

Wireless Network Structure - v1.3

Simon Mudd

C/Hermanos García Noblejas 5, Esc 1, 2B
Madrid
28037
España/Spain
sjmudd@pobox.com

Joaquín Béjar García

C/Barberán y Collar 22, 1º D
Alcalá de Henares
28805
España/Spain
shuodata@terra.es

Ángel Moncada Fernández

Paseo de la Estación 1, 1º C
Alcalá de Henares
28807
España/Spain
c4n99@hotmail.com

\$Author: sjmudd \$ \$Date: 2002/02/23 10:02:31 \$ \$Revision: 1.4 \$
Copyright © 2001 by Simon Mudd y MadridWireless
Copyright © 2002 by Simon Mudd, Ángel Moncada "c4n", Joaquín Béjar
"ShuoData"

Redistribution and use in source (SGML DocBook) and 'compiled' forms (SGML, HTML, PDF, PostScript, RTF and so forth) with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code (SGML DocBook) must retain the above copyright notice, this list of conditions and the following disclaimer as the first lines of this file unmodified.
2. Redistributions in compiled form (transformed to other DTDs, converted to PDF, PostScript, RTF and other formats) must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Important: THIS DOCUMENTATION IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This is the Wireless Network Structure Document, a document which tries to give some general guidelines to groups which are building community wireless networks, enabling them to achieve a well designed scalable network which will be easy to connect to similar wireless networks worldwide.

The interest in wireless networks has increased enormously in the last few years, especially since recently when costs have decreased and the hardware has become more widely available. It is hoped that a document such as this will help combine the knowledge of those who have experience with building networks of this type and will avoid problems which may later make a global Internet of wireless networks difficult to achieve.

Table of Contents

1. Introduction	3
2. What is a Wireless Network?	4
3. IP Addresses	4
4. Routing	8
5. Network Topology	12
6. Hosts, Domains and DNS	13
7. Addition of a New Node	14
8. Firewalls, Security, QoS, NAT and Routing to the Internet	16
9. DNS Update Robot	18
10. User Authentication	19
11. Roaming	19
12. Hardware	19
13. Wireless Groups	20
14. Communities	21
15. References	21
16. Contributors	23

1. Introduction

This document tries to give some guidelines about how to build a community wireless network. It explains the structure of the different wireless networks, how the nodes and clients are connected and how the IP traffic is routed between the different nodes organised by an individual or a group. Taking into account that the different wireless groups are working towards a common goal, to setup a wireless networks in various place throughout the world, this document also tries to give information about how the different groups could connect together or how they could connect to the Internet.

This document can not hope to answer all the questions related to building a community wireless network, but it does attempt to cover some of the more practical aspects which will be common to any group considering starting a project of this type. Most of these considerations if treated or at least considered at the beginning of a project can avoid mistakes which are difficult to rectify later. It is clear to us at the moment that there is an important interest in this subject, and that even if the growth of some of the current projects is less than their core members expect, that there is still a potential for creating extremely large networks, each of which will requiring some careful coordination to work effectively.

The use of common standards and network structures greatly simplifies the tasks needed to interconnect the wireless networks and also minimises the management effort which is common to each network.

Feedback and comments about how to improve this document are always welcome, so don't be shy. If you know more about this subject than I do help me out and get your name down in the list of credits.

I wrote the original version of this document in Spanish. Seeing that there might be a wider potential audience if the document were written in English I translated the Spanish version. As English is my native tongue and it is difficult to maintain a document in several languages further changes to this document will be made in English.

The latest version of this document can be found at <http://www.pobox.com/~sjmudd/wireless/network-structure/> (<http://www.pobox.com/~sjmudd/wireless/network-structure/>). I will also add pointers to the latest version in Spanish.

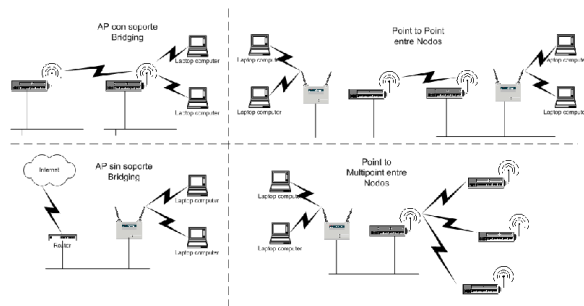
2. What is a Wireless Network?

A wireless network as described in this document is a network of wireless local area networks (LAN) connected together to form a metropolitan network (MAN), usually located in one geographical area, such as a city or small town. Several wireless interface standards currently exist, some operate within licensed and others within unlicensed spectrum, some point to point, others point to multi-point, and yet others more flexible. The most common readily available standard at the moment is the 802.11 family (802.11, 802.11a, 802.11b and 802.11g). This is consumer equipment that operates on an unlicensed radio frequency.

Each wireless network is composed of various *nodes* connected together. A node is a collection of various PCs or other equipment connected together directly using the IP network and within direct radio range. A node consists of at least one router and one or more clients. The clients normally require little configuration and talk only to the router, whilst the router will route it's own data and that of its clients to the rest of the network. It will also participate in exchange routing information with other nodes to ensure it always knows how to reach the rest of the network. The nodes can be connected together by radio links or by other means. The term node can loosely be associated with the router/host which manages each node's own local network. Due to the limited range of the radio signals a large number of nodes will be required to provide coverage to a whole town, thus requiring a complex mesh of connections between the nodes to provide a robust network.

The network's clients, the people who connect to the nodes from their home or office, make up the complete network. The nodes without clients form each group's network infrastructure.

Figure 1. Types of Node in a Wireless Network



3. IP Addresses

3.1. Introduction

This document talks almost exclusively about IP version 4, as initially a basic network infrastructure is required and

it is easier to use a well known and understood protocol, with which tested tools can be used.

Nevertheless, it should be possible to implement an IPv6 network at the same time as the IPv4 network without the two networks interfering with each other. It is also clear that the future of networking and the Internet is with IPv6 and that complicated and production networks already exist based exclusively in IPv6. As more information becomes available regarding the network structure I will include it in this document.

A group of IP addresses are required to setup a wireless network.

The following sections explains different aspects relating to which IP addresses could be used by the wireless communities globally, and then how the address space used by a particular wireless group could be managed internally. Finally there is also a recommendation as to the individual assignments at the node level.

3.2. IPv4 Addressing

Each wireless group will need a range of IP addresses to enable the following types of connections:

- Connections between clients within a node
- Connections between nodes
- Connections with other wireless networks (optional)

If a wireless group considers that it *might* connect in the future to another wireless group it is vital that the ranges of IP addresses used do not conflict with those used by any other group.

Various international wireless groups have already setup their own networks and have begun to use private (RFC 1918) IP addresses mainly to avoid having to consult third parties and also to avoid the costs associated with requesting public IP addresses.

When a request is made for public IP addresses there is a certain requirement to connect these IP addresses to the Internet and to justify the number of IP addresses requested. This may often be difficult for most wireless groups, most of which are new projects and who may find it difficult to anticipate the real number of IP addresses needed.

For this reason it is recommended that the IP addresses used are assigned from the private RFC 1918 networks.

Although the use of public IP addresses is not considered necessary, this may change in the future, when there is a large enough user base to justify this or if for example there is an interest of people on the Internet to connect IN to a wireless group.

The three groups of IP addresses designated by RFC 1918 for private use are:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

If a group uses up the block of IP addresses which has previously been agreed and needs a new assignment of addresses it should contact the other wireless groups and agree on a new block which avoids IP address conflicts if this is at all possible.

3.2.1. Wireless Group Level Assignments

Currently there is no globally agreed mechanism to assign addresses within the RFC 1918 space amongst the different wireless groups.

The best approximation that currently exists is the following URL:

<http://www.freenetworks.org/moin/index.cgi/NetworkAddressAllocations>
(<http://www.freenetworks.org/moin/index.cgi/NetworkAddressAllocations>) which lists the addresses used by those groups who have volunteered this information.

It is recommended that any new group which is interested in having a unique set of IP addresses, register its usage at this location. There is no agreed standard as to the number of addresses that should be assigned to a group, but it is recommended that the requested allocations be conservative, as it is always possible to request another block at a later stage.

3.2.1.1. Client Connections

For the allocation of IP addresses used by clients connecting to the network and the nodes it is recommended that the range 10.0.0.0/8 be used before using addresses from the other RFC 1918 blocks.

3.2.1.2. Inter-Node Assignments (links within one group)

While not necessary it is often more convenient to use a separate range of addresses for the network connections within a group used to connect the different nodes. For this use it is recommended that an assignment is made from the range 172.16.0.0/12, avoiding the intra-group assignment mentioned in Section 3.2.2.

3.2.2. Intra-Group Assignments (links between different groups)

It is recommended that a subrange of 172.16.0.0/12 should be reserved for connections between different wireless groups.

As an initial approximation we can assume that if 1000 groups have 4 connections to other groups, each connection being a point to point connection we will need 16000 addresses. Thus we can use 172.16.0.0/18 (-172.16.63.255) as the range for these assignments. This should be sufficient in the immediate future.

The addresses from this range which are actually used for this purpose should be registered in a public place to avoid duplication.

3.2.3. Assignments within a Wireless Group to a Node

The local assignment of a block of IP addresses to a node will be centralised locally by some of the group's members. These members will decide the procedures for assigning blocks of IP addresses, the number of IP addresses each block will have and the requirements which each node must fulfill to be added to the network.

If a node is not connected to any other node then it can use any IP address range it wants. However it would be convenient that it uses an address from the range 10.254.0.0/16 recommended on the freenetworks.org website for non-connected networks. If you use these addresses you will not need to request a block from your local wireless group.

3.2.3.1. Standard Assignment

To each node a block of addresses will be assigned from the group's global assignment mentioned. Each node will consist of at least 32 IP addresses of which 30 will be usable. In principle one address will be used by the actual node/ router leaving the remaining addresses for use by clients.

Considering the normal range over which signals will be propagated and the number of clients to be expected in the area this number of IP addresses should be sufficient.

The block of 32 addresses will be assigned in the following way:

10.x.y.0	Network Address
10.x.y.1	Router or node's IP Address
10.x.y.2-30	The node's Clients' IP Addresses
10.x.y.31	Broadcast address

The netmask in this case will be 255.255.255.224.

Each class C network, 10.x.y.0/24, will be composed of 8 sub-net whose last digit ends in .0, .32, .64, .96, .128, .160, .192 y .224.

The assignment of the addresses 2-30 to the different clients can be done in whichever way is deemed most appropriate, but the most practical way of doing this in a wireless network is using the DHCP protocol, and having the node/router assign the address.

The advantage of using the DHCP protocol is that at the moment of assigning the IP address to the client the following additional information can be given to the client:

- The IP address of the router in the network
- The IP addresses of the name servers which should be used
- The domain name of the network or node

This ensures that the configuration requirements for the client's system is minimised.

3.2.3.2. Assignment of Larger Blocks

As the assignment of blocks of 32 IP addresses may be insufficient in urban zones with a high population density, it may be necessary to consider assigning additional blocks of 32, 64, 128 or even 256 IP addresses to a node, each block with its appropriate network address and netmask.

Assignment of larger blocks in this way is only recommended when it is considered necessary, although this should be a local decision made by each group. The new assignment may be for a new larger block which replaces the previous assignment, or of a second discontinuous block which can be used in addition to the block(s) previously assigned.

The structure of the larger blocks of addresses should follow the same form as has been described in the previous section, with the difference that the number of IP addresses assigned to clients is increased.

3.2.4. Multicast Address Support

Need to add a comment here that routers should support multicast routing and addresses. This will allow services like ntp to be used more easily. What other services would be interesting?

3.3. IPv6 Addressing

The recommendations relating to the methodology of IPv6 address assignments have yet to be defined.

Note: that the following are simply ideas. Anyone with a better understanding of IPv6 could certainly help me out.

IPv6 addresses consist of 128 bits, 64 bits being a "network prefix" and the remaining 64 bits being a host address.

The different network prefixes has various different uses, but one which could be immediately interesting for us would be to use the concept of a site-local scope, normally this would be an organisation's site. We could initially define site-local to be a global wireless scope. Doing this allows us to have a global network addressing which can't be connected to the Internet, but it allows us to start playing.

4. Routing

Given the probability that a wireless group will consist of a large number of nodes and the likelihood of an interest in connecting to other groups with similar interests, the management of the routes between different networks will be quiet complex.

4.1. Dynamic vs. Static Routing

There are two ways of routing from the local node to other hosts on the network and they are using static or dynamic routing. Each method has advantages and disadvantages, but when a network grows dynamic routing is the only reasonable way of managing the network. For this reason we have to contemplate the use of dynamic routing protocols instead of the use of static routes in *all* the nodes of a network.

Various programs exist which enable us to setup dynamic routing in the majority of operating systems, so there should be no problem setting up a node to use dynamic routing.

- *Zebra* is a program for Unix systems which can manage most of the protocols mentioned in this document. It is also free software which can be used under the GPL license.
- *gated* is another package for Unix, but only available in binary form. This package has a much longer heritage than *zebra* and may be more stable. Newer versions of this package are available, but only commercially. Educational institutions may be treated differently.
- *routed* is another standard package provided on most Unix platforms. It is limited to using only the RIP protocol, which may not be suitable in a large network, especially if the network is not very stable. However for small networks it works very well. Just make sure you use a version of *routed* which supports RIP-2 and thus can work with class-less networks.

The use of any routing daemon and the dynamic routing protocols will be transparent to the end-user and will be a matter for the node's administrator to setup when connecting one node to another. From the client's point of view the routing will be configured automatically when he connects to the network using the DHCP protocol.

The use of dynamic routing protocols is not mandatory, but it is recommended. In some cases a static route may be sufficient to make the connection to another node.

4.2. Routing between Nodes

When connecting nodes together a different range of IP addresses will be used to those of the group's client network (10.x.x.x). The connections could be established between just two nodes configured as point-to-point links, but in situations where several nodes can hear each other the nodes can be configured to be within a common network, thus allowing them to share information more efficiently and avoid unnecessary hops.

The IP addresses used for the inter-node connections will be from the block 172.16.0.0/12, starting with 172.16.64.0/30 and continuing with 172.16.64.4/30, 172.16.64.8/30, ... according to the number of links used. This would be the case of point-to-point links, where the netmask will be 255.255.255.252 and will contain 2 useful IP addresses (one for each end of the link). For larger networks a larger network will be assigned using the appropriate netmask.

Due to the large number of networks which will probably exist within a wireless group the routing between the nodes can become quite complex. To resolve this issue it will probably be necessary to use an Interior Gateway Protocol (IGP), such as RIP (Routing Information Protocol) or OSPF (Open Shortest Path First), the last protocol being a more complex but sophisticated option. If the group's network consists of a small number of nodes static routing could be contemplated, though it is not recommended.

The use of dynamic routing avoids manual modifications and ensures that the connection to new nodes on the network takes place immediately. For this reason its use is recommended whenever possible.

For the same reasons mentioned earlier with the client IP addresses, the use of the IP addresses selected for interconnecting nodes within a wireless group should *NOT* conflict with the addresses used by other wireless groups. For this reason each group should register the IP addresses blocks used for inter-node links if they are different to the IP addresses used by their clients. If this is not done it may not affect the routing between client nodes on both networks, but it will make debugging routing problems impossible when trying to analyse traffic moving from one network to another, and therefore is not recommended at all.

While it is possible to mix protocols on the same network this is not advisable as the routing traffic will increase and also there will be the added complexity of systems which must translate the routing information from one protocol to another. Thus each wireless group should endeavour to decide on the routing protocol it will use internally and try and ensure that all routing within the network between nodes uses this protocol.

As it may not be possible to trust everyone in your network it may be necessary for the node's administrators to put in place authentication methods to ensure that incorrect routing information is not injected into the network.

A separate document will be required which will explain the minimum configuration needed to setup a program such as zebra to correctly route IP traffic using one of the IGP protocols such as RIP or OSPF.

4.3. Routing with Other Groups

Whenever a connection by a wireless group to an external system is envisaged, in other towns, countries or areas it is very important to ensure that there are no conflicts between the different IP addresses used by the groups, and that no

other important problems are likely to arise.

A wireless group can use the same types of Inner Gateway protocols (IGP) to exchange routing information with another group as it does internally between nodes, but it is probably better to use an Exterior Gateway Protocol (EGP). This at least is standard practice on the Internet.

Routing with other groups should probably be arranged using the Border Gateway Protocol (BGP) and this is something which needs further study. The advantage of this strategy is that each system/group is treated as an autonomous system and there is no need to have knowledge of a group's internal routes, only the points of access to the group, the networks it contains and the connections it has to other groups.

The range of IP addresses used for the inter-group connections is mentioned earlier and the addresses used should be made public to avoid IP address conflicts.

As it may not be possible to completely trust all the information provided by another group's another and also to avoid false information being injected into the network it may be necessary for the node's administrators to put in place authentication methods to ensure that incorrect routing information will not adversely affect the group's network's correct functionality.

A separate document which describes the best way to configure a node which is linked to others will need to be produced.

If a wireless group is considered as an autonomous system (AS) it will need to be assigned a number using some code which uniquely identifies it. In the majority of cases the group will not have its own AS number. It is recommended that when a group needs a new AS number that it contacts the other wireless groups and it should be assigned with a number within the private AS range recommended by RFC 1930. This range of numbers is 64512-65534.

It will be useful if a register of the assigned AS numbers used by the wireless groups is kept in a public place (web site) so that it can be consulted by the different wireless groups.

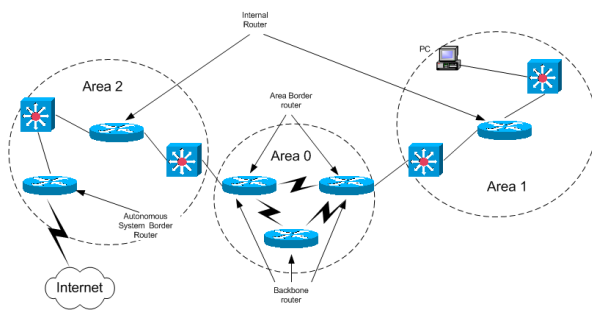
The actual AS number is not important, it is simply an autonomous system identification number. In the same way that it is imperative that the IP addresses used by connected groups are not duplicated, it is also very important that a new group doesn't use a AS number assigned to another group, as this will confuse the routers considerably.

4.4. OSPF

Open Shortest Path first (OSPF) is a non-proprietary link-state routing protocol.

- It can be used freely and is known to run on a large number of platforms which may be offering this type of service to the network and being a link-state protocol differentiates it from RIP or IGRP which are distance-vector protocols.
- OSPF doesn't continually broadcasts a list of all its routes to its neighbours, but only broadcasts the changes it detects in the network topology, thus avoiding the unnecessary use of the network's bandwidth. This is vastly more efficient than distance-vector algorithms which depend on the assigned timers to periodically broadcast local routing information to the rest of the network. Using OSPF the convergence time when a network changes may be as short as 4 or 5 seconds, compared to as long as 180 seconds with RIP.

The OSPF topology is based on connected areas in a hierarchical structure. The OSPF autonomous system can be divided in different areas and each area can be connected to the backbone area (area 0) represented in the following figure:

Figure 2. Open Path Shortest First (OSPF)

The routers which form an OSPF network are named according to their position and function within the network in the following way:

Internal Router: A router with all networks connected directly within the same area. These only maintain a single copy of the routing algorithm.

Area Border Router: ABR is a router which connects an area to area 0. It shares the information between the two areas and manages those networks which are shared between them.

Backbone Routers: These are the routers which belong to area 0 and are responsible for the propagation of the networks between the different areas.

Autonomous System Boundary Routers: These are routers connected to other AS or to Internet. They also tend to be the routers which exchange routing information with other IGP and EGP routers which may not be using OSPF.

4.4.1. Wireless OSPF

In the following diagram we can see the different ways in which we can connect the areas or node at the routing level in a wireless network. A VPN option has also been included which can be very useful, especially when connecting to different wireless networks between towns or when the distance between two nodes is too large and it is necessary to establish the link over the Internet.

In this way we can define the area 0 being situated at the main node, and preferably with a high bandwidth Internet connection and to which the other networks would be connected.

In the situation where nodes can not be connected directly to the area 0 directly or by VPN a virtual link to connect it to area 0 will be required.

4.4.2. OSPF compared to Other Protocols

There will be certain situations in which certain systems will not support OSPF, and in this case another protocol such as RIP can be used, as long as it is RIP version 2, or Cisco's EIGRP both of which supports classless networks. Nevertheless the ABR will need to support OSPF to ensure that it doesn't lose the complete network information.

It will be necessary at the moment that complete networks are connected to use protocols which can publish summarised versions of the networks within an AS as this will considerably reduce the amount of routing information which needs to be transferred between the different routers.

4.5. BGP

The Border Gateway Protocol (BGP) is defined in RFC 1771 and is currently in its fourth version. It is the most popular of the EGP protocols and has been used almost without change since 1995.

The function of BGP is similar to that of an IGP router such as OSPF which learns the optimal routes to reach the rest of the nodes and networks within an autonomous system (AS). The difference is that BGP works with networks of different autonomous systems, publishing its own networks and determining through which of the other autonomous systems a third can be reached.

BGP also has various filtering functions which allow us to decide whether to inform each of our neighbours routers or not about the different networks to which we are connected.

Due to this functionality the use of BGP is recommended to interconnect different wireless networks, instead of using an IGP like OSPF.

4.6. Support for Multicast Routing

Support for multicast addresses should be included in the nodes' routers, as this allow for applications which use the bandwidth of the network more efficiently.

Support for multicast addresses is provided by most operating systems, but additional software is required to support multicast routing.

I need to add some more information here about what software is required and for what multicast addressing can be used. First thoughts include NTP as a start.

5. Network Topology

Until now we have only been talking about the IP address that will be used within the network for connecting clients, nodes and the different wireless groups. We have also talked about the routing between these different components, but only in as much as the protocols which will be used and not the way in which the different nodes should be connected.

The interconnection of the nodes in a network consisting of more than five nodes can be achieved in a variety of ways. The moment that the number of nodes increases, the number of different ways of connecting the nodes rises exponentially. Nevertheless for obvious reasons it is best not to build a network from a random structure.

Normally when a network is designed the expected traffic and number of hosts connected is studied, the needs of the users and various other things so that a structure can be devised which can give the best possible service to the clients. Wireless networks which grow in an uncontrolled way will require a special design or a continual adjustment to the structure to ensure that the services offered can be done so effectively.

The following points are those which should be taken into account when we design a network:

- Avoid congestion in a single point in the network.
- Reduce the number of hops between one host and another where possible.
- Try and ensure that multiple links to other nodes in the network exist from one node. If one node fails the other link can be used, and if we are using dynamic routing this change will be immediate and transparent to the users.

- Use tools which can monitor the network and prevent future problems.
- Separate client traffic, from traffic between nodes.
- Avoid as much as possible manual configuration and use standard configurations for each of the different installed components.
- Use links between nodes with the highest possible bandwidth (where possible by radio).
- Maintain good communications with the nodes' administrators. Normally the people who maintain a company network manage the whole network: with a wireless network each administrator manages his *own* node so that communication between the different administrators is very important when solving problems which might occur.

It will be important during a network's initial stages of growth to discuss the addition of new nodes and the best place to connect them to, as the tools which could be used to monitor the various parts of the network.

6. Hosts, Domains and DNS

It may be useful to use the DNS to name each IP address related to a node, permitting the translation from hostname to IP address and vice versa.

In principle each wireless group will be responsible for its own domain and the assignment of names to the IP addresses of its nodes. If a service of this type is offered then it is recommended that the DNS server for the domain is also accessible from the Internet.

In this document the domain name used will be represented generically as `_${GROUP}`, but it could be for example: `redlibre.net`, `madridwireless.net` or a sub-domain managed by the corresponding group.

All the nodes and clients could be named in a similar fashion to ease their identification:

First a name will be given to each node: `NODE="node"`. The node name should be short.

It will be convenient if each group were to maintain a public web page with information about its nodes and the configuration and position of each one. This way future clients will be able to locate the nearest node to them.

6.1. Resolving DNS Names

Within each node the hosts/nodes/clients will be named as a sub-domain of `_${NODE}.${GROUP}`, in the following way: `"name" . ${NODE} . ${GROUP}`.

The recommended names to include in the DNS are the following:

Name	Description	IP Address
network	network address	10.x.y.0
router	the node's router	10.x.y.1
client1	the address of the node's first client IP address	10.x.y.2
...		
client29	the address of the node's last client IP address	10.x.y.62

Name	Description	IP Address
broadcast	broadcast address	10.x.y.63
netmask	the node's netmask	255.255.255.224

We should point out that the addition of the information in the DNS is for a simple reason: to help with the identification of IP traffic within the network. It is quite useful.

Other host names could be assigned in the DNS and this will be optional and a question for the node's administrator if the hostname is a sub-domain of the node, or of the "global" DNS administrator if the hostname is global to the domain.

For example the assignment of the name `www.node23.madridwireless.net` will be a question for the MadridWireless'node23 administrator, and the assignment of the name `www.madridwireless.net`, as should appear logical, will be a question for the administrator of the domain `madridwireless.net`.

6.2. Inverse DNS Resolution

At the same time as there will exist a relation name -> IP, the name server will also be configured to be able to make the inverse resolutions: IP -> hostname. This is very useful for identifying the source of IP traffic in the network.

Therefore it will be necessary to have the following types of records:

```
0.0.64.10.in-addr.arpa.    IN PTR    network.${NODE}.${GROUP}.
1.0.64.10.in-addr.arpa.    IN PTR    router.${NODE}.${GROUP}.
...
```

The nameserver to resolve these inverse addresses still needs to be defined.

We should also note that to carry out the inverse resolutions a common name server will be required, capable of resolving addresses from different wireless groups. This is different to the situation when a normal hostname is resolved because in the latter case this can be managed independently by each group.

[The inverse IP to name resolution can be delegated as well, and this is something which will need studying in the future.]

It is suggested that the reverse mappings are *NOT* modified from their standard values so that there is an orthogonal mapping of the form:

```
clientX.${node}.${group}    IN A      a.b.c.d
d.c.b.a                     IN PTR    clientX.${node}.${group}
```

To ease the management of these multiple names the use of a web or mail tool such as the `ampr.org` robot could be used. See below for an explanation of the functionality provided by this robot.

7. Addition of a New Node

The steps needed to request the creation of a new node will be determined locally by each group in another document and each group will have to be contacted for the relevant details.

The creation of a new node will start a process of creating the recommended names in the DNS. If possible this will be done in real-time, and if this is not possible then the process should be done at least daily.

To add a new node to the network it will be useful if the following data is available:

- name: Node name (alphanumeric, name which can be used in the DNS)
- description: Free text description of the node
- admin: Name of the node's administrator
- password: encrypted password for updating data
- email: node administrator's email address
- tel: Node administrator's telephone number (*)
- location: Node's location: free format, but suggesting "Zone, town, postcode, country"
- frequency: Frequency/channel used
- type: Type of node (AP/Ad-hoc)
- comments: comments (*)
- ip-range: IP range
- dns-delegated: delegated dns : yes/no, (initially no)
- dns-main: main name server: IP address (*)
- dns-secondary: secondary name server: IP address (*)
- links: list of direct links to other nodes (*)
- internet: link to Internet? (yes/no) (*)
- created: date/time of creation of node
- deleted: date/time that node was deleted [normally blank]
- change-last: date/time of last change to node's data
- change-by: person/email of person who made the last change
- change-num: serial number of last change made

The fields marked with (*) will be optional.

All this information could be stored within the DNS, therefore eliminating the need for an external database, adding each field with the indicated name and assigning to it a TXT record. Nevertheless for privacy reasons, making all the information public, may not be desirable and therefore the use of a database may be both necessary and desirable.

For example if we know that there is a node `node23` for a group `_${GROUP}` the command `dig txt admin.node23._${GROUP}` will give us:

```
admin.node23._${GROUP} IN TXT "Simon Mudd"
```

If any of the node's information is modified the last 3 fields would be updated as appropriate.

With the data given above the following DNS information could be generated automatically:

(1) Domain Information

The following IP address records as indicated before.

```
network.${NODE}.${GROUP}      IN A 10.x.y.0
router.${NODE}.${GROUP}       IN A 10.x.y.1
client1.${NODE}.${GROUP}      IN A 10.x.y.2
...
client29.${NODE}.${GROUP}     IN A 10.x.y.62
broadcast.${NODE}.${GROUP}    IN A 10.x.y.63
netmask.${NODE}.${GROUP}     IN A 255.255.255.224
```

(2) Inverse Information

X PTR type registers permitting the inverse resolution of the hostname from the IP address:

```
z.y.x.10.in-addr.arpa. IN PTR xxx.${NODE}.${GROUP}.
```

8. Firewalls, Security, QoS, NAT and Routing to the Internet

8.1. Do we need a Firewall?

Until now we have been talking of the wireless networks as if they were the only networks which existed. There will be a lot of wireless administrators who will have a node connected to other networks, such as the internal company or home network or maybe a connection to the Internet. Bearing this in mind the information which moves from one network to another may need protection for a variety of reasons. Perhaps the administrator doesn't want anyone to enter into his own private network, but he doesn't mind offering wireless facilities to others, or the links to other nodes.

To solve this problem the only reasonable solution is to install and configure a firewall, a technique clearly defined in various places on the Internet, and whose objective is simply to filter the IP traffic which passes between the different networks within a node, filtering information or allowing it to pass without hindrance as required.

Starting with the premise that we want to setup a firewall, we need to take into account several things. There are various possible solutions, some are operating system dependent and there are also commercial solutions which work on a variety of operating systems.

In Linux there are various options which depend on the version of the kernel being used: the main ones being IPCHAINS and the newer IPTABLES. FreeBSD and other BSD versions use ipfw. The advantage of using the facilities provided by the kernel is that they come with the operating system, although they options to use these facilities may not be included in the kernel which is being used. See the relevant manuals as to how to include this functionality in your operating system.

The URL as to how to configure a firewall with IPTABLES in Linux is

<http://www.boingworld.com/workshops/linux/iptables-tutorial/iptables-tutorial/iptables-tutorial.html>
(<http://www.boingworld.com/workshops/linux/iptables-tutorial/iptables-tutorial/iptables-tutorial.html>). There also exist various HOWTO documents for Linux which explain how to configure a firewall, and there is ample documentation for BSD too.

To configure a firewall correctly several standards should be followed, starting with the design of the node. Some of the factors which should be taken into account are:

- the different interfaces to which the firewall is connected
- the different networks and associated ip addresses connected to the firewall
- The desirability or otherwise of traffic passing from one network to another over each specific interface
- The different IP services which should be allowed or disallowed (http, smtp, dns, ping) using tcp, udp, icmp, etc.
- If it is necessary to convert the IP addresses as they leave an interface (NAT) and enter a specific network.

A firewall is going to normally have the following connections and networks connected to it:

- IP addresses of the node's network
- IP addresses of the wireless group's network
- IP addresses of the network(s) to other node(s)
- IP addresses of the internal network
- A link to the Internet (which uses the remaining IP addresses)

Only when looking at the matrix of possible connections between one network, and taking into account that we have to treat IP traffic in both directions do we begin to see the complexity involved in the configuration of this type of firewall.

The majority of the firewall configurations permit us to decide whether to allow or deny traffic through the firewall, but we can normally also define whether to log traffic which attempts [fails to] pass through the firewall to a file or not.

The policy which should be followed with the logs generated by a firewall should be to maintain them for a certain period of time, perhaps 3 months, so that if some incident occurs we will have a record of the event.

We should also note that a node should *NOT* filter traffic whose source and destination addresses belong to the group's network, because this will obstruct the correct functioning of the network.

If a group decides to connect to another group then the traffic to the other wireless group should not be filtered either. If various nodes have implemented a firewall, they should be given enough time to change their firewall configuration before confirming connectivity to the other group.

One recommendation is to use a IDS (Intruder Detection System) which allows us to detect intruders who try to break into our network, from any of the networks which is connected to the firewall.

There are various IDS, amongst them being snort <http://www.snort.org> (<http://www.snort.org>) and the policy regarding the period of time to store log files should be the same as with the firewall.

8.2. The Connection to Internet

A lot of people are interested in wireless networks as a cheap way to access Internet using someone else's connection.

In principle a connection to Internet can be offered by a node but we ought to bear in mind that connections of this type require the originating IP address be changed to the real address connected to the Internet, using a technique called NAT. This is the case at least when the wireless IP addresses are private.

In these cases it will not be possible to connect from the Internet "inside" for the same reason: the wireless network's IP addresses are not public and therefore they can't be routed from the public Internet.

Nevertheless the connection to Internet, even when using NAT, does allow the use of a large number of services such as DNS, email, web and ftp access amongst others.

We ought to point out that the maximum speed of a wireless network using the 802.11b protocol is 11Mb/s significantly faster than the typical speed that most people are connected to Internet from home even when using ADSL, whose download speed doesn't normally exceed 256kb/s.

Therefore those who offer Internet access to others might easily see their Internet connection saturated if they don't take appropriate steps.

8.3. Multiple Default Routes in a Network

Finally it is worth mentioning that the choice of accessing Internet may not be available from only one place in the network: it may be a service offered by several wireless nodes. The management of these multiple routes within the network to the "default route" can be quite complicated as most routing software doesn't treat this very well and it may well be worth studying the best way to manage these "special" routes.

8.4. QoS

Quality of Service goes here

9. DNS Update Robot

A simple way to avoid the manual maintenance of the DNS information would be to use a robot, which can update the information remotely. This robot could be controlled by email or even through a web interface though the latter is something which could be studied in the future.

An example of this is the robot used by the ampr.org domain, which manages the update of host names and IP addresses via email.

A message is sent to the robot's email address, sending commands in a specific format.

Based on the ampr.org domain DNS robot I have written something a little more sophisticated, which allows the following commands:

1. Add an IP address, MX host, Name server, Text record or new CNAME

```
name ADD A 1.2.3.4
```

```
name ADD CNAME another-name
name ADD MX priority mx-host
name ADD NS name.server
name ADD TXT "some text"
```

2. Delete the same data

```
name DEL A 1.2.3.4
name DEL CNAME another-name
name DEL MX priority mx-host
name DEL NS name.server
name DEL TXT "some text"
```

3. Show the stored information

```
name INFO
name ?
```

After making any changes the robot confirms its actions sending a message to the sender of the original message with the results of its actions.

The format as used in the ampr.org domain won't work with a wireless group for various reasons:

1. Each wireless group is managed independently - one robot is needed by domain or group.
2. It will probably be necessary to assign a password to the node's administrator to enable him to modify data only from *his* node.
3. A global password would be required allowing global data to be modified, limiting access to a group of people who control the domain/group.
4. An ideal situation would be to feed this robot from an application which assign new IP address ranges and which generates the new data required for the DNS.

As the robot now exists, anyone who is interested in using it should send me an email to <sjmudd@pobox.com>. Currently once the data is stored the zone file used by the name server is updated and the name server is then instructed to update it's configuration. The robot is written in perl and requires little more than a couple of scripts to put in action.

10. User Authentication

11. Roaming

12. Hardware

The following links give information about hardware which could be used to setup a node or a client connection to a wireless network.

- <http://www.3com.com>
- <http://www.cisco.com>
- <http://www.orinocowireless.com>
- <http://www.stechcomm.com>

13. Wireless Groups

The following list includes some of the groups in Spain and around the world which are working with wireless networks.

13.1. Wireless Groups in Spain

The following list of groups and their URLs indicate the best place to start to find further information about their activities. The majority of the groups run mailing lists and there is a certain duplication of traffic amongst these lists.

- Alcalá Wireless <http://www.alcalawireless.com> (<http://www.alcalawireless.com>)
- Barcelona Wireless <http://www.barcelonawireless.net> (<http://www.barcelonawireless.net>)
- MadridWireless <http://www.madridwireless.net> (<http://www.madridwireless.net>)
- Málaga Wireless <http://malagawireless.xphera.net> (<http://malagawireless.xphera.net>)
- <http://www.palamos.net> (<http://www.palamos.net>)
- <http://www.pucelawireless.net> (<http://www.pucelawireless.net>)
- Redlibre <http://www.redlibre.net> (<http://www.redlibre.net>)
- Santiago de Compostela Wireless <http://www.scqwireless.com> (<http://www.scqwireless.com>)
- Sevilla Wireless <http://www.sevillawireless.net> (<http://www.sevillawireless.net>)
- Zaragoza Wireless <http://www.zaragozawireless.net> (<http://www.zaragozawireless.net>)

13.2. Other Groups around the World

- CanadaWireless <http://www.canada-wireless.net> (<http://www.canada-wireless.net>)

- IrishWan <http://www.irishwan.org> (<http://www.irishwan.org>)
- BC Wireless <http://www.bcwireless.net> (<http://www.bcwireless.net>)
- <http://www.nora-wireless.net> (<http://www.nora-wireless.net>)
- <http://www.nycwireless.net> (<http://www.nycwireless.net>)
- <http://www.seattlewireless.net> (<http://www.seattlewireless.net>)
- France Wireless <http://www.la-grange.net/2001/02/openwireless.html> (<http://www.la-grange.net/2001/02/openwireless.html>)
- Melbourne: Digital and Wireless (<http://www.wireless.org.au>)
- <http://www.novawireless.org> (<http://www.novawireless.org>)

14. Communities

- Open Wireless Network Forum <http://www.opennetworks.rg3.net> (<http://www.opennetworks.rg3.net>)
- <http://www.freenetworks.org> (<http://www.freenetworks.org>)
- <http://www.personalteco.net> (<http://www.personalteco.net>)

15. References

Address Allocation for Private Internets

- RFC 1918

BGP, Border Gateway Protocol

- RFC 1771

RIP, Routing Internet Protocol

- Version 1, RFC 1058
- Version 2, RFC 2453

OSPF, Open Shortest Path First

- Version 2, RFC 2328
- Version 3, RFC 2740 (for IPv6)

DHCP, Dynamic Host Control Protocol

- RFC 2131
- R. Droms, "Dynamic Host Configuration Protocol", 3/97. <http://www.dhcp.org> (<http://www.dhcp.org>)

Zebra, A routing software package for TCP/IP networks

- <http://www.zebra.org> (<http://www.zebra.org>)

Wireless Router HOWTO

- <http://www.rage.net/wireless/wireless-howto.html> (<http://www.rage.net/wireless/wireless-howto.html>)

Building Wireless Community Networks

- O'Reilly and Associates, January 2002
- Rob Flickenger
- ISBN 0-596-00204-1

Designing Large-Scale LANs

- O'Reilly and Associates, January 2002
- Kevin Dooley
- ISBN 0-596-00150-9

El protocol 802.11b

- <http://standards.ieee.org/getieee802/portfolio.html?agree=ACCEPT>
(<http://standards.ieee.org/getieee802/portfolio.html?agree=ACCEPT>)

Melbourne: Digital and Wireless networking RFC

- <http://www.wireless.org.au/wiki/?RFC> (<http://www.wireless.org.au/wiki/?RFC>)

Melbourne: Digital and Wireless Architecture

- <http://www.wireless.org.au/wiki/?architecture> (<http://www.wireless.org.au/wiki/?architecture>)
- Reliable Internet Connectivity with BGP <http://www.bgpbook.com/> (<http://www.bgpbook.com/>)

16. Contributors

The following list of contributors have given me feedback on this document:

- Roger Venning <r.venning@telstra.com>
- Bruce Potter <gdead@shmoo.com>