

## Planning your Wireless Network

### **1. Infrastructure or Adhoc mode.**

Adhoc mode is used when several wireless workstations establish links without the use of a Network Gateway or Wireless Access Point.

Use Adhoc mode if you wish to join several wireless clients to each other in a small area and you do not need these devices to access your Internet connection or other “wired services”. If you include a Wireless Access Point (AP) in your network this changes the network to Infrastructure Mode.

When connecting to an Adhoc network you must know the following parameters in order to configure your Client Adapter correctly to join the Adhoc network:

- Network Name (SSID)
- Network Channel
- Encryption type (none, 64bit WEP, 128bit WEP, WPA)
- Encryption keys (only if encryption is enabled)

You can also use Infrastructure mode if you wish to join several wireless clients together over a wider area as well as offer them access to “wired services” (such as a LAN with Network printers or Servers). An Infrastructure-mode network requires the use of one or more Access Points (AP’s) to be installed. NetComm Wireless Routers operate as Access Points and are a great way of sharing your Internet connection wirelessly.

*Note: Access Points can only operate in Infrastructure mode. Adhoc networks are often temporarily setup between two or more Wireless clients to share files at a conference etc.*

When connecting to an Infrastructure network you must know the following parameters in order to configure your Client Adapter correctly to join the Infrastructure network:

- Network Name (SSID)
  - Encryption type (none, 64bit WEP, 128bit WEP, WPA)
  - Encryption keys (only if encryption is enabled)
- ### 2. Positioning of AP & Client Adapters

Generally Adhoc networks work across shorter ranges than Infrastructure networks because there is no Access point (which naturally acts as a repeater station –extending range). Both types of Wireless LANs (WLAN's) work best when the signal is unobstructed by metal or other thick structures containing metal.

When positioning Wireless devices remember the following guidelines:

- Access Points should be located in the center of their intended coverage area
- An AP with an Omni antenna transmits in a sphere from the antenna
- Where possible the AP should be placed in the ceiling, this gives best overall range because it reduces obstructions.
- A wall that is 30cm thick becomes 42cm thick on a 45 degree diagonal. Therefore the signal will be depleted even more when the direct line of sight between to Wireless devices passes diagonally through an interfering wall.
- Avoid placing AP or Client Adapters near strong interference created by other devices such as cordless phones, microwaves etc.
- Perform a full site survey at the four corners at the fringe of your network to determine if there are any other wireless networks present and what channels they are using.
- Avoid using Channels that are adjacent to one another (e.g. Use Channels 1, 6 & 13 when using three AP's in the same area)
- For maximum range keep AP's and Client Adapters away from metal structures or conductive materials (such as cubicle framing, window frames, computers, lights, phones, heavily-trafficked areas and speakers)

### ***3. Channels, SSID & Roaming***

In an Adhoc Network each device must be told what channel to use in addition to the Network name (SSID).

Infrastructure mode works differently to Adhoc because the Access Point tells the Client Adapter what channel to use; all the Client Adapter needs to know in order to find the network is the SSID.

When you first setup your Wireless network you should perform a site survey using the NetComm Wireless utility that comes with your Client Adapter. When you know what channels are currently being used make a list of the Channels that

are **not** being used and choose a channel that is the most numerically distant from the all of the 'used' channels.

Then choose a Network name (SSID) that is suitable to identify your wireless network.

*Note: For security it is best not to use an SSID that describes you, your wireless product, your company, your location or the services available.*

Roaming is a way of running an Infrastructure Wireless Network in an area that needs more than one AP to obtain complete coverage. Roaming works by using the same SSID for each access point but by placing them on different channels and with their fringe radio coverage slightly overlapping. When a Client adapter comes into range of an AP with the correct SSID it will associate with the AP and join the network, if the Client Adapter moves out of range of the first AP and into range of another AP (with the same SSID) then the Client Adapter will change channel to suit the new AP and maintain connection to the same Wireless network.

#### **4. Wireless Encryption & Security**

Adhoc networks and Infrastructure networks can both use wireless encryption to keep their data secure and prevent unauthorised associations. Infrastructure networks also have a few extra security measures that allow you to make your wireless network more secure than an Adhoc network. The most common Wireless Network Security features are:

- Effective range / Radio partitioning
- SSID
- Broadcast Beacon Disabling
- MAC address filtering
- Encryption (WEP, WPA-Psk)
- Third party Authentication (WPA-Radius / 802.11i / 802.11x EAP TLS)
- Digital Certificates

##### **Effective Range**

When planning your wireless network it is best to position your Access Points and Client Adapters away from the perimeter of your property where possible. Obviously the first goal is to ensure reception to all areas but remember that the

more your wireless emissions leak outside the property, the more likely unauthorised access can be obtained without the property being entered.

### **SSID**

A difficult-to-guess SSID provides, in a way, simplified security - although it may be easily found by a site survey, whoever finds it may not know who it belongs to. Best practice is to keep it secret where possible and ensure it does not describe you, your wireless product, your company, your location or the services available.

### **Broadcast Beacon Disabling**

Some Access Points allow you to disable the Broadcast Beacon to make the Wireless Network harder to find. However this does hide the network more from the 'casual browser' and is neither an effective way of protecting your data as it travels in the air nor a way of preventing unauthorised access.

### **MAC Address Filtering**

In most Access Points it is possible to only allow Wireless Clients with known MAC addresses to associate with the Access Point. Your Access Point will maintain an "Authorised MAC Address table" where you must enter the MAC address of each Wireless Client Adapter you want to allow to access the AP. MAC address filtering does not prevent unauthorised interception of your data as it travels through the air. MAC addresses can also be intercepted and cloned (or spoofed) so that an unauthorised Wireless Client adapter could be made to pretend to be an authorised Client Adapter and gain access to the network. MAC filtering has the advantage of not adding any overheads to the packet and therefore maintains maximum throughput.

### **Encryption**

Wired Equivalent Privacy (WEP) is available in 64 bit and 128 bit standards and is configured using a key of Hexadecimal characters to encrypt your data before it is transmitted. This maintains the integrity and privacy of your data; however your WEP key can be determined if enough data is 'sniffed' as it passes between Access Point and Client adapters. Because the WEP key is common to every Client adapter on the network it is also necessary to change the keys in every client adapter in order to recover from a stolen key. WiFi Protected Access (WPA) builds upon the WEP method but has two alternate methods, namely:

---

## • WPA – PSK & RADIUS

WPA – PSK uses a **Pre-Shared Key** similar to WEP but it has an improved system that prevents the keys from being determined by 'sniffing'.

WPA – PSK offers the small scale simplicity of WEP but with increased security that prevents 'Key cracking' WPA – RADIUS uses a RADIUS server to provide centralised and per-client key management system. Because RADIUS servers are already used in large scale network it provides a scalable and manageable solution to large companies.

Both forms of WPA will prevent your data being readable if it is intercepted by 'sniffing' and it will prevent unauthorised associations on your wireless network.

### **Third party Authentication 802.11x / 802.11i**

These are standards and draft standards often used similar to WPA that incorporate alternative methods of authentication including Certificates and Biometric technologies (such as thumb printing etc).

## **5. Configuring Client Adapters**

### **Mode (Adhoc or Infrastructure)**

When configuring your Wireless Client adapter you must first determine if you are connecting to an Adhoc Network or an Infrastructure network. Choose the appropriate mode for your network and apply the changes.

### **SSID**

In Adhoc mode or Infrastructure mode set this to be the same for every Client Adapter (and matching the AP if in Infrastructure mode).

*Note: Most Client adapters allow you to set the SSID as "ANY" this tells the Client Adapter to associate with the first wireless network it finds.*

### **Channel**

The Channel does not need to be specified when using Infrastructure mode as it will change to suit the access point. In Adhoc mode you must ensure that all Client Adapters you won't to join the network are configured to use the same channel.

### **Encryption**

When using WEP the Keys should be common to all Client adapters and Access Points, you must also which key (1, 2, 3 or 4) is currently being used.

If using other Encryption such as WPA – PSK you should ensure that encryption is setup correctly between your AP and Client Adapters.

WPA – RADIUS this encryption is outside the scope of this document but if compulsory to join the network it must be configured correctly before you can associate with the network.

*Note: If a Wireless Network has encryption enabled you will not be assigned an IP address or be able to associate with the Network until you have encryption configured correctly.*

### **IP Addresses**

It is important to note that Wireless Networks operate in a similar manner to Wired Networks. Usually Broadcast protocols such as DHCP will work across them seamlessly; therefore if you have a DHCP server available on your network it should be able to dynamically assign an IP address to any clients. Your IP address should be considered closely if you are running an Adhoc network because you are less likely to be running a DHCP server. Windows defaults for a DHCP clients usually fall back to the Automatic Private IP Address (APIPA) scheme when no DHCP server is available, which means that your Adhoc devices will end up with an IP address in the range 169.xxx.xxx.xxx. This is fine for setting up a temporary network but for something more permanent you may wish to assign static IP addresses to each client device.

## **6. Sharing Resources**

### **File Sharing over Wireless**

Once you have your Wireless device connected you may wish to access to files on a server or another Client. This can be done in several ways depending on your Network operating system and architecture. The simplest example for Windows users is to use 'mapped network drives' – but remember to do this you must either map the drive via an IP address (e.g. [\\10.0.2.10\sharename](#)) or use full UNC path names to your network drives.

### **Network Printing, Email and Web browsing**

All these services should work automatically over your wireless network the same way as if you were connected to the wired network. If these services are not working you should check that you can 'ping' via your Wireless network and that the IP Address, Subnet mask and Gateway are correct for your Network (generally the same as for the wired network).