix-like operating systems. Variants with similar functionality are also available, such as tracepath on modern Linux installations and tracert on Microsoft Windows operating systems. Windows NT-based operating systems also provide pathping, which provides similar functionality.

If you are a MS-DOS or Windows user or the traceroute command if you are a Linux / Unix variant user. To use this command you must be at the command prompt or shell.

Once at the prompt, assuming that the address is again 102.55.92.2, type:

tracert 102.55.92.2

or

traceroute 102.55.92.2

This should begin listing the hops between the computer and network devices. When the connection fails, determine which device is causing the issue by reviewing the traceroute listing.

Troubleshooting basics
Verify connections / LEDs

Verify that the network cable is properly connected to the back of the computer. In addition, when checking the connection of the network cable, ensure that the LEDs on the network are properly illuminated. For example, a network card with a solid green LED or light usually indicates that the card is either connected or receiving a signal. Note: generally, when the green light is flashing, this is an indication of data being sent or received.

If, however, the card does not have any lights or has orange or red lights, it is possible that either the card is bad, the card is not connected properly, or that the card is not receiving a signal from the network.

If you are on a small or local network and have the capability of checking a hub or switch, verify that the cables are properly connected and that the hub or switch has power.

Adapter resources
Ensure that if this is a new network card being installed into the computer that the card's resources are properly set and/or are not conflicting with any hardware in the computer.

Users who are using Windows 95, 98, ME, 2000 or XP, verify that Device Manager has no conflicts or errors. Additional help and information about Device Manager and resources can be found on our Device Manager page.

Adapter functionality

Verify that the network card is capable of pinging or seeing itself by using the ping command. Windows / MS-DOS users ping the computer from a MS-DOS prompt. Unix / Linux variant users ping the computer from the shell.

To ping the card or the localhost, type either
ping 127.0.0.1

or

ping localhost

This should show a listing of replies from the network card. If you receive an error or if the transmission failed, it is likely that either the network card is not physically installed into the computer correctly, or that the card is bad.

Firewall

If your computer network utilizes a firewall, ensure that all ports required are open. If possible, close the firewall software program or disconnect the computer from the firewall to ensure it is not causing the problem.

Additional time

In some cases it may take a computer some additional time to detect or see the network. If after booting the computer you are unable to see the network, give the computer 2-3 minutes to detect the network. Windows users may also want to try pressing the F5 (refresh) key when in Network Neighborhood to refresh the network connections and possibly detect the network.

ipconfig /all
What information ipconfig gives:
IP Address – Unique address assigned to a network adapter. A computer with multiple network adapters has an IP address for each one, and each one must be in a different subnet.
Subnet Mask – Used in conjunction with the IP address to determine which subnet an adapter belongs to. At the simplest level, communication is only possible between two network adapters when they're in the same subnet.
Default Gateway - IP address of a computer or router, on one of this computer's local area networks, that knows how to communicate with subnets not present on this computer. For an Internet connection, the default gateway is a router belonging to your Internet service provider, and all access to sites on the Internet goes through it. For an ICS client, the deWhen ping fails, you'll see one of these error messages:
Request timed out - The IP address is valid, but there's no reply from it. If the IP address is on a local area network, the most likely cause is a firewall program blocking the ping.
Unknown host <name> or Ping request could not find host <name> - The computer name doesn't exist on the local area network. Make sure that NetBIOS over TCP/IP is enabled.
Destination host unreachable – The IP address isn't on a local area network, and the default gateway can't access it. Either there's no default gateway, its address is wrong, or it isn't functioning.fault gateway is the ICS host. If you use a hardware router, it serves as the default gateway.
DHCP Server – If an adapter is configured to obtain an IP address automatically, this is the address of the server that provides it. It could be your ISP, an ICS host, or a hardware router.
DNS Servers – IP address of one or more Domain Name Server computers. DNS servers translate Internet names (like www.practicallynetworked.com) to their IP addresses (like 63.146.109.227).

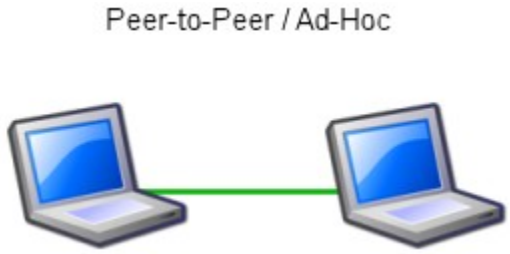
Wireless

Wireless local area network (WLAN) links devices via a wireless distribution method.

Types of WLAN

ad-hoc

An ad-hoc network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk.



Bridge

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

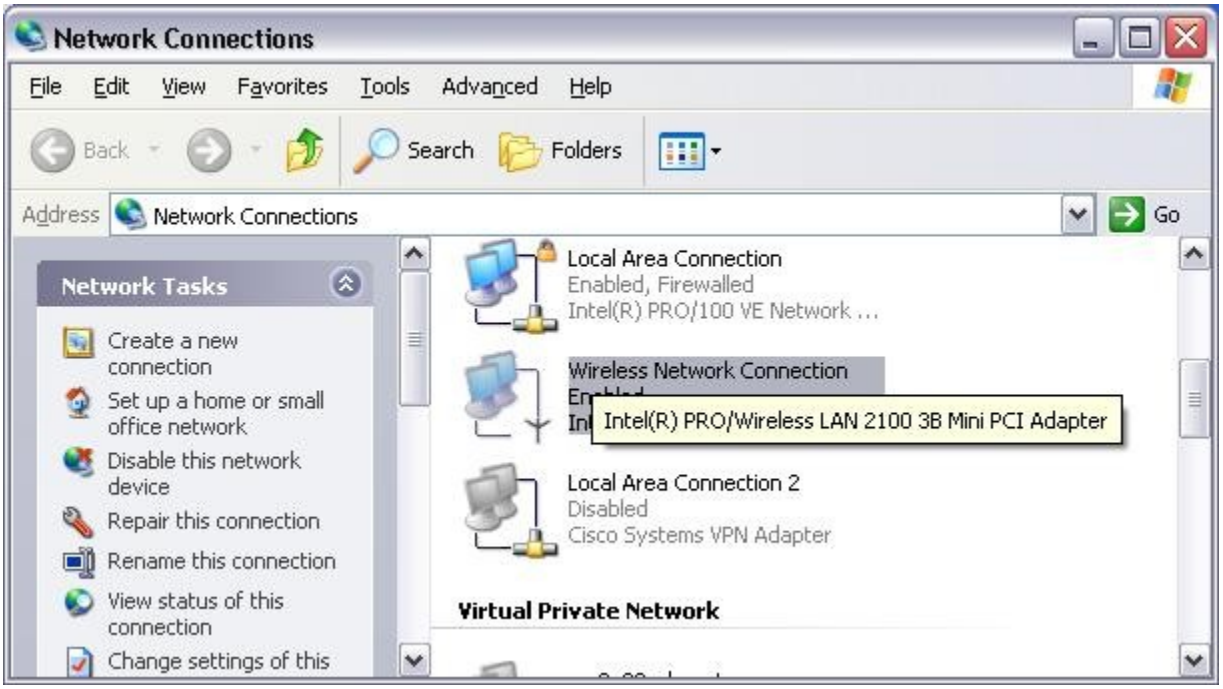
Hotspot (Wi-Fi)

A hotspot is a physical location that offers internet access over a wireless LAN through the use of a shared internet connection and a single router.

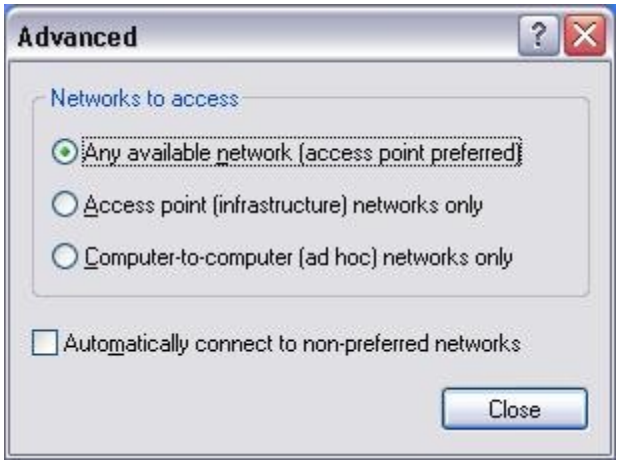
Connecting to Wireless LAN using Win XP

I. To configure your builtin wireless LAN card:

1. On ***Start Menu*** , click ***Connect To*** and then ***Show all connections***
2. Then you will see the screen as shown on left. Right click ***Wireless Network Connection*** and select ***Properties***



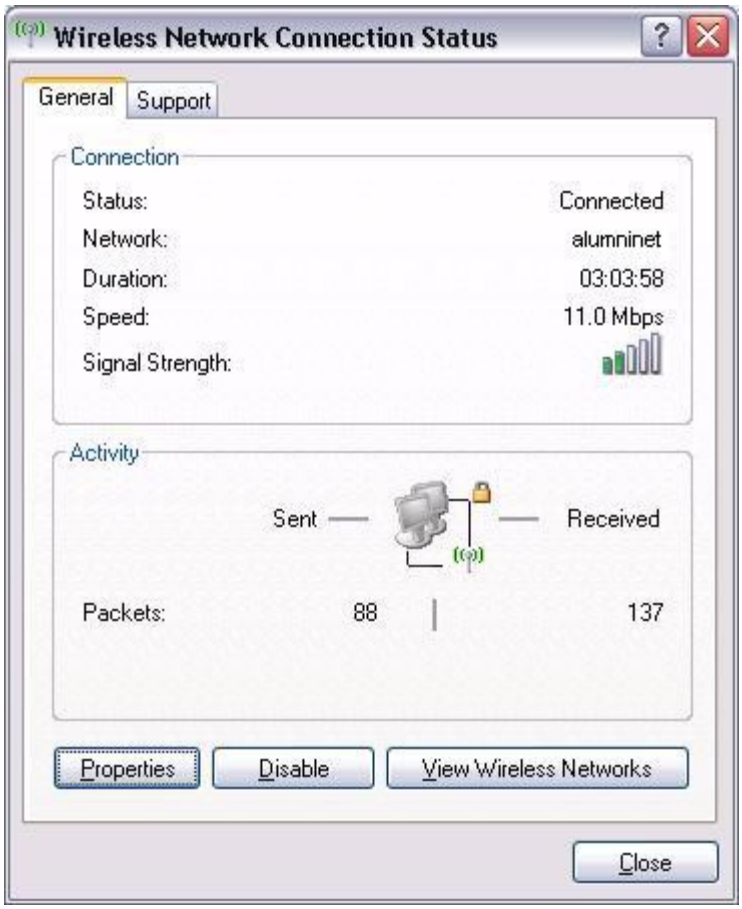
II. Click ***Wireless Networks*** tab and then click ***Advanced***, deselect ***Automatically connect to non-preferred networks*** and click ***Close***.



and then click ***Add...*** in ***Preferred networks***.

III. Fill in the name ***SSIDnetworkName*** in the field ***Network name (SSID)*** and select ***Disabled*** in ***Data Encryption***

Click ***OK***. If the network can be found, the status of the builtin wireless LAN card show ***Connected***.


Wireless Network Connection Status
General
Support
Connection
Status:
Connected
Network:
alumninet
Duration:
03:03:58
Speed:
11.0 Mbps
Signal Strength:
Activity
Sent
Received
Packets:
88
137
Properties
Disable
View Wireless Networks
Close

Wireless Security

What is SSID (Service Set IDentifier)
The SSID is a secret key which is set by the network administrator.
You must know the SSID to join an 802.11 network. However, the SSID can be discovered by network sniffing. By default, the SSID is part of the packet header for every packet sent over the WLAN.

SSID Security Issues
The fact that the SSID is a secret key instead of a public key creates a key management problem for the network administrator. Every user of the network must configure the SSID into their system. If the network administrator seeks to lock a user out of the network, the administrator must change the SSID of the network, which will require reconfiguration of the SSID on every network node. Some 802.11 NICs allow you to configure several SSIDs at one time.

Default SSID's
Most 802.11 access point vendors allow the use of an SSID of "any" to enable an 802.11 NIC to connect to any 802.11 network. This is known to work with wireless equipment from Buffalo Technologies, Cisco, D-Link, Enterasys, Intermec, Lucent, and Proxim. Other default SSID's include "tsunami", "101", "RoamAbout Default Network Name", "Default SSID", and "Compaq".

Disabling SSID Broadcasting
Many Wireless Access Point (WAP) vendors have added a configuration option which lets you disable broadcasting of the SSID. This adds little security because it is only able to prevent the SSID from being broadcast with Probe Request and Beacon frames. The SSID must be broadcast with Probe Response frames. In addition, the wireless access cards will broadcast the SSID in their Association and Reassociation frames. Because of this, the SSID cannot be considered a valid security tool.

Wired Equivalency Protocol (WEP)

What is WEP it is a deprecated (out of date/not used) algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are thus more susceptible to eavesdropping than wired networks.

Why not to use WEP
In August 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir published a cryptanalysis of WEP that exploits the way the RC4 cipher and IV is used in WEP, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network. Depending on the amount of network traffic, and thus the number of packets available for inspection, a successful key recovery could take as little as one minute. If an insufficient number of packets are being sent, there are ways for an attacker to send packets on the network and thereby stimulate reply packets which can then be inspected to find the key. The attack was soon implemented, and automated tools have since been released. It is possible to perform the attack with a personal computer, off-the-shelf hardware and freely available software such as aircrack-ng to crack *any* WEP key in minutes.

Wi-Fi Protected Access (**WPA** and **WPA2**)
WPA2 replaced WPA; like WPA, WPA2 requires testing and certification by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, which is considered fully secure. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.

Pre-shared key mode (PSK, also known as *Personal* mode) is designed for home and small office networks that don't require the complexity of an 802.1X authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters

Setting up WPA2 on a Eircom router
http://www.bartbusschots.ie/blog/?p=793

Troubleshooting Wireless

1. Start by rechecking your physical connections -- a common culprit that is often overlooked. Check your wireless router's WAN port link to your cable/DSL modem and LAN port links to Ethernet clients. Make sure that WAN and LAN cables are inserted tightly and the status lights are on at both ends. If not:

* Try swapping Ethernet cables to isolate a damaged cable.

* Check your router's manual to make sure that you're using the right type of cable -- some WAN uplinks require cross-over cables.

* If status lights are still off, connect another device like a laptop to the affected WAN or LAN port. If status changes, to device you just replaced may be failing link auto-negotiation. Check port configurations at both ends and reconfigure as needed to match speed and duplex mode.

2. Next, verify that your client's wireless adapter is installed and working properly On a Windows client, select your wireless connection from the Network Connections panel and verify that its status is "Enabled."

* If the adapter is not listed, there may be a problem with the associated PC Card slot or USB adapter cable. If removing and reconnecting the adapter does not help, use Device Manager to uninstall / reinstall that adapter.

* If the adapter is listed but the connection cannot be enabled, use the Properties panel to spot resource conflicts or update the driver.

3. Next, verify that your wireless router's LAN settings are correct. Use your router's admin utility to determine its LAN port IP address and subnet.

* Make sure the router's DHCP server is set to assign IPs using a non-overlapping range in the same subnet as the LAN port address.

* If your router's DHCP Server is set to filter access by MAC address, add your client's MAC address to that "allowed device" list.

* Check your router's Log or Status page to verify that an IP address is indeed assigned to your wireless client whenever it connects.

4. Next, verify your client's TCP/IP settings. Although we describe using Windows to manage wireless connections here, troubleshooting is conceptually similar when using any other connection manager (e.g., Intel, Linksys).

* Open the Network Connections panel and select your wireless connection. If the status is still "Disabled," return to step 2.

* If status is "Not Connected," use View Available Networks to select your wireless network and click Connect. If your network's name does not appear in Available Networks or you cannot connect to your network, go to step 8 to debug wireless settings.

* While attempting to connect, status may change briefly to "Acquiring Network Address," then "Connected." At that point, use Status/Support to determine the client's assigned IP address. If the client's IP is 0.0.0.0 or 169.254.x.x, click Repair. If that problem persists, go to step 8.

* Otherwise, if the connected client's IP address is not in your router's LAN subnet, use the Properties / Internet (TCP/IP) panel to reconfigure the connection to get an address automatically and repeat step 4.

5. Once your client has a valid IP address, use "ping" to verify network connectivity. Run a command window from the client's start menu and use it to ping your router's LAN IP address as shown in Figure 5.

* If pinging your router repeatedly fails, skip to step 6.

* If pinging your router is successful, then ping any other wired or wireless LAN client that you wish to share files or printers with. If that ping fails, then the destination may be using a firewall to block incoming messages.

On Windows XP SP1 or earlier, use the connection's Properties panel to temporarily disable the Internet Connection Firewall.

On Windows XP SP2 or later, use the client PC's control panel to temporarily disable the Windows Firewall.

If no Microsoft firewall was running, check for a third-party personal firewall like ZoneAlarm and temporarily disable it.

* After disabling the destination's personal firewall, ping that client again. If ping is now successful, then the firewall you disabled may also be blocking Windows Network protocols. Reconfigure the firewall to permit the traffic you want to exchange between LAN clients. For example, to share files and printers, permit incoming NetBIOS connections from your LAN subnet. Don't forget to re-enable the firewall when finished!

6. If your wireless client still cannot connect, get a valid IP address, or ping your router, it's time to consider wireless-specific problems. The router and client must use compatible 802.11 standards and the same network name (SSID). Use your router's admin utility to view WLAN settings and compare them to your client's wireless connection parameters.

* If your router's network name does not appear in the client's Available Networks list, enable "SSID broadcasts" on your router. Alternatively, add the network name to your client's Preferred Connections manually. Be sure to match the router's SSID exactly, including capitalization.
* With an 802.11b client, you must use an 11b, g, or n router. If any 11b clients are present, enable b+g protection on your 11g router.
* With an 802.11a client, you must use an 11a router. For dual-band products, you may configure both ends to use 11b/g, a, or both.
* 802.11g or 11n clients can generally use 11g or n routers. However, in mixed 11g/n WLANs, disable any vendor extensions (e.g., turbo mode).

7. If a matched wireless client and router can "hear" each other but still cannot connect or exchange traffic, look for a security mismatch. The client must support the security mode required by the router: Open, WEP, WPA, or WPA2. Unless the WLAN is open (unsecured), the router and client must also have (or dynamically receive) the same keys used to encrypt traffic between them. Compare your router's WLAN security settings to your client connection's preferred network properties and attempt to match them.

* If your router uses WEP, set the client's encryption to WEP and match the router's authentication type (open or shared). Copy the router's first WEP key to the client, translating from ASCII to hex if needed.
* If your router uses WPA-Personal, set the client's authentication to WPA-PSK and match the router's encryption type (TKIP or AES). Use the router's passphrase as the client's network key; capitalization counts!
* If your router uses WPA2-Personal, set the client's authentication to WPA2-PSK and use the router's passphrase as the client's network key.
* If your router uses WPA or WPA2-Enterprise, set the client's authentication to WPA or WPA2 respectively, match the router's encryption type, and continue 802.1X set-up in step 8.

Making the Wireless Home Network Connection in Windows XP Without a Router
http://www.microsoft.com/windowsxp/using/networking/expert/bowman_02april08.msp
x