Rural/Remote Wireless Research Project: Final Technical Report

Aug 30 2004

Addendum Added Nov 29 2004

Sponsored by Algonquin College, CIDA, IC, and NCIT

Doug Reid, Ian Easson, and Wahab Almuhtadi

Final Amended Version

Rural/Remote Wireless Research Project:

Final Technical Report

Remote/Rural Wireless Project

Research and Project Team

Name	Position in Team	Organization
Jack Treuhaft	Director, Applied Research and Development,	Algonquin College
Nelson Rogers	Project Manager, Applied Research and Development,	Algonquin College
Wahab Almuhtadi	Researcher and Project Manager,	Algonquin College
Doug Reid	Researcher	Network Planning Systems Inc.
Ian Easson	Researcher	Network Planning Systems Inc.
Shawn Rickard	Student, Associate Researcher	Algonquin College
Shannon Parkes	Student, Associate Researcher	Algonquin College
Chris Welsh	Student, Associate Researcher	Algonquin College
Doug Johnson	Student, Associate Researcher	Algonquin College
Salaman Khan	Associate Researcher, Graduate Student	Carleton University

Participating Organizations and Contact Information

Name	Organization	E-mail	Phone	Fax
Les Breiner	Science and Technology Group, CIDA	les_breiner@acdi-cida.gc.ca	(819) 994-4656	(819) 997-0945
Gerry Briggs	Broadband for Rural and Northern Development, Industry Canada	briggs.gerry@ic.gc.ca	(613) 948-5045	(613) 948-5044
Mohamed Zaid	Senior Research Consultant, NCIT	mzaid@ncit.ca	(613) 993 1161	(613) 993-1160
Edward Bebee	Managing Director, Genstar Consulting Group Inc.	Edbebee@Genstarconsultinggroup.Com	(613) 741-7838	(613) 742-1952
Ian Easson	CEO & President, Network Planning Systems Inc.	Easson@netplansys.com	(613) 721-1778	(613) 721-1778
Doug Reid	CTO, Network Planning Systems Inc.	dougr@netplansys.com	(613) 721-1778	(613) 721-1778
Jack Treuhaft	Director, Applied Research & Development, Algonquin	treuhaj@algonquincollege.com	(613)727-4723 ext. 5278	(613)727-7633
Nelson Rogers	Project Manager, Applied Research & Development, Algonquin	rogersn@algonquincollege.com	(613)727-4723 ext. 5040	(613)727-7633
Wahab Almuhtadi	Professor, Electronics & Electro-Mechanical Studies, Algonquin	almuhtw@algonquincollege.com	(613)727-4723 ext. 3403	(613)727-7663
Morris Ure-	Dean, School of	uroemovm@	(613)727-	(613)727-

Name	Organization	E-mail	Phone	Fax
movich	Advanced Technology, Algonquin	algonquincollege.com	4723 ext. 3343	7633
Steve Finnegan	Academic Chair, Electronics and Electro-Mechanical Studies, Algonquin	finnags@algonquincollege.com	(613)727-4723 ext. 3310	(613)727-7633

Contents

Figures

Tables

Checklists

1. Introduction

Project Overview

This is a joint project sponsored by Algonquin College, the Canadian International Development Agency (CIDA), Industry Canada (IC), and the National Capital Institute of Telecommunications (NCIT). The project research is being carried out by faculty and students of Algonquin College, along with researchers from Network Planning Systems Inc.

The project is focused on Canadian and international Wireless Internet technology and know-how, as applied to the developing countries (especially Asia Pacific) and to rural and remote Canadian locales (including remote First Nation communities).

The primary objective is to develop solutions using *off-the-shelf equipment* that are cost effective and practical for deployment under a unique set of conditions of climate, power, terrain, special service needs, and other factors. Thus, there is *no primary research* being done as part of this project.

The project work is in two primary parts: the development and testing of a Basic Configuration, and then of a more Advanced Configuration.

The main deliverable of this research project is a “Cookbook” of recommended approaches, technologies to employ, and system solutions that will meet the above challenges. It is intended that this Cookbook will be distributed to the world community, although its publication and distribution are *not* part of this project.

This is the final technical report on the project. It incorporates material from the following:

- Basic Configuration Report (in its entirety)
- Advanced Configuration Report (in its entirety)
- Some sections from earlier reports:

The Advanced Configuration is designed to enable a basic layer 2 wireless network with one or two AP nodes to be expanded into a multi-node system. To do this effectively requires a different approach from simply extending a bridged LAN such as used in the Basic Configuration.

In a bridged LAN, the amount of overhead traffic (signalling, etc.) grows faster than the number of bridged nodes increases. With backhaul radio links interconnecting the nodes, overhead traffic can reduce net information traffic throughput significantly. This happens because bridges broadcast overhead traffic to all parts of the network, even if that is unnecessary.

Basic Configuration Activities

At the beginning of March, the Wi-Fi lab and its equipment became available to start the applied phase of the work. The Basic Configuration was first demonstrated in mid-May, at short ranges. Since that time, issues with longer ranges were identified and overcome.

At the Wi-Fi lab, the Wi-Fi elements that make up the Basic Configuration were set up and tested to determine what settings provide good throughput performance and stability while remaining fairly straightforward to set up by non-expert people.

Another activity was to procure and try out various software tools for field strength measurements and throughput analysis of the radio links as well as the overall system. This test equipment and software was successful.

In parallel, analyses were carried out to predict the expected range and coverage of the 2.5 GHz 802.11g and b modes. These calculations were verified in the field. The work involved appraising several propagation models for different types of areas (urban, suburban, and rural), antenna types, tower heights, and power levels. Both directional backhaul and omni-directional coverage are involved. A test antenna array was assembled and initially tested outdoors.

Advanced Configuration Activities

This report provides a summary of the Advanced Configuration, its performance, and recommendations for its use in the field.

The main focus of this work was to try out firmware variants on the LinkSys and D-link APs to provide a higher degree of layer 2 switching capabilities such as VLAN and layer 3 routing capabilities. As part of this effort we also investigated low cost routers and switches used for enterprise networks that could be used with standard APs. In addition, the capabilities to do extension of AP coverage using store forward repeatering as well as classic duplex repeatering were investigated.

Summary of Basic Configuration Results

The Basic Configuration is successful. We have demonstrated the suitability of the system architecture and equipment.

In order to succeed, it was necessary to make changes in the firmware, minor equipment modifications, and default configuration settings. Such changes should be easily handled by users with guidance such as the Cookbook.

The system performance was very good. The Basic Configuration has not impaired throughput or latency significantly so far. We still have to test the “near / far user” case.

Propagation problems due to manufacturer-set diversity and undocumented settings were identified and overcome. Once the internal antenna switching was disabled, link behaviour was as expected. Viable distances can be achieved, but the user must be wary of path obstacle clearance issues.

Direct RF interference between nearby circuit boards (for APs and Bridges) was identified as a problem. It was solved by using simple enclosures with appropriate RF shielding.

Summary of Advanced Configuration Results

The Advanced Configuration work showed promising results, with some success in the areas investigated.

The use of VLANs in a wireless LAN context is an area that is just being tentatively introduced in commercial APs. The need for VLANs even in WiFi mesh networks is apparent, to enable traffic balancing so that links between APs are utilized more efficiently. In addition, it enhances some security aspects.

Third party alpha firmware was procured and tried with the LinkSys AP that had VLAN capabilities as part of the advanced features set. This was trialled with some positive results. These showed that layer 2 broadcasts were blocked on the ports subtended by the LinkSys.

The firmware used is still very much in a development state. Thus, the behaviour of the network was somewhat unstable. The set-up interfaces were also incomplete, making confirmation of settings difficult. Similar routing firmware was also looked at and found to be to not functional as of yet. The upside of this work is that a more hardened release of the VLAN firmware is expected to be available by year end and thus can be considered for later use in small cookbook networks.

The repeatering of signals was very successful. The APs can be used very successfully by people in the field to simply extend AP coverage or interlink APs. The newest firmware releases by D-link And LinkSys as well as Proxim provide excellent repeater features with easily used graphic user interfaces. We have demonstrated the suitability of the system architecture and equipment. When attempted, the repeater operation did not introduce any significant latency or reduction in bandwidth.

One of the salient conclusions when formulating the network architectures is that standalone low-cost router or switch packages can be used in conjunction with standard APs, enabling very stable LAN networks to be set up. In cases where multiple APs are used, the introduction of these functions will increase the efficiency in the inter-AP links as well as backhaul facilities by very significant percentage (as much as 40%+ reduction in overhead traffic).

Equipment Readiness for the Target Applications

Off-the-shelf equipment is not usable out of the box using the supplied information from the manufacturer. However, once configured according to rules we have discovered and documented in this Report, the system is very stable. These configurations can be stored in Flash memory so that if the system resets, it can return to a functioning state without user intervention.

LinkSys

We also found that the LinkSys Firmware does not support the needed features out of the box. However, alternative 3rd party firmware documented in this Report works well enough to allow non-diversity antenna operation and single antenna selection.

D-Link

The D-Link allows more versatile bridging options. It provides the needed configurations. However, the settings must be modified from the default settings in order to be able to utilize its bridging modes:

- The hidden antenna diversity settings must be shut down for external antenna use.

- The receiver must be fixed to not scan in the event of a Loss of Signal (LOS).
- Addressing defaults must be changed to engage the network properly (static IPs)
- MAC #s need to be set for bridging.
- The power should be set to the highest level (+17 dBm).

Long Distance 802.11b Timing Issues

Given the 802.11b IEEE standard, the MAC layer if implemented precisely using the tight timing tolerances defined in the IEEE specifications will be extremely sensitive to transmission roundtrip delays. Thus, with this specification, the likely outcome makes any long distance links greater than 3 to 4 km an impossibility for the 11 Mbps rate to be maintained. This is not surprising since the 802.11 spec was designed with Local Area Networks in mind, where distances are less the several hundred metres.

The core of the timing problem is the 10 microsecond Short Inter-Frame Spacing interval. This delay of 10 millionths of a second is all the 802.11b specification allows for certain high priority packets to begin to be received in response to the invitation to send. If the ACK message or data packet is delayed beyond this dwell time, the packet is not received and the protocol responds with the transmission rate of the link to be dropped. This reduction rate results in a longer dwell period to be used waiting for the response.

Doing some basic calculations provides the following results:

```
Speed of Light (299.8 m/µSec) x 10uSec for the SIFS =
2,998 metres or 9,836 feet or 1.86 miles.
```

Obviously that isn't very far, and the fact that people have documented reliable 11Mbps connections over much longer distances implies something is being miscalculated.

Fortunately, it turns out that the 802.11b spec as implemented by ASIC vendors is done in a much more lenient manner for the MAC. The 802.11b spec requires other peers to wait at least as long as the Distributed Point Coordination Function Inter-Frame Space (DIFS) before attempting to transmit. Any seemingly lost frames are also delayed at by at least the DIFS interval plus some "contention window" time which is an exponential backoff.

If the math is redone allowing for a typical MAC timing with at least 2xSIFS + DIFS the results look more favourable for longer distances.

```
Speed of Light (299.8 m/µSec) x (10 + 10 + 50) =
20,986 metres (21km) or 68,852 feet (13 miles)
```

Our measurements so far show no significant problems at +4Km in a backhaul link using APs in a wireless bridging mode. We will be confirming +8Km to see if significant throughput limiting occurs at 8.0 km given adequate S/N.

The above calculation may be optimistic, however there is enough empirical evidence from other researchers and users in the field that confirm even greater distances (>>30Km).

Point-to-multipoint systems using 802.11b should be able to achieve 4 to 5 km service radius given the above. Greater distances will be very dependent on the number of total users as well as their relative distance from the serving AP. Greater distances for point-to-multipoint with many clients will end up with extremely high amounts of contention and collisions due to the delays in critical control packets.

Equipment Packaging Conclusions

As shipped by the manufacturer, the packaging is only suitable for internal use, not outside use:

- Repackaging is needed for ruggedness
- RF connectors need to be upgraded
- There needs to be lightning protection for external antennas
- Power surge protection is needed
- Generally inadequate RF shielding needs to be improved, especially if there are other APs nearby. A metal box with shielding (NEMA box) is required for outdoor operations. Such a box retails for about $50 USD. It:
  - Solves the Signal to Interference issues
  - Solves weatherproofing issues, and provides shielding, heat sink cooling, and a mount for connectors. It is also mast mountable.

Simple low-cost fixes are available to mitigate the above issues. It is interesting to note that manufacturers such as D-Link are now providing lower-cost outdoor solutions providing much of the above for under $1500 US.

Netstumbler Deficiencies

Our initial enthusiasm for the Netstumbler software waned considerably as we began to understand its limitations more. Specifically, as we began using it for antenna alignment, the following deficiencies came to light:

- Netstumbler's active scanning is not useful for detecting APs that are not in Infrastructure AP mode or are set to not respond to these interrogation messages as a security measure. In the above cases, active scanning will only show the APs when they happen to emit data bursts, and thus will display the presence of the AP very infrequently. In addition, the software is designed to ignore subsequent transmissions if they are not coming from standard APs.
- A second drawback for antenna alignment is the delay that active scanning tools sometimes exhibit in showing the presence of an active AP. We noted in a number of instances a very significant delay of up to 60 seconds or more before an active AP will be detected initially or not updated as to the current status. This is very problematical when using these utilities to determine field strengths for the purpose of antenna alignment since the adjustment process is much more efficient if a real time feedback is available for positioning the antenna.
- The use of Netstumbler and similar tools is appropriate for establishing links if it is used with recognition of the limitations imposed by their design. For general coverage checking for an AP, it will work well providing the user has a good idea

of the signal availability. The user must however allow a settling time of at least one minute before moving to a new orientation or location of their adapter card to ensure readings are captured.

- For alignment of directional antennas, Netstumbler is of more marginal effectiveness, since the user must wait a period of time for the software to capture the AP. Thus initially finding the signal can be a long process using small incremental adjustments and waiting each time to get a broadcast from the distance AP. Once the signal is captured the process can speed up since the interrogation and response cycle is about one second allowing the user to make fine adjustments to the antenna at a reasonable rate to get an optimized field strength.

Summary Comments (Added Nov 29 2004)

The concepts as originally developed for validation in this test work have proved out to be quite usable as a basis for deploying rural Wi-Fi. This was further proven out with additional investigative work required to solve problems with maintaining previously achieved bridge connections early on in the project. Though this work delayed the completion of the project, it revealed many important insights that will hopefully make it easier for communities to do DYI broadband WLANs.

Several important lessons were learned in this work particularly about the reliability and quality of the current range of wireless products offered by well-known vendors. The phrase *buyer beware* certainly comes to mind here as well as well as never assume things will not change significantly over time. Our experience with the D-Link bridge units showed problems in out-of--box performance variances as well as degradation over time as was the case with the D-link field unit. This caused a lot of sleuthing trying to figure out what part of the system was going down such as connector problems, path problems, RF output stage problems and so forth. The intermittent nature of the problems made it difficult to pin down the problems.

The DWL2100 AP/WLAN bridges were selected as substitute hardware for the ailing DWL900s. This product clearly showed much better adherence to specifications and matched originally expected performance benchmarks in the field. The unit provided very stable operation in the Basic configuration setup, The RF testing systems using NetStumbler and or Kismet quickly spotted the bridge's signal. The DWL2100 was also used in AP mode and proved to be very compatible with a number of PCI and PCMCIA cards on hand including Netgear, US robotics, and Oriinico (Agere), which was not the case with the DWL900,

The wisdom to pass along here is that in selecting equipment to use in the field acceptance should be done using several units to weed out units that do not meet advertised specifications. The quality control used for consumer equipment is very marginal at best, and is one of the reasons it is less expensive than commercial grade counterparts. For situations where the performance envelope is being pushed, the actual performance capabilities must be known or it will be difficult to pin down problems if assumptions are incorrect about unit's characteristics.

2. Overview of Basic Configuration Setup

Overview

This Chapter provides a qualitative discussion of the Basic Configuration architecture and configuration issues for its elements and links. A later Chapter (6) provides details of specific configuration settings.

The intent of the Basic Configuration is to provide a system set-up that can be documented and easily duplicated by an end-user with reliable results. This proved to be somewhat more convoluted then we first anticipated, due to a number of characteristics of the Wi-Fi equipment. However, the problem was brought to a successful conclusion.

The D-Link and LinkSys systems that the Basic Configuration utilize are very representative of the technology available in the under $150.00 USD price range.

Off the shelf, the features, documentation, and firmware of this type of equipment are tailored for residential and office use, making it a nearly plug and play experience for the user. To use this equipment for remote Wi-Fi installations calls for a fair departure from the mainstream application the equipment has been targeted for by the vendor. Fortunately, a number of the AP's features enable them to be useful for our target application. However, some of these required features are hidden or not addressable with the standard firmware loads supplied with the equipment.

With the very high focus on Wi-Fi technology, we found many 3rd party solutions to provide new features or allow access to previously non-modifiable system settings. The use of these solutions can pose some risk with the typical issues such as viruses, untested software and compatibility problems. However, several sources were found that were deemed all right to use (at your own risk) by the equipment manufacturer.

The Basic Configuration

Two views of the Basic Configuration are shown in Figure 2-1 and Figure 2-2 below. These views each emphasize different aspects of the configuration.

Figure 2-1: Basic Configuration: One View

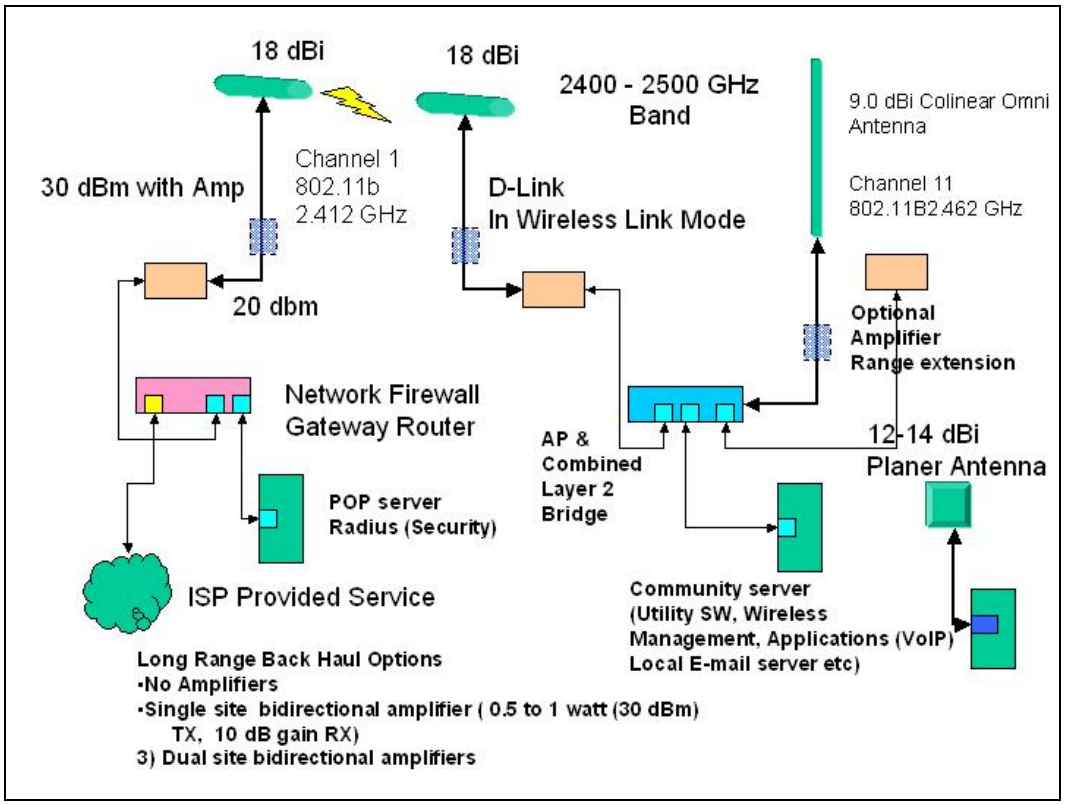
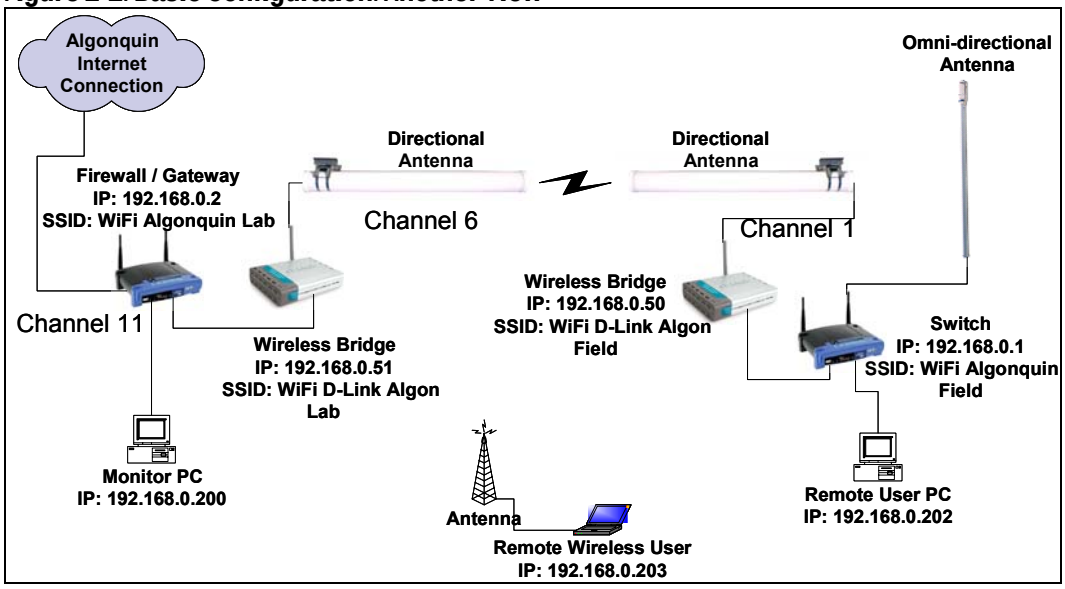


Figure 2-2: Basic Configuration: Another View



LinkSys Setup

APs behind an Existing Firewall

For most part, the firmware provided by the manufacturer proved to be adequate for setting up the LAN layer 2 and 3 architecture. For example, the LinkSys is oriented

to provide a gateway / router solution to be used with Cable and ADSL modems. The use of the LinkSys as a remote AP requires it to be used behind an existing Firewall router. This requires that the LinkSys router AP be configured as a transparent bridge. All default settings such as RIP and DHCP server settings need to be overridden. The AP also has to be assigned an IP to be visible to the existing Gateway router in-place at the ISP.

LinkSys wireless routers such as the RTG54 are very versatile and utilize Micro C Linux as its OS on a P2 equivalent processor. It also comes with a large amount of resident memory that allows new applications to be easily created for it.

LinkSys AP Bridging Configuration

The LinkSys model WRT54G AP selected for the AP testing provides a wide range of useful features that helped the setup of the basic configuration.

The primary feature is the bridging hub that is used in the AP site. This feature enabled the simplification of the AP architecture, with the LinkSys providing both an AP function as well as a bridging hub to link the backhaul D-Link into the AP while providing additional Ethernet ports for a local test computer and a connection for another backhaul link if desired.

The AP can also provide network firewall functions and router functionality for interfacing into a WAN network or ISP gateway. In the lab, a LinkSys is being used in this manner as well as to provide local wireless coverage in the Lab

This LinkSys model has proven to be a very flexible device with options to use other 3rd party firmware that has been approved for usage by LinkSys. The LinkSys unit incorporates a Linux operating system along with a well-resourced microprocessor that can support many additional features that can be useful for useful for remote applications. The majority of these utilities are available as shareware and can be downloaded from the Web (www.sveasoft.com). These capabilities will provided a basis for looking into other features that could be incorporated in subsequent architectures for rural use.

In Figure 2-3 and Figure 2-4 below are several sample screen shots of the LinkSys configuration screens that will be used in the Cookbook to help illustrate the setup operations.

Figure 2-3: LinkSys Setup Screen 1 of 2

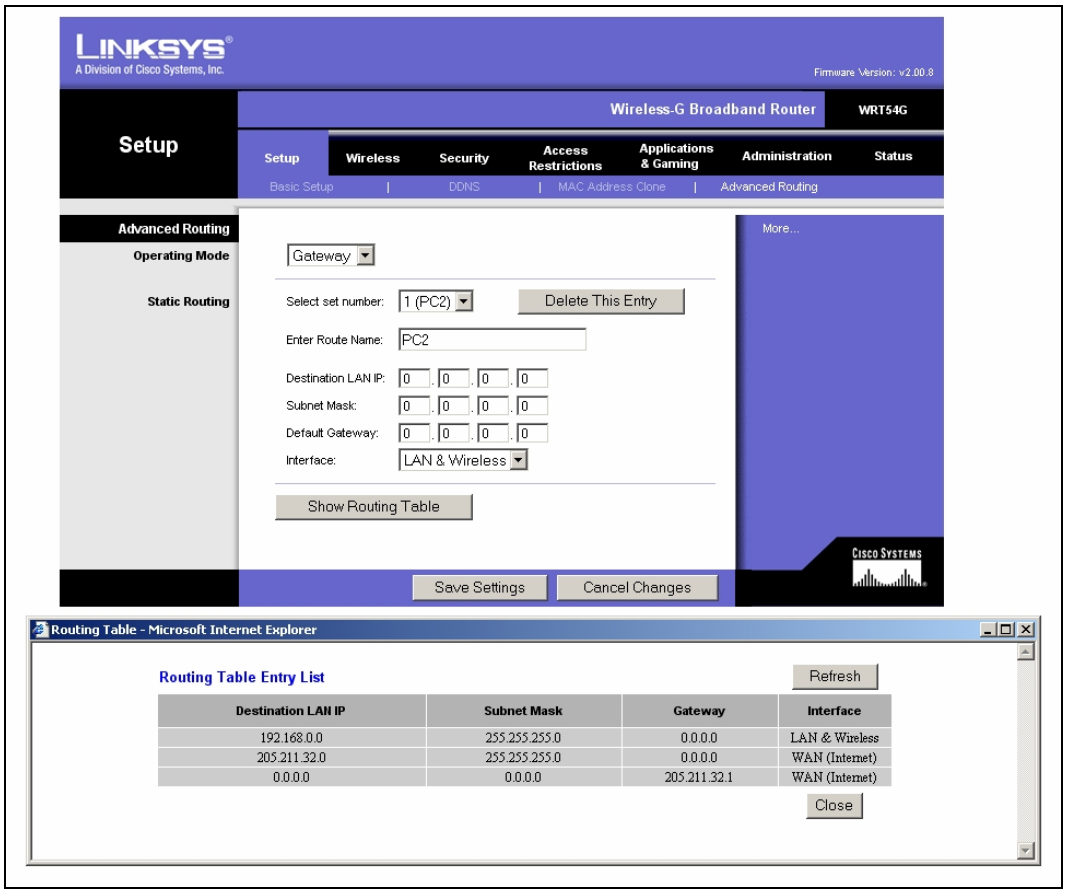
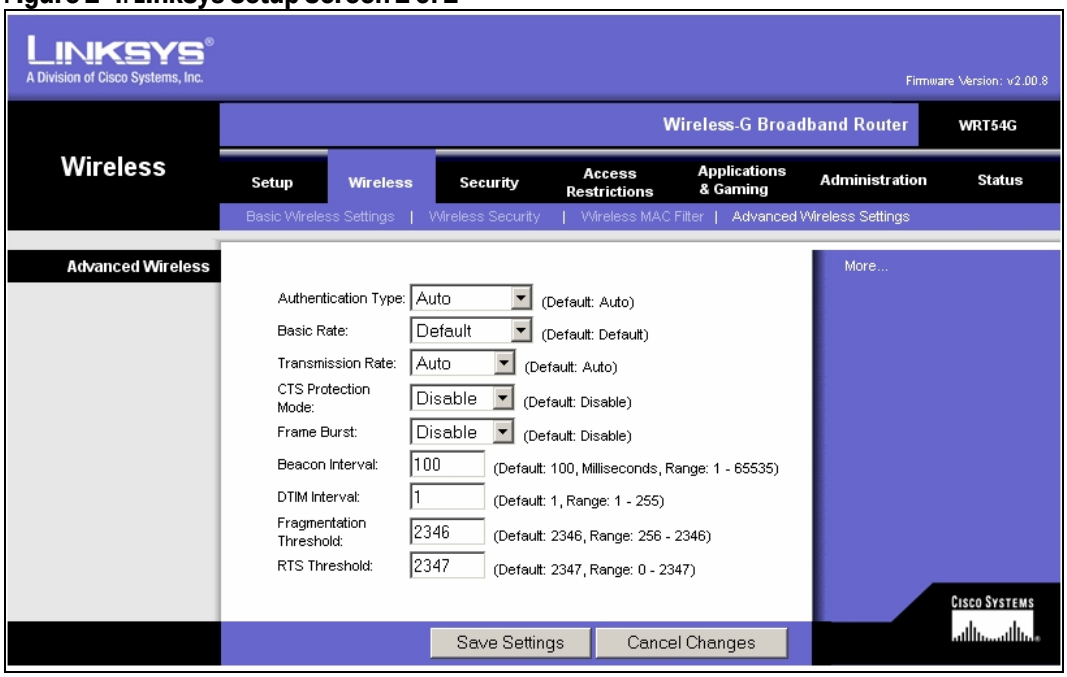


Figure 2-4: LinkSys Setup Screen 2 of 2



LinkSys with External Antennas

The use of the LinkSys AP which obviously featured antenna diversity posed a problem to using the units with a high gain external omnidirectional antenna. To our surprise, the standard firmware of the LinkSys does not allow the user to change the diversity settings.

We considered combining the two antenna connections together, but in analysis a 3 dB plus power penalty would be an unacceptable loss.

We then sought solutions from other Wi-Fi groups and forums to see if alternative viable solutions existed. A 3rd party software company was found that provided a replacement firmware with the feature to address the diversity settings turning off one antenna port. This allows the external antenna to be used exclusively.

LinkSys – D-Link PC Card Issues

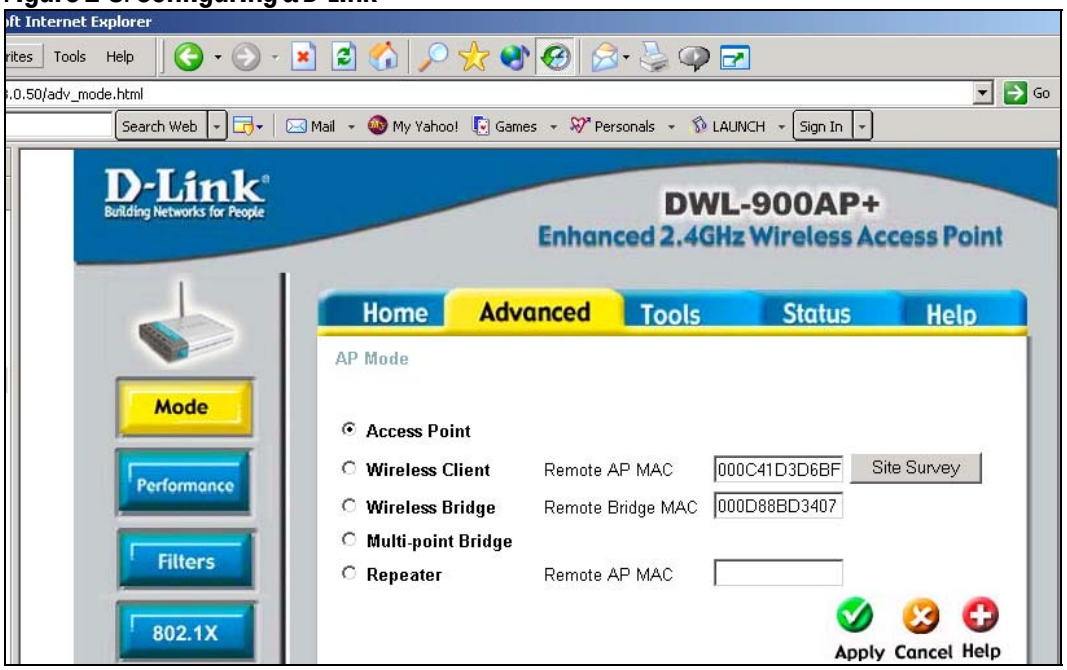
In testing several of the D-Link client adapter cards, a compatibility problem was uncovered between the USB D-Link PC Adapter DWL-120. The cards failed to connect to the LinkSys AP on most attempts. If a connection was forced, it would collapse very easily. The D-Link cards otherwise performed correctly with the D-Link AP. A literature search showed up a few cases of interoperability problems; however the problem does not seem to be widespread. The DWL-120 is an older model and thus may require a firmware upgrade to be compatible with more recent equipment. This is an issue that will be explored further to form part of the guidance for equipment selection in the Cookbook. There have been at least two generations of the hardware put out in the market, and thus consumers must beware of buying outdated versions.

D-Link Bridge Setup

The D-Link's standard configuration as a wireless bridge was very straightforward to set up. This is done by simply informing the bridge units of the MAC ID of the unit it corresponds with. This bridge mode proved to very transparent, with no significant packet legacy at the highest baud rates.

The D-Link can be easily utilized as an AP or backhaul transceiver. In Figure 2-5 below, the D-Link bridge configuration is very straightforward. In Figure 2-1, the configuration choices are given that allow D-Link APs to be set up as point-to-point wireless bridges. In this mode of operation, a transparent connection is set up at layer 2. This requires that the both D-Links know the other's MAC addresses. This arrangement excludes other users from using the D-Links for AP addresses but does not guaranty immunity from deliberate Wi-Fi hackers.

Figure 2-5: Configuring a D-Link



Note that the D-Link's highest baud rates achieved were +22Mb/s, whereas the 802.11b standard calls for 11 Mb/s baud rates. The D-Link was able to double this rate by employing a variety of non-standard techniques. Most residential Wi-Fi equipment now employs such "Turbo" techniques to try and achieve competitive differentiation. It is likely that many of these currently non-standard techniques will become part of the next increment (802.11n) to the 802.11 family of standards.

Problems with the D-Links came to the fore when the units were put into field service. In the field it was noted that the links were unstable and displaying unexpected variance in signal levels and loss.

As is explained in the antenna diversity section (page 2-7), the D-Link incorporates a "hidden" diversity antenna inside the package besides the externally connected one. In our Basic Configuration, the D-Link would often favour the local internal antennas since it would "hear" the local test LinkSys running in the lab. In doing so, the high gain antenna connected to the D-Link would go dormant or only radiate at a very low residual signal level. This switching was not apparent due to the bursty statistical nature of the 802.11b and g signals. The result of this caused a lot of wild goose chases trying to determine where faults in equipment may be causing the intermittent behaviour.

In certain situations, normal operation would be seen through the bridge link when the D-Link's external antennas were close enough to each other for the external antenna to be favoured. As soon as the distance increased between the antennas, the diversity logic switch would go internal as soon as a local AP signal was heard. This was resolved by digging out where in the firmware the ability to stay exclusively on the external antenna was found.

Diversity Antenna Switching

Many off-the-shelf APs such as D-Link, LinkSys, SMC, Proxim, and US Robotics use very similar RF ASIC 2.4 GHz transceivers that feature diversity antenna switching stages. AP packages will either have connectors for two antennas or have one external antenna connector, with an internal antenna connected directly to the circuit board. These arrangements are meant to be used for typical indoor applications where the external antennas are small 10 cm stub antennas.

In outdoor applications involving external high gain antennas, the antenna diversity operation *must* be turned off. The AP must be set to use the same single antenna at all times. If left engaged, the unit will improperly switch between an external antenna and the remaining package-mounted or internal antenna. This disrupts the signal feed to and from any externally mounted antenna unit, causing intermittent disruption of the links. This is especially true in those cases where there are other nearby 802.11b or g signal sources. The AP will switch between antennas, favouring the antenna with the best signal strength. Thus, when trying to receive more remote weaker user signals over the external antenna, the AP will can miss them if there are strong signals very close by being received on the other low gain antenna.

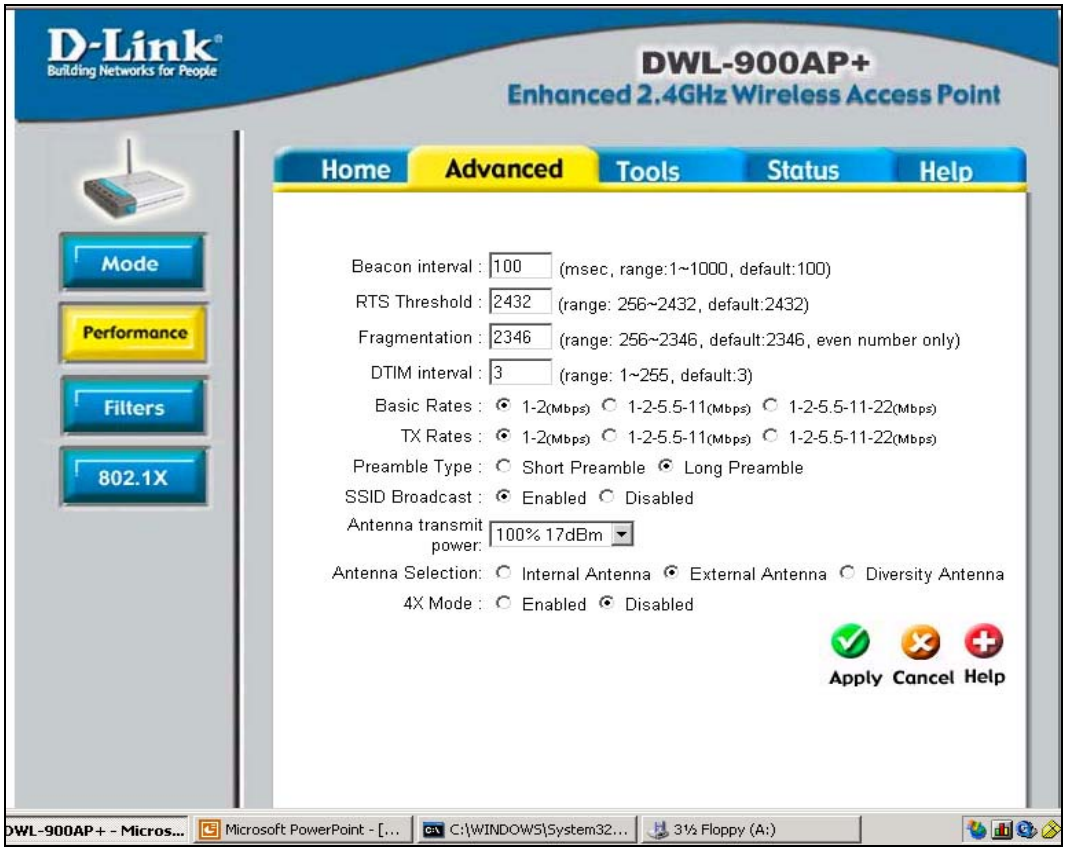
The 802.11b and g standards also incorporate a feature for the AP to reduce signal power if the user is nearby, to reduce overall spectral loading for multiple AP applications. This power reduction can cause problems again with the external link where maximum power is required. To get around this problem, the power level must be *fixed*.

Unfortunately, not all APs make it straightforward to configure them to disable the diversity operation and have the power level fixed. For example, the D-Links used for the backhaul portion of the demonstration system are fitted with only one external antenna and have an internal package antenna. The supplied documentation does *not* make it obvious that the unit employs diversity or that it can be configured in the firmware to be disabled with the capability to specify which antenna feed to use.

In our backhaul field experiments, intermittent operation and low power were noted with the D-Links. In these cases, the units were set (by default) to automatic antenna selection operation based on received signal strengths, which disrupted the backhaul link. In the Basic Configuration test set up, local LinkSys APs were also used at each end on different channels in the 802.11b band. Even with the wide frequency spacing, the strong local signals that were seen on the internal D-Link antennas caused a switching from the external antenna to the internal antenna whenever the local APs did a transmission burst.

The D-Link transceiver thus needs to be set for external antenna use only. See Figure 2-6.

Figure 2-6: Disabling Antenna Diversity and Setting Other Detailed Configuration Parameters



Base Configuration Addendums

Power Disruption and System Recovery Issues

In our experiments, momentary power disruptions that we subjected the units to resulted in some unexpected hangs in the recovery of the units. By design, the APs are to refer to the firmware stored in flash ROM with the configuration data intact. The LinkSys units restored correctly most times. However, one of the D-Links on occasion hung or went back to default settings. This behaviour is of some concern if the units are being used as repeaters in poorly accessible locations. Manual intervention should not be required to recovery from a simple power break.

A minimum of 15-minute Uninterruptible Power Supplies (UPS) should be used with the main APs to ensure acceptable reliability and manual reset / reconfigure actions. The use of UPS units brings on some additional costs and complexity. However in trade-off we feel it should be an item for the Cookbook to include.

Preserving Information

AP units all consistently have non-volatile flash memory that stores the last configuration set-up put in by the person administrating the system. This has shown to be fairly reliable. But, as a precaution, the user should take screen shots of forms they have modified plus save any notes they used during the system's first set-up.

In one instance due to a power interruption we did have one unit revert back to default settings requiring the set-up procedure to redone. Also if an equipment failure occurs, the configuration stored in the unit is not recoverable.

Recovery Aspects

The AP units recovering from a power failure will reboot their firmware. If custom configured, they will reload the selected parameters set by the user, The APs will go on the assigned channel and send out bursts to see if other units are reachable. Once contact is established, the AP will resume its assigned mode of operation (as an AP, Wireless Bridge, Repeater, or Client, for example).

This was exercised a number of times. Most times, the units recovered the connection and restored the link. However, there were instances of “hung-up” restart processes. These required a hardware reset on the AP package to be pressed manually. The hang up could also be cleared by again disrupting power to the unit.

This behaviour was observed more often when there were either surges or quick successive power breaks that occur typically during thunderstorms. This indicates that the equipment may require a time out hardware reset feature to allow an automatic reboot if the unit fails to fully come on line.

User Set-up Aspects

In setting up “new” user links with the Basic Configuration, no issues arose with access or transparency of the WLAN segments and backhauls as long as DHCP settings were set up with the Internet firewall at the IPOP (Internet Point of Presence). User participation was straightforward.

However, we have encountered problems with “used” computers that have been previously set up with LAN-wired NIC cards and networking software from previous users. With the aspect that many of the user groups building system on low budgets, used computers will be the rule, all with a wide range of Operating systems and networking software.

To minimize the start-up woes which we have experienced, computer systems should be cleaned up as much as possible of applications or OS network settings that can interfere with proper WLAN operation. Often this manifests itself in IP setting problems with interference from installed LAN software. Administrator access must be used in order to defeat many of the settings and uninstall problem applications or disable the start up of unnecessary programs or services during boot time. Temporary files should be deleted, and the hard disk defragmented. We also found that shareware “RAM optimizers” help in low memory situations, because they unload unnecessary information from RAM, thus freeing up more RAM for the Wi-Fi applications.

Once the computers were normalized and WLAN drivers installed, configuration and proper operation was quite straightforward.

Equipment Packaging

Equipment built for residential use has compromises between costs and its ability to continue to operate well in more hostile environments. Temperature extremes, moisture, resistance to electromagnetic interference and resistance to mechanical

shock are examples of where tradeoffs have been done. In home environments, thee factors are usually in a benign range and will not impact equipment operation significantly.

For rural or remote applications, it is quite likely that one or more of these factors will be outside the product's tolerance. However, basic products such as home Wi-Fi equipment can be modified to some extent to enhance their capability to provide acceptable performance without triggering high costs.

EMI Shielding

Most low-cost Wi-Fi APs have been designed to be used as standalone units, with no other APs in close proximity and a limited number of client transceivers nearby. As a result, more stringent commercial specifications for EMI emissions and susceptibility have been waived (IEEE-ANSI) with consumer FCC part 15 rules applied.

However, equipment configurations for rural/remote applications will have multiple APs, some in bridge mode, repeater and AP. Thus, the use of shielding solutions like that shown in Figure 2-7 and Figure 2-8 below is required.

Figure 2-7: Enclosing an AP within a NEMA Box

Figure 2-8: Enclosing a Bridge within a NEMA Box

Environmental

Consumer AP packages are designed to operate in partially environmentally controlled areas typical of a household. This is contrast to some commercial grade equipment that requires much tighter control of ambient conditions. The consumer product will operate satisfactorily in temperatures from approximately 5 C to +30 C without noticeable problems. Similarly, humidity of less then 60% is acceptable.

Weatherproofing and Humidity

Using the equipment in outdoor conditions will require that the AP unit be placed in a reasonably airtight and waterproof container. If the container is not airtight, condensation can build up in the box as well as water leaking from rain and dew. High humidity will fail the circuit board, especially if there is salt brine in the air in coastal areas.

Overheating

A problem with enclosing the APs will be keeping the AP electronics below 40 C on hot days. Cooling can be accomplished by using metal enclosures that provide for some convective airflow around the box using metal fins. Vents in the box are not desirable since moisture and insects can easily get in. In very hot areas, the metal enclosures should be mounted in shadowed areas or have a sunshield and painted a light colour.

Fireproof

If the enclosure selected is plastic or resin material (that has metal screen or film applied for EMI shielding), it must have fire retardant properties. This is especially true if the AP unit will be mounted near flammable objects. Lightning can ignite the box if the materials are flammable.

Antenna Structures

Cables

The cables used to interconnect the 802.11b APS to mast-mounted external high gain antennas must be low loss and durable to take on widely varying weather. The LNR 400 coaxial cable selected for the work exhibited both qualities with a loss of 0.2 dB per metre. This loss characteristic was verified with actual cable runs. See Figure 2-9.

Figure 2-9: LNR 400 Coax Cable

Less expensive cable such as RG58 (1.0 dB/m loss) can be used for short runs under 1-2 meters with minimal loss. This cable is more flexible and is better suited for linking to desktop adapter cards or to indoor window mounted antennas, for example.

Cable not designed for UHF or microwave frequencies should be avoided since excessive loss will be experienced at 2.5GHZ.

Antenna and Cable Connectors

Most antennas come with Type N connectors mounted on the antenna package for easy hook-up to the cable feed. These connectors are fairly rugged. However, care must be taken in handling the cable connector to prevent excess stress on the mounted connector. See Figure 2-10.

Figure 2-10: Antenna Connector

Unfortunately, not all Wi-Fi equipment has Type N connectors. Thus, adapters must be used to connect to reversed SMC connectors mounted on the equipment. The use of rigid sleeve adapters is acceptable. However, the adapter can be a source of failure, as was discovered in the project. The use of adapters that have a short flexible coaxial cable joining the two connectors allows easier handling and is less likely to fail.

These cable adapters have some insertion loss in the 0.5dB range. Similarly in line connectors to lengthen cable will introduce loss. It is important to minimize the number of these connectors to ensure maximum RF power into the antenna as well as receiver sensitivity. Typically, three connector sets are acceptable, with losses being less then 1.5 dB.

Waterproofing

Any external connectors or equipment must be weatherproofed to prevent moisture from entering the connector. Moisture will absorb energy in the connector and also lead to corrosion that will degrade RF performance.

The weatherproofing was done with rubber-based self-sealing insulating tape that makes an impermeable bond to itself and to the connector. Ordinary vinyl electrical tape can be used, but it will not last.

The antennas are waterproof. However, units that are enclosed with radomes have small drainage holes to allow any condensation to drain out. It is important that the antenna be mounted such that one of the drain holes is facing downwards.

Coaxial cable which has the outer cover damaged or peeled back should be taped to prevent water getting inside the cable.

Antenna - Cable VSWR

In using standard coaxial cable (50 Ohm) rated for low loss at 2.5 GHz, care must be taken in how the cable is terminated at the AP or client adapter card as well as any intermediate connectors or connector adapters to avoid standing waves, as measured by the Voltage Standing Wave Ratio (VSWR). Another issue is any place where the cable has been kinked or crushed by improper handling or mounting of brackets to hold a cable in place. High VSWR will also result if the cable or connecters have gotten moisture in them or have been exposed to high heat causing

insulation to break down. This can happen if the cable carried a high current due to a lighting antenna strike. In the event that this occurs, replacement of the cable is required.

In our testing, minor VSWR was encountered with the cable adapter not seating correctly, causing a mismatch in impedance and thus lowering transmit output power.

Lighting Arrestor Failure Causing VSWR

The use of lighting arrestors is required, as has been pointed out in this document. However, if an antenna lighting strike has occurred, the arrestor can be damaged affecting the performance of the antennas system severely. In the Cookbook, the proper installation and the need to replace these units will be presented.

Towers

Use of towers for range and coverage enhancement proved very successful in the experimental work carried out in this project. The towers provide the essential antenna elevation to get over near field obstacles and allow the establishment of useful service areas.

For the Wi-Fi project, a section tower manufactured by Delphi Inc. was used. This tower comes in 10 foot sections that are simply bolted together. The top of the tower is constructed so that a steel mast pipe can be mounted along with extra items such as an antenna rotator. These have been designed for rural television antenna use and can easily support a number of typical 2.5 GHz antennas. With guy wires, this type of tower can be used up to 80 feet (26 m). At lower heights the tower can be supported by a building using a special mounting bracket, eliminating the need for guy wires. The tower is very durable, rated at winds over 160 kph.

A 40 foot tower can be set up by three people in less then an hour, complete with antennas and cabling. Standard carriage bolt hardware is required along with simple tools (wrenches, pliers etc). See Figure 2-11.

Figure 2-11: Tower

In-situ masts or poles can be used for attaching antennas as long as the structure can bear the weight and wind loading. It is very important that the mast used does not sway in moderate to heavy winds. Excessive antenna movement of over 10 degrees will impact the link performance due to misalignment of the antenna's field patterns.

Lightning - Arresting, Rods, and Grounds for Towers and Roof mounted Antennas

The use of lightning arrestors is mandatory for any towers or antenna structures mounted on buildings or stand alone. The tower structure itself should be grounded as well as the antenna to prevent damage to the antenna and equipment attached to it.

Antenna Arrestor

For the project, an inline coaxial lightening arrestor unit was used. This prevents high voltage induced by the lightning strike from reaching the transmitter. The arrestor is grounded (earth ground).

Wood Poles

If a wooden pole is used, a top-mounted lightning rod must be used to discharge the lightning to ground. If not, the coaxial cable will bear the brunt of the current flow damaging it severely.

Note – The antenna arrester should not be the only protection in place since it will be inadequate to handle the discharge.

Grounding Rods

Grounding rods made of copper pipe or solid copper rod (> 3 cm in diameter) should be used. The rod should be 1.5 to 2 m in length and be driven into the ground at least 1 m. This will ensure the electrical flow is discharged into the soil without harming equipment. The rod must have cable clamps connecting them to the copper ground cable.

Ground Cable

For our experiment, a 6# copper wire was used to link the tower and the coaxial lighting arrestor to a proper earth grounding point. On the tower, a copper grounding clamp was used to connect the cable from the antenna and then to the earth ground. This was done to prevent any discharge between the antenna and tower itself. A full reference for proper lightning safety is given in the reference section.

3. Test and Measurement Systems and Procedures

Using Freeware and Modified Antenna Adapter Cards

In order to confirm operation and coverage of an area, an adequate means of determining if an acceptable signal level exists must be used. For our experiments, this proved to be a bit of a dilemma, given that use of professional equipment and software would be well beyond the means of many groups trying to set up a basic system.

We did an extensive search for adequate, low-cost or free software tools that could be used with some reliability to help testing in the lab and the field, and in deploying a system.

Our answer was to use Netstumbler, which is well-known freeware testing tool. Until quite recently this software had many drawbacks including its' lack of compatibility with many of the PC adapter cards on the market including the D-Link units selected for the experiment. However, a new release of the freeware has been made that is compatible to more readily available cards such as US Robotics and LinkSys.

We believe the Netstumbler program can be used with guidance by anyone to aid them with their set-up. In operation, the program addresses the adapter card on the PC laptop and scans the entire 802.11 band the card covers. All AP signals received are identified with all their characteristics displayed textually in a table providing received power levels in dBm, Signal to Noise, Baud rate, SSID, Security settings, and time of signal burst received, amongst other data. This table is updated continuously and will update each entry as new transmission bursts are received. From this, a relatively inexperienced user can determine if they have an adequate signal to sustain successful data transmission. In figure 3.1 below a screen shot of some actual measurements is shown from the field laptop.

For remote set-up, high gain antennas must be utilized and thus the adapter card used for RF measurement must be able to have a connector to allow antenna hook up.

In describing this technique in the Cookbook, cards that already have this feature and that are compatible to the Netstumbler software such as ORINCO (Proxim) are

recommended. If other compatible cards are available without external connectors, a connector can be mounted on the card and connected in place of the internal antenna.

This is not recommended except in cases where there is local expertise to carry out the procedure. We are including this procedure in the Cookbook since PC cards that feature external antenna connectors are not readily available.

For our measurement system, a US Robotics cards was modified and a photographic and drawings will be rendered to show the procedure.

RF and Performance Measurement Systems

Types of Systems

The determination of the coverage patterns, performance, and antenna requirements for users requires the use of easily installed and operated PC-based Wi-Fi performance measurement software. Specialized instruments are available such as Yellow Jacket (ref) which somewhat costly and thus hard to justify when budgets are very limited and the use of the instrument is primarily in the installation phases. Our investigations thus far have identified several approaches to inexpensively configure a Wi-Fi equipped laptop computer into a useful site survey instrument. In order to do this several freeware applications can be procured that run on a Linux or Windows OS. These applications are:

- "*Bing*" and "*PC-Pitstop*" provide the ability to measure packet rates and throughput rates over the system.
- RF measurement tool software such as the freeware *Netstumbler* were tried to was used to measure and evaluate RF and 802.11b and g performance with different ranges and field strengths. The application was also configured to allow the monitoring of a service for an extended time period allowing the observation of path stability, traffic statistics and other characteristics.

As part of the project, several of the laptops were initially configured with Linux partitions because the version of Netstumbler 3 required Linux. During the project, however, a new version (4.0) became available which supported Windows, so the Linux OS was not needed. The notebooks are employed in the field measurement work to verify propagation models and service capabilities. Desktop PCs with the D-Link PCI Wi-Fi adapter cards are also being used in conjunction with various antenna combinations for the omnidirectional coverage as well.

Conclusions

We achieved considerable success using the "Netstumbler 4.0" freeware. This new version runs on Windows and supports a much wider variety of off-the-shelf PC Wi-Fi adapters. Minor modifications to connect external antennas were required.

We found that it can track multiple signals simultaneously; see Figure 3-2. It is very fast in updating, and can provide real-time histogram displays. (See Figure 3-3, which shows drop-outs due to inappropriate antenna diversity switching.) It also allows log and statistical information to be kept on individual APs and signals. We found it to be very useful for finding signals for antenna alignment.

Figure 3-1: Netstumbler Screen

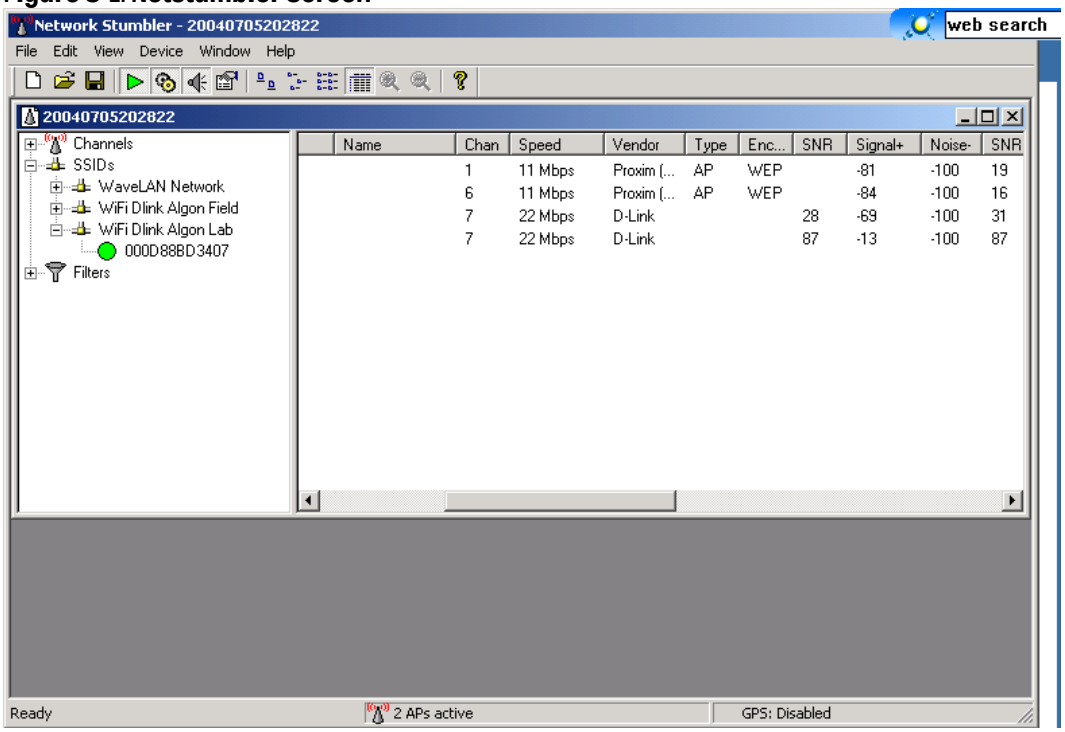


Figure 3-2: Netstumbler Screen Showing Multiple Signals Being Tracked

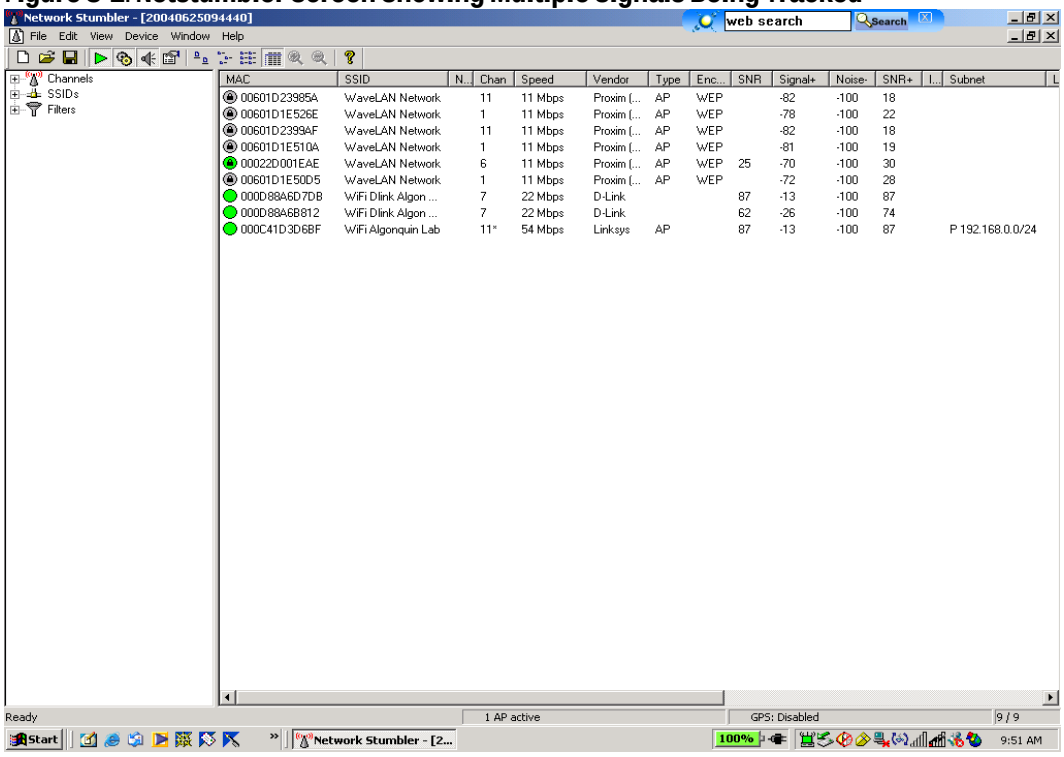


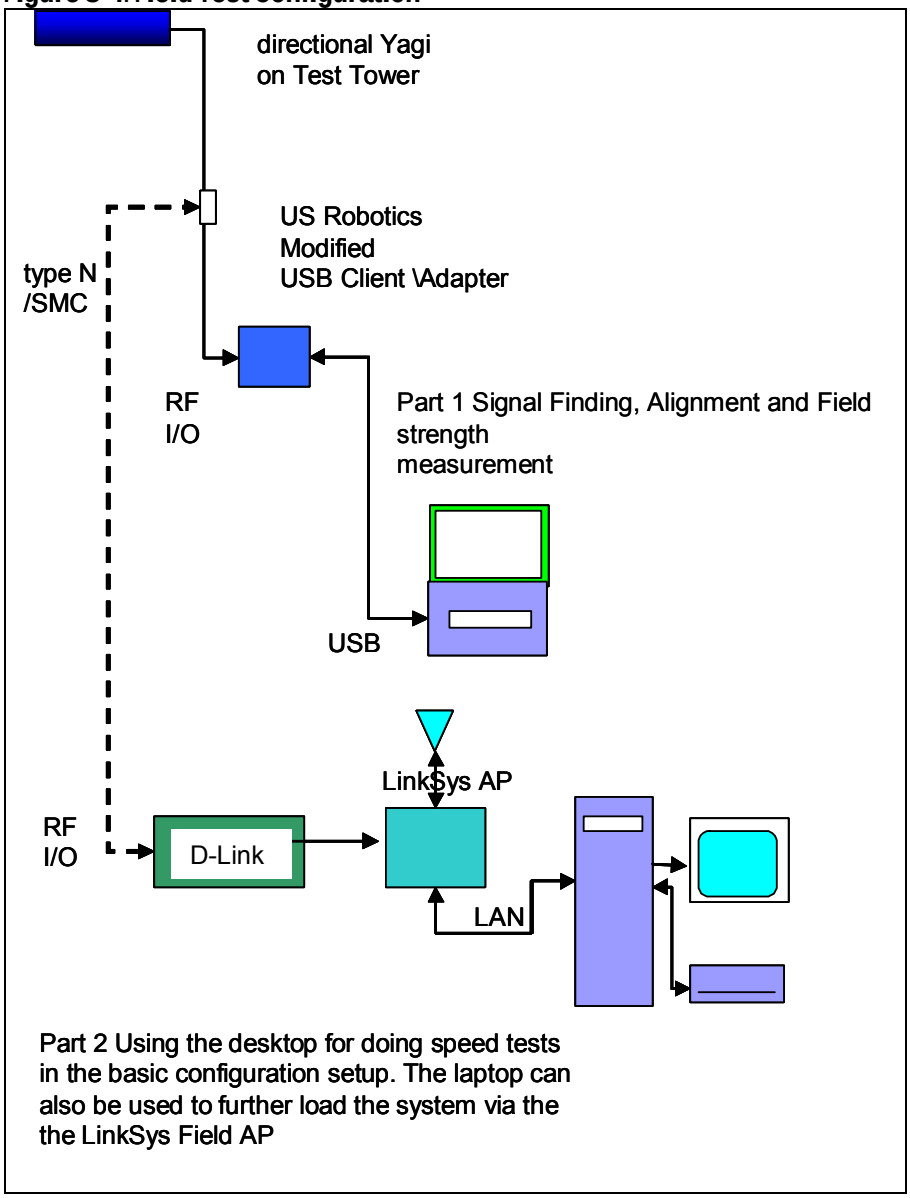
Figure 3-3: RF Real Time Readings off Bridge Link

Field Test Setup

The field test setup used for the study was selected and adapted with the end community user in mind. Fortunately, with the high amount of interest in Wi-Fi, Netstumbler 4.0 has just been released. It is very versatile running on Laptops and desktop computers, and is compatible with a wide range of wireless client adapter cards. Used with adapter cards that allow external antennas to be connected, the combination provide a RF field strength measurement system, site survey tool, radio configuration verifier and link performance logging capability. This has shown to be quite reliable, responsive (takes real-time measurements quickly) and user-friendly.

This setup should enable communities to set up links without the need for expensive RF test equipment in most situations.

Figure 3-4: Field Test Configuration



Measurement Procedures

AP Backhaul Link Test Setup

The relevant AP settings for the backhaul link testing include:

- Low baud rate (2Mb/s)
- Long Preamble
- Beacon on
- RTS longest period
- 4X mode disabled on D-Links.

Field Strength Measurement Routine

- Use the laptop with the USB test adapter
- Hook up the directional antenna to the USB adapter
- Start the reception test using Netstumbler program
- Look for any active APs
- Identify the D-Link SSID from the lab link
- Re-orient the antenna in both bearing, polarization, and tilt for best reception.
- Record the received power levels.

Latency, Link Baud Rate and Throughput Test Routine

- Connect the field D-Link to the antenna
- Log into the field D-Link on the local PC
- Survey for the Lab D-Link
- Establish a connection over the D-Link bridge to the Lab
- Record the D-Link displayed data as well as other the presence of any other APs
- Establish a connection over the D-Link bridge to the lab computer
- Ping and record the latency
- Carry out the Ping test
- Set up speed throughput test with software
- Record the throughput rate
- Try streaming using WinAmp, and record the rates.

Outline of RF Link Analysis (details in later section)

- Carry out Map layout of the proposed RF link.
- Determine Antenna bearings from the location of remote AP
- Carry out a Path analysis
  - Look for Obstructions – Fresnel zone clearance issues
  - Minimum tower Heights – grazing tradeoffs
  - Building in fade margins – signal 10 dB over -87dBm
  - Decide antenna height required from tables
- Determine Antenna gain – higher gain for margin
- Power settings of AP
- RF measurement – “sniffing”

- Antenna steering (both ends) to achieve peak levels
- Incremental adjustment procedures; one end, then other
  - Tilt
  - Azimuth plus and minus
  - Antenna aiming link confirmation

- Bridge establishment once the RF link has been verified.

4. Propagation Field Testing and Predictions

Overview

Field testing commenced in June, with initial tests of the backhaul roof-mounted antenna at Algonquin College (B-block), the tower-mounted 18 dBi directional Yagi antenna, and the 9 dBi omnidirectional antenna. A portable tower was constructed to allow the testing to be easily moved to various locations. A series of tests as listed below are scheduled to be carried out to verify the prediction models and performance of the links at various distances from both a SNR and protocol performance perspective.

The omnidirectional testing also looks at the uniformity of the coverage around the AP antenna. The intent is to confirm the service contours around the antenna in order to evaluate what antenna gains are required by the end users to provide as uniform performance as possible in the coverage area for all users.

The prediction curves based on several propagation models for urban, suburban and rural/open terrain situations are shown later in the report. These curves will be compared against from the field measurements. When validated, these models are to be included in the Cookbook in an easy-to-use format for persons to lay out their coverage area and antenna requirements.

In addition, the situations where amplifiers are required to maintain performance criteria are also to be determined in the testing to be part of the Cookbook guidance information.

Based on the information above, the Cookbook will provide a set of easy-to-use RF link budget tools. These tools will allow the planner to select the right combination of antenna height, antenna gain, and type as well as need for additional transmitter power amplifiers power settings of APs and use of receiver pre-amplifiers.

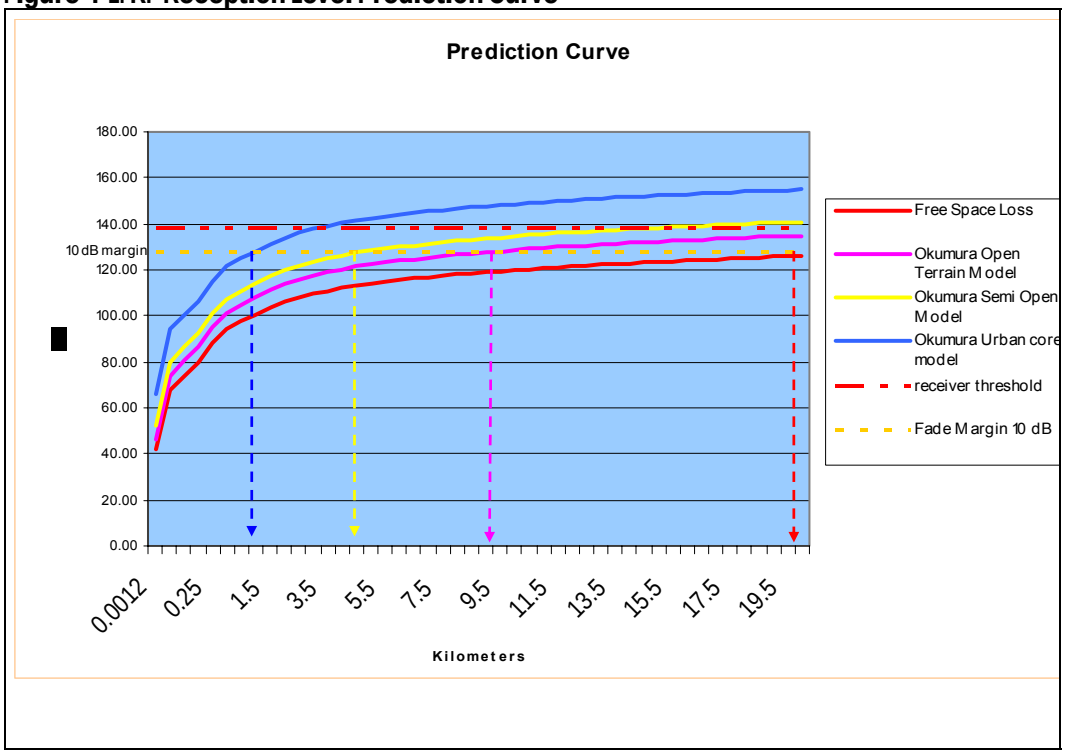
Propagation Characteristics Prediction Work

Summary

In preparation for the field measurement work, several propagation models have been exercised to provide expected values to compare against. For this project, an in-house model plus several existing empirical based popular models are being employed for the basis of comparison. The intent is to select and appropriately format valid RF coverage tools that can be easily used by persons to plan out their system

initially before buying hardware and locating / installing it. The tools should be able to provide a recommended antenna type and tower height, for a given distance from the AP site to the backhaul POP location. The models include empirical based models by Okumura and Hata, as well as standard microwave link equations. The calculated propagation curves are shown in the Figure 4-1 below. The curves are based on a spreadsheet modelling tool that will be documented in cookbook and in the final technical Report.

Figure 4-1: RF Reception Level Prediction Curve



Prediction Tables and Tools

Table 4-1: Prediction Table

At each location an RF field strenght will betaken as well as ping test for latency and Throughput speed	Distance From the AP Km	A dB FSPL	Antenna(1) Type Planar	Antenna(2) Type Yagi	TX power dBm		Distance From the AP Km	Tower Height Required (AGL Above ground level)) Assuming same Base Elevation as	Receive Level (Predicted))	Receive Level (Predicted)	Receive Level (Predicted)	Measured			
										dBm	dBm		Ping Test	Link Baud R	Throughput
							Kilometers	Meters	Open(4M)	Suburban(4M)	Urban(4M)	dBm	Ms	1,2,5,11,54	Kbytes/second
Test 1 Calibration for 3 Heights	0.5	93.98	17dBi	19 dBi	17		0.5	4	-59.25	-65.25	-79.25				
Test 2 (4 meters)	1	100.00					1	4	-65.57	-71.57	-85.57				
Test 3 (4 meters)	2	106.02					2	4	-71.89	-77.89	-91.89				
Test 4 (2 heights 4 & 6)	3	109.56					3	4	-75.59	-81.59	-95.59				
Test 5 (6 Meters)	4	112.05					4	4	-78.21	-84.21					
Test 6 (6 Meters)	5	113.98					5	4	-80.25	-86.25					
Test 7 (6 Meters)	6	115.57					6	4	-81.91	-87.91					
Test 8 (2 heights 6 & 9)	7	116.91					7	4	-83.31						
Test 9 (9 Meters)	8	118.07					8	4	-84.53						
Test 10 (9 Meters)	9	119.09					9	4	-85.61						
Test 11 (9 Meters)	10	120.00					10			Required Measurements					
Test 12 (9 Meters)	11	120.83					11								
Test 13 (9 Meters)	12	121.59					12			Marginal Link		1 Mb?s - Very little Fade margin < 5dB			
Further out will be attempted only if results warrant -	13	122.28					13			< 3dB Fade Margin - Poor Availability					
	14	122.93					14			Link Below Radio Receiver Margin. Not Viable					
	15	123.53					15								
	16	124.09					16								
	17	124.61					17								
	18	125.11					18								
	19	125.58					19								
	20	126.02					20								

In Table 4-1 above, the expected RF receive level predictions are shown for various terrain characteristics and antenna heights. This table will be further tailored for the Cookbook to allow the user to predict the reach for a given antenna gain, power available from the AP into the antenna, tower height, and type of terrain they are in. This table will include factors for climate to take account of rain fades and other factors.

The models used are based on empirical propagation models for Okumura and Hata. Field testing has shown the models to be reasonable for predicting suburban and rural propagation losses for paths that do not have radio line of sight clearance (<.6F1, where F1 represents the first Fresnel zone).

The user can quickly determine from the tables if the intended path will be viable or not. Also, they can determine what antenna height, power, and gain are needed to establish the link and what the signal level that they should be expecting as well as the fade margin available. This will be done as a set of tables as well as an interactive spreadsheet tool.

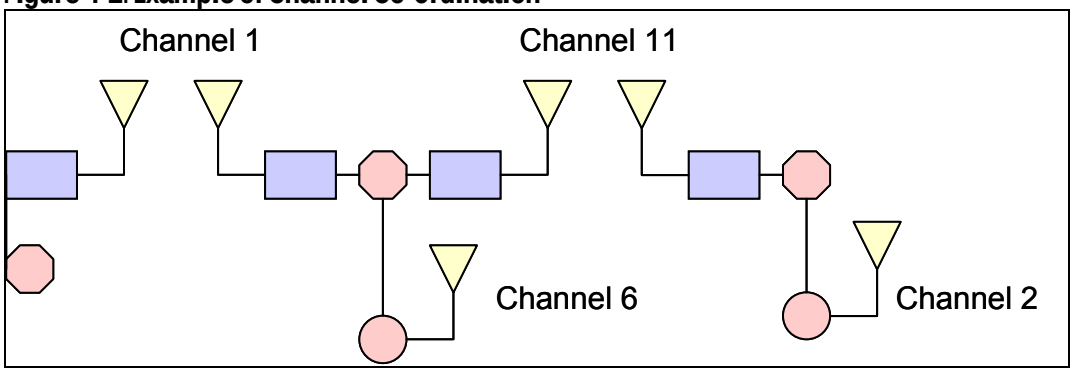
Radio and Antenna Configuration

Channel Setting

The 802.11b 2.4 GHz band has up to 14 overlapping channels with 3 channels (1, 6, and 11) that can be considered as having guard bandwidth spacing between each other. For remote applications where APs and backhaul elements will be using the same 2.45 GHz band, channel selection will be done to provide as much isolation as possible between APs or wireless bridges that are within 100 – 200 metres of each other. For example, channel 1 would be used for the backhaul radio link with chan-

nel 11 used for the AP. If another backhaul is being used Channel 6 would be used. See Figure 4-2.

Figure 4-2: Example of Channel Co-Ordination



RF Field Survey

As part of setting up a system and determining locations for the AP, backhaul links, and repeaters, an RF survey should be done to discover any potential sources of interference that will result in degraded S/I. These sources can be from existing microwave systems or other APs that operate in the same 2.4 to 2.5 GHz band. In most rural or remote locations, there will likely not be any sources of problems.

Once a WLAN has been put in, any expansion such as additional APs or backhaul systems must be deployed so they are not in direct interference with existing systems. This will require power adjustment and specific frequency selection.

S/I in Multiple Radio Sites

In rare occasions, there may be a number of private APs and other devices in the 2.4 to 2.5 GHz band operating in the intended service area. Depending on the emitted power and proximity to the AP or wireless bridge antennas, unacceptable levels of Interference (S/I – Signal to Interference ratio) can cause slow throughput or failure of the data connection due to excessive error rates.

Channel reassignment is one tactic to reduce S/I. However, this may not be possible in some locations. The next tactic is to use more directional antennas to provide a higher degree of isolation from the interfering units. The last resort is to see if offending RF sources can be moved to different frequencies as well as locations.

Antenna Diversity

As was discussed earlier for remote extended links, antenna diversity is not utilized and must be disabled on the APs. Diversity using dual external antennas can be considered if fading is a problem on a long link. Here the AP would be connected to two high-gain antennas, with one antenna below the other on a mast. This makes the link much more robust against seasonal fades.

Power Settings

The default power settings of the LinkSys and D-Link APs were found to be at minimum or medium settings (33 mW). For the target applications of the basic configuration, the units were set to run at +52 to +75 mW. The D-Link maximum power is 17 dBm or 52 mW. The maximum AP power available from similar AP equipment is

100 mw or +20 dBm. The maximum EIRP (Effective Isotropic Radiated Power) allowed in North America is +30 dBm or 1 Watt. With + 18 dBm antenna gain, for example, this limit will not be exceeded:

```
+18 dB + 17 dBm – 7 dB losses = 28 dBm
(D-Link Bridges)

+9 dB + 18 dBm – 4 dB losses = 23 dBm (LinkSys)
```

Path Profiles

In planning the link, a path profile diagram helps to visualize where significant obstacles are and what clearance is needed to overcome their effects. The distance to the obstacle can be estimated from either tower or antenna location. From this, the clearance needed to overcome the obstacle can then be determined.

In Figure 4-3 below, a simplified profile of a point-to-point link is shown. In an ideal situation, a clear line of sight is possible with adequate clearance over structures or natural features between the antennas being.6 F1. In order to achieve acceptable radio line of site clearance, any obstacle along the path must be at least 0.6F1 meters below the optical line of site bore line between the antennas. If this clearance is not achieved, the effect is multi-path reflections of the radio propagating field stemming from the object. The direct and multi-path waves will interfere with each other at the receive antenna, which can cause very significant loss in level due to the fields cancelling each other out. Constructive addition of the fields can also occur. Since there is a relative delay between the direct and reflected path, data transmission performance can be degraded significantly.

In our testing, path clearances were often marginal with grazing over obstacles occurring (<<F1 clearance). This is more the typical case in suburban and forested areas where there are numerous obstacles along the radio path. The propagation models used for predicting the propagation losses in our test are based from Okumura's empirical based results for urban, suburban, and open areas. The prediction formulas combine the free space loss with derived penalty factors due to insufficient clearance, which vary by type of area and the heights of the antennas and frequency of operation.

Figure 4-3: Example Clearance Profile

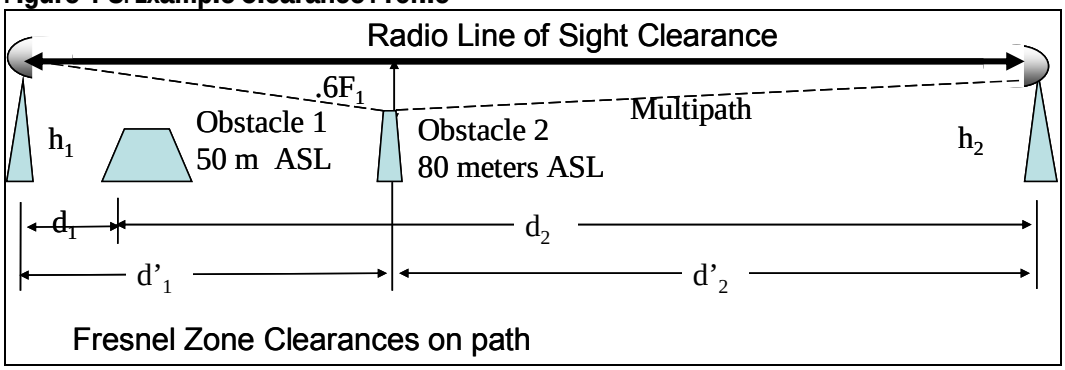


Table 4-2: Typical Path Clearance Calculations for F1 Fresnel Zone

Freq. (GHz)	d1 (km)	d2 (km)	D (path link) (km)	F1 Radius (m)	0.6 F1 (m)
2.4	1	9	10	10.59	6.36
2.4	2	8	10	14.13	8.48

Freq. (GHz)	d1 (km)	d2 (km)	D (path link) (km)	F1 Radius (m)	0.6 F1 (m)
2.4	3	7	10	16.18	9.71
2.4	4	6	10	17.30	10.38
2.4	5	5	10	17.66	10.59
2.4	6	4	10	17.30	10.38
2.4	7	3	10	16.18	9.71
2.4	8	2	10	14.13	8.48
2.4	9	1	10	10.59	6.36

Topographic Maps

In considering a radio path in any given area of the region to be covered, obstacles and terrain characteristics must be considered along the intended radio link's path. Examples are hills, buildings, stands of trees, and water. The elevation of the ground that the antenna towers will be sitting on must also be taken into account. Large obstacles can be terrain features such as ridges or thick stands of trees that lie in the foreground of the antenna pattern.

Tower Height – Terrain Advantage

For best signal level, when determining the height of the tower required to clear over the obstacle, the clearance must exceed optical clearance by at least several metres depending on how close the obstacle is. In the Cookbook, a table will be provided to allow the user to determine a good estimate of the tower height needed.

To accomplish sufficient clearance over known obstacles or to extend reach of the backhaul link, the user can take advantage of the combined terrain ASL (Above Sea Level) and antenna height. If the land between the sights is lower in elevation, clearance can be achieved with lower antenna heights, thus reducing costs. Also, lesser gain antennas can be considered if radio signal level margins are more than required.

Again, this factor will be part of tables and prediction tools that are to be part of the Cookbook.

Antenna Alignment

The establishment of point-to-point or point-to-multipoint links requires critical attention to antenna alignment once the tower height has been determined.

Setting up directional antennas to establish a point-to-point or point-to-multipoint radio links must consider several factors before deployment. These factors are height, polarization, azimuth, and bearing. The best path link performance will be realized when these parameters are adjusted to best signal received.

The antenna bore or centreline is where the maximum gain of the antenna will be realized must be established between the antennas. In order to achieve this alignment with the least difficulty, a compass bearing between the antennas must be established with the antennas adjusted to that bearing. To fine tune the link, the actual AP can be used or a substitute 2.4 GHz transmitter can be used. At the receiving end an AP in client mode or a test receiver can be employed. Using the received RF carrier level as a guide, the receiving antenna is first incrementally adjusted in both azimuth and bearing to maximize the received signal level. Once is done, the transmit antenna at the fare end is finely adjusted to peak the signal level,

Note: It is assumed that for this test that the line of sight and clearance aspects have been accounted for with the appropriate antenna elevation employed.

Bearing

A directional antenna needs to be aligned along the same boreline of the far end antenna in order to realize the maximum gain on the radio link afforded by design of the antenna over a reference dipole antenna. Usually, directional antennas have beamwidths of 15 to 50 degrees.

The bearing adjustment of the antenna requires an initial coarse adjustment and then fine tuning of the pointing direction to maximise the received level at the transceiver of the antenna and the antenna's site.

The bearing can only be adjusted once the tower or other structures are put in place at the height required to get RLOS (radio line of site) clearance.

For backhaul links where both antennas are critically aligned, it is important that the supporting structures are stable and have wind resistant antenna mountings.

Polarization

The antenna polarization (horizontal or vertical) must be adjusted to maximize received levels. The initial adjusted position is what is used on the far end antenna with both antennas adjusted in the same plane of propagation. In deploying the antenna, the same polarization settings must be used.

Once the antenna has been raised, minor adjustments to the polarization setting were done to achieve better signal receive levels. In our field measurements, it was found that due to path obstacles (grazing) a polarization shift occurred which necessitated some readjustment.

The antenna used for the test work displayed very good polarization performance. Using horizontal polarization for one antenna and vertical for the other provides up to 40dB isolation between the antennas.

Tilt

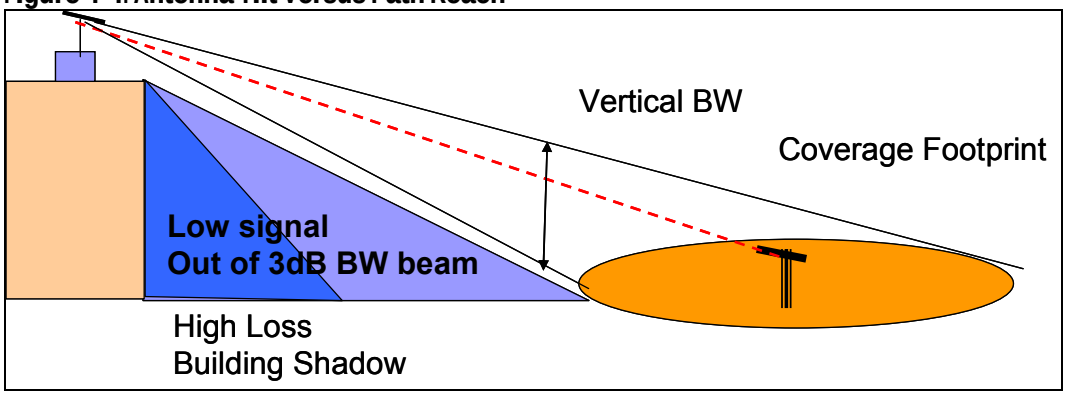
On radio paths where one tower will be higher than the far end tower, the directional antennas must be tilted slightly to realize the maximum gain advantage provided by an antenna along its bore line. In point-to-multipoint distributions, high / low antenna elevation combinations are common, since the central antenna structure will use a high tower to clear obstacles to users furthest out from the central sight. The required tilt of the antennas is quite small – on the order of 0.5 to 3 degrees, depending on distance between the antennas and the relative tower height difference.

In testing both the backhaul links and AP coverage, tilt was adjusted to maximized received levels. Typically, up to 3 dB improvement was seen using with 2 degree tilt up for the low elevated antenna (4 meters) 1.5 Km out from the high antenna site (30 meters). As the range increased between the antennas, the tilt adjustment tended towards 0 degrees (antenna parallel to earth plane as expected).

In the Cookbook, antenna tilt will be included as part of the setting up of both point-to-point backhauls and point to multi-point AP-client links. In the typical application scenario envisaged, the AP distribution tower will be at least 12-14 meters in height

with the client antennas being elevated to 4 to 5 meters depending on the surrounding structures. In Figure 4-4 an illustration of tilt alignment is shown.

Figure 4-4: Antenna Tilt Versus Path Reach



Antenna Isolation

On towers using multiple antennas, care must be taken to ensure that the antennas do not introduce strong signals into co-mounted antennas. Isolation is achieved by orientating the antennas with respect to each other. In certain cases, metal screening is also used. The reason for this isolation is to ensure that the receiver has minimal S/I problems.

Good rules of thumb are:

- Directional antennas should all use horizontal polarization if an omnidirectional vertically-oriented antenna is used
- Omnidirectional antennas should be mounted above and behind directional antennas, with a vertical position. The spacing should be a least 0.5 metres.
- With back-to-back directional antennas, a wire screen should be used between the repeaters antennas back to prevent excessive Interference from antenna back lobes.

RF Setup Procedures

The procedures for setting up either backhaul or AP–client links are related. However, there are some differences that must be taken into account to properly establish the links for best performance. In the following, an overview of the procedures are given below.

Backhaul Links

The following basic procedures are required to get the wireless bridge set up from a POP out to the AP site for distribution. All testing and antenna alignment should be done in fair weather conditions. Excessive rain and any other precipitation (fog, heavy mist) in the coverage must not be present during the tests.

1) The AP unit is set up in AP Infrastructure mode with its beacon interval set at 100ms to ensure that the signal is seen by the receiver quickly when it is in scanning mode.

2) The AP units used must have the capability to exclusively utilize an external antenna connected via cable to the radio This will require the firmware settings to be accessed and changed or new firmware to allow for antenna non-diversity operation.

3) Power settings of the APs must be set at maximum level available. Typically this is +17 dBm or 52 mw.

4) Do a site survey for any other APs that may be operating nearby and select a channels that is as far as possible from the APs seen.

5) Determine the distance between the two antenna sites. Knowing the tower heights and type of terrain, look up the expected path loss from the supplied tables.

6) Do a path analysis ensure there are no major obstructions blocking the antenna LOS to the far end. If there is, consider moving the tower or raising the antenna such that the obstacle can be adequately cleared (.6F1 if possible) Note: With more distance objects (200M+) where the line of sight path is just grazing over the obstacle, the far end AP's signal may be still usable but significantly lower then what a clear path will deliver. This can be acceptable as long as the received level is +10 dB above -87 dBm. Other wise, the antenna must be raised to have the radio path raised until a higher level is achieved.

7) Initial Antenna bearing, tilt and polarization alignment. The antenna should be aligned so that is on the bore line as much as possible of the far end antenna by using the reciprocal bearing value (degrees) of the far end antenna. For example, given an antenna with 260 degrees bearing, the reciprocal is 260–180 = 80 degrees.

   - Initial tilt set at 0 degrees
   - Polarization set to same as the far end antenna (horizontal or vertical)

8) Once the coarse alignment has been done, the RF level measurement can be done. Connect the antenna to the RF measurement computer (laptop with a client card) and start your measurement software such as Netstumbler. The software will scan the 2.4 GHz 802.11b/g b and show all APs being received. The Netstumbler GUI will provide each APs SSID and signal level in dBm at the input to the adapter card from the site's antenna.

9) Fine Antenna Bearing Alignment. If the desired AP SSID is seen (the far end AP), note the receive level and other data being shown such as SNR and throughput rate. Turn the antenna slowly right (about 5 degrees) of the coarse alignment bearing used. Note if the signal is increasing or decreasing and see if the level peaks. If no peak is found, return to the original bearing and now go to the left. Set the antenna bearing for the best level.

10) Adjust antenna tilt alignment. Adjust the antenna tilt up 1-2 degrees then down 1-2 degrees. Note any peaks in signal level. Again set the antenna for maximum level.

11) Polarization should be changed +/- a few degrees to see if there is a signal peak observed. Due to tower slant or other factors in the radio path, RF polarization can be shifted and thus some peaking can be achieved in the signal level.

12) For a backhaul link, have someone at the far end antenna carry out a fine tuning antenna alignment as well. This ensures that the antennas are optimum in their alignment.

13) Once the AP – Client link has been established, the local and far end APs can now be switched into wireless bridge mode. This requires that each AP be put into wireless bridge mode to establish the transparent layer 2 link between the Internet POP and the remotely located AP for distribution. This is done as follows:

    a. Set both APs to wireless bridge mode.

    b. Enter the MAC # of the far end AP into the configuration information of the local AP. Similarly, enter the MAC# of the local AP in the far end AP configuration window.

    c. The two APs should be passing layer 2 traffic or at least administrative messaging.

    d. Once the bridge is working, connect the bridge AP to the Omni-directional AP to provide Internet coverage for remote users.

14) Trouble shooting: If no or an unexpectedly weak signal is being received at the location:

    a. Ensure all connectors and cables are properly placed and that the test coax cable is rated for 2.4 GHz and has low loss.

    b. Ensure all equipment is working properly. Verify with closer-in measurements to see if the RF test system as well as the APs are working properly.

    c. Try rotating the antenna by 90 degrees. Polarization setting can be in error or shifted radically by path grazing. If such a shift has occurred, raise the antenna 3 meters or more to see if the polarization goes back to the proper orientation.

    d. Given that the desired signal is still not seen at the location:

        i. This indicates possible configuration problems with the test APs

        ii. Insufficient antenna elevation over obstacles for path clearances.

        iii. The site location is too far from the transmitter. An intermediate repeater may be required. Errors in distance estimations may also have occurred.

        iv. Excessive interference from a non-Wi-Fi source such as amateur radio, industrial (microwave used), or other non-Wi-Fi radio communication systems in bands adjacent or within the 2.4-2.5 GHz band.

Omnidirectional Coverage

Aligning clients to an omni-directional AP is a less convoluted procedure than establishing a backhaul link. Here, a client antenna is adjusted in height and then simply aimed at the central AP and adjusted for peak signal. The height determination again is looked up on the supplied tables, which consider the central AP antenna

height, obstacles on path, and distance from the AP. The same procedures are used as in the backhaul except for the need to align the main AP antenna. The measurements can be done with the AP in operation without any interference.

Once the client's antenna has been mounted and aligned for best signal at the prescribed elevation at their location, the client's adapter card is simply connected to the antenna and service started.

The approach used to determine the nominal client radio links to the central AP is described in the section below.

AP Service Contours

In Figure 4-5 below, a simplified contour figure is showing an AP that is centrally located to cover a local community with Wi-Fi service. In this figure, the expected path losses are shown with the distance back to the antenna tower. The intent of the RF contours is to show the expected loss in signal strength with distance for a given antenna height elevations at either end of the link. Again, tables derived from the prediction tools will give what requirements are needed to achieve the desired receive level.

The approach used for the AP coverage is to try within the limits of the system provide everyone with similar RF signal Levels any where in the prime service area. Doing it this way will result in the more uniform service quality,

In Figure 4-5, the antenna gain and elevation requirements for the end user are given along with the expected receive levels.

Figure 4-5: Calculated Service Contours

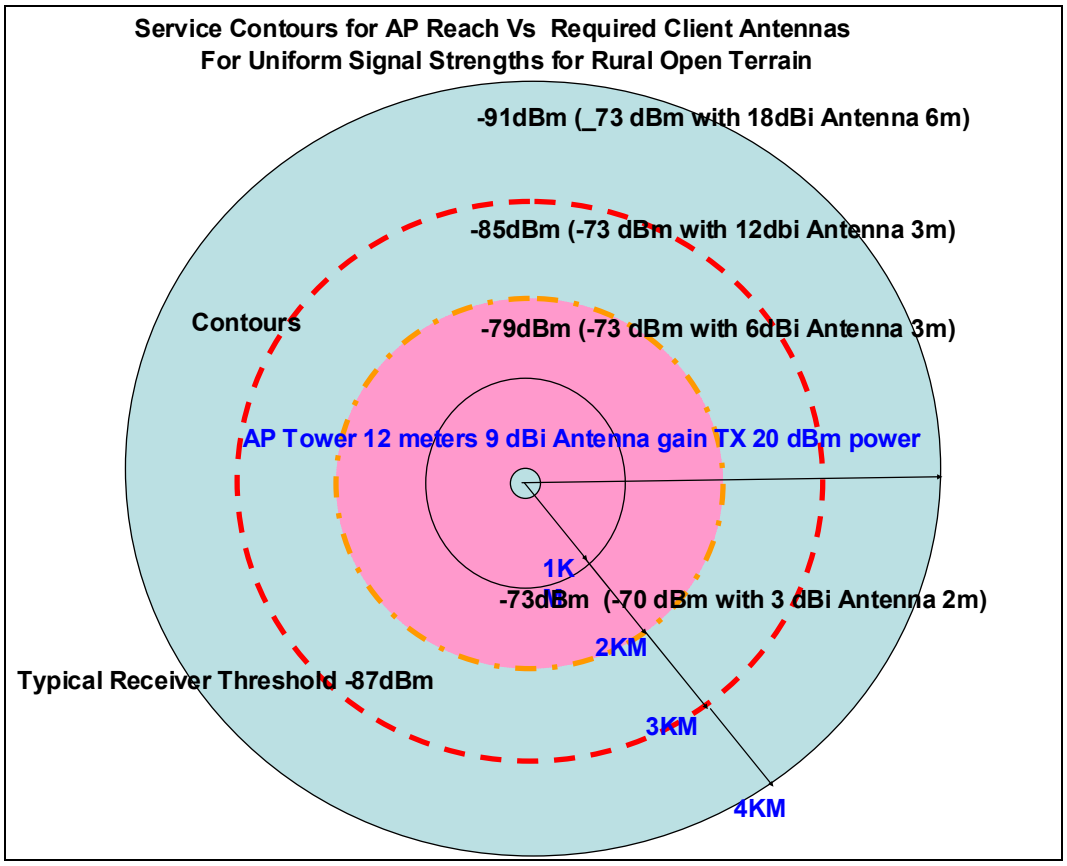


Table 4-3: Coverage versus Radius

Coverage Radius Zone Radius (Km)	Area (Sq-Km)	Low Rise Dwellings in Coverage Area (50 units per sq Km)	Field Strength (dBm)	User Antenna Gain Range For Uniform Receive Levels (dB)
1	3.14	157		1 - 3
2	12.57	628		6
3	28.27	1412		12
4	50.26	2513		18

Propagation Testing Results

Close-In AP/User Coverage Tests

Range was tested with a 3 metre mounted 9 dB Omni and a laptop 2 dB antenna. Reliable links were established up to 400 metres. We achieved 11 Mb/s with 7 dB fade margin at 400 metres (-79 dBm) (-87 dBm crash threshold). Beyond 400 metres, there was intermittent link failure. This was done the campus area with a high amount of foreground reflections causing multipath signal cancellation.

Initial high-gain tests with a 12 dBi 2 metre elevated client antenna 1 kilometre away provided a signal level of -62 dBm with significant obstructions in the antenna field of view. More testing for longer reach has been underway in more open terrain representative of the intended rural-remote locations.

Near Field Measurements

For link backhaul setup, the AP mode is selected to “find” the signal. Once the link is RF established, the D-Links are put into Wireless Bridge mode. See Figure 2-5.

A 0.5 km 2.4 GHz backhaul link consisting of the 17 dBi planar antenna mounted on the B block building (AGL of 22 Metres) and a mast-mounted 18 dBi Yagi portable antenna with an AGL of 4 metres were used for benchmarking tests. The signal levels achieved were consistent with the model. We verified the losses calculated (5.5 dB) for the lengths of AMR 400 coaxial cable (25 m)and connectors and power settings of the D-Link APs. The D-Links provided a reliable 11Mb/s rate in 802.11b mode as expected. 802.11g mode was also tried. In g mode, 54 Mb/s was achieved but was found to be somewhat unstable, with the link defaulting down to b node intermittently (11Mb/s). Factors in this behaviour include interference from other APs in the area and the distance the protocol is working over.

Linksys Results as an Omnidirectional AP

The first test using the LinkSys AP with the omnidirectional antenna was unexpectedly very poor and unstable. Measurements were quite varied at the same distances from the portable antenna. The LinkSys wireless router was used in this test since it provides a bridging function needed in the basic system configuration. This model has diversity antennas which can be programmed to operate using both or single antennas. The standard firmware that is supplied by LinkSys with the unit allows changes to the antenna diversity settings. But, we found out that the unit does not allow the complete disabling of the function. As a result, the LinkSys AP was still switching the transmitter section of the unit between the two antenna connec-

tions on the package. The 9 dBi antenna was connected to the left port. This switching resulted in the unstable readings.

To remedy the problem, new firmware supplied by a 3rd party LinkSys affiliate was located and downloaded into the unit. This allowed the total defeat of the antenna diversity settings and enabled the unit to operate only through the left antenna connection and therefore the mast mounted omnidirectional antenna.

This problem will likely be encountered with other diversity employing units such as US-Robotics and SMC among other combination router-Hub APs on the market. These will be verified and listed in the Cookbook with cautions as how they can be utilized. Appropriate firmware sources will also be provided where applicable, with instructions of how to upgrade the units for single antenna operation.

Modified LinkSys Omni-directional Successful Results

The test results with the modified LinkSys were quite stable and provided signal levels that were on average tracking the predicted values shown in the section above. The presence of large buildings and a lot of near field clutter (cars, light poles, etc.) caused multipath problems and thus some reading anomalies.

Several range tests were tried using a laptop D-Link adapter card and Apple Notebook computer equipped with an ORINCO adapter unit and internal antenna. Both provided very similar results for a range that exceeded 550 metres from the AP tower. At 550 metres, the link speed varied between 5 and 2 Mb/s depending on the orientation of the laptop. This is expected since the laptop antenna has some directivity even though it is very low in gain (1 dB typically).

Test using elevated (2-3 meter high gain antennas) provided excellent results with the Omni directional antennas set at 12 meters in suburban terrain. Very stable signal levels were achieved providing 11 - 5 Mb/s over 2.5 kilometres. The client antenna utilized was a 14dBi directional Yagi elevated 2m above the ground.

These tests also are supporting the viability of using 802.11b both for backhaul and AP operation in a rural context. The AP and backhaul antennas were arranged to minimize cross-coupling and the channels were set at opposite ends of the 802.11b/g allocated spectrum. This ensured insignificant S/I (> 40 dB isolation) problems between the radio links. However this does not preclude using 802.11a or other radio standards such as 802.16 when it is more commercially viable.

Backhaul Link Testing and Results

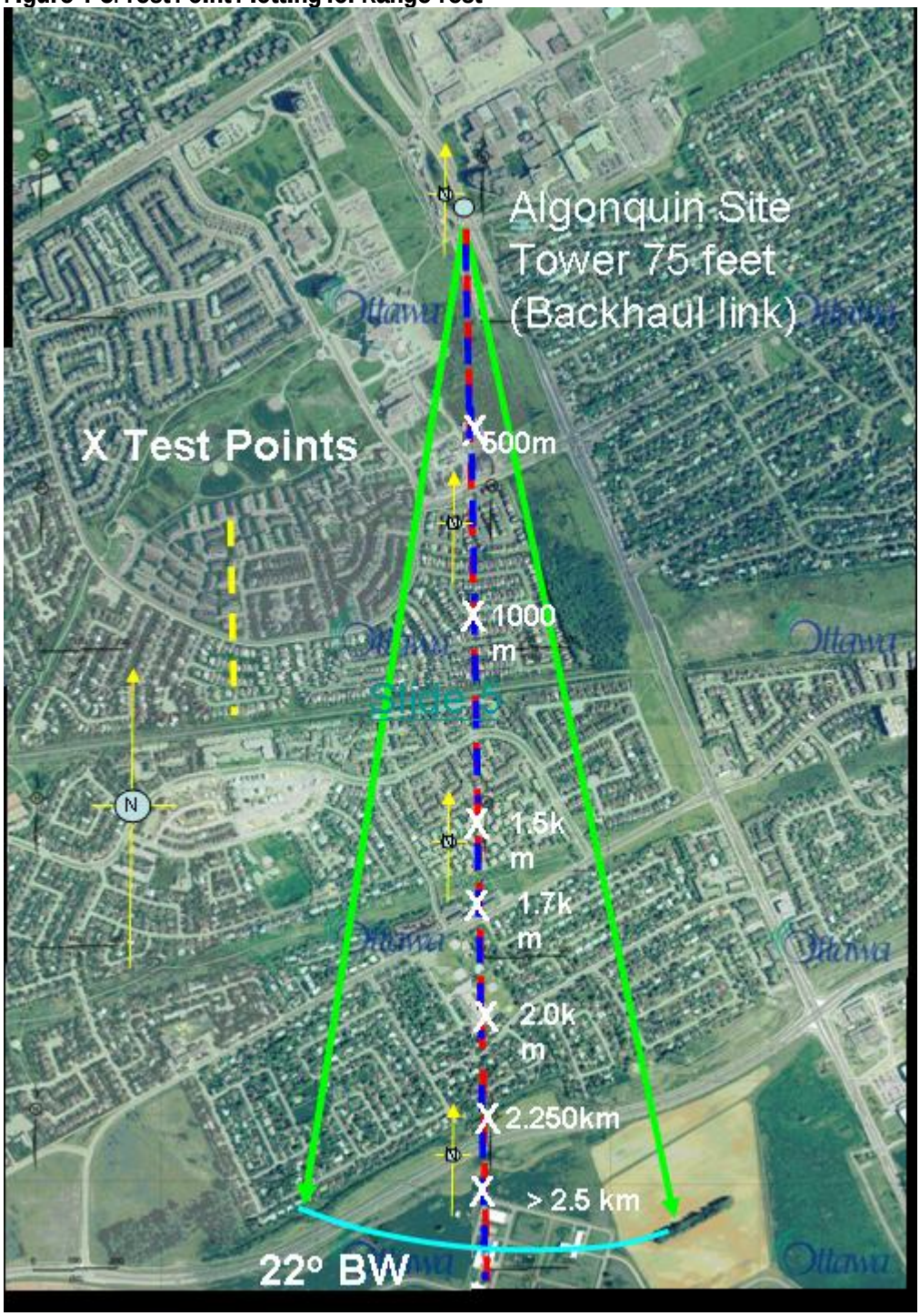
In Figure 4-6 below, the directional antenna's coverage pattern is shown for the primary lobe of the backhaul primary antenna. The locations for taking readings were specified along the centre axis of the antenna pattern to ensure that maximum gain advantages are realized. The intent of the testing is show that a viable backhaul link can be established to support the remote AP deployment.

At each location, the test tower was raised in order to gain a height advantage for LOS alignment of the two directional antennas. In order to ensure maximum gain, the receiver antenna is axially aligned and tilted slightly upward.

The receive antenna is first connected to a small client receiver to "find" the desired signal among other stations that may be received. Identification of the AP is straightforward using a unique SSID (identifier).

Once the proper signal has been acquired, the received signal performance measurements are carried out to verify the stability of the link as well as the impact of in-band interference on net throughput by causing excessive packet errors.

Figure 4-6: Test Point Plotting for Range Test



The measurements taken along the boreline of the antenna generally followed the suburban prediction models used for paths with marginal clearance. The impact of near objects such as heavily foliated trees was very significant (>8dB), as expected

with 2.5 GHz. When the antenna was pulled back by 100-200 metres so that the path was grazing the trees, the values measured were within 3-4 dB of the predicted value. (Again the models we using add penalty losses for antenna heights that are less then that required to have radio line of sight clearance over obstacles (RLOS) where the Fresnel zone clearance must be >.6F1.)

The greatest distance confirmed to date has been at 8 Km with a 28 dBi antenna parabolic antenna on a 3 metre masts. This was done to allow us to simply “sniff” out the signal using the measurement techniques described earlier. This proved to be quite successful with a marginal but consistent signal being received at around -80 dBm, which is consistent with the prediction model values.

Raising the antenna to 12 metres, which is our test tower maximum, will provide the required margin for service. In this location, more than 10 dB can be gained resulting in a > -70 dBm signal, which is acceptable for the backhaul path. A higher fade margin is desirable (>10 dB) especially in areas with heavy rains.

Increasing antenna height up to where RLOS is achieved results in the best case propagation path, and should be done for best performance. However, depending on the net distance from the far-end radio, sufficient signal level margins for good performance can be achieved without having the antenna placed at the ideal RLOS height which incurs higher costs. In summary, grazing paths are usable when adequate fade margin exists.

5. Basic System Performance Results

Overview

Once improper antenna diversity settings and shielding were dealt with, the performance was comparable to that of a LAN. Throughput on the D-Link was up to 22Mb/s Max. Typically at 2.0 Km, we achieved up to 11.0 Mb/s.

The LinkSys g-mode port speeds were up to 54 Mb/s. However, this was achieved at short range only, since the protocol is quite limited in range and is unsuitable for building a Wi-Fi WAN.

The highest impact on throughput was RF level. When the signal levels fall lower than -83 dBm, the rate falls to < 5 Mb/s to 1 Mb/s at crash.

Latency of much less than 1 ms was not an issue. Latency was tested with Ping.

The Basic Configuration was then loaded with multiple users and multiple media streams, using the “Bing” Bandwidth tester. Rates of 4.5 to 6 Mb/s were typical in this type of setup.

Lab Test Results

The first stage of hardware testing was to set up the Basic Configuration as described, and configure the APs in their respective roles of the overall architecture. The system was tested in the lab both for the Interim report on performance characterization of Basic Configuration.

The Basic Configuration was initially set up in the lab as well as initially field tested to ascertain what if any impairment would be encountered with the chaining of multiple APs. The laboratory set-up negated any latency introduced by the radio transmission delays and therefore provided a good baseline to appraise the throughput achieved through the bridges and the cascaded 802.11b MACs.

The Basic Configuration for the most part used the set-up routines that accompanied the hardware. The D-Link and LinkSys updates of the software that is used to access the AP from a user’s AP were required to enable access to the latest features.

Throughput Numbers

The following are excerpts from the throughput test using various types of network speed appraisal software, Ping tests, and File transfer timing Test. These tests were carried out to provide a baseline performance level under “ideal” conditions. Similar tests will be done over a field-deployed system during the RF testing runs.

The results will vary to some degree due to the effect of the Internet loading at the time of the test. Other PC to PC LAN test software is being tried to compensate.

In general, the rates seen over the wireless bridge and the AP together (no transmission distances involved) were the same as a wired 100BaseT LAN. Within the lab, the APs and backhaul operated in 802.11g mode providing 54 Mb/s on the RF links. The cascading of the 802.11 MACs and LinkSys bridge and routers did not offer any observable latency or throughput problems. With this benchmark, the impact of the longer transmission distances both from a round trip messaging and scheduling timing of the 802.11b MACs can be ascertained as well as the reduced throughput rates that are used by the protocol as the signal strength weakens. Packet rates are being logged in these tests to see if at a given throughput rate that the data BER (bit error rate) is not excessive resulting in a high amount of packet resends by the applications being used. Multimedia streaming has been used to benchmark the packet rates and have shown to be a useful indicator.

Back Haul Bandwidth test in Laboratory over Basic System Architecture

- Tested with PCpitstop.com download speed test
- Network configuration, internet→ LinkSys1→Dlink1→Dlink2→LinkSys2→ wireless connection to 3 PC's / 1 computer off LinkSys2 hub.
- In DOS window "ping <ip> –T –L 65500" command used on three computers to flood back haul link between Dlink1 and Dlink2 wireless bridge.

PCpitStop used on one of PC's through wireless connection. The results are given below in Table 5-1 and Table 5-2.

Table 5-1: Test 1 – Ping Turned Off, Benchmark Test

Description	Your Results
Bandwidth Down	1765 Kb/s
Bandwidth Up	1001 Kb/s
Average Ping	0 ms
Ping Loss	100%
TCP Receive Window	(default)
External IP Address	205.211.32.32
Internal IP Address	192.168.0.204
Browser	MSIE 6.0;.NET CLR 1.1.4322
IE current cache	2 MB
IE max cache	1 MB

Table 5-2: Test 2 – Ping Used to Flood Network

Description	Your Results
Bandwidth Down	1196 Kb/s
Bandwidth Up	435 Kb/s
Average Ping	0 ms
Ping Loss	100%
TCP Receive Window	(default)
External IP Address	205.211.32.32

Description	Your Results
Internal IP Address	192.168.0.204
Browser	MSIE 6.0;.NET CLR 1.1.4322
IE current cache	2 MB
IE max cache	1 MB

Note: Guide to flooding network

In windows

```
Select Start
Select Run
Type cmd or command
Use ping command:
Then Ping <ipaddress> –t –L 65500
Where –t = Ping host till stop.  Use ctrl+C to stop
       -L = Send packet size 0 to 65500
 e.g., ping 192.168.0.2 –t –L 65500
```

Field measurements using www.PCPitstop.com:

Network configuration, internet→ LinkSys1 (gateway) →Dlink1→500m RF link →Dlink2→LinkSys2 (Lan AP)→ wireless PC and PC2

PC2 in field measured download rates:

481 kb/s,

589 kb/s,

234 kb/s,

2124 kb/s,

518 kb/s,

598 kb/s

wireless PC in field measured download rates: 2392 kb/s, 1402 kb/s, 481 kb/s, 2205 kb/s

Audio and Video Streaming and VoIP

Wireless LANs are somewhat capable of handling streaming applications such as real-time MP3 audio as well as up to MPEG2 video, when there are limited numbers of users. Real-time conferencing applications such as Netmeeting perform without any noticeable latency impairment from going over the wireless link, given that there is no significant contention.

Streaming video (up to 1.0 Mb/s) was tried over the Basic configuration as well as through a repeater. In the test, using several software-based network testing tools we measured the throughput and also created “busy” traffic to see when the audio and or video link would be impacted by the bandwidth sharing over a 11Mb/s wire-

less link. In carrying this test out, a 500 Kb/s video stream signal was streamed off the internet. This did not show signs of delay or data loss until background traffic exceeded over 2 Mb/s generated by a Windows-based Ethernet test tool. At this point, minor delay impairments were seen with the video stopping and re-buffering.

In real applications with a number of users, having a number of simultaneous wide-band streams will result in considerable reduction in performance to other users. If a number of the users are present, lower throughput rates will be due to lower signal levels or distance from the AP. The slower rates (1.0 to 5.5 Mb/s) will also slow the 802.11 MAC scheduling, resulting in streaming delays to the users that can hit higher channel bit rates.

Netmeeting and Yahoo network conferencing applications were tried over the basic configuration. These utilize a form of VoIP and were found to work as well as they did on a wired LAN network over the same internet gateway. These services ran in a simplex manner using a “Push to Talk” operation. The audio processing (codecs and filters) was done in the application software.

Real-time VoIP such as used to replace typical POTS (Plain Old Telephone Service) was not attempted. There are VoIP sellers on the Web that allow connection to any telephone. These application are “Push to Talk” and thus similar to conferencing. Applications such as H323 can work over WLANs; however, latency will be a prominent concern due to contention with other user traffic. This inability to control the QoS for the VoIP call can cause dropouts in the service which in turn does not meet the Grade of Service requirements for commercial telephony. This can be a problem on wired LANs as well. However, as pointed out above, the WLAN environment is different due to the scheduling aspects of the 802.11 MAC with users at different distances from the AP.

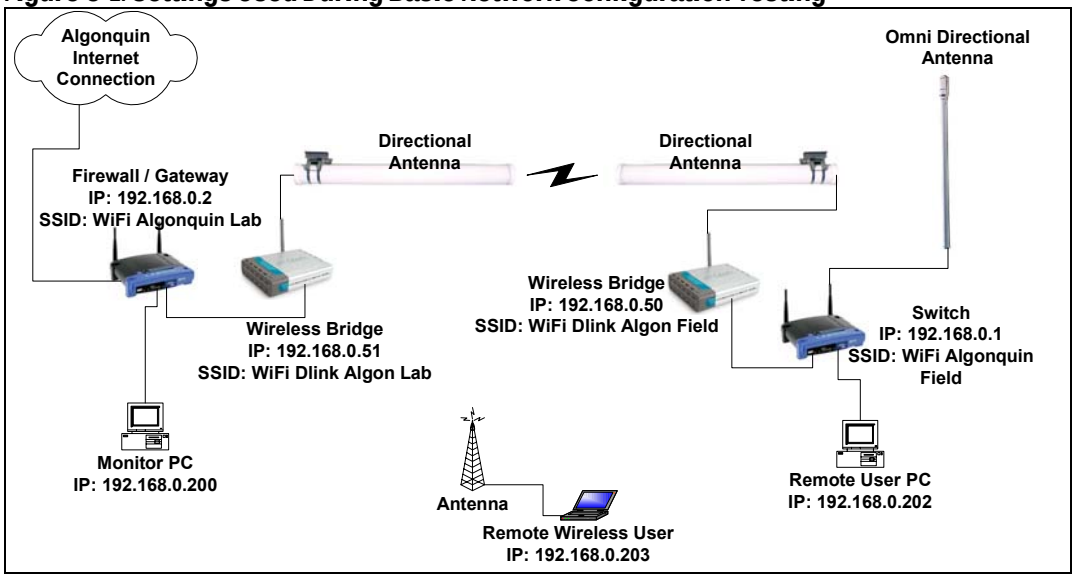
From the above characteristics and witnessed test results, performance in a large coverage WLAN will not match a typical LAN network with the same number of users. It is important to take in account the typical traffic profile when looking at the range spread (distance from the AP) and the number of expect simultaneous users.

6. Basic Configuration Equipment Details

Overview

Figure 6-1 shows the equipment referenced in this chapter.

Figure 6-1: Settings Used During Basic Network Configuration Testing



LinkSys 1 (Wi-Fi Algonquin Lab) Configuration

This is configured both as a Firewall and as a Gateway that provides access to the Internet. It is the only DHCP server on the network.

Table 6-1: LinkSys 1 Identification Parameters

Parameter	Value(s)
Model	WRT54G ver2, Wireless-G Broadband Router
Serial number	CDF50CC99765
Firmware versions tested	• V2.00.8 (default version) • V2.02.7 official LinkSys US firmware upgrade • Svesoft satori V2.00.8.75V pre-release • Svesoft samadhi2 v2.00.8.65V stable release

Table 6-2: Router Port (WAN) Configuration, Internet Port

Parameter	Value(s)
Mode	Gateway
MAC address	00:0C:41:D3:D6:BE
Login Type	Automatic Configuration DHCP
IP address	205.211.32.32 (DHCP Served)
Subnet Mask	255.255.255.0

Parameter	Value(s)
Default Gateway	205.211.30.30

Table 6-3: Local Port (LAN) Configuration, four-port Switch

Parameter	Value(s)
MAC address	00:0C:41:D3:D6:BD
Four-port switch:	
MAC address	192.168.0.2
Subnet Mask	255.255.255.0
DHCP Server	Enabled
Start IP address	192.168.0.249
End IP address	192.168.0.249

Table 6-4: Wireless Port Parameters

Parameter	Value(s)
MAC address	00:0C:41:D3:D6:BF
Mode	Mixed
SSID	Wi-Fi Algonquin lab
DHCP Server	Enabled
Channel	2

LinkSys 2 (Wi-Fi Algonquin field) Configuration – four-port Switch

This is used as a switch. Only the four-port LAN ports are utilized. The WAN Internet port is not used.

Table 6-5: LinkSys 2 Identification Parameters

Parameter	Value(s)
Model	WRT54G ver2, Wireless-G Broadband Router
Serial number	000C41D3D6D5
Firmware versions tested	• V2.00.8 (default version) • V2.02.7 official LinkSys US firmware upgrade • Svesoft satori V2.00.8.75V pre-release • Svesoft samadhi2 v2.00.8.65V stable release

Table 6-6: LinkSys 2 Router Port (WAN) Configuration, Internet Port

Parameter	Value(s)
Mode	Gateway (However, the setting does not matter since the WAN Internet port is not used)
MAC address	00:0C:41:D3:D6:B8
Login Type	Automatic Configuration DHCP
IP address	205.211.32.32 (DHCP Served)
Subnet Mask	255.255.255.0
Default Gateway	205.211.32.1

Note that the Internet port is not used.

Table 6-7: Local Port (LAN) Configuration, four-port Switch

Parameter	Value(s)
MAC address	00:0C:41:D3:80:E2
Four-port switch:	
MAC address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Disabled

Table 6-8: Wireless Port Parameters

Parameter	Value(s)
MAC address	00:0C:41:D3:D6:BF
Mode	Mixed
SSID	Wi-Fi Algonquin field
DHCP Server	Disabled
Channel	11

Description of the LinkSys WRT54G

This is a four-port LAN switch. A single IP address and MAC address are assigned to all four switch ports. It has one WAN Internet port.

The device has three MAC addresses assigned to the Wireless port, WAN port, and the LAN ports. The MAC address listed on bottom of LinkSys case with serial number is the MAC address of the Ethernet port.

It has left and right antennas, which can set to Left/Right/Diversity transmit and receive.

The Operating Mode can be set as Gateway or Router, but not both:

- Gateway

  The WAN port routes the Internet to the four-Port switch. The WRT54G acts as a Firewall. There is a limitation, however: it cannot communicate with other WRT54G Routers on the network.

- Router

  It can communicate with other Routers. The limitations are that the WAN port will not pass an Internet connection through the WAN to a LAN.

Issues with the WRT54G

All four LAN ports have one single IP address. Therefore it is unable to route traffic on the LAN side.

You cannot have two LinkSys Routers on one network and receive Internet connectivity at the same time. Instead, you must set one LinkSys to Gateway operating mode and use the second WRT54G LAN's four-port hub functionality only (therefore, do not use the WAN port on the second WRT54G). This is due to fact that the WRT54g configured as a Gateway will not communicate with another Router, and the WRT54G configured as a Router will not connect to Internet.

In the Router Firewall and Block WAN traffic option, you cannot ping through the Router when "Block WAN traffic" is enabled.

The WRT54G blocks all WAN remote connections. You cannot make a remote connection through WAN port to LAN ports. The WRT54G settings do include VPN access, but the functionality does not work.

To configure the LinkSys, the PC must have same network address as it. Note: if you set the IP address and subnet mask on the WRT54G to have a different network address than that PC used to configure the WRT54G, communication will be lost. The user will have to change the PC's TCP/IP properties again to match the network address of the WRT54G.

D-Link 1 (Wi-Fi D-Link Algon Lab) Configuration: Wireless Bridge

The antenna was set to: Left antenna transmit and receiver. Other settable parameters are listed in the tables below.

Table 6-9: D-Link 1 Identification Parameters

Parameter	Value(s)
Model	DWL-900AP+ AirPlus 2.4GHz Wireless Access Point
Hardware Version	C2
Serial number	BN0H53C000435
Firmware versions tested	• 3.02 (default factory version) • 3.06 official US D-Link upgraded firmware

Table 6-10 D-Link 1 Configuration, Ethernet Port

Parameter	Value(s)
MAC address	00:0D:88:A6:D7:DB
IP address	192.168.0.51
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DHCP Server	Disabled

Table 6-11: Wireless Port Parameters

Parameter	Value(s)
MAC address	00:0D:88:9E:43:75
Mode	Wireless Bridge
SSID	Wi-Fi D-Link Algon lab
Channel	7
Wireless Bridge→ Remote Bridge MAC	00:0D:88:A6:B8:12

D-Link 2 (Wi-Fi D-Link Algon Field) Configuration: Wireless Bridge

Table 6-12: D-Link 2 Identification Parameters

Parameter	Value(s)
Model	DWL-900AP+ AirPlus 2.4GHz Wireless Access Point
Hardware Version	C2
Serial number	BN0H53C000432
Firmware versions tested	• 3.02 (default factory version) • 3.06 official US D-Link upgraded firmware
Antenna	Left antenna transmit and receiver

Table 6-13 D-Link 2 Configuration, Ethernet Port

Parameter	Value(s)
MAC address	00:0D:88:A6:B8:12
IP address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DHCP Server	Disabled

Table 6-14: D-Link 2 Configuration, Wireless Port Parameters

Parameter	Value(s)
MAC address	00:0D:88:A6:D7:DB

Parameter	Value(s)
Mode	Wireless Bridge
SSID	Wi-Fi D-Link Algon field
Channel	7
Wireless Bridge→ Remote Bridge MAC	00:0D:88:A6:B8:12

D-Link Characteristics

In Wireless Bridge mode, D-Links must have same Network ID's as each other but not same as network computers. It has both an internal and an external antenna. It can set to internal/external/diversity transmit and receive. The D-Link has 2 MAC addresses for the wireless port and the Ethernet port. The MAC address listed on bottom of D-Link case with serial number is the Ethernet port MAC.

- Wireless bridge is not class dependent. i.e., PC's on Ethernet ports can be Class B, D-Link class C. In this example, computers cannot ping the D-Link but can transmit over the D-Link wireless bridge.
- PC1(192.168.2.100) ←→ D-Link (192.168.1.1) ←→ Wireless connection←→ D-Link (192.168.1.2) ←→ PC1(192.168.2.100)

  PC's can communicate over wireless bridges through D-Link's, but PC's cannot ping the D-Link.

Wireless Cards Connected to Remote PC's

Table 6-15: 11Mbps Wireless USB Adapter – D-Link Identification Parameters

Parameter	Value(s)
Model	DWL-120
Hardware Version	V.E1
Serial number	H28L13A000868
MAC ID	00055D9F29CC
Interface	USB adapter

Table 6-16: D-Link Air Plus – DWL-G650 Identification Parameters

Parameter	Value(s)
Model	DWL-G650
Hardware Version	B2
Serial number	BN20237000170
Firmware version	2.23
MAC ID	00:40:05:31:AA:9B
Antenna	Internal and external antenna. Can set to internal/external/diversity transmit and receive. Antenna 1 = external antenna, Antenna 2 = internal antenna
Interface	PCI card. Will connect to WRT54G LinkSys

PC Configuration

The following are the general settings that apply to computers on the network. TCP/IP properties are required to communicate with other devices on network. DNS settings are specific to Algonquin College; they are required to receive Internet connectivity within the Algonquin college network.

Table 6-17: TCP/IP Properties

Parameter	Value(s)
Network address	192.168.0.0
Subnet mask	255.255.255.0
Gateway	192.168.0.2 (LinkSys Gateway)

Table 6-18: DNS Properties

Parameter	Value(s)
DNS servers	• 205.211.30.22 • 205.211.30.21 • 192.197.88.3
DNS Suffix search list	• Ottawa.ad.algonquincollege.com • Ad.algonquincollege.com • Algonquincollege.com

Network Setup Steps

Note

For the Basic Network Configuration, it is suggested that all ports and network devices have the same network address. Set the monitor PC connected to the LinkSys Firewall to receive DHCP addresses, so as to be able to test the DHCP functionality. Set the remaining computers on the network to have static IP addresses. If during testing, the RF link is unable to connect, any computers with DHCP addresses will lose connection to the DHCP server and be unable to receive DHCP-served TCP/IP properties.

Configure PC's

Checklist 6-1: Configure PC's

Step	Step Description	Notes	Done?
1	Set the LinkSys WRT54G factory default address to be IP:192.168.0.1 with subnet mask: 255.255.255.0	Configure static TCP/IP properties of the PC to communicate with LinkSys WRT54G and D-Link DWL-900AP+. The IP address and subnet mask must have same the network address as the LinkSys and D-Link in order to access each device's configuration settings.	☐ Yes ☐ No
2	Set the D-Link DWL-900AP+ factory default address to be IP:192.168.0.50 with subnet mask: 255.255.255.0		☐ Yes ☐ No
3	Configured the PC to have the static network address 192.168.0.0. (recommended)	This will enable communication to both the LinkSys and the D-Link.	☐ Yes ☐ No
4	Ensure that the correct DNS servers and suffix	Needed for Internet connectivity.	☐ Yes ☐ No

Step	Step Description	Notes	Done?
	search list parameters are entered		

Configure the LinkSys Firewall

Checklist 6-2: Configure the LinkSys Firewall

Step	Step Description	Notes	Done?
1	Connect the Ethernet cable from the PC to any of the four LAN ports on the WRT54G	Ports are labeled 1 to 4.	☐ Yes ☐ No
2	Connect the WRT554G Internet WAN port (labeled Internet) to Internet connection		☐ Yes ☐ No
3	Configure the Internet port to receive DHCP addresses.		☐ Yes ☐ No
4	Configure the WRT54G mode as Gateway.	The WRT54G will act as the Internet firewall.	☐ Yes ☐ No

Configure WRT54G Wireless Connection

Checklist 6-3: Configure WRT54G Wireless Connection

Step	Step Description	Notes	Done?
1	Set the SSID name.		☐ Yes ☐ No
2	Select the broadcast channel.	Ensure that the channel does not conflict with any other devices on network.	☐ Yes ☐ No
3	Configure the WRT54G to act as a DHCP server. Set the start and end IP addresses of the DHCP range.		☐ Yes ☐ No
4	Configure the TCP/IP properties of the LAN ports. The same IP address will be assigned to all four LAN ports.	If you set the IP address and subnet mask on the WRT54G to have a different network address from that of the PC used to configure the WRT54G, communication will be lost. You will have to change the PC's TCP/IP properties again to match the network address of the WRT54G.	☐ Yes ☐ No
5	Select antenna Transmit and Receive settings. Set antenna diversity off. Select one antenna for both transmit and receive.	This option is not available with the factory firmware version. Firmware capable of adjusting the antenna characteristics must be	☐ Yes ☐ No

Step	Step Description	Notes	Done?
		loaded. Svesoft firmware version Samadhi2 V2.00.8.65 was used in the test configuration.	

Configure the LinkSys Switch

Checklist 6-4: Configure the LinkSys Switch

Step	Step Description	Notes	Done?
1	Connect the Ethernet cable from the PC to any of the four LAN ports on the WRT54G	Ports are labeled 1 to 4	☐ Yes ☐ No
2	Set the WRT54G to either Router or Gateway operating mode.	The WAN port labeled "Internet" will not be used. Therefore the operating mode does not matter, since only the LAN port switch capabilities will be used. This setting only dictates the behavior of the WAN port.	☐ Yes ☐ No
3.1	Set the SSID name.	Step 1 of configuring the WRT54G wireless connection	☐ Yes ☐ No
3.2	Select the broadcast channel, and ensure that channel does not conflict with any other devices on network.	Step 2 of configuring the WRT54G wireless connection	☐ Yes ☐ No
4	Disable the WRT54G DHCP server feature.	The LinkSys firewall is already configured to act as a DHCP server. It is possible to have more than one DHCP server on the network. However, for simplicity, there will only be one DHCP server in the Basic Network Configuration.	☐ Yes ☐ No
5	Configure the TCP/IP properties of LAN ports. The same IP address will be assigned to all four LAN ports.	If you set the IP address and subnet mask on the WRT54G to have a different network address than that of the PC used to configure the WRT54G, communication will be lost. You will have to change PC TCP/IP properties again to match network address of WRT54G.	☐ Yes ☐ No

Step	Step Description	Notes	Done?
6	Select the antenna transmit and receive settings. The antenna diversity must be turned off. Select one antenna for both transmit and receive.	This option is not available with the factory firmware version. Firmware capable of adjusting the antenna characteristics must be loaded. Svesoft firmware version Samadhi2 V2.00.8.65 was used in the test configuration.	☐ Yes ☐ No

Configure the D-Links

For each D-Link used in wireless bridge, follow the procedure in Checklist 6-5.

Checklist 6-5: Configure the D-Links

Step	Step Description	Notes	Done?
1	Connect the Ethernet cable from the PC to the Ethernet port on the D-Link.		☐ Yes ☐ No
2	Configure the TCP/IP properties of the Ethernet port. The same IP address will be assigned to all four LAN ports.	If you set the IP address and subnet mask on the WRT54G to have a different network address than that of the PC used to configure the WRT54G, communication will be lost. You will have to change PC TCP/IP properties again to match the network address of WRT54G.	☐ Yes ☐ No
3.1	Set the SSID name.	Step 1 of configuring the D-Link wireless connection	☐ Yes ☐ No
3.2	Select the broadcast channel. Ensure it does not conflict with other wireless channels in the area.	Step 2 of configuring the D-Link wireless connection	☐ Yes ☐ No
4	Enter the MAC address of the other D-Link that will complete the wireless bridge.	Configuring the D-Link operating mode as a Wireless Bridge. You must enter the MAC address of the Ethernet port. Do *not* enter the MAC address of wireless port. The MAC address listed with serial number on bottom of D-Link is the Ethernet MAC address.	☐ Yes ☐ No
5	Disable the DHCP server option.		☐ Yes ☐ No
6	Select Antenna setting.		☐ Yes ☐ No

Step	Step Description	Notes	Done?
	Turn diversity off.		

Connect the Basic Network Configuration

Ping the network devices to ensure connectivity. From the monitor PC, ping devices in the order given in Checklist 6-6.

Checklist 6-6: Ping to Check Basic Network Configuration

Step	Step Description	Notes	Done?
1	LinkSys Gateway LAN IP address		☐ Yes ☐ No
2	D-Link wireless bridge connected to LinkSys Gate-way		☐ Yes ☐ No
3	D-Link wireless bridge connected to LinkSys Switch		☐ Yes ☐ No
4	LinkSys switch LAN port		☐ Yes ☐ No
5	Remote PC's connected to LinkSys LAN port		☐ Yes ☐ No
6	Internet address (e.g., www.yahoo.com).	To ensure Internet con-nectivity	☐ Yes ☐ No

Outline of Possible Issues during Testing

Dynamic Addresses

If the connection to the DHCP server is lost, the computer will be unable to receive an IP address. The computer will be unable to communicate with any devices on network.

Static Addresses

You must ensure that the DNS properties are configured to receive Internet connections.

DHCP Conflicts

Having more than one DHCP server on network can add latency by increasing the amount of traffic from responses to DHCP requests.

It complicates IP address ranges. You must check which DHCP server has served the address each time the computer is started.

D-Link Site Survey

There is a feature included with D-Link to survey and report the SSID of all wireless networks detected. The site survey does not report the SSID of any D-Links in wireless bridge mode.

LinkSys WRT544G

- Blocking WAN traffic

  The LinkSys Router does not allow a VPN (Virtual private Network) of SSH connections through the Firewall, even though there are options to enable VPN and SSH connections. Third party firmware must be loaded to use VPN and SSH.

- Blocking Ping

  It is impossible to “ping” through the LinkSys Firewall when the “Block WAN traffic” option is enabled.

- Router versus Gateway

  In Gateway mode, the WRT54G cannot communicate with another WRT54G Router. A second WRT54G will not pass information through the Firewall from the other WRT54G (Gateway). In Router mode, the WRT54G cannot receive an Internet connection. The WRT54G can act as Gateway or Router, but not both at same time.

Antenna Diversity

You must ensure diversity is off. Otherwise, the antenna will connect to the strongest signal. That strongest signal may not be RF connection. The result will be what appears to be a loss of connection, but is simply the device selecting another signal automatically.

All devices used during testing have more than one antenna. Never assume there is only one antenna on a device simply because only one antenna can be seen. There may be internal antennas. Switching automatically between antennas will most probably result in an intermittent link.

Table 6-19: Antenna Arrangements of APs Used in Project

AP	Antenna Arrangement
D-Link DWL-900AP+	Internal/external antenna
DWL-G520	Internal/external antenna
LinkSys WRT54G	left/right antenna

Confirm Connection

Measure the RF connection with an RF sniffer, not with network connectivity. To test the RF signal availability, use the antenna and an RF signal detection tool such as Netstumbler. Do not try to test the RF link simply by checking network connectivity. If network connectivity is present over an RF link, the strength of the RF link is still unknown. If network connectivity is not present, it is hard to determine if the lack of connection is due to weak connection or a network configuration error.

Troubleshooting the RF Connection with the D-Link Wireless Bridge

Network Configuration A

In this configuration, the field LinkSys is configured as a four-port switch.

Table 6-20: Configuration A

Link	Parameter	Value(s)
Internet ↔LinkSys AP		
	SSID	Wi-Fi Algonquin Lab
	Mode	Gateway
	IP	192.168.0.2
↔D-Link		
	Mode	Wireless bridge
	IP	192.168.0.51
↔Directional Antenna		
↔RF link		
↔Directional Antenna		
↔D-Link		
	Mode	Wireless bridge
	IP	192.168.0.50
↔LinkSys four-port LAN switch		
	SSID	Wi-Fi Algonquin field
	Mode	N/A
	IP	192.168.0.1
↔Field test LAN:	Note: Clients receiving Internet through omni-directional antenna are connected to the LinkSys Wireless Port and Clients connected directly to LinkSys four-port LAN Ethernet ports.	
PC1(192.168.2.100)		
↔D-Link (192.168.1.1)		
↔Wireless connection		
↔PC1(192.168.2.100)		

D-Link Wireless Bridge Configurations

Table 6-21: D-Link 1 (Wi-Fi Lab): Wireless Bridge Identification Parameters

Parameter	Value(s)
Model	DWL-900AP+ AirPlus 2.4GHz Wireless Access Point
Hardware Version	C2
Serial number	BN0H53C000435
Firmware version	3.02

Table 6-22: D-Link 1 (Wi-Fi Lab) Configuration, Ethernet Port

Parameter	Value(s)
MAC address	00:0D:88:A6:D7:DB
IP address	192.168.0.51
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Table 6-23: D-Link 1 (Wi-Fi Lab) Wireless Port Parameters

Parameter	Value(s)
MAC address	00:0D:88:9E:43:75
Mode	Wireless Bridge
SSID	Wi-Fi gonq lab
DHCP Server	Enabled
Channel	7
Wireless Bridge→ Remote Bridge MAC	00:0D:88:A6:B8:12

Table 6-24: D-Link 2 (Wi-Fi Field): Wireless Bridge Identification Parameters

Parameter	Value(s)
Model	DWL-900AP+ AirPlus 2.4GHz Wireless Access Point
Hardware Version	C2
Serial number	BN0H53C000432
Firmware version	3.02

Table 6-25: D-Link 2 (Wi-Fi Field) Configuration, Ethernet Port

Parameter	Value(s)
MAC address	00:0D:88:A6:B8:12
IP address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Table 6-26: D-Link 1 (Wi-Fi Field) Wireless Port Parameters

Parameter	Value(s)
MAC address	00:0D:88:A6:D7:DB
Mode	???
SSID	???
DHCP Server	???
Channel	???
Wireless Bridge→ Remote Bridge MAC	???

Troubleshooting Steps

Establish a D-Link Transmission from the Algonquin Lab (Room B374)

Checklist 6-7: Troubleshooting – Establish D-link Transmission from Lab

Step	Step Description	Notes	Done?
1	Disconnect the power from the Wi-Fi field D-Link.		☐ Yes ☐ No
2	Connect the cable from the antenna on the roof to the D-Link wireless antenna port.		☐ Yes ☐ No
3	Ensure the Ethernet port from the Wi-Fi Field D-Link is connected to the LinkSys router.		☐ Yes ☐ No
4	Connect power to the Wi-Fi field D-Link.		☐ Yes ☐ No
5.1	Ensure the computer is connected to the LinkSys four-port switch Ethernet LAN.	Steps 5: Test the Wi-Fi field D-Link transmission status	☐ Yes ☐ No
5.2	Turn on the computer connected to LinkSys LAN.		☐ Yes ☐ No

Step	Step Description	Notes	Done?
5.3	Log onto Windows.		☐ Yes ☐ No
5.4	If you are able to see the "Log on to:" option in the Windows log on screen, select "this computer", and not the Algonquin college Woodroffe domain. The password is "wireless" and the username is "wireless".		☐ Yes ☐ No
5.5	Select "Start"		☐ Yes ☐ No
5.6	Select "Run"		☐ Yes ☐ No
5.7	Open the command prompt window. Depending on the Windows version, type "cmd" or "command" and press the Enter key.		☐ Yes ☐ No
5.8	Type "ipconfig" at the command prompt.		☐ Yes ☐ No
5.9	Ensure that the computer has received an IP address from the LinkSys DHCP server.		☐ Yes ☐ No
6.1	Ping the Wi-Fi Lab D-Link wireless bridge using the following command: Ping <Wi-Fi Field D-Link IP address>, i.e., ping 192.168.0.50	Steps 6: set the static IP address	☐ Yes ☐ No
6.2	If you unable to ping the D-Link, disconnect the power and reconnect to initialize the D-Link. Wait 30 seconds for initialization to complete. Attempt to ping the Wi-Fi Field D-Link again.		☐ Yes ☐ No
6.3	Open Internet Explorer.		☐ Yes ☐ No
6.4	Type the IP address of the Wi-Fi Field D-Link into the Internet Explorer address bar, i.e., 192.168.0.51.		☐ Yes ☐ No
6.5	A password prompt window will appear. Enter the		☐ Yes ☐ No

Step	Step Description	Notes	Done?
	password “admin” and leave the username blank. Press the Enter key.		
6.6	The D-Link DWL-900AP Enhanced 2.4GHz Wireless Access Point page should appear in Internet Explorer. Select the Advanced tab at the top of the D-Link DWL-900AP page.		☐ Yes ☐ No
6.7	Select the Mode button, if it is not already selected.		☐ Yes ☐ No
6.8	Select “Site Survey”. This may take up to 10 minutes.		☐ Yes ☐ No
6.9	Ensure the D-Link can see any networks to ensure the antenna is working.		☐ Yes ☐ No

Establish D-Link Transmission from the Field Setup (Wi-Fi Field D-Link)

Checklist 6-8: Troubleshooting – Establish D-link Transmission from Field

Step	Step Description	Notes	Done?
1	Connect the setup.		☐ Yes ☐ No
2	Power on the PC.		☐ Yes ☐ No
3.1	Open network properties. In Windows XP, select “Start” and then “Settings and Network connections”. Select the LAN (Local Area Network) connection properties, either by double clicking on the icon and selecting the Properties button, or right clicking the LAN connection icon and selecting Properties. In the Properties window, select the General Tab. In “This connection uses the following items” window, select Internet Protocol (TCP/IP). Select the Properties button. Ensure “obtain an IP address automatically. Select OK to close TCP/IP properties and Select OK on LAN connection window.	Steps 3: Determine if the connection is already established:	☐ Yes ☐ No
3.2	Select “Start”.		☐ Yes ☐ No

Step	Step Description	Notes	Done?
3,3	Select “Run”.		☐ Yes ☐ No
3.4	Open the command prompt window. Depending on the Windows version, type “cmd” or “command” and press Enter.		☐ Yes ☐ No
3.5	Type “ipconfig” at the command prompt.		☐ Yes ☐ No
3.6	Ensure that the computer has received an IP address from the LinkSys DHCP server. If an IP address has been DHCP served, it will have network address 192.168.0.x. If an IP has not been DHCP served, Windows will assign automatically an IP address that will start with 169.X.X.X.		☐ Yes ☐ No
4	Type “ipconfig /?” to determine the command to release the DHCP address. Typically, the command is “ipconfig /release”.		☐ Yes ☐ No
5	Type “ipconfig /?” to determine the command to renew the DHCP address. Typically the command will be “ipconfig /renew”.		☐ Yes ☐ No
6	Determine if IP is not DHCP served, RF link not established and computer not receiving IP address form Wi-Fi Algonquin Lab LinkSys DHCP server in Algonquin College LAB.	If the IP is not DHCP served, the RF link is not established.	☐ Yes ☐ No
7	Statically set the IP to communicate with the D-Link. They are now on different LANs.		☐ Yes ☐ No
8	Ping the D-Link.		☐ Yes ☐ No
9	Connect to the D-Link through Internet Explorer.		☐ Yes ☐ No
10	Ensure that D-Link can see any networks to ensure that the antenna is working.		☐ Yes ☐ No

Extended Reach Advanced Settings

For very long backhaul links, a Lucent/Orinoco "demo" ad-hoc mode can be used. This was implemented by Lucent before the IEEE had standardized the IBSS peer-to-peer mode of operation for wireless bridging that the D-link and similar products incorporate now. In order go over single hop distances of over 25 – 40 km, this special mode **does not send ACKs** and is thus will prevent messages from being timed. This will work for long point-to-point as well as long range point-to-multipoint configurations with low user density (about 10 active users). The more users there are the higher the probability of collision of transmissions

You can still access this mode via any Prism or Hermes chipset under Linux with the right wireless tool commands. Below is a list of useful wireless configuration commands that can be used to tune a card for long distance, high latency links. You will need a good antenna and card for this to work at 11Mbps at a decent distance.

Firmware modifications (example)

```
dev=eth0

# Put card in ad-hoc mode

iwconfig $dev mode ad-hoc

# Disable RTS as this is a point-to-point link - probably not needed

iwconfig $dev rts off

# Place a fragmentation threshold - more loss on precarious p-t-p links

# If you are using point-to-multipoint setting this lower would be a good idea

iwconfig $dev frag 1024

# Fix the rate at 11Mbps - remember what I said about good antennas / cards / amps for this distance and rate...

iwconfig $dev rate 11M

# Turn on the old ad-hoc "demo" mode for peer to peer

iwpriv $dev set_port3 1

# You can verify that you are using the ad-hoc mode if the

# AccessPoint BSSID/MAC in iwconfig is reported as all zeros.

# If it is your MAC or the peer's MAC, you are using IBSS ad-hoc
```

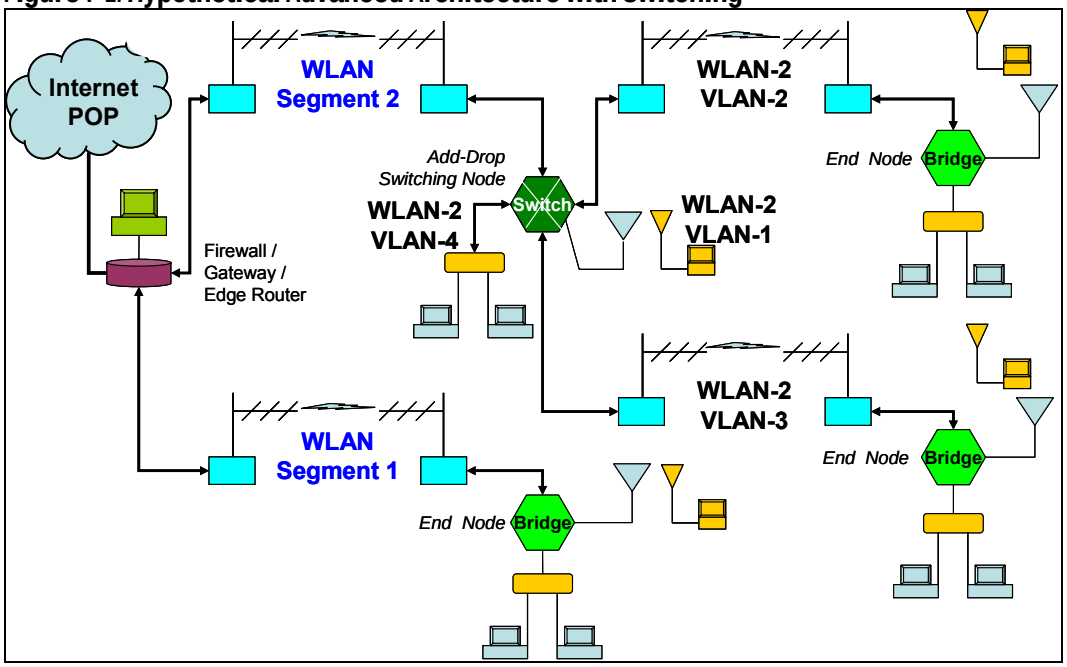
7. Advanced System Setup

Overview

This Chapter provides a qualitative discussion of the Advanced Configuration architecture and configuration issues for its elements and links. A later Chapter provides details of specific configuration settings.

Figure 7-1 below shows how switching can be used in the Advanced System to partition (segment) the wireless networks into sub-networks.

Figure 7-1: Hypothetical Advanced Architecture with Switching



Overview of VLANs

All approaches to reducing the impact of overhead traffic consist of partitioning a network into sub-networks. Then the propagation of broadcast traffic is confined to the network segments where it is needed.

A popular method of partitioning the network so that overhead traffic is more controlled is the Virtual LAN (VLAN) concept[1]. It restricts the amount of inter-nodal communication to the nodes assigned on the same VLAN, which is sub-network. In-

[1] A good overview of VLANs is at:
http://www.cisco.com/warp/public/cc/pd/wr2k/cpbn/tech/vlan_wp.htm.

terconnection between VLANs is done via a common routing node that can be implemented at one central node. The latter could be at the POP.

With networks partitioned into VLANs, broadcasts are contained within the VLAN they originated in. Broadcast traffic on one port of the routing node is replicated only for those ports that belong to the same VLAN.

The VLAN approach is a common approach in enterprise networks to provide organizational isolation between various user communities in an organization. In a multi-community situation, a VLAN is assigned to each community. This removes the need to have overhead packets between other VLAN communities. There will be overhead back to the common VLAN switch router. However, the broadcast traffic is much reduced compared to having all nodes intercommunicating with each other.

Using VLAN switching instead of classic routers also achieves better performance by reducing latency. Administrative workload is also reduced because routers require a more time consuming configuration process than switches.

A minor downside of a VLAN is that it requires some administrative work for a group to operate the network. The initial set-up will require some expertise to arrange the network properly and to make it easy to add users or additional network nodes.

The good news with the VLAN approach is that it is now being supported by Linux-based APs. Commercial 3rd party software is now available for equipment such as the LinkSys AP to allow the configuring of the firmware for VLANs.

The use of VLANs does not preclude re-using equipment from a previously built basic network. A hybrid network is very feasible, allowing a basic network or several basic configurations to link together.

VLAN Details

Definition

A VLAN is a logical grouping of switch or router ports into sub-networks called workgroups. With VLAN support, network managers can define workgroups independently of the underlying network topology.

Virtual Workgroups

A workgroup model is used where it is assumed that most of the traffic in a workgroup stays in the same broadcast domain. If the 80/20 rule is maintained, i.e. 80% of the traffic is local and only 20% will need to pass the router, then significant performance improvements can be achieved.

Routers are needed between VLANs. In addition, security concerns can be addressed better. If private port switching is implemented in switches, then the traffic on the single user segment would be from its VLAN.

Types of VLANs

Layer 1 VLAN

These are VLANs based on layer 1 information, i.e. ports. In this type of VLAN, the network manager of the AP switch assigns a set of ports to each VLAN. This is the

simplest kind of VLAN support. It is called *port grouping* or *port switching*. Messages are broadcast in a particular segment. But, if two persons on the same segment want to be on different VLANs, that is not possible. This would be the approach for subtending remote APs as VLAN hubs, as shown in Figure 7-2 below.

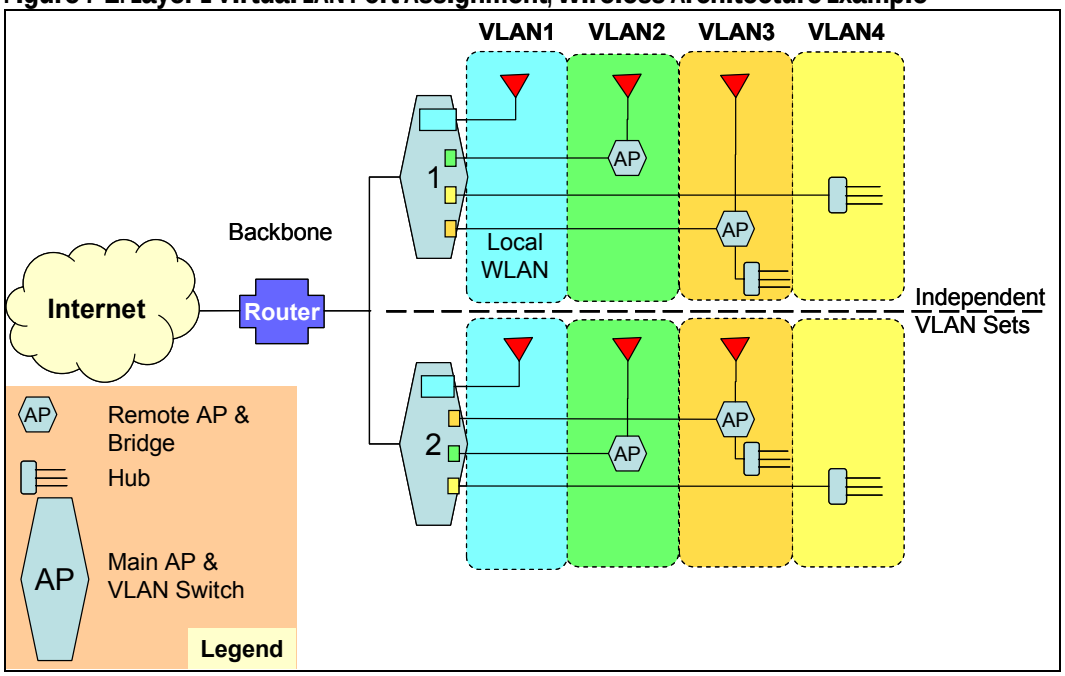
Layer 2 VLAN

These are VLANs based on Layer 2 (MAC) layer addresses. The membership of a user depends on their MAC addresses. The main advantage of this approach is that it provides full user mobility. Another way of implementing it could be VLANs based on MAC protocol type field. This is also called a *bridge-based VLAN*. This is more useful if all APs are VLAN switches with individual users assigned to VLANs. This is not as useful for unloading the interlinks.

Layer 3 VLAN

These are VLANs based on layer 3 information. VLAN membership depends on MAC layer protocol field and the *subnet field*. The VLAN configuration is learned by the switch, so no manual configuration is required. This is also called a *Virtual subnet*.

Figure 7-2: Layer 1 Virtual LAN Port Assignment, Wireless Architecture Example



There can be multiple, independent sets of VLANs as shown in Figure 7-2.

The ideal situation would be a switch supporting all three levels of VLANs, chosen by the user at will. The user would then configure the VLANs using a Graphical User Interface.

Desirable Switch Characteristics

A number of desirable characteristics for the AP switch to be used to support VLANs are:

- A switch that does not drop frames. At least four 100BaseT ports with 1.0 Gb/s throughput are desirable.
- *Path buffering switches* have better performance.
- Latency should be low.

  This is not a very big concern. The average latency for a minimum size packet through a *cut-through switch* is 45.6 µs. For a *store-and-forward switch*, it is 51.5 µs. Since the difference is so small, store-and-forward switches are generally preferred.
- Only for time sensitive applications such as VoIP, cut-through switches should be preferred over store-and-forward ones.

8. VLAN Test Results

Setup

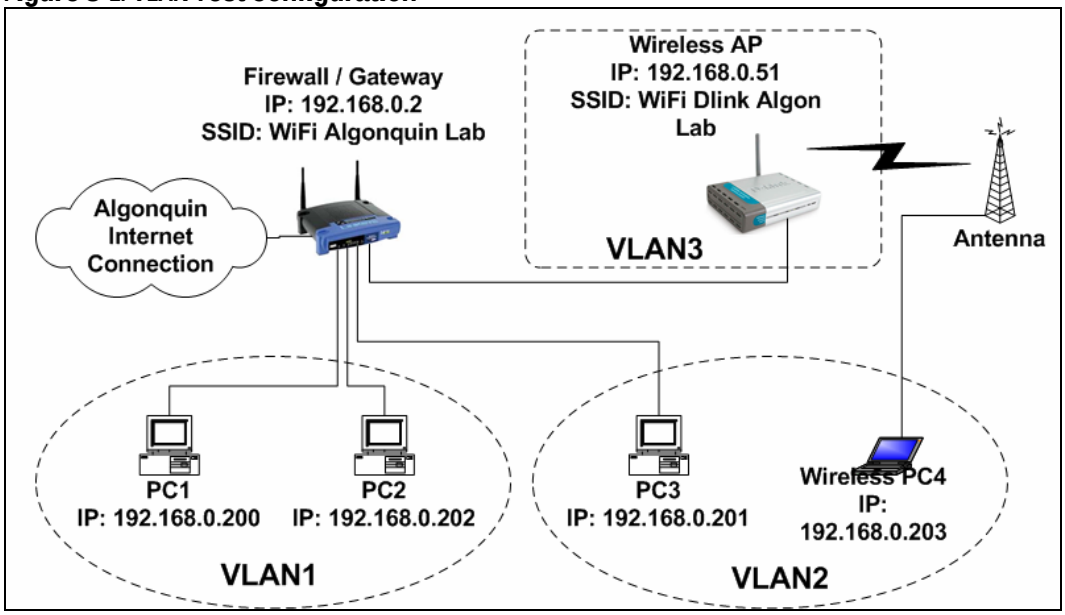
Overview

The LinkSys router was refitted with Sveasoft firmware. This firmware allowed each of the Ethernet ports and the WLAN to be assigned a unique VLAN identity. In the test sets, computers were assigned to the same VLANs ID using two of the four ports available on the LinkSys AP wireless switch / router. The 3rd port was assigned to the D-Link configured as a wireless bridge with its own unique VLAN assignment. The LinkSys WLAN was also assigned a unique VLAN ID.

In this arrangement, layer 2 MAC messages were sent between the two wired computers on the same VLAN. Simultaneously, traffic was observed on the wireless links and on the gateway WAN connection back into the college network.

Refer to the network diagram (Figure 8-1) to view the advanced network VLAN test configuration. Four computers and one D-Link Access point were split into three VLAN connections on the LinkSys switch. A Ping broadcast command was used to flood the network. The test software Analog X ran on all computers to view the incoming TCP/IP bit rate on each computer[2]. Ethereal was used to capture IPs and search packet for VLAN information to confirm VLAN protocol.

Figure 8-1: VLAN Test Configuration



Hardware

We used the Linksys WRT54G, with Alchemy pre5.2.3 V2.04.4.8 software loaded.

---

[2] See Appendix A for a list of all test software used or tried.

Alchemy was provided by the third party Sveasoft. Alchemy is currently under development. Alchemy 5.2.3 is a pre-release to subscribing customers ($20 annually). Stable software has not yet been released. Therefore Alchemy software still has intermittent bugs:

- VLAN intermittently stops broadcast
- DHCP server works intermittently

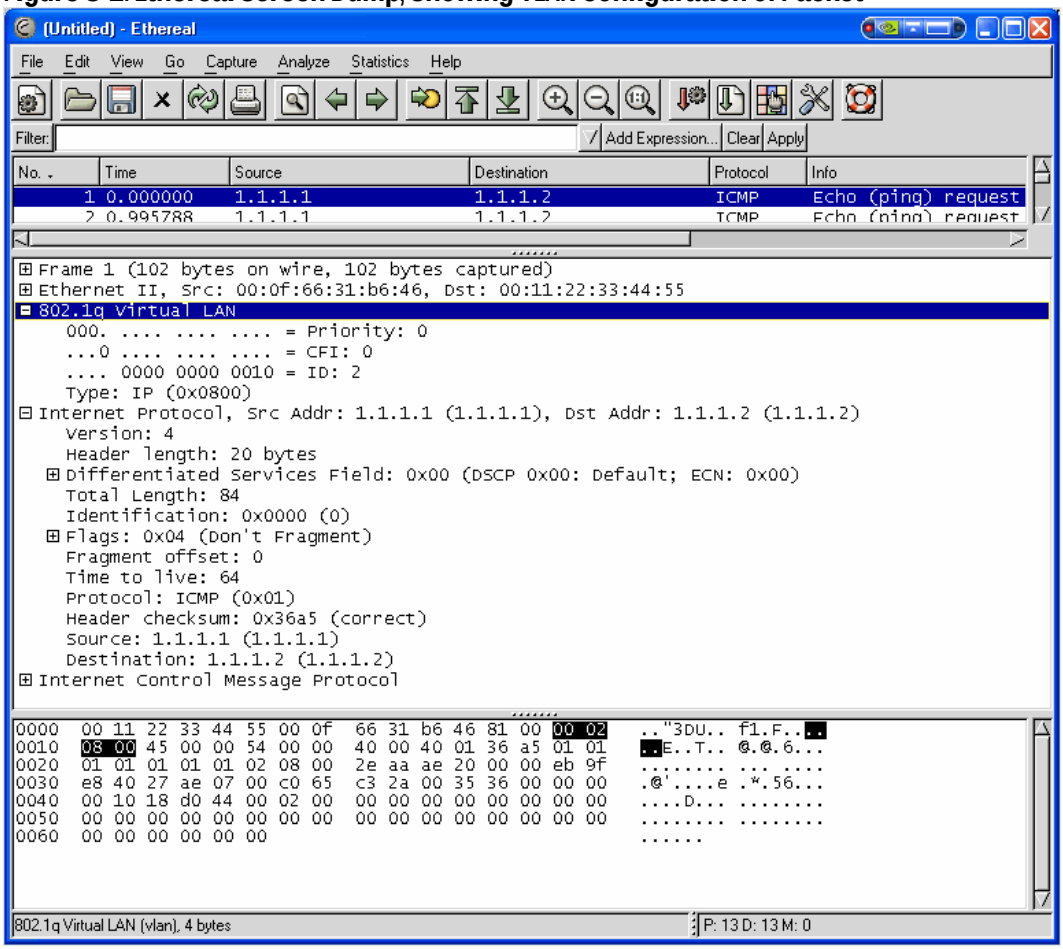
Test Programs

Ethereal Network Protocol Analyzer

An Ethereal network protocol analyzer was used to capture and save TCP/IP packets sent and received by the port on computer. It can open a packet and confirm its VLAN routing. See Figure 8-2 for an example of a packet with its VLAN routing

For further information on http://www.ethereal.com/.

Figure 8-2: Ethereal Screen Dump, Showing VLAN Configuration of Packet



AnalogX Netstat live

Analog X ran on all computers to visually confirm if broadcast would cross VLANs. It can send a broadcast command and watch which computers have received the broadcast. Computers on separate VLAN's should not receive broadcast from other VLAN's.

Ping broadcast command

The ".255" extension in ping is the default broadcast command. It sends bing to all ports on the network. The command is used to flood network and see if the VLAN stops broadcast messages from crossing between assigned VLANs.

```
Ping 192.168.0.255 –t –l 65500
-t for continuous ping
-l 65500 set ping packet size to 65500 bytes
```

Results

This test verified the expected isolation between the VLANs. There was no significant activity seen on the ports assigned different VLAN IDs. The latency in the node was observed to be higher (> 200 µs), since the VLAN involved interaction at the LinkSys CPU. This was not a surprise and should not result in problems in small-scale networks.

The throughput capability did not seem significantly impaired. However, definitive tests must be run with varying degrees of traffic loading through the LinkSys node. Initial testing showed some impact on throughput in comparison to a standard LinkSys bridge without VLAN. The observations still need to be further quantified to see the impact of increasing traffic on other VLANs.

Interpretation of Results

Further testing is needed to determine where the practical limits of this approach lie. With medium loading (25 users per AP) and a limited number of VLANs, performance is expected to be acceptable for smaller networks of 2-4 APs. In larger networks, hardware-based bridges and VLAN switching capabilities must be implemented to prevent bottlenecks at the AP switches.

9. Routing Node Hybrid Approach

Overview

This approach may be important only for the largest Cookbook-based networks approach. Indeed, it may be irrelevant for *any* Cookbook project, because of the complexity involved in setting up and running the network, and because of the costs involved. For that reason, the approach underwent little testing as part of this project.

In this hypothetical approach, the set of inter-AP links and backhaul to the point of presence gateway form a true Wireless WAN (WWAN) backbone. The intent here is to make each WLAN subtended by the APs self-contained, so that intra-LAN traffic and housekeeping and other overhead data are kept within bounds of the AP. This approach keeps the capacity of the inter-AP links available for traffic.

Scalability is also less problematic with a WWAN approach, since a new AP can be added with minimal disruption to the ones in service.

Load sharing can also be facilitated by the WWAN approach. Routes are homed to the gateway by different backhaul links from the AP.

This approach can also be combined with VLANs if the network expands to include more linked APs.

Expected Set-Up Issues

The above WWAN approach will require a significant increase in configuration work by the people implementing the system. IP addresses must be pre-assigned to the nodes to ensure that all elements can home on the respective nodes and to ensure that the peripheral nodes have defined routes to the serving router. This usually involves setting up static IP relationships that must be maintained in the network.

Gateways

In a multiple router network, one router will be given the role as the network firewall and DHCP server among other network functions such as firewall and IP filtering for security. For a small network, the router functions within the distribution network will utilize the simple RIP routing protocol.

Expected Performance

With additional routers in the path between the end-user and the network, packet latency will increase compared to the non-routed case. The increase will depend on the number of network routers that the packets must transverse. This can somewhat bottleneck the network.

Hybrid Approach Test Setup

Several 3rd party software suppliers were looked into, including Sveasoft who represent a large body of contributors developing Linux-based applications for APs such LinkSys, Orinoco, and D-Link. Routing firmware in alpha release was utilized with mixed results. The firmware employs RIP protocol to be used. (OSPF is coming later.) This allows the four ports and the wireless LAN that the AP provides to be defined as specific LAN segments (LAN or VLAN). The routing tables and IP mapping are done in the CPU of the LinkSys. Thus, the latency will likely be very significant compared to simple bridging through the unit.

Hybrid Approach Test Results

The firmware's current version was found to be not very functional at this time.

Not all the forms (GUI) to enter routing information were complete. Inactive items or simply blank pages were sometimes displayed. It appears that some functional parts are there to allow developers to experiment with and refine. As is often the case with shareware, there is no guaranty when fixes or refinements will be made available.

The latest firmware release from LinkSys is August 4th 2004, which must be used in conjunction with experimental firmware loads from now on. This area is swiftly developing. It is expected that refined and tested firmware will allow the AP to do formal routing.

10. Range Extension Approaches Using Repeater Configurations

Overview

It is expected that in many deployment areas, direct line-of-site paths will be limited in range due to significant path obstacles such as hills and heavy tall forests. Such situations will require the use of repeaters to push out the range or to get around obstacles to these isolated users. Repeaters will also be needed to inter-link communities, as well as reach POP locations.

So, as a part of the Advanced Configuration work, several types of repeatering modes were attempted with reasonable results.

Two companies in particular (D-Link and Proxim) have focused on this area. They offer their current set of AP products with a rich range of repeater and wireless bridging capabilities.

In investigating the capabilities of the D-Link AP, several approaches for range extension become very feasible to consider. The following configurations were tried and found to be viable for use in a Cookbook context.

Store-and-Forward Repeaters

Overview

D-Link has implemented the 802.11b standard that allows APs to be set up as a store and forward repeater. Such a repeater can thus pass messages between an originating AP and a more remote client. Here the repeater is acting as an AP *proxy*, with the end client seeing the originating AP through the “transparent” repeater.

Unlike classical microwave radio links where two complete radio transceivers are used for the repeater to serve either direction (*duplex*) of the radio link, the 802.11 repeater runs in half duplex, with one transceiver. Packets from the originating AP are received and stored and then retransmitted to the end client(s). The clients’ traffic is similarly received, stored, and then forwarded to the AP. This method slows

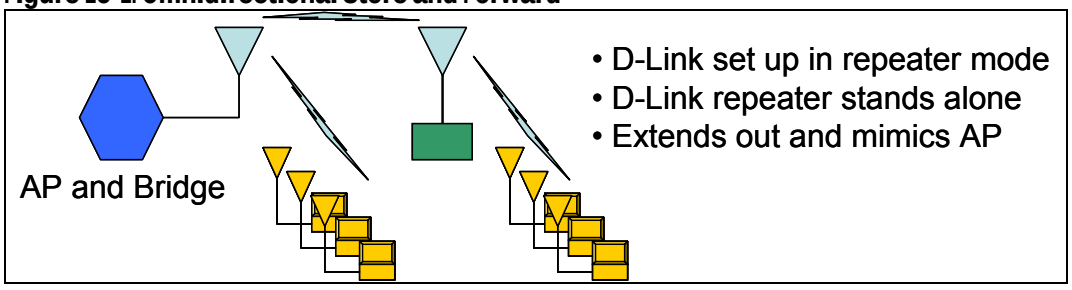
net traffic throughput by 50%. However, since the originating AP and client are also half-duplex, the real throughput is not impacted compared to a direct AP.

AP Range Extension Using a Single Store-and-Forward Repeater

Daisy chaining to sub AP/repeater nodes

The use of APs in a store-and-forward repeater chain is very similar in principle to that used in setting up ad-hoc networks between wireless clients. The first repeater mimics the first AP and rebroadcasts the packet to the next repeater that then stores and forwards the packet to the end client. This does introduce a small amount of latency at each repeater which is < 100 µs per hop. See Figure 10-1.

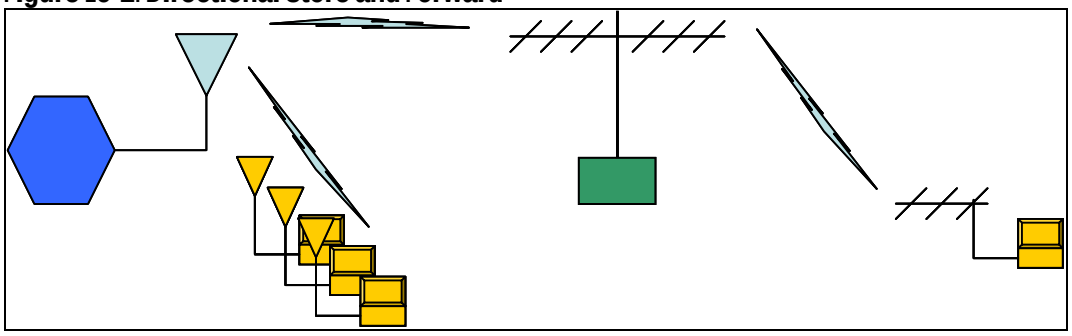
Figure 10-1: Omnidirectional Store and Forward



Using dual repeater nodes with directional antennas

In this approach, directional antennas can be used to extend the reach to remote clients. This can be accomplished by using an antenna combiner / splitter unit. This allows the repeater to be very cost effective, since only one 802.11b unit is required to provide the relay function. See Figure 10-2.

Figure 10-2: Directional Store and Forward



Diversity antenna settings

Any AP used with external antennas must have the diversity antenna system disabled in its firmware. This is extremely important for proper repeater operation with the external antennas to achieve any range. You cannot rely on the AP to automatically select the correct antenna port (if it has two) or an external port or integrated (internal) antenna within the AP package. If diversity is left enabled, the AP will intermittently switch between antennas, thus disrupting the data flow.

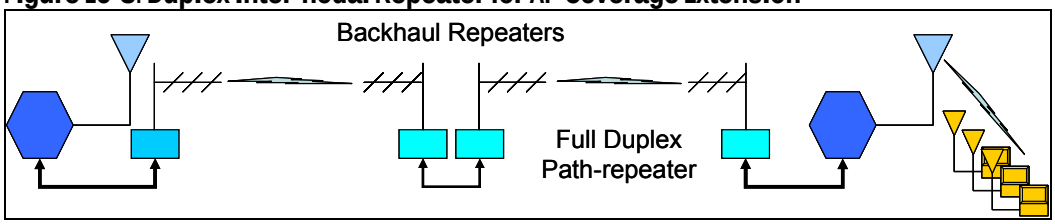
Backhaul and AP Interlink Repeating Mode

This configuration is the classic half duplex repeater operation with flow-through data (no store-and-forward) at the bandwidth of the link. Here the packet data are only slightly buffered before they is retransmitted to next repeater station or end terminal. This type of repeater configuration is to be used when it is required to backhaul an AP to a POP or interconnect APs in a daisy chain.

The APs used in such a structure are set up as simple wireless bridges, as was the backhaul link in the basic configuration architecture. The repeater consists of two APs in wireless bridge mode that are connected back-to-back via a 100 Mb/s Ethernet link. Each bridge AP is associated on a 802.11b MAC basis with the corresponding transceiver at the other end of the link. In this mode no other AP or client can connect to the AP repeater bridges unless they know the MAC ID explicitly. This arrangement, though less vulnerable than open APs, should have basic WEP enabled as well as use unique user ID and passwords to log in to the AP bridges' administration system.

Channel (frequency) planning must done to prevent excessive S/I. The use of repeaters requires that care be taken in the assignment of channels (frequencies) to prevent system self-interference. Each repeater pair, i.e, near and far end will have the same channel assignment since the 802.11b transceivers are half duplex. Thus in a typical set-up, an alternating pattern of 3 channels can be used such as (4,7,10). After the third link, the same channel can be used again (4) since interference will be not significant from the first repeater link.

Figure 10-3: Duplex Inter-nodal Repeater for AP Coverage Extension



Test Results

This methods were tried successfully in the lab. We observed only a small increase in the latency of packets using pinging round trip measurements. Typically, the ping roundtrip delays increase from approximately 19 ms to 21 ms with the store-and-forward repeater mode. The increase is not that significant. It will only become a minor problem if a long chain of these types of repeaters are used, which is unlikely.

Using back-to-back repeaters did not introduce any noticeable delay in the round trip measurements. The latency introduced was of the same magnitude as seen with wireless bridging of tens of microseconds. Throughput was not impaired, with the same 11 up to 22 Mb/s seen on the D-link bridges used in the basic configuration.

11. Powering Remote Sites

Overview

Solar power was explored as one of the number of solutions available. For the project, a 70 Watt panel was utilized together with four 6V 250 A-H batteries. The batteries supplied power to a 12/120 Volt *DC-to-AC power inverter*. This system can sustain up to a 700 Watt AC load draw from the batteries.

Recommendations

The power budget in Table 11-1 was utilized to estimate the adequacy of the system to maintain continuous power to the AP site.

Table 11-1: Power Requirements and Supply

Item	Power Need per unit	Number of Units	Duty Cycle 24 hours	Amp Hours	Daily Amp Hours
Backhaul Radios	**5.0 Watts** (0.6 Amps @12V)	2 (max)	80%	2 x 0.6 Amps x 1 hr x 0.8= **0.96 Amp-hours**	24 x 0.96 = **23.04 Amp-hours**
AP / Switch	**11.0 Watts** (0.92 Amps @12V)	1	90%	1 x 0.92 x 1hr x 0.9 = **0.83 Amp-hours**	24 x 0.825 = **19.80 Amp-hours**
Inverter Power Draw (idle)	**2.4 Watts** (0.2 Amps @12V)	1	100%	1 x 0.2 x 1hr x 1.0 = **0.20 Amp-hours**	24 x 0.2 = **4.80 Amp-hours**
Inverter dissipation with load (10% loss)	Load total = 16 Watts @12 Volts 1.333 Amps 1.333 x 0.1 = 0.133 Amps (dissp) 0.133 *12V = **1.6 Watts**	1	85%	1 x 0.133 x 1hr x 0.85 **=0.11 Amp-hours**	24 x 0.113 = **2.72 Amp-hours**
Totals	**20.0 Watts**			**2.10 Amp-hours**	**50.36 Amp-hours**
Solar Generation Per Panel	**70 Watts** 5.15Amps @13.6 Volts Full Sun	2 panels	10 hours average (year round) Canada mid - latitudes		**103 Amp-hours**

For a basic AP node, the package consisted of one backhaul module and one AP transceiver module. The power draw is under 20 Watts. One solar panel will power the system adequately.

With three transceivers, as shown above, one 70 Watt panel is marginal. A larger panel of 100 watts will suffice. Using two 70 Watt panels will exceed needs.

Using 12 Volt input *DC-to-DC converters* to directly supply the electronics reduces power needs to some degree compared to using a 120 VAC inverter plus the power supplies that are typically supplied with off-the-shelf APs. The 1 to 2 Watts power saving should provide better reserve margins when there is poor solar conditions.

The batteries used with solar powered installations must be deep discharge lead-acid types used for RV or marine applications. The batteries must be able to sustain the load without significant terminal voltage (10%) drop up to the point of exhaustion. The batteries must be able to be *float charged* by the solar panels without the *memory effect* that is typical of NiCad battery technology. In the latter, charging the battery before it is totally discharged results in significant capacity loss.

Battery capacity for solar-powered AP relay nodes should provided for 24 hours of full system operation. This is a Telco objective to maintain system availability. After 24 hours with no power, a power contingency mode must be implemented to stretch remaining power another 6 hours if possible.

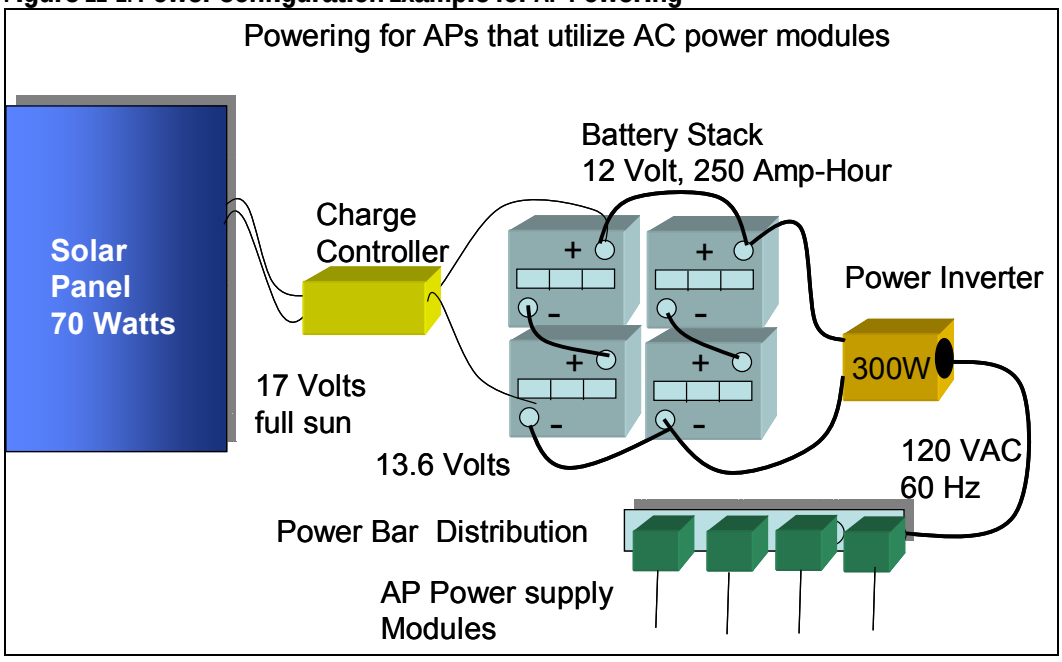
Sizing the Power Supply

In order to power the AP node as described with solar or other alternative power sources, several factors must be considered to determine how much power the source can deliver over time as well as the amount of time the source will be unavailable.

With wind and solar power, the power generated will be directly in proportion to the amount of wind or sunlight. Thus, there definitely will be prolonged periods of no solar or wind power generation. where the batteries must provide all the power. In sizing the system for continuous operation, the charging system must provide enough power to charge the batteries while providing power directly to the loads. The batteries must be sized to provide sufficient capacity to supply during the down time of the power sources. The calculations in Table 11-1 show that the 70 watt panel would be sufficient for the system as described. However, at more Northern latitudes, the very reduced number of daylight hours require an alternative source to the solar panel provide adequate daily charging. In this case, wind as well as backup small gas powered generators (5 Watt) will be required to cover the shortfall.

For our experiment, four 6V batteries were arranged in a series / parallel configuration providing about 125 Amp-Hours per 12 Volt set or 250 Amp-hours at 12 Volts. See Figure 11-1. This system used a 70 Watt inverter to provide power to a desktop computer and monitor as well as several laptops in the test van. For AP powering, a lower power inverter can be used to save on power losses and costs. For a three-transceiver node a 150 to 300 watt inverter will suffice. The panel as well as a small battery charger were used to maintain battery charge. This arrangement provided fairly stable AC power. There were no problems with excessive AC inverter electrical noise interfering with the radio operation. The inverter used was a stepped pseudo sine wave type that does put out a fair amount of radio frequency interference.

Figure 11-1: Power Configuration Example for AP Powering



12. Antenna Alignment Procedures

Overview

The alignment of antennas over point-to-point and point-to-multipoint links requires a very methodical approach to ensure the best RF levels and therefore data throughput can be achieved \with the given situation (terrain, climate, tower heights etc.). The following presents the techniques that were employed with mixed success with poor ability to detect 802.11b signals at range when signals grew weak.

RF Monitoring Methods

For the test work several versions of shareware were used to do RF monitoring to allow the set-up and alignment of antennas to establish backhaul links as well as appraise coverage of the APs for clients. This approach generally worked well however there are a number of caveats for the type of software used and the specific tasks it will be applied to.

In the field work carried out for the project, several behaviors were observed that can lead to misinterpretation of the performance of links as well as difficulty in determining if signals are present or not.

Active Scanning RF Monitoring Tools

The most known software Netstumbler was employed by the project to determine RF performance and throughput for that phase of the work. This tool employs active scanning, whereby it interrogates the band to discover APs that may be on air. It will pick up unsolicited transmissions as well (passive). However, it will ignore these transmissions later on if it cannot establish a response to its direct sending of an interrogation message to the AP. Similar behaviour is also seen with the Site Survey utilities that come with client adapter cards as well as APs.

This active scanning is very useful for determining if AP coverage is accessible for users who wish to log in. However, it is not useful for detecting APs that are not in Infrastructure AP mode or are set to not respond to these interrogation messages as a security measure. In the above cases, active scanning (only) will show the APs only when they happen to emit data bursts, and thus will display the presence of the AP very infrequently. In addition, the software is designed to ignore subsequent transmissions if they are not coming from standard APs.

Real Time Response Limitations

A second drawback for antenna alignment is the delay that active scanning tools sometimes exhibit in showing the presence of an active AP. We noted in a number of instances a very significant delay of up to 60 seconds or more before an active

AP will be detected initially or not updated as to the current status. This is very problematical when using these utilities to determine field strengths for the purpose of antenna alignment since the adjustment process is much more efficient if a real time feedback is available for positioning the antenna.

Use in the Cookbook for Coverage Checking and Antenna Alignment

The use of Netstumbler and similar tools is appropriate for establishing links if it is used with recognition of the limitations imposed by their design. For general coverage checking for an AP, in a village for example, it will work well providing the user a good idea of the signal availability. The user must however allow a settling time of at least one minute before moving to a new orientation or location of their adapter card to ensure readings are captured.

For alignment of directional antennas, Netstumbler is of more marginal effectiveness since the user must wait a period of time for the software to capture the AP. Thus initially finding the signal can be a long process using small incremental adjustments and waiting each time to get a broadcast from the distance AP. Once the signal is captured the process can speed up since the interrogation and response cycle is about 1 second allowing the user to make fine adjustments to the antenna at a reasonable rate to get an optimized field strength.

Passive Scanning Tools

Passive tools are available and are commonly available as shareware running on computers that have Linux operating systems. Many commercial packages are available both for Windows and Linux. A well-known shareware called Kismet is available as beta quality software and works on laptops or desktops running a Linux partition. This software is compatible with a number of common WiFi adapter cards, including D-link, Linksys, Orinoco, and SMC. The literature from the Web site and user forums indicates there are known bugs that can cause some stability and compatibility problems. The main feedback is that is useful particularly for antenna alignment purposes.

Real time Response

With passive scanning, real time response will be considerably faster to make procedures such as antenna adjustment much less arduous. The downside of some passive scanners is that they can be difficult to use if there is presence of many spurious signals in the band they are scanning. Since they are passive they will attempt to demodulate and recover packets off any signals in the band. If there are a number of signals especially not 802.11, the real time response of the tool can be impaired. For use in more areas that are less populated and less likely to have interference the above should not be a significant problem.

Use for the Cookbook

Several passive scanning tools will be included in the cookbook particularly for use in cases where directional antennas are involved, requiring fine adjustment to bearing, height, and tilt. Kismet is an example of a tool that has some maturity for use.

Again, these softwares are Linux-based and therefore users must have a computer outfitted with Linux.

The upside of using a Linux platform is that older computers (P1 and P2 class) can be used successfully with Linux. The Linux OS is available from the Web and can be obtained for very low cost or free. Using Linux opens up the possibility to employ many different Linux utilities designed to help operate and manage wireless LANs.

Direct RF Measurement Approach

The classical way to measure RF field strength is to use a CW source transmitter (Continuous Wave) and RF field strength meter or more ideally a sensitive spectrum analyzer. This provides a direct raw observation of the RF levels being provided by the RF link under measurement. This is the most real time technique that can be employed and can allow antennas set-up and link appraisal to be done quickly and effectively. Of course for other measurements concerning the performance at layer 2 this level measurement can only infer that the performance will be ok.

Use in the Cookbook

Direct measurement techniques are definitely part of the cookbook since they are ideal for doing real time antenna alignment procedures on point-to-point links where directional antennas are needed. With immediate response, weaker signals can be found faster and then fine adjustments done to maximize the signal. The RF test equipment will also provide a quick means to ensure connections, coax cables antennas, and WI-FI radios are in good working order.

RF Alignment Procedures

The cookbook procedure for aligning antennas and defining coverage areas will utilize several methods in concert with each other to set up and maintain the WLAN–network.

Specifically, step-by-step procedures are in preparation to guide the user through the process of setting up the AP site, the backhaul links, and the links to each client or user in the community.

Site Location and Installations

The criteria for site locations, antenna selection, use of amplifiers and tower heights have been discussed previously in this report. This resolves most of the major issues in terms of overcoming major obstacles, path losses, link budgets, best locations to achieve reasonable line of site coverage to most users and proximity to supporting systems such as power. Given this has been done with some care, the process to optimize the installations to ensure adequate signal levels must be done.

The main variables that now can be adjusted to ensure adequate receive levels are Antenna Clearance and Fine Adjustment of the Antenna Orientation.

Antenna Clearance and Initial Antenna Bearing Adjustment- Tower Height adjustment

The path to the far-end antenna must be verified to ensure that as much as possible a line of sight (radio line of sight respecting the 1st Fresnel zone clearance of.6J1)

can be seen. For the tower heights selected. The procedures have been described earlier in the report and will be detailed in the cookbook.

Fundamentally, the procedure outline is:

- Map study

  Determine from the map the AGL of the antennas with the proposed tower heights to see that major obstacles are cleared. This requires the use of topographic maps (1:50000 or better) and visual inspection from aerial photos or inspecting the radio right of way from the ground.

- Optical path Inspection

  Once the above is satisfactorily completed, a person can spot the location of the far end antenna on the horizon using the proposed antenna heights through the use of a telescope with the aid of a strobe light, bright flashlight or signaling mirror. If not, the radio link is grazing obstacles or is below the optical horizon which will result in severe signal loss. (See urban signal strengths predictions for non-line-of-sight paths in spreadsheet.)

  Note: Line of sight may not be always achievable. But, the path can still be viable with diffraction as long as the path distance is shortened to make up for the graze loss.

- Tower Height adjustment

  If the line of sight cannot be seen because of obstacles on the path such as buildings or tree ridges, tower height or change in position is required for best performance. If signal strengths are high enough, losses can be tolerated if the path is grazing on short paths. On longer paths, graze losses can destroy any fade margin available on the link in a free space loss context or simply make the path unusable.

- Coarse antenna bearing alignment

  Given the far end antenna location is determined from visual observation, the bearing of the antenna can be set fairly accurately allowing further fine tuning using RF levels as a criteria using appropriate instrumentation.

- Antenna tilt set at 0 degrees initially

- Antenna polarization set to the same orientation as the far-end antenna

- Direct RF alignment coarse bearing

  In the event that visibility is too poor (< 1-2Km) due to weather or pollution, the use of a direct radio direction finding technique is prescribed. Here, the far-end antenna sends a test signal that can be searched for at the local end of the link.

  This method can work as long as a there is a reasonable estimate of antenna height and bearing is determined by doing the initial site analysis from map and loss charts information.

  For this technique to work properly, a passive RF measuring technique as described earlier must be employed to allow efficient mechanical scanning with the directional antenna. The more gain and thus more directional an antenna is, the

more critical small changes in the antennas orientation will be. In addition, higher power should be used if possible (1 Watt limit for ERP).

Fine Adjustment of the Antenna Orientation

This stage of aligning the antenna assumes that a suitable antenna, gain, and polarization as well as tower height/location have been selected and implemented. Once up on the mast, the antenna has roughly oriented to the map bearings and optical or radio direction finding alignment, tilt adjusted to 0 tilt, and polarization set to horizontal or vertical as indicated on the antenna (and identical to the far-end antenna setting)

For this stage, the antennas can be utilizing the actual 802.11 transceivers or use a CW signal with a spectrum analyzer. Here fine adjustments can be done to peak signal performance. It is expected that tilt and polarization will require minimal readjustment. The bearing can be significant with a few degrees change making a profound difference in signal level. Here slight shifts above and below the coarse bearing adjustment should be done to see any improvement.

If 802.11 RF tools are used, passive mode is recommended to be able to adjust the antennas accurately.

In a point-to-point link, once one directional antenna has been peaked, the far-end antenna can now be similarly adjusted to further optimize the bore sight alignment of the two antennas. The best signal strength will be observed when the antennas are exactly in centerline with each other.

A typical range of adjustment is shown below:

- Tilt +/- 5°
- Bearing +/- 10°
- Polarization Alignment +/- 30°.

If there is no signal initially observed, the bearing swing can be widened if the initial bearing adjustment appears way off. Before doing any radical changes, double check that the far end is still transmitting properly and that nothing has changed on the path such as heavy rain or other obstructions causing loss is occurring.

Troubleshooting and VSWR

If the path is still not viable, troubleshooting is required of the antennas cables, transmitters and receivers are as well as any testing software or instrumentation. A main culprit of inadequate signal levels is VSWR. Given all major elements are operational, VSWR test equipment should be obtained and used on the transmitter end of the link. If for some reason the antenna is not impedance matching to the transmitter (50 ohms), a major portion of the RF signal energy is simply dissipated at the transmitter. This can result in measured level losses well over 20 dB making a link unusable. Note that corrosion or moisture in antenna connectors can be a major loss problem as well as coaxial cable damage (crushing or kinking) and antenna feeder problems VSWR of 1.6 or lower is acceptable for most applications.

A detailed troubleshooting table will be part of the cookbook in this section. Many of the problems have been encountered in our field-testing and have been difficult to pin point at times. Since the radio link has some many single points of failure includ-

ing measurement systems, diagnosis often requires additional equipment and configuration to determine the fault.

13. Disaster Recovery

Overview

Networks fail. Whether it's lightning or a bit of static electricity causing the problem, you need a plan to recover from the disaster. This Chapter documents in detail the plan we developed as part of this project. A version will go into the Cookbook.

Confirm the Network is Working

- In the DOS prompt window, use *ipconfig* to confirm the TCP/IP settings of the computer, as follows:

Item	Value	Notes
IP Address	192.168.0.x	**Note1 below
Subnet Mask	255.255.255.0	
Gateway	192.168.0.2	WRT54G Internet gateway / DHCP server
DNS Services	205.211.30.33 205.211.30.21 192.197.88.3	
DNS Suffix	Ottawa.ad.algonquincollege.com Ad.algonquincollege.com Algonquincollege.com	Primary DNS

- Use *ping* to confirm the network connections

  Refer to the Advanced Configuration diagram for all IP addresses and the network layout. If there is a connection problem, confirm all RF and Ethernet cable connections.

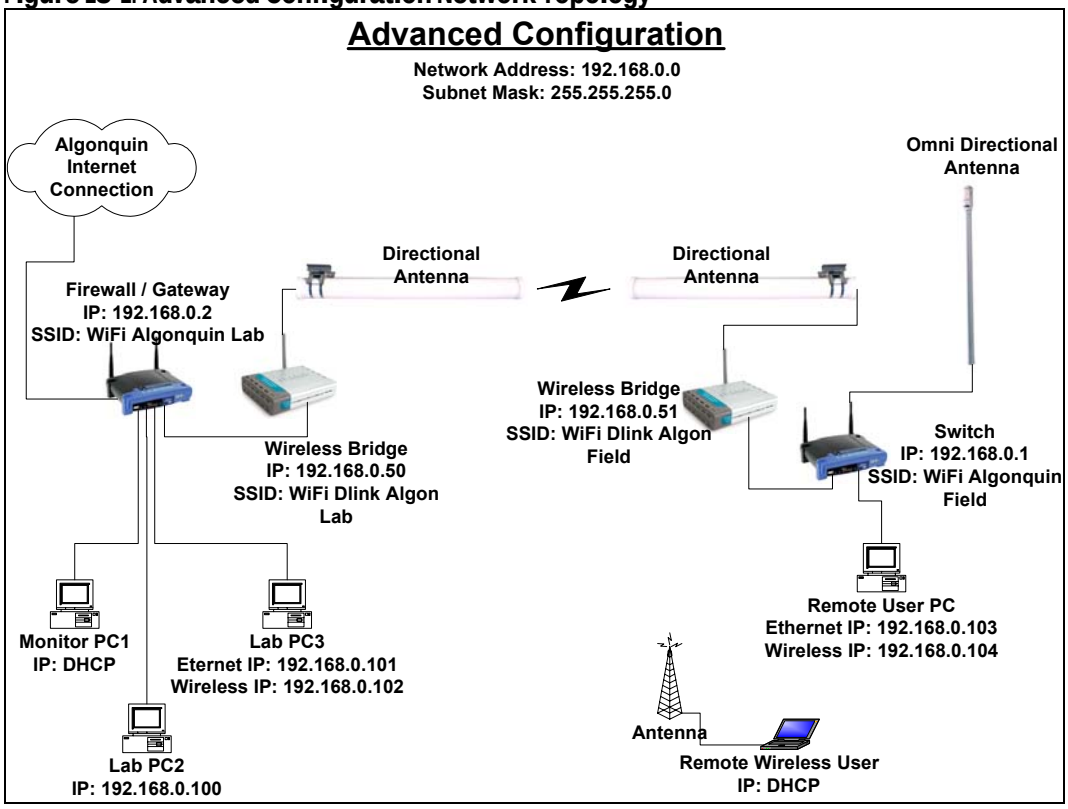
- Use Netstumbler to confirm the presence of an RF link on broadcasting AP's.

****Note 1**: Below is a list of static addresses on the network. Gateway Linksys WRT54G is a DHCP server with a DHCP IP address range of 192.168.0.200 to 192.168.0.50

IP Address	Node
192.168.0.0	Reserved
192.168.0.255	IP Broadcast
192.168.0.1	Field Linksys
192.168.0.2	Lab Linksys
192.168.0.50	Lab D-Link
192.168.0.51	Field D-Link
192.168.0.100	Lab PC2
192.168.0.101	Lab PC3 Ethernet
192.168.0.102	Lab PC3 wireless
192.168.0.103	Field PC Ethernet
192.168.0.104	Field PC wireless

Network Topology

Figure 13-1: Advanced Configuration Network Topology



Known Errors

Below is a list of know errors that can cause network failure.

Antenna Diversity Settings

Equipment	Setting	Value	Notes
Lab WRT54G	TX / RX Antenna	Auto	Not used as AP
Field WRT54G	TX / RX Antenna	Left	Cable to omni-directional
Lab D-Link DWL-900AP+	Antenna setting	External	
Field D-Link DWL-900AP+	TX / RX setting	External	
Lab PC D-Link DWL-G520	Antenna switch	1	External antenna
Lab PC D-Link DWL-G520	Antenna Tx	1	External antenna
Field PC D-Link DWL-G520	Antenna switch	1	External antenna
Field PC D-Link DWL-G520	Antenna Tx	1	External antenna

Beacon Interval Settings

- Ensure the D-Link and WRT54G Beacon Interval is 100ms.

- If the Beacon Interval is too short, the RF link will not be detected by listening devices.

Field D-Link DWL-900AP+ Start-up Crash

- If the field D-Link is unresponsive after power up (i.e., cannot ping IP address), power cycle the D-Link. The device has occasionally frozen during initialization after power-up and is unresponsive.
- If accessible, ensure that the D-Link WAN LED is flashing or on solid.
- If the LED is off and there is no sign of flashing, then the D-Link has crashed during initialization.

Field Linksys WRT54G Start-up Crash

- If the field Linksys is unresponsive after power up (i.e., cannot ping IP address), power cycle it.
- If the device is still not responsive, then reload the firmware *(refer to the section "*Reload the Firmware*" on page 13-10)*

D-Link card frequency range

D-Link wireless cards have a frequency detection range of 2.4 GHz to 2.462GHz. However, the Linksys AP broadcast range is able to go higher than the D-Link wireless card. To avoid mismatches, ensure that the Linksys WRT54G SSID broadcast channel is below 12.

Router / Wireless Bridge Failure Procedures

If the D-Link DWL-900AP+ wireless bridges or the Linksys WRT54G router/4-ports switches begin to act intermittently or are unresponsive, follow the procedures below until the devices are acting as expected.

Power Cycle the Device

Note: If the WRT54G or DWL-900AP+ are power cycled, all user settings will be saved and not lost.

Linksys WRT54G

When the Linksys is initializing after a power cycle, the Power LED on front will flash. Normal operation will begin when the Power LED stops flashing. Check connections to ports and ensure that corresponding LED's on front panel (i.e., WLAN, Internet, and ports 1-4) are flashing to indicate traffic activity.

D-Link DWL-900AP+

When turned on, the DWL-900AP+ Power LED will be on solid. It does not flash during initialization. If after power cycle the D-Link is still not responsive, try power cycling device again. The Field D-Link intermittently freezes during initialization. If the WAN LED is off, then the D-Link has probably frozen during initialization and needs to be restarted.

Check all connections and ensure that the corresponding LED's are flashing to indicate traffic activity. The WAN port is associated with the antenna and the LAN port is associated with the Ethernet port.

Reload the Firmware

If power cycling the device does not restore functionality, then reload the firmware. There are two possible scenarios when reloading the firmware.

- Communication with the device and access to the web interface is still possible.

  In this case, to reload the firmware, the user should:

  - Upgrade the firmware
  - Factory reset the device, using the web interface or the RESET button
  - Power cycle the device
  - Change the computer IP to match the factory default network address of the device *(refer to the section "*Default Settings*" on page 13-13)*
  - Reload the user settings.

- Communication with the Linksys and access to the web interface is not possible.

  In this case, to perform a factory reset, the user should:

  - Factory reset the device using the RESET button
  - Power cycle the device
  - Change the computer IP to match the factory default network address of the device *(refer to the section "*Default Settings*" on page 13-13)*
  - Upgrade the firmware
  - Factory reset the device using the RESET button
  - Power cycle the device
  - Reload the user settings.

Firmware Filenames

- Linksys WRT54G: Firmware_Satori-4_0G.bin

  Firmware_Satori-4_0G.bin file will load the third party Sveasoft firmware Satori-4.0 v2.07.1.7sv onto the Linksys. This firmware allows for antenna diversity settings on the Linksys.

- D-Link DWL-900AP+: dwl900AP+_firmware_307b1.bin

  dwl900AP+_firmware_307b1.bin file will load the official D-Link firmware version 307b1.

Loading the Firmware

WRT54G

Refer to the section “Network Topology” on page 13-8. Access the webpage interface by typing in the IP address of the WRT54G into the address bar of the web browser (preferably Internet Explorer).

- Select the Administration Tab
- Select the Firmware Upgrade Tab
- Select Browse
- Select the file Firmware_Satori-4_0G.bin

Note: If the firmware upgrade is interrupted before completion, the Linksys may no longer be functional. Ensure that the power will not be turned off during the upgrade. Only upgrade firmware from a computer that is directly connected to the Ethernet port; do not upgrade firmware over the RF link.

- Select the Upgrade button
- The Upgrade status bar will begin to move
- Select continue once the upgrade is complete

All user settings will remain the same; therefore communication with Linksys WRT54G will still be possible.

Note: after loading firmware, always reset factory defaults and power cycle the device.

D-Link

Refer to the section “Network Topology” on page 13-8. Access the webpage interface by typing in the IP address of the DWL-900AP+ into the address bar of the web browser (preferable Internet Explorer).

- Select the Tools Tab
- Select the firmware Button on the left-hand side
- Select the Browse Button
- Select the file dwl900AP+_firmware_307b1.bin

Note: If the firmware upgrade is interrupted before completion, the Linksys may no longer be functional. Ensure that the power will not be turned off during upgrade. Only upgrade the firmware from the computer that is directly connected to Ethernet port; do not upgrade firmware over the RF link.

- Select the Apply button
- The upgrade status bar will begin to move
- Select continue once the upgrade is complete

All user settings will remain the same; therefore communication with D-Link DWL-900AP+ will still be possible.

Note: After loading the firmware, always reset the factory defaults and power cycle the device.

Restoring Factory Defaults

Factory reset can be performed using the web interface or the RESET button on the back of the device.

WRT54G

Button method:

- There is a brown button labelled RESET located on the back of the Linksys WRT54G.
- To perform a factory default reset, press and hold the button until you see the Power LED on the front panel begin to flash.

Webpage interface method:

- Access the webpage interface by typing in the IP address of the WRT54G *(refer to the section "*Network Topology*" on page 13-8)* into address bar of the web browser (preferably Internet Explorer).
- Select the Administration Tab
- Select Factory Defaults
- Check Yes, for Restore Factory Defaults
- Select Save settings.
- Watch and ensure that Power LED on front panel begins to flash, which shows WRT54G is re-initializing.

Note: Factory Defaults have now been restored. Refer to the section "Default Settings" on page 13-13.

D-Link

Button method:

- There is a brown button labelled RESET located on the back of the D-Link DWL-900AP+
- To perform a factory default reset, press and hold the button until you see all LED's on front panel to flash off and back on.

Webpage interface method:

- *Refer to the section "*Network Topology*" on page 13-8.* Access the webpage interface by typing in the IP address of the DWL-900-AP+ into the address bar of the web browser (preferably Internet Explorer).
- Select the Tools Tab
- Select the System Button on left-hand side
- Select the Restore button
- Watch and ensure that all LEDs on front panel flash, which shows that the DWL-900AP+ is re-initializing.

Note: Factory Defaults have now been restored. Refer to the section “Default Settings” on page 13-13.

Default Settings

Once factory defaults are loaded onto the devices, the default IP addresses and subnet masks should be installed, as listed below.

Linksys WRT54G Factory Defaults:

IP Address	192.168.1.1
Subnet mask	255.255.255.0

D-Link DWL-900AP+ Factory Defaults:

IP Address	192.168.0.50
Subnet mask	255.255.255.0

To communicate with devices, the computer’s IP address and subnet mask will have to be set to have the same network address as the device.

14. Technical Report Addendum

Overview

This chapter supplements the work reported in the technical report issued in August 2004. The activities summarized occurred from end-August to mid-November. During this time, additional investigations were done in the following areas:

- Behaviour of active scanning 802.11 network detection software such as NetStumbler for use in antenna alignment with weak signals
- Testing of several passive scanning techniques operating on Linux software.
- Improvement in hardware to make towers safer and easier to put up
- Trying out behaviour of several different adapter cards for use as part of a RF measurement unit
- Troubleshooting and discovering faults in 802.11b D-Link bridges
- Replacement of D-Link DWL 900 with DWL2100 type AP bridges
- Reconfiguring the DWL2100 for bridge operation and non-diversity operations
- Range tests and demonstration of the system.

RF Measurement Systems

Further investigation of the behaviour of 802.11 RF and network discovery tools was done to find out the basis of intermittent detection of the 802.11b signals being emitted by the Algonquin labs wireless bridge.

Several significant idiosyncrasies were found with NetStumbler and other active scanners in doing range and antenna alignment procedures:

- With more distant signals, a long delay can occur before a solid indication of the presence of a signal can often occur.

  This problem was due in part to the adapter card scanning for all the channels for active APs and missing the beacon signal from the far-end AP.

- Active scanners require sending a packet back to the originating AP to verify the signal and link parameters.

  Under weak signal conditions, the probe signal is not detected and the scanner fails to indicate the presence of the AP.

- Measurements taken by the NetStumbler and similar software tools lag the actual measurement indicated onscreen by up to 10 seconds compared to the actual received level

In antenna alignment operations, this lag had to be accommodated in adjusting the antenna bearing. This lag also resulted in missing signals that were very weak, and thus would mislead setup procedures.

Passive Scanning Tools

To overcome some of active scanning limitations, several groups have developed passive scanning applications that can run mainly on PCs that run the Linux or UNIX operating systems. The most popular software tool is called “Kismet”. Kismet which will work with a range of adapter cards and APs (that have Kismet loaded on them) over a LAN.

Passive scanning signal emitted from APS as well as adapter cards were detected very quickly and at very low signal levels. The immediate indication of signal level on the computer screen made operations such as antenna alignment much easier.

The tool provides the signal source identity (SSID), mode, MAC ID, S/N ratio, and noise and signal power using RSSI bar graph indicator.

The main drawback of Kismet and similar tools is that they require the PC or Laptop be loaded with a Linux partition. This was done for the testing. However, it took some time to gather all the applications required to run the system properly.

A CDROM was produced that contains the necessary software and instructions to run Kismet with a PCI on desktop or PCMCIA adapter card on a laptop. A D-Link DWL-150 and US robotics USB adapter were also tried, but were found to be incompatible with the available drivers for adapters on Linux.

Kismet on the AP

A local-remote variant of Kismet was tried, with the AP being loaded with a version of Kismet that allowed remote reporting to a laptop over Ethernet. This worked well, but did not report information on actual signal levels at the AP that was not as useful. This deficiency is being addressed and a more capable version is due out in early 2005.

Tower Hardware Improvements

The continued using of the tower brought to light some concerns on how to better rig the tower. The guy wires were improved using more rugged clamps and special wire “thimbles” as described in the cookbook to prevent wire shearing. The clamps used on the wires were also upgraded and doubled to prevent any wire slippage. These changes were checked with published practices for commercial antenna tower installations. These guidelines were documented in the cookbook in the chapter on tower installation.

Compatibility Testing with Several Different Adapter Cards

As part of the RF field testing work, several different adapter cards were tried besides the original units purchased for the project. For use with NetStumbler it was found that certain cards were not compatible with the software. These were found

to be older models of the DWL PC cards (DWL 600-610) and Orinoco card that have been based an Agere chipsets.

Fortunately, the newer versions of these cards utilize TI Asics and work well with both Kismet and NetStumbler software. It was also verified that US Robotics Broadcom units worked with NetStumbler fairly well. All the cards functioned well in standard use.

Troubleshooting the DWL 900s

The DWL900s used for the point-to-point backhaul link were quite successfully used for the first portion of the project. However, significant problems started to become apparent in the setting up and maintaining of the link as time went on. Performance also deteriorated slowly over time, with the units providing less throughput for the same channel characteristics.

Field DWL900

The field DWL900 appeared to have increasing difficulty locking into the signal from the college unit, even at higher signal levels. Benchmark tests were repeated to verify operation. In these tests bridging would occur. However, it would take a number of minutes (compared to seconds before) for the bridges to lock onto each other. This could be attributable to many things, including interference. However, there were also indications of possible equipment problems, when the unit would freeze during bootup and requiring a reset/restart to restore operation. Once the signal was captured, normal function would be observed.

The above behaviour suddenly became worse in October with the DWL900 field unit losing bridge connections suddenly or going into a lower operating bandwidth mode, requiring a reset and reconnection to restore normal baud rates. These would be maintained for a short duration and then problems would re-start. At this point, it also appeared to be very sensitive to temperature and failed repeatedly at temperatures below 12 C (estimated).

Lab DWL900

The DWL900 lab unit appeared much more stable. However, there were continuing problems. The unit lapsed back to diversity operation infrequently, despite the firmware settings. In monitoring the unit with NetStumbler in the field, it was found that the DWL900 would not always respond to the probe signal from the adapter card. This increased the time to detect the signal and made it difficult to orient antennas. This behaviour was distance-dependent and got worse as transmission delay increased.

The loading of the DWL900 into the feed cable to the roof-mounted antenna showed some VSWR issues. This was noted by changing lengths of coax segment in the room and observing the local field emission form the D-Link box. The VSWR was not measured directly. However, from relative readings we estimated it was over 2:1, which is significantly too high.

Replacing the DWL900s with DWL2100s

It was decided to change the 900s with the same model since there was increasing degradation in the field unit's behaviour. The DWL900 was found to be discontinued by D-Link. As a result, it was very hard to get.

The next generation unit was the DWL2100 that is an 802.11g unit with 802.11b retro-compatibility. This model offers a wide range of features, including those required for doing point-to-point LAN bridging.

In the literature from D-Link, some known deficiencies were corrected in the DWL2100 design from the DWL900. One of the problems that stood out was to do with impedance matching problems with the diversity external antenna. The others were to do with the radio MAC and that may have had some impact on our performance. The antenna problem causes VSWR (voltage standing wave ratio) problems which results in not all the power available from the transmitter being coupled into the cable. The same problem can also cause the incoming signal from the antenna to be reduced in level. This can significantly impair the range that can be achieved with reliable data throughput.

In field testing, the DWL900 did have significant range. However, the RF Signal levels varied from test to test and generally were at the low end of the expected values. These lower levels also resulted in reduced digital bandwidth available from the channel.

Reconfiguring the DWL2100

The DWL2100 is a fully featured AP and bridge system. It can be configured as a standard AP, a point-to-point bridge, and a point-to-multipoint bridge (the DWL900 cannot be). The unit offers 802.11g as a default mode of operation and can be commanded to operate in auto-adaptive or manual mode. The unit can provide up to 108.0 Mb/s in a turbo mode for short range down to 1 Mb/s in 802.11 mode for very long links.

For the wireless backhaul, the DWL2100 was placed into point-to-point bridge operation to link the Internet gateway (LinkSys in Lab) to the AP bridge (LinkSys in the field). This was the exact configuration used for the DWL900.

Figure 14-1: Setting the Mode

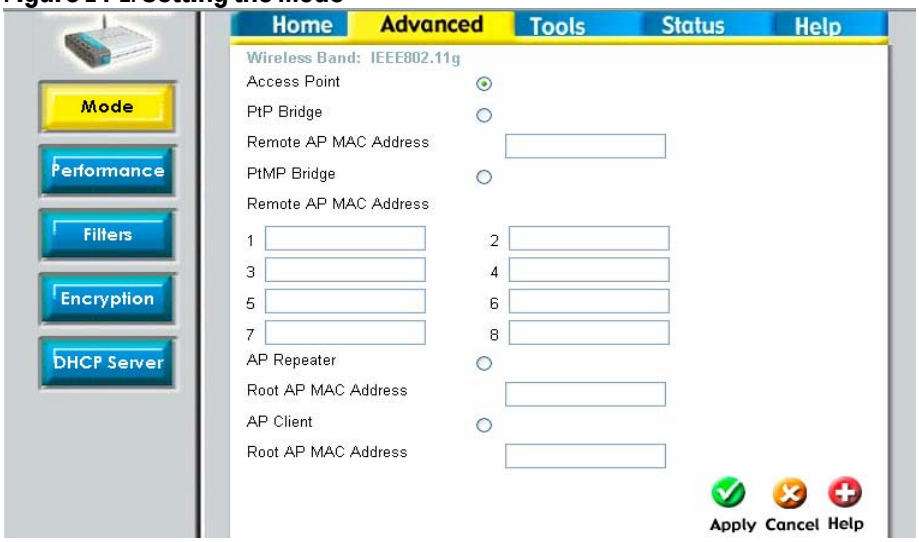
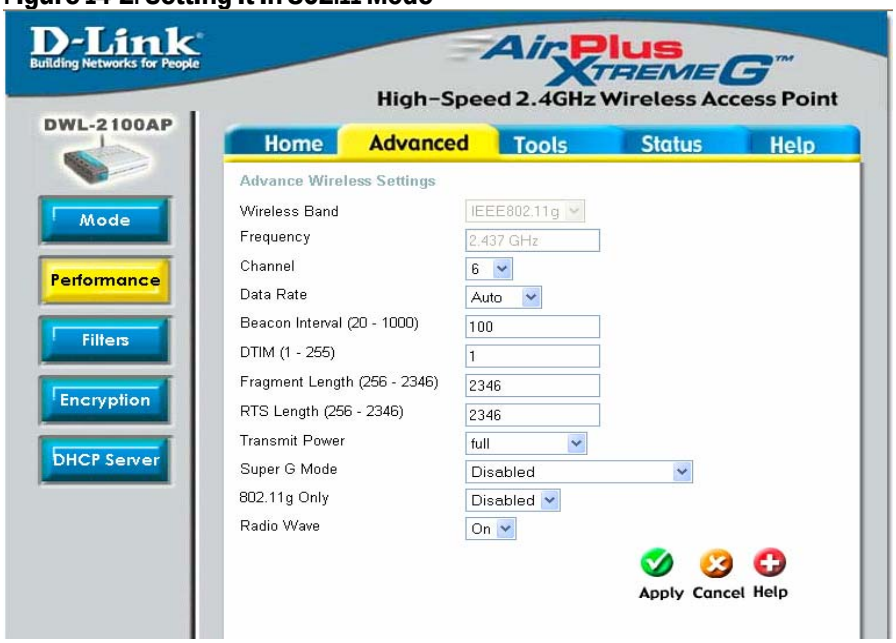


Figure 14-2: Setting it in 802.11 Mode



For the field test, a static address was assigned to the DWL 2100's. The one in the lab was assigned 192.168.0.52 and the field unit was assigned IP 192.168.0.53. This placed the units in the same domain as the gateway and the AP hub (LinkSys) in the field.

Figure 14-3: Setting the IP Address

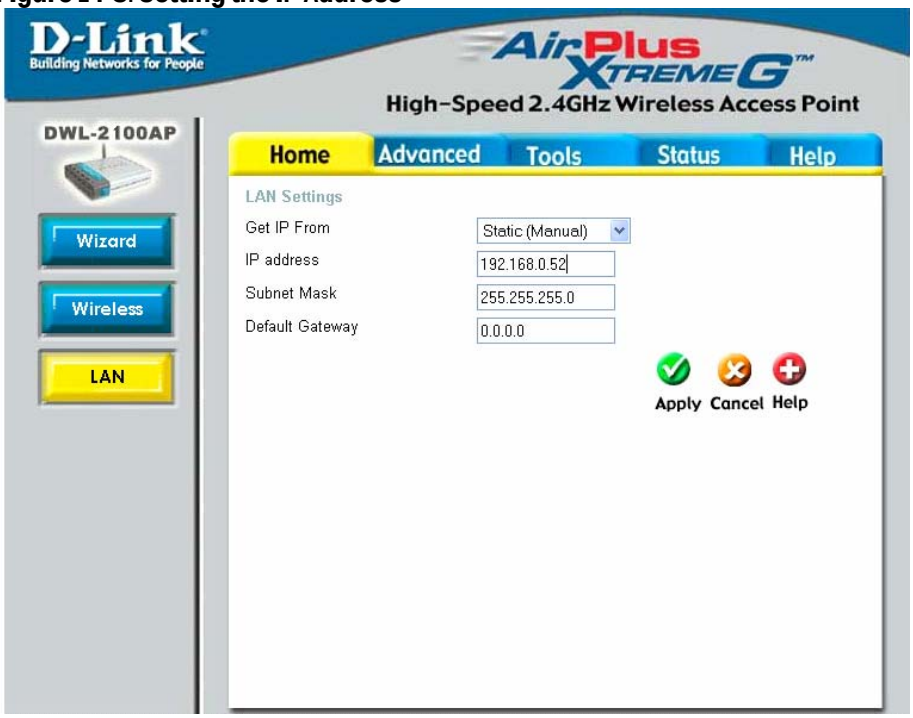
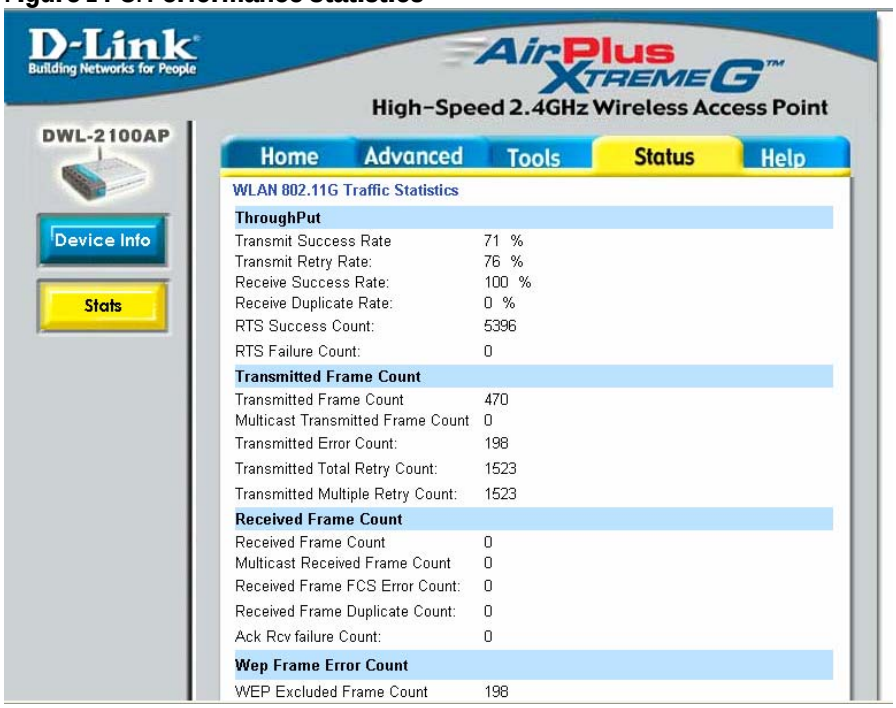


Figure 14-4: DHCP Server

pport.dlink.com/techtool/dwl2100ap/emulator/html/dhcpdyna.html

Figure 14-5: Performance Statistics



The DWL 2100 also offers a MIBs (management Information base) like report page to allow the user to get immediate reports on the system performance. This is in complement to the OAM environment that can be accessed through Telnet discussed below.

The diversity settings of the DWL2100s had to be changed by using a TELNET session to access the operating systems. This was done through the command prompt on a PC connected via Ethernet cable to the DWL2100. This provided access to an OAM / SNMP environment that was not previously available with the DWL900s. In this environment, by asking for the list of commands, the command for antenna setting and diversity disabling are there. The syntax is simply either typing set ant 1 on, set diversity off, and so forth. The power of the transmitter can be set here as well as maximum.

The OAM environment allows access to port statistics, RF receive levels of all stations the DWL2100 is receiving and host of other features. This environment is usually only available with commercial units.

DWL2100 OAM Command Set Including SNMP

Table 14-1: List of Access Point CLI Commands

config wlan	config wlanX
connect bss	connect to bssX
del acl	Delete Access Control List
del wdsacl	Delete WDS Access Control List
del key	Delete Encryption key
find bss	Find BSS
find channel	Find Available Channel
find all	Find All BSS

[Note: The above command instructs the unit to scan all channels and find any APs or Bridge units that it is receiving. It also provides readout of the signal level power for all the stations received. This feature can be used as a test system to locate signals and adjust antenna alignments without requiring a special test receiver. The command was used and it proved to be very like Kismet using passive scanning to find signals.]

dhcps help	Display DHCP Server Command Help
get 11gonly	Display 11g Only Allowed
get 11goptimize	Display 11g Optimization Level
get 11goverlapbss	Display Overlapping BSS Protection
get acl	Display Access Control List
get wdsacl	Display WDS Access Control List
get wdsap	Display WDS Access Point
get aging	Display Aging Interval
get antenna	Display Antenna Diversity
get association	Display Association Table
get authentication	Display Authentication Type
get autochannelselect	Display Auto Channel Select
get apmode	Display AP Mode(runtime)
get apmodenext	Display AP Mode after reboot
get beaconinterval	Display Beacon Interval
get burstSeqThreshold	Display Max Number of frames in a Burst
get burstTime	Display Burst Time
get channel	Display Radio Channel
get cipher	Display Encryption cipher
get config	Display Current AP Configuration
get countrycode	Display Country Code
get ctsmode	Display CTS mode
get ctsrate	Display CTS rate
get ctstype	Display CTS type
get dhcpc	Display DHCP Clinet State
get domainsuffix	Display Domain Name Server suffix
get dtim	Display Data Beacon Rate (DTIM)
get encryption	Display Encryption Mode
get extendedchanmode	Display Extended Channel Mode
get eth2wlan	Display Eth2Wlan Broadcast packet filter state
get fragmentthreshold	Display Fragment Threshold
get frequency	Display Radio Frequency (MHz)
get gateway	Display Gateway IP Address
get groupkeyupdate	Display Group Key Update Interval (in Seconds)
get hardware	Display Hardware Revisions
get hostipaddr	Display Host IP Address
get ipaddr	Display IP Address
get ipmask	Display IP Subnet Mask
get key	Display Encryption Key
get keyentrymethod	Display Encyrption Key Entry Method
get keysource	Display Source Of Encryption Keys
get login	Display Login User Name
get nameaddr	Display IP address of name server
get power	Display Transmit Power Setting

get radiusname	Display RADIUS server name or IP address
get radiusport	Display RADIUS port number
get rate	Display Data Rate
get rtsthreshold	Display RTS/CTS Threshold
get rootapmac	Display Root AP MAC Address
get rootapinfo	Display Root AP Information
get shortpreamble	Display Short Preamble Usage
get shortslottime	Display Short Slot Time Usage
get sntpserver	Display SNTP/NTP Server IP Address
get ssid	Display Service Set ID
get ssidsuppress	Display SSID Suppress Mode
get station	Display Station Status
get SuperG	Display SuperG Feature Status
get systemname	Display Access Point System Name
get sta2sta	Display wireless STAs to wireless STAs connect state
get eth2sta	Display ethernet to wireless STAs connect state
get telnet	Display Telnet Mode
get timeout	Display Telnet Timeout
get tzone	Display Time Zone Setting
get uptime	Display UpTime
get wirelessmode	Display Wireless LAN Mode
get wlanstate	Display wlan state
help	Display CLI Command List
ping	Ping
reboot	Reboot Access Point
quit	Logoff
set 11gonly	Set 11g Only Allowed
set 11goptimize	Set 11g Optimization Level
set 11goverlapbss	Set Overlapping BSS Protection
set acl	Set Access Control List
set wdsacl	Set WDS List
set aging	Set Aging Interval
set antenna	Set Antenna

[Note: The above command allows setting external antenna only – non diversity operation.]

set authentication	Set Authentication Type
set autochannelselect	Set Auto Channel Selection
set apmode	Set AP Mode
set beaconinterval	Modify Beacon Interval
set burstSeqThreshold	Set Max Number of frames in a Burst
set burstTime	Set Burst Time
set channel	Set Radio Channel
set cipher	Set Cipher
set ctsmode	Set CTS Mode
set ctsrate	Set CTS Rate
set ctstype	Set CTS Type
set dhcpc	Set DHCP Clinet State
set domainsuffix	Set Domain Name Server Suffix

set dtim	Set Data Beacon Rate (DTIM)
set encryption	Set Encryption Mode
set extendedchanmode	Set Extended Channel Mode
set eth2wlan	Set Eth2Wlan Broadcast packet filter state
set factorydefault	Restore to Default Factory Settings
set fragmentthreshold	Set Fragment Threshold
set frequency	Set Radio Frequency (MHz)
set gateway	Set Gateway IP Address
set groupkeyupdate	Set Group Key Update Interval (in Seconds)
set hostipaddr	Set Host IP address
set ipaddr	Set IP Address
set ipmask	Set IP Subnet Mask
set key	Set Encryption Key
set keyentrymethod	Select Encryption Key Entry Method
set keysource	Select Source Of Encryption Keys
set login	Modify Login User Name
set nameaddress	Set Name Server IP address
set password	Modify Password
set passphrase	Modify Passphrase
set power	Set Transmit Power
set radiusname	Set RADIUS name or IP address
set radiusport	Set RADIUS port number
set radiussecret	Set RADIUS shared secret
set rate	Set Data Rate
set rootapmac	Set Root AP MAC Address
set rtsthreshold	Set RTS/CTS Threshold
set shortpreamble	Set Short Preamble
set shortslottime	Set Short Slot Time
set sntpserver	Set SNTP/NTP Server IP Address
set ssid	Set Serviceset ID
set ssidsuppress	Set SSID Suppress Mode
set SuperG	Super G Features
set systemname	Set Access Point System Name
set sta2sta	Set wireless STAs to wireless STAs connect state
set eth2sta	Set ethernet to wireless STAs connect state
set telnet	Set Telnet Mode
set timeout	Set Telnet Timeout
set tzone	Set Time Zone Setting
set wlanstate	Set wlan state
set wirelessmode	Set Wireless LAN Mode
timeofday	Display Current Time of Day
version	Software version
snmp adduser	Add User To SNMP Agent
snmp deluser	Delete User From SNMP Agent
snmp showuser	Show User In SNMP Agent
snmp setauthkey	Set User Auth Key
snmp setprivkey	Set User Private Key
snmp addgroup	Add User Group

snmp delgroup	Delete User Group
snmp showgroup	Show User Group
snmp addview	Add User View
snmp delview	Delete User View
snmp showview	Show User View
snmp addcomm	Add Communication String
snmp delcomm	Delete Communication String
snmp showcomm	Show Communication String
snmp addhost	Add Host To Notify List
snmp delhost	Delete Host
From Notify List	
snmp showhost	Show Host In Notify List
snmp authtrap	Set Auth Trap Status
snmp sendtrap	Send Warm Trap
snmp load_default	Load SNMP Default Setting
tftp get	Get a file from TFTP Server.
tftp uploadtxt	Upload the configuration of the device to TFTP Server.
tftp srvip	Setup the TFTP Server IP address.
tftp update	Update the file to the device.
tftp info	Information about the TFTPC setting.

Range Tests and Demonstration of the System

Highly Improved Performance

The DWL2100 was first used with the lab DWL900 in the lab locally and then over a short hop of 800 meters. The DWL2100 operated satisfactorily with the DWL900, despite the degradation observed with the DWL900s RF output at that time. Here the link achieved over 4.5 Mb/s throughput on average but was not consistent.

When the second DWIL2100 arrived, the backhaul bridge was tried with again with the DWL2100s. The performance was very acceptable, with constant levels and throughputs topping 5.6 Mb/s. RF levels were found to be over 10 dB higher with no unexpected dropouts as observed with the DLW900 (cause thought to be diversity switch not staying disabled).

In addition, it was found that the active scanning Netstumbler WLAN network detection software detected the DWL2100 signals from the Lab immediately, unlike the DWL900 where up to a minute or more would elapse before detection.

The DWL2100 was successfully bridged a 2.2 Kilometres using a 14 dB antenna as well as the 28 dB antenna. Operating the DWL2100 in the Lab as an AP direct to laptop connection was maintained to over 2.0 kilometres using a 12 dB antenna mounted on the windshield of the test vehicle.

The throughput in bridge mode with the 28 dB antenna achieved up to 6.0 Mb/s through the Linksys bridge in the test vehicle. The radio throughput was 802.11b at 11.0 Mb/s. This was found to be stable with no significant drops out during the several hours of operation and monitoring. Three laptops were linked via the AP and one computer via an Ethernet connection were set to stream video or ping continu-

ously through the bridge to the lab gateway. There was no noticeable problems in the AP or the bridge link causing drops outs during the test period.

RF receive levels were measured from the 28 dB parabolic antenna. These were observed on the Laptop Netstumbler RF test unit using the US Robotics modified card. The levels were as high as -60 dBm with an average of around -63 dBm. This was with the antenna elevated 3 meters with marginal line of site (< 0.6F) clearance. With this level, the link could be easily be extended to over 6.5 kilometres or further with levels of approximately -78dBm or better to provide around 5.5 MB/s radio throughput for around 3.0 Mb/s Ethernet throughput.

Using the DWL900, levels of -87dbm at 6.7 kilometres were achieved using a 28 dBi parabolic antenna at 3 Meters (Fallowfield Mall near Pinecrest). With the same setup, it is expected that the DWL2100 would provide at least 8 dB better.

Final Comments

The concepts as originally developed for validation in this test work have proved out to be quite usable as a basis for deploying rural Wi-Fi.

Several important lessons were learned in this work, particularly about the reliability and quality of the current range of wireless products offered by well-known vendors. The phrase *buyer beware* certainly comes to mind here as well as well as never assume things will not change significantly over time. Our experience with the D-Link bridge units showed problems in out of the box performance variances as well as degradation over time as was the case with the D-link field unit. This caused a lot of sleuthing trying to figure out what part of the system was going down such as connector problems, path problems, RF output stage problems and so forth. The intermittent nature of the problems made it difficult to pin down the problems.

The wisdom to pass along here is that in selecting equipment to use in the field acceptance should be done using several units to weed out units that don't meet advertised specifications. The quality control used for consumer equipment is very marginal at is one of the reasons it is lees expensive then commercial grade counterparts. For situations where the performance envelope is being pushed, the actual performance capabilities must be known or it will be difficult to pin down problems if assumptions are incorrect about unit's characteristics.

15. Appendix A: Acronyms

The acronyms in Table 15-1 are the ones used in this milestone report and in the previous ones.

Table 15-1: Acronyms

Acronym	Meaning	Definition	Notes
AC	Alternating Current		See DC
ACK	Acknowledgement		
AGL	Above Ground Level		Used for specifying how high a tower or other object is above its immediate surroundings
AP	Access Point	A radio access point (wireless data base station) that is used to connect wireless data devices (stations) to a wireless local area network (WLAN).	
ASL	Above Sea Level		
BER	Bit Error Rate	A ratio of the number of errors to data bits received on a digital circuit.	BER is usually expressed in exponential form.
BT	Bhutan Telecom		
CDR	Call Data Record	Computer records, often stored on tape, which record information about each telephone call sent or received	
CIDA	Canadian International Development Agency		
CPE	Customer Premises Equipment	All telecommunications terminal equipment located on the customer's premises	Including telephone sets, private branch exchanges (PBXs), data terminals, and customer-owned coin-operated telephones.
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance		A low-level protocol used in Ethernet
dB	DeciBel	A technique for expressing voltage,	Typical references include volts, watts or

Acronym	Meaning	Definition	Notes
		power, gain, loss or frequency in logarithmic form against a reference.	Hz. Decibels are calculated using the expression: dB = 10*log(x/y).
dBi	DeciBel		Referenced to an isotropic radiator
dBm	DeciBel		Referenced to milliwatts
DC	Direct Current		See AC
DHCP	Dynamic Host Configuration Protocol	Protocol for automating the configuration of computers that use TCP/IP	
DIFS	Distributed Point Coordination Function Inter-Frame Space		
DRMASS	Digital Radio Multiple Access Subscriber System		
EHAAT	Effective Height Above Average Terrain		One of the means used to characterize an antenna's height.
EIRP	Effective Isotropic Radiated Power		
EMI	Electromagnetic Interference		
ERP	Emitter, Receiver, Processor; Exterior Router Protocol		
FRCS	Federal Reserve Communications System		
FTP	File Transfer Protocol		
F/B	Front to Back Ratio		
GoS	Grade of Service	A characteristic of a communications system.	For example, in a telephone network, this refers to the probability that a phone user will be able to get a free trunk when they lift the telephone receiver.
GHz	Gigahertz	A frequency measurement which equals one billion hertz.	
GPS	Global Positioning System	Network of 24 Navistar satellites that orbiting the Earth at 11,000 feet above the surface that provide signals that allow the calculation of position information.	Used for determining the latitude, longitude, and elevation of a location
Hz	Hertz	A radio frequency	

Acronym	Meaning	Definition	Notes
		measurement (one hertz = one cycle per second).	
IC	Industry Canada		A Canadian Government department
ID	Identification		
IEEE	Institute of Electrical and Electronics Engineers		
IP	Internet Protocol	A set of instructions defining how information is handled as it travels between systems across the Internet.	
IPOP	Internet Point of Presence	POP for Internet	
ISM	Industrial, Scientific and Medical radio bands	A frequency band that is authorized for the use of instrument, scientific and medical radio devices.	Also used for Wi-Fi
ISP	Internet Service Provider		
IT	Information Technology		
LAN	Local Area Network	A small data network covering a limited area, such as within a building or group of buildings.	
LCR	Least Cost Routing		
LOS	Line of Sight	A description of an unobstructed radio path or link between the transmitting and receiving antennas of a communications system.	
MAC	Medium Access Control	A system of rules used to move data from one physical medium to another	
Mb/s	Megabits per second		
MPPT	Maximum Power Point Tracking		Used in solar energy
MTBF	Mean Time Between Failure		
NAT	Network Address Translation		NAT devices translate IP addresses so that

Acronym	Meaning	Definition	Notes
			users on a private network can see the public network, but public network users cannot see the private network users.
NCIT	National Capital Institute of Telecommunications		
NEMA	National Electrical Manufacturers Association		As in “NEMA box”
NIC	Network Interface Card		
NOC	Network Operations Centre	A facility or organization responsible for maintaining, monitoring, and troubleshooting a network infrastructure.	
OAM	Operations, Administration and Management		
OS	Operating System		
OSPF	Open Shortest Path First	An IP routing protocol	OSPF
PC	Personal Computer		
PCI	Peripheral Component Interconnect		The main bus interconnection standard in PCs
PCMCIA	Personal Computer Memory Card International Association		PC card standard
PDA	Personal Digital Assistant		
POP	Point of Presence	A place where there is a major connection to the Internet	
PSTN	Public Switched Telephone Network	Standard domestic and commercial phone service.	
PV	Photovoltaic		
QoS	Quality of Service	The ability to define a level of performance in a data communications system.	
RADIUS	Remote Authentication Dial-In User Server / Service	A server for authentication, authorization and accounting of endpoints and endpoint aliases.	
RF	Radio Frequency		

Acronym	Meaning	Definition	Notes
RIP	Routing Information Protocol	One of the most commonly used Interior Gateway Protocols in the Internet, which helps network routers dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are. Although RIP is still actively used, many experts considered it as obsoleted by OSPF.	
RLOS	Radio Line Of Sight		
RTS	Ready To Send		
RX	Receive		
SBC	Single Board Computer		
SNMP	Simple Network Management Protocol	A standard protocol used to communicate management information between the network management stations (NMS) and the agents (e.g., routers, switches, network devices) in the network elements.	By conforming to this protocol, equipment assemblies that are produced by different manufacturers can be managed by a single program.
SNR	Signal to Noise Ratio	Final relationship between the video or audio signal level to the noise level. Ratio of the signal power to the noise power in a specified bandwidth, expressed in dbW	
SOHO	Small Office-Home Office		
SSH	Secure Shell.	A security system that lets you create encrypted tunnels for any Internet protocol via port forwarding	
SSID	Service Set Identifier	A unique identifier for an Access Point	
S/I	Signal to Interference		

Acronym	Meaning	Definition	Notes
	ratio		
S/W	Software		
TCO	Total Cost of Ownership		
TKIP	Temporal Key Integrity Protocol	A new security protocol that is used in the 802.11 system that uses dynamically changing keys	Replaces the static security keys used in the original 802.11 system. Formerly WEP2.
TX	Transmit		
UPS	Uninterruptible Power Supply		
USB	Universal Serial Bus	An industry standard data communication interface that is installed on personal computers.	
UV	Ultraviolet		
VAC	Volts AC		
VLAN	Virtual Local Area Network	As opposed to LAN. a logically segmented network mapped over physical hardware.	
VoIP	Voice over Internet Protocol	A technology for transmitting ordinary telephone calls over the Internet using packet-linked routes.	VoIP is not simply for voice over IP, but is designed to accommodate two-way video conferencing and application sharing as well.
VPN	Virtual Private Network	Private, or restricted, communications networks which use encryption and other security measures to transmit information through a public network such as the Internet and avoid unauthorized use	
VSWR	Voltage Standing Wave Ratio	A ratio of maximum to minimum voltage in the standing wave pattern that appears along a transmission line that is due to the adding of the forward and reverse travelling waves.	VSWR can be used as a measure of impedance mismatch between the transmission line and its load.
WAN	Wide Area Network	A network of computers and intercon-	

Acronym	Meaning	Definition	Notes
		nected LANs typically spread out over a large area.	
WWAN	Wireless Wide Area Network	As opposed to a fixed WAN	

16. Appendix B: Technical Terminology

The terms in Table 16-1 are the ones used in this report and the previous ones.

This table and its successors in future milestone reports will be used two ways in the final Cookbook:

- As terms to be avoided if at all possible
- As terms to be defined when absolutely necessary.

Table 16-1: Technical Term Definitions and Notes

Term	Definition	Notes
100BaseT	100 Mbps baseband data transmission over twisted-pair copper wire	
24/7	24 hours a day, 7 days a week	Used to indicate a system that is highly reliable, as in “the system is available 24/7”.
802.11	The set of wireless local area network (WLAN) industry standards that were developed by the IEEE for wireless network communication.	
802.11a	A version of the 802.11 wireless local area network (WLAN) industry standard that was developed by the IEEE for wireless network communication.	It was developed to operate in the 5.7 GHz spectrum and permits data transmission speeds up to 54 Mbps.
802.11b	A wireless local area network (LAN) system.	It operates in the 2.4 GHz frequency band and has a data transfer rate up to 11 Mbps.
802.11g	A wireless local area network (LAN) system.	It operates in the 2.4 GHz frequency band and has a data transfer rate up to 54 Mbps.
802.11i	An enhanced security protocol that is used in the 802.11 system.	It uses dynamically changing keys to replace the static security keys used in the original 802.11 system.
Addressing	A mechanism for identifying the address of a called endpoint in terms of the network, such as an IP address	
Amp	Amplifier	
Amplifier	A device for converting an input	Amplifiers increase both the de-

Term	Definition	Notes
	signal (usually low level) into a larger version of itself.	sired signal and unwanted noise signals.
Antenna directivity	The degree to which the radiation patterns of an antenna deviates from omnidirectional.	
Antenna diversity	The use of multiple antennas to receive multiple instances of the same signal and then make use of the otherwise redundant data contained within these signals	This allows the system to be more robust against the many factors that degrade signal reliability.
Antenna steering	Adjusting the angles of two antennas that face each other so that the RF signal is maximized.	
Antenna tilt	The angle of an antenna relative to the horizontal.	
Authentication server	A server that manages the encryption keys that validate the identity of customers and enable voice privacy services.	A single authentication server may process validation requests using different keys, random numbers and encryption algorithms.
Autorecovery	The ability of a system to recover to it original state after a failure.	
Availability	The % of time a system is available to do its functions.	
Azimuth	Horizontal direction expressed as the angular distance between the direction of a fixed point (as the observer's heading) and the direction of the object	
Backhaul	The portion of an access network between the access point and the intended termination point (e.g., switch or POP)	
Balun	Balanced/Unbalanced	
Band	A more or less well-defined range of wavelengths, frequencies, or energies	
Bandwidth	The amount of data that can be transmitted in a fixed amount of time.	For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).
Baud	A unit of signalling speed equal to the number of signal events per second.	Not necessarily the same as bits per second.
Beamwidth	The width (in degrees) of an antenna directivity pattern	
Best-effort	Refers to treatment of a call without regard to pre-defined Quality of Service	
Bidirectional	Simultaneous two-way communications	
Blocking	Refusal of a system to accept a request for use of a vital system	

Term	Definition	Notes
	resource(e.g., call attempt to use a voice circuit)	
Boot (noun)	Waterproof connector	
Boot (verb)	Start a system up	
Bore line	A reference line established by the linear extension of the bore axis of a gun.	Used to refer to center line of antenna pattern
Bridge (noun)	A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol.	
Bridge (verb)	To connect using a Bridge	
Bridge-based VLAN	A Layer 2 VLAN	Bridge-based VLAN
Broadband	Of, relating to, or being a communications network in which a frequency range is divided into multiple independent channels for simultaneous transmission of signals (as voice, data, or video)	
Bursty	Tending to arrive in bursts.	Refers to traffic characteristics.
Cascaded	Arranged in a series configuration	
Channel	A general term used to describe a communications path between two systems.	Channels may be either physical or logical depending on the application. An RF channel is a physical channel, whereas control and traffic channels within the RF channel would be considered logical channels.
Channel assignment	The assignment of a link to a channel	
Cisco	A manufacturer of communications equipment	
Client	The client part of a client-server architecture.	Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.
Coaxial cable	A transmission line in which the signal carrying conductor is covered by a dielectric and another conductor.	
Collinear	In a straight line	
Coverage area	The geographical reach of a mobile communications network or system.	
Cut-through switch	A switch in which as soon as an incoming packet's header has been received, a forwarding decision is immediately made, before the packet is completely received.	
D-Link	A manufacturer of consumer	

Term	Definition	Notes
	wireless equipment	
DC-to-DC converter	A circuit which converts DC power from one voltage to a another.	It is a special class of power converter.
Deep discharge battery		
Digital	Describes when information - speech, for example - is encoded before transmission using a binary code — discrete, non-continuous values	Digital networks are rapidly replacing analog ones as they offer improved sound quality, secure transmission and can handle data as well as voice.
Drop-out	A spot on a data stream from which data has disappeared	
Duplex	A duplex communication system is one where signal can flow in both directions between connected parties	
Dynamic network address	An IP network address that can change from moment to moment.	As opposed to fixed network address.
Ethernet	A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976.	Ethernet uses a bus or star topology and supports data transfer rates of 10/100/1000 Mbps. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.
E-mail	Electronic mail	
Fade margin	The amount of margin (usually in dB) needed to be set aside to account for signal fading	
Fresnel zone	An elliptical area on either side of the straight line of sight that must also be clear for a long-range wireless network to work.	
Firewall	A system designed to prevent unauthorized access to or from a private network.	Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.
Firmware	Software (programs or data) that has been written onto read-only memory (ROM).	Firmware is a combination of software and hardware.
Float charged		
Gain	Increase in voltage, current and/or power.	Gain is expressed as a ratio of amplifier output value to the corresponding amplifier input value.
Gateway router	A router that performs conversions between different coding and transmission formats.	The gateway does this by having many types of commonly used transmission equipment and / or circuits from different carriers to

Term	Definition	Notes
		provide a means of interconnection. See Bridge
Guyed	Steadied or reinforced with a guy	
Hacker	A slang term for a computer enthusiast.	The term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation. The pejorative sense of hacker is becoming more prominent largely because the popular press has co-opted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data.
Half-duplex	A half duplex system allows communications in both directions, but only one direction at a time (not simultaneously).	Also called simplex
Hata model	Common name used for the Okamura-Hata model used to predict signal strength levels in land-mobile systems.	
Histogram	A representation of a frequency distribution by means of rectangles whose widths represent class intervals and whose areas are proportional to the corresponding frequencies	
Host	A computer system that is accessed by a user working at a remote location.	Typically, the term is used when there are two connected computer systems. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal.
Hub	A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN.	A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
Impedance	The apparent opposition in an electrical circuit to the flow of an alternating current that is analogous to the actual electrical resistance to a direct current and that is the ratio of effective electromotive force to the effective current	
Interloper	Some one that intrudes into a network or system	
Key	A password or table needed to decipher encoded data.	
LAN segment	In networks, a section of a Local Area Network that is bounded by bridges, routers or switches.	Dividing an Ethernet into multiple segments is one of the most common ways of increasing

Term	Definition	Notes
		available bandwidth on the LAN. If segmented correctly, most network traffic will remain within a single segment, enjoying the full bandwidth. Hubs and switches are used to connect each segment to the rest of the LAN.
Latency	In networking, the amount of time it takes a packet to travel from source to destination.	Together, latency and bandwidth define the speed and capacity of a network.
Layer 1		
Layer 1 VLAN	A VLAN that is segmented on the basis of Layer 1 (physical) information, such as a physical port.	
Layer 2		
Layer 2 VLAN	A VLAN that is segmented on the basis of Layer 2 (bridging) information	
Layer 3		
Layer 3 VLAN	A VLAN that is segmented on the basis of Layer 2 (routing) information	
Lightning Arrestor	A device that is intended to shunt lightning away from a piece of equipment so that the latter is not damaged.	
Link budget	A calculation involving the gain and loss factors associated with the antennas, transmitters, transmission lines and propagation environment.	Used to determine the maximum distance at which a transmitter and receiver can successfully operate.
LinkSys	A manufacturer of consumer wireless equipment	
Load sharing	Sharing a load between two or more elements	
Lobe	A representation of the transmission directional efficiency of a radio antenna.	The larger the major lobe, compared with minor lobes, the more directive the system.
Mains	Of or relating to electrical utility distribution mains <mains voltage>	
Memory effect	An effect seen in some rechargeable batteries that causes them to hold less charge.	Also known as lazy battery effect
Metric (noun)	A standard of measurement	
Monopole	A radio antenna consisting of a single often straight element	
Multi-path interference	A propagation effect resulting from the reception of signals that have taken two or more paths from a transmitter to a receiver.	The effect can cause audio distortion in a radio receiver or ghost images in a TV set.
Near field (n or adj)	The region of the field of an antenna between the close-in reactive field region and the far field region wherein the angular field	

Term	Definition	Notes
	distribution is dependent upon distance from the antenna.	
Network recovery	The ability of a network to get back to the state it was in just prior to some sort of interruption of operation (e.g., due to a power failure)	
Network partitioning	Dividing a network into parts, which can be separately identified and managed.	Also known as segmenting. A network switch is used to interconnect network segments.
Node	A point of connection in a network.	A node is often a device on the network that can process a transmission or forward it to another node.
Ohm	The practical meter-kilogram-second unit of electric resistance equal to the resistance of a circuit in which a potential difference of one volt produces a current of one ampere	
Omni	An omni-directional antenna, which provides roughly equal power at all angles around it	
Overhead traffic	Traffic above and beyond the data traffic which is the aim of a data network.	
Packet	A piece of data transmitted over a packet-switching network such as the Internet.	A packet includes not just data but also address information about its origination and destination.
Path buffering switch		
PC Card	A computer device packaged in a small card about the size of a credit card and conforming to the PCMCIA standard.	
Pigtail	A short length of cable extending from a transmitter or receiver and used to make a connection to that equipment.	Copper, coaxial, or fibre.
Ping	A protocol that sends a message to another computer and waits for acknowledgment	Often used to check if another computer on a network is reachable
Planar Antenna	A flat antenna	
Point-to-multipoint	A set of direct links between one network node and many network nodes	
Point-to-point	A direct link between two network nodes.	
Polarization	The action or process of affecting radiation (including radio waves) so that the vibrations of the wave assume a definite form	Types include: linear, circular, horizontal, vertical.
Port	a. An entrance to or exit from a	A hardware port is an outlet on a

Term	Definition	Notes
	data network. b. A connection point for a peripheral device.	piece of equipment into which a plug or cable connects.
Port grouping	Treating a set of ports as if they were equivalent in some sense.	
Port switching	Switching on the basis of a port, so that each is its own collision domain.	
Power budget	The maximum amount of power available for all uses	
Power inverter	A circuit for converting direct current electrical power to alternating current.	Most inverters interrupt the incoming direct current to create a square wave. This is then fed through a transformer to smooth the square wave into a sine wave.
Power management	A technique for managing the transmit power in base stations and mobiles to a minimum level needed for proper performance. Downlink power control applies to base stations and uplink power control to mobiles.	Power control is used in nearly all wireless systems to manage interference, and in the case of mobiles, to extend battery life.
Primary lobe	Main lobe of an antenna directivity pattern	
Propagation	The process of transfer of a radio signal (electromagnetic signal) or acoustic signal (sound) from one point to another point.	
Protocol	An agreed-upon format for transmitting data between two devices.	The protocol determines the following: • The type of error checking to be used • Data compression method, if any • How the sending device will indicate that it has finished sending a message • How the receiving device will indicate that it has received a message
Proxy	A computer network service which allows clients to make indirect network connections to other network services.	A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource, possibly by connecting to the specified server, or by serving it from a cache.
Radome	A cover that protects an antenna from the extremes of climate while allowing electromagnetic signals (radio waves) to pass through without attenuation.	The Radome is usually constructed from plastic or fiberglass.
Range	The space or extent included or covered by a wireless system	

Term	Definition	Notes
Range Extension	Methods to extend the range of a wireless systems	
Rated	Assigned a normal capacity or power	
Reach	The capability of successfully communicating with a device in the network from another device in the network	
Real-time	The actual time during which something takes place	
Repeater	A network device used to regenerate or replicate a signal.	In a data network, a repeater can relay messages between subnetworks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.
Repeater chain	Set of Repeaters, connected in a single chain	Sometimes called Daisy Chain
RG58	A type of coaxial cable	50 Ohms
Round robin	A method for allocating tasks or functions on a rotating basis	
Router	A device that forwards data packets along networks.	A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.
Scalability	The ability of a system to an increase in the number of users or amount of services it can provide without significant changes to the hardware or technology used.	
Server	A computer in a network that is used to provide services (e.g., as access to files or shared peripherals or the routing of e-mail) to other computers in the network	
Setscrew	A screw screwed through one part tightly upon or into another part to prevent relative movement	
Sniffer	A program or process used by to monitor a data stream for a specific pattern such as an address or specific content	Packet sniffers are sometimes used inappropriately to discover passwords or credit card numbers.
Span	Any link on a route	
Standby generator	An electrical generator which is used only in the case of power loss	
Static network address	An IP network address that does not change over time	As opposed to dynamic network address
Store-and-forward switch	A type of network switch, similar to a cut-through, but where each frame is buffered completely and, typically, checksummed on each	

Term	Definition	Notes
	router before being sent out on the outgoing link.	
Stub antenna	A small stubby antenna, typically used in cell phones or Wi-Fi cards	
Subnet Mask	A mask used to determine what subnet an IP address belongs to.	An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.
Sub-network	A network segment	Subnetting allows you to break down a large network into smaller ones which result in reduced network traffic, simplified administration and smoother performance.
Switch	In networks, a device that filters and forwards packets between LAN segments.	Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.
Terminus	Either end of a communications route	
Throughput	The actual traffic supported, as opposed to the raw bandwidth.	Bandwidth that does not result in throughput may be due to packets containing errors, retransmissions, erroneous routing and many other causes.
Topography	The configuration of a surface, including its relief and the position of its natural and man-made features	
Transceiver	A radio transmitter-receiver that uses many of the same components for both transmission and reception	
Transparency	A condition in which an operating system or other service allows the user access to a remote resource through a network without needing to know if the resource is remote or local.	
Virtual subnet	A Layer 3 VLAN	
Watch dog	A device or system that continu-	

Term	Definition	Notes
	ally monitors specific functions of devices or systems (usually mission critical systems) to ensure they continue to operate within predetermined limits.	
Wind loading	The stress placed on a structure due to the wind	
Wind rating	The stated operating limit of a structure expressible as maximum wind speed that can be sustained without serious damage	
Wireline	Type of network connected via wires (cables)	As opposed to Wireless
Wire mesh antenna	An antenna whose dish is composed of a metallic mesh	
Yagi antenna	A highly directional type of antenna	There are other types of highly directional antennas, but the Yagi is quite popular

17. Appendix C: References

This is an set of references

[1] IEEE 802.11g ™ standard, Standards Board of the Institute of Electrical and Electronics Engineers, 2003.

[2] D. Reid, Ian Easson, W. Almuhtadi, “Rural and Remote Wireless Broadband Research Project, Milestone Report #1” submitted in December 2003 to CIDA, Industry Canada, and NCIT.

[3] D. Reid, Ian Easson, W. Almuhtadi, “Rural and Remote Wireless Broadband Research Project, Milestone Report #2” submitted in April 2004 to CIDA, Industry Canada, and NCIT.

[4] D. Reid, Ian Easson, W. Almuhtadi, Rural and Remote Wireless Broadband Research Project, Milestone Report #3” submitted in June 2004 to CIDA, Industry Canada, and NCIT.

[5] D. Reid, Ian Easson, W. Almuhtadi, “Rural/Remote Wireless Research Project, Report on Basic System” submitted in August 2004 to CIDA, Industry Canada, and NCIT.

[6] The Jhai PC and Communication System Project, http://www.jhai.org/jhai_remoteIT.htm.

[7] Clif Cox, Bhutan Migration to New Technology (Wireless VoIP) Mission Report, prepared by ITU, 2002, http://www.bhutan-notes.com/clif/

[8] Dr. Onno W. Purbo, WiFi and VoIP projects, http://sandbox.bellanet.org/~onno/, http://www.apjii.or.id/onno/, http://onno.vlsm.org, http://www.bogor.net/idkf/

[9] Field measurements using: www.PCPitstop.com

[10] Field measurements using: Downloads | NetStumbler.com

[11] Linksys manuals and websites for WiFi equipments http://www.linksys.com/products/

[12] Dlink manuals and websites for WiFi equipments http://www.dlink.com/products/category.asp

[13] www.sveasoft.com provides a basis for looking into other features that could be incorporated in subsequent architectures for rural use.

[14] Thomas Maufer, “Field Guide to Wireless LANs for Administrators and Power Users, A”. Prentice Hall, 2003.

[15] Lee Barken, “How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN “”. Prentice Hall, 2003.

[16] Shelly Brisbin, “Build Your Own Wi-Fi Network”. McGraw-Hill, 2002.

[17] Janice Reynolds, “Going Wi-Fi: A Practical Guide to Planning and Building an 802.11 Network”. CMP Books, 2003.

[18] James LaRocca, “802.11 Demystified: Wi-Fi Made Easy (Telecommunications)”. McGraw-Hill, 2002.

[19] Simon R. Saunders, “Antennas and Propagation for Wireless Communication Systems”. John Wiley & Sons, 1999.

18. Appendix D: Bandwidth Test Software

AnalogX Netstat Live

This displays:

- Real-time data indicating current incoming and outgoing TCP/IP protocol throughput
- Current rate, maximum rate, minimum rate and average rate
- How many route hops data must pass through
- Bottlenecks on network.

See http://www.analogx.com/contents/download/network/nsl.htm.

Networx Version 3.1

This package:

- Shows current ports open on computer and what ports are connected to
- Measures current incoming/outgoing traffic in Kbytes/s
- Records throughput measurements to calculate hourly, weekly, or monthly rates to determine network characteristics over different periods of time.

See http://www.softperfect.com/products/networx/.

Bing win32_i386 1.1.3

Bing is a Linux software tool. Bing win32 is a version of Bing that has been converted to run on windows based systems. Bing measures the network bandwidth (not throughput) between any to ports on the network. The port does not have to be local to machine. Therefore PC 1 is able to measure bandwidth between the PC2 Ethernet port and PC3 Ethernet port. Bing will measure bandwidth until the user stops measurement and report the average, maximum, and minimum bandwidth measurements. Thus, the user is able to measure bandwidth average over a few seconds or for a few days.

RaccoonWorks Speedtest v1.4

This package tests network throughput. It transfers a user-selected file over the network and calculates throughput by dividing the file size by the transfer time.

The speed test consists of a server and client. The server program is started and the user must select a file to transfer. It is recommended that a compressed file (i.e., zip of.rar) be transferred so that the TCP/IP protocol is unable to compress the file and affect results. The client program is able to log into the server program and measure throughput between computers, or is able to connect to a http website and measure throughput from an internet page.

Qceck and ixchariot

This measures throughput and response time of network. It is able to measure the speed of different protocols: TCP/IP, UDP, IPX or SPX.

See http://www.ixiacom.com/products/performance_applications/pa_display.php?skey=pa_q_check.

19. Appendix E: LinkSys Firmware and Software

WRT54g v2.02.7_US_Code Official Software

This is the official LinkSys software. It does not have the following capabilities:

- Telnet
- Antenna diversity
- VLAN

In addition, SSH does not work.

Samadhi2_v2.2.00.8.6

This firmware has all the capabilities of the official Linksys firmware, but has antenna diversity enabled. The LinkSys default is to automatically select the left or right antenna for transmit or receive based on signal strengths. This firmware allows the user to select antenna to transmit and receive. It is possible to set one antenna as transmit and the other as receive, or set one antenna to both transmit and receive. It also has Telnet capability.

Satori V2_2.00.8.7.sv-pre1

This firmware has all the capabilities of the official Linksys firmware, but has added capabilities for WDS (Wireless Distribution System). For documentation on WDS, see http://www.pafree.net/media/TB-046.pdf.

WDS results in more communication and handshaking being required between computers, which would slow down wireless link. WDS is not favourable compared to a VLAN capable system.

The firmware also allows for antenna diversity selection, and has Telnet capability.

Alchemy 5.2.3

This firmware has VLAN capability. It allows up to 15 VLANs on one network. It also has Telnet and SSH capabilities.

20. Appendix F: Network Device Settings Reference

Lab WRT54G: Internet Gateway

Table 20-1: Lab WRT54G Setup Tab Settings

Setup Tab	
Basic Setup settings:	
Router Name	WRT54G Lab
MTU	Auto
Local IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DHCP Server	Enabled
Starting IP Address (of DHCP server range)	192.168.0.200
DDNS settings:	
DDNS Service	Disabled
MAC Address Clone settings:	
MAC Clone	Disabled
Advanced Routing settings:	
Operating Mode	Gateway
Static Routing	Not used. Therefore no changes are required.

Table 20-2: Lab WRT54G Wireless Tab Settings

Wireless Tab	
Basic Setup settings:	
Wireless Mode	AP
Wireless Network Mode	Mixed
Wireless Network Name (SSID)	WiFi Algonquin Lab
Wireless Channel	2 – 2.417 GHZ
Wireless SSID Broadcast	Enable
Security settings:	
Security Mode	Disabled
MAC Filter settings:	
Wireless MAC Filter	Disabled
Advanced settings:	
Authentication Type	Auto
Basic Rate	Default
Transmission Rate	Auto
CTS Protection Mode	Disable
Frame Burst	Disabled

Wireless Tab	
Beacon Interval	100 ms
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
Tx Antenna	Auto (WRT54G gateway not used as AP in lab)
Rx Antenna	Auto **Note**: Antenna settings of right or left are orientated as if looking at the router rear panel (the side with Ethernet ports). Therefore, the left antenna is the antenna next to the RESET button and the right antenna is next to the DC power adapter plug.
Xmit Power	28
WDS settings:	
All settings disabled	

Table 20-3: Lab WRT54G Security Tab Settings

Security Tab	
Firewall settings:	
Firewall Protection	Disabled
Block Anonymous Internet Requests	Off
VPN settings:	
IPsec Passthrough	Enabled
PPTP Passthrough	Enabled
L2TP Passthrough	Enabled

Table 20-4: Lab WRT54G Access Restrictions Tab Settings

Access Restrictions Tab	
Internet Access settings:	
Status	Disabled
PC's	Allow Internet access during selected days
Days	Everyday
Times	24 Hours
Blocked Services	None

Table 20-5: Lab WRT54G Applications & Gaming Tab Settings

Applications & Gaming Tab	
Port Range Forward settings:	
Ports forwarded	None
DMZ settings:	
DMZ	Disabled

Table 20-6: Lab WRT54G Administration Tab Settings

Administration Tab	
Management settings:	
Router Password	admin
Remote Router Access	Disabled
AP watchdog	Disabled
Bandwidth Mgmt	Disabled
Boot wait	On
Cron	Enabled
Dhcpd	Enabled

Administration Tab	
Static Allocations	No entries
DNS Masq	Enable
Local DNS	Enabled
Loopback	Enabled
802.1x	Enabled
NTP Client	Enabled
Server IP	No entries
PPTP Server	Disabled
Resetbuttond	Enabled
Routing	Enabled
SSHD	Enable
Password Login	Disabled
SSHD Port	22
Authorized Keys	No entries
Syslogd	Disabled
Telnet	Enable
Tftpd	Enable
UPnP	Disable
Log settings:	
Log	Disabled
Diagnostic settings:	
No settings	
Factory Default settings:	
Restore Factory Defaults	No

Table 20-7: Lab WRT54G Status Tab Settings

Status Tab	
Router settings:	
Firmware Version	Satori-4.0 v2.07.1.7sv
MAC Address	00:0C:41:D3:D6:BE
Router Name	WRT54G Lab
DMZ	Disabled
Login Type	Automatic Configuration - DHCP
IP Address	205.211.32.32
Subnet Mask	255.255.255.0
Default Gateway	205.211.32.1
DNS 1	205.211.30.22
DNS 2	205.211.30.21
DNS 3	192.197.88.3
Local Network settings:	
MAC Address	00:0C:41:D3:D6:BD
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
DHCP Server	Enabled
Start IP Address	192.168.0.200
End IP Address	192.168.0.249
Wireless settings:	
MAC Address	00:0C:41:D3:D6:BF
Mode	AP
Network	Mixed
SSID	WiFi Algonquin Lab
DHCP Server	Enabled
Channel	2
Rate	54 mbps

Status Tab	
Encryption	Enabled

Field WRT54G: Switch / AP

Table 20-8: Field WRT54G Setup Tab Settings

Setup Tab	
Basic Setup settings:	
Router Name	WRT54G Field
MTU	Auto
Local IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.0.2
DHCP Server	Disabled
DDNS settings:	
DDNS Service	Disabled
MAC Address Clone settings:	
MAC Clone	Disabled
Advanced Routing settings:	
Operating Mode	Gateway
Static Routing	Not used. Therefore no changes are required.

Table 20-9: Field WRT54G Wireless Tab Settings

Wireless Tab	
Basic Setup settings:	
Wireless Mode	AP
Wireless Network Mode	Mixed
Wireless Network Name (SSID)	WiFi Algonquin Field
Wireless Channel	12 – 2.417 GHZ
Wireless SSID Broadcast	Enable
Security settings:	
Security Mode	Disabled
MAC Filter settings:	
Wireless MAC Filter	Disabled
Advanced settings:	
Authentication Type	Auto
Basic Rate	Default
Transmission Rate	Auto
CTS Protection Mode	Disable
Frame Burst	Disabled
Beacon Interval	100 ms
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
Tx Antenna	Left (Cable to omni-direction antenna)
Rx Antenna	Left (Cable to omni-direction antenna) **Note**: Antenna settings of right or left are orientated as if looking at the router rear panel (the side with Ethernet ports). Therefore, the left antenna is the antenna next to the RESET button and the right antenna is next to the DC power adapter plug.
Xmit Power	28

Wireless Tab	
WDS settings:	
All settings disabled	

Table 20-10: Field WRT54G Security Tab Settings

Security Tab	
Firewall settings:	
Firewall Protection	Disabled
Block Anonymous Internet Requests	Off
VPN settings:	
IPsec Passthrough	Enabled
PPTP Passthrough	Enabled
L2TP Passthrough	Enabled

Table 20-11: Field WRT54G Access Restrictions Tab Settings

Access Restrictions Tab	
Internet Access settings:	
Status	Disabled
PC's	Allow Internet access during selected days
Days	Everyday
Times	24 Hours
Blocked Services	None

Table 20-12: Field WRT54G Applications & Gaming Tab Settings

Applications & Gaming Tab	
Port Range Forward settings:	
Ports forwarded	None
DMZ settings:	
DMZ	Disabled

Table 20-13: Lab WRT54G Administration Tab Settings

Administration Tab	
Management settings:	
Router Password	admin
Remote Router Access	Disabled
AP watchdog	Disabled
Bandwidth Mgmt	Disabled
Boot wait	On
Cron	Enabled
Dhcpd	Enabled
Static Allocations	No entries
DNS Masq	Enable
Local DNS	Enabled
Loopback	Enabled
802.1x	Enabled
NTP Client	Enabled
Server IP	No entries
PPTP Server	Disabled
Resetbuttond	Enabled
Routing	Enabled
SSHD	Enable
Password Login	Disabled
SSHD Port	22
Authorized Keys	No entries
Syslogd	Disabled
Telnet	Enable

Administration Tab	
Tftpd	Enable
UPnP	Disable
Log settings:	
Log	Disabled
Diagnostic settings:	
No settings	
Factory Default settings:	
Restore Factory Defaults	No

Table 20-14: Field WRT54G Status Tab Settings

Status Tab	
Router settings:	
Firmware Version	Satori-4.0 v2.07.1.7sv
MAC Address	00:0C:41:D3:D6:D6
Router Name	WRT54G Field
DMZ	Disabled
Login Type	Automatic Configuration - DHCP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS 1	**Note** :The Field WRT54G is only used as a switch. Therefore, no settings are required on the Internet port.
DNS 2	
DNS 3	
Local Network settings:	
MAC Address	00:0C:41:D3:D6:D5
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Disabled
Wireless settings:	
MAC Address	00:0C:41:D3:D6:D7
Mode	AP
Network	Mixed
SSID	WiFi Algonquin Field
DHCP Server	Disabled
Channel	12
Rate	54 mbps
Encryption	Enabled

Lab DWL-900AP+: Wireless Bridge

Table 20-15: Lab DWL-900AP+Home Tab Settings

Home Tab	
Wireless settings:	
AP Name	WiFi D-Link Algon Lab
SSID	WiFi D-Link Algon Lab
Channel	7
Authentication	Open System
WEP	Disabled
LAN settings:	
LAN IP	Static IP address
IP Address	192.168.0.50
Subnet mask	255.255.255.0
Gateway	192.168.0.2

Home Tab	
DNS Server	0.0.0.0
DHCP settings:	
DHCP server	Disabled

Table 20-16: Lab DWL-900AP Advanced Tab Settings

Advanced Tab	
Mode settings:	
Wireless Bridge	Selected
Remote Bridge MAC	00 0C 41 D3 D6 BF
Performance settings:	
Beacon interval	100ms
RTS threshold	2432
Fragmentation	2346
DTIM interval	3
Basic Rates 1-2Mbps	
Tx Rates	1-2 Mbps
Preamble Type	Long
SSID Broadcast	Enabled
Antenna transmit power	100% 17dbm
Antenna selection	Internal Antenna
Filter settings:	
Disabled MAC Filters	On
Advanced settings:	
802.1x settings:	
802.1x	Disabled

Table 20-17: Lab WRT54G Status Tab Settings

Status Tab	
Device Info (Ethernet) settings:	
MAC Address	00-0D-88-A6-B8-12
IP Address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway	192.168.0.2
DHCP Server	Disabled
Device Info (Wireless) settings:	
MAC Address	00-0D-88-AC-36-73
SSID	WiFi D-Link Algon Lab
Encryption Function	Disabled
Channel	7
AP mode	Wireless Bridge

Field DWL-900AP+: Wireless Bridge

Table 20-18: Field DWL-900AP+Home Tab Settings

Home Tab	
Wireless settings:	
AP Name	WiFi D-Link Algon Field
SSID	WiFi D-Link Algon Field
Channel	7
Authentication	Open System
WEP	Disabled
LAN settings:	
LAN IP	Static IP address
IP Address	192.168.0.51
Subnet mask	255.255.255.0

Home Tab	
Gateway	192.168.0.2
DNS Server	0.0.0.0
DHCP settings:	
DHCP server	Disabled

Table 20-19: Lab DWL-900AP Advanced Tab Settings

Advanced Tab	
Mode settings:	
Wireless Bridge	Selected
Remote Bridge MAC	00 0D 88 A6 B8 12
Performance settings:	
Beacon interval	100ms
RTS threshold	2432
Fragmentation	2346
DTIM interval	3
Basic Rates 1-2Mbps	1-2Mbps
Tx Rates	1-2 Mbps
Preamble Type	Long
SSID Broadcast	Enabled
Antenna transmit power	100% 17dbm
Antenna selection	Internal Antenna
Filter settings:	
Disabled MAC Filters	On
Advanced settings:	
802.1x settings:	
802.1x	Disabled

Table 20-20: Field WRT54G Status Tab Settings

Status Tab	
Device Info (Ethernet) settings:	
MAC Address	00-0D-88-BD-34-07
IP Address	192.168.0.51
Subnet Mask	255.255.255.0
Gateway	192.168.0.2
DHCP Server	Disabled
Device Info (Wireless) settings:	
MAC Address	00-0D-88-B6-6D-8F
SSID	WiFi D-Link Algon Field
Encryption Function	Disabled
Channel	7
AP mode	Wireless Bridge

21. Appendix G: Propagation Model Calculations

The tables on the next few pages document the propagation model we have used and validated. They are available as a separate integrated spreadsheet, both as part of this report and as part of the Cookbook.

Table 21-1: Propagation Model Inputs

Tx Power +(TxGain+RxGain) - (TxCable Loss+ Rx Cable Loss)- (Rx Sig. Str.)	*Input Parameters*	
Antenna S1 Ht(meters)	*25*	m
Antenna S2 Ht(meters)	*10*	m
Cable Loss (dB)	*8*	dB
Power TX (dBm)	*17*	dBm
Antenna Gain TX (dBi)	*18*	dBi
Antenna Gain RX (dBi)	*18*	dBi
Frequency	*2450*	MHz

Table 21-2: Propagation Formulas

		Loss / Gain Factors			Antenna Height Advantage		
					Constraints (Tower Heights above average ground Level AGL)		
		Parameters				Factor	
		G(hre) =	20log(hre / 3)		10 meters or higher	hre	Receive Antenna Height
RX Threshold	-88	A(f,d) =	35				
RX NF	4.5	G(the) =	20log(hte /200)		25 meters or higher	the	Transmitter Antenna Height
		G(area) =	33	Open Area	G(Area) @ 2.4 GHz from the Curves		Emperical Penalty Factor
			27	Suburban			
			13	Urban			

Table 21-3: Predicted Path Loss as Function of Distance

	Point to Point Clear Path Line of Site	>.6F1 clearance		Path Loss with Less than .6F1 clearance		
Distance (Km)	**FSL (dB)**	**Receive Level(dBm)**	**Fade Margin (dB)**	**Open**	**Subur-ban**	**Urban**
0.05	74.16	-29.16	58.84	82.47	88.47	102.47
0.1	80.18	-35.18	52.82	88.79	94.79	108.79
0.25	88.14	-43.14	44.86	97.14	103.14	117.14
0.5	94.16	-49.16	38.84	103.47	109.47	123.47
0.75	97.68	-52.68	35.32	107.16	113.16	127.16
1	100.18	-55.18	32.82	109.79	115.79	129.79
1.5	103.71	-58.71	29.29	113.49	119.49	133.49
2	106.20	-61.20	26.80	116.11	122.11	136.11
2.5	108.14	-63.14	24.86	118.14	124.14	138.14
3	109.73	-64.73	23.27	119.81	125.81	139.81
3.5	111.06	-66.06	21.94	121.21	127.21	141.21
4	112.22	-67.22	20.78	122.43	128.43	142.43
4.5	113.25	-68.25	19.75	123.51	129.51	143.51
5	114.16	-69.16	18.84	124.47	130.47	144.47
5.5	114.99	-69.99	18.01	125.34	131.34	145.34
6	115.75	-70.75	17.25	126.13	132.13	146.13
6.5	116.44	-71.44	16.56	126.86	132.86	146.86
7	117.09	-72.09	15.91	127.53	133.53	147.53
7.5	117.68	-72.68	15.32	128.16	134.16	148.16
8	118.25	-73.25	14.75	128.75	134.75	148.75
8.5	118.77	-73.77	14.23	129.31	135.31	149.31
9	119.27	-74.27	13.73	129.83	135.83	149.83
9.5	119.74	-74.74	13.26	130.32	136.32	150.32
10	120.18	-75.18	12.82	130.79	136.79	150.79
10.5	120.61	-75.61	12.39	131.23	137.23	151.23
11	121.01	-76.01	11.99	131.66	137.66	151.66

Distance (Km)	FSL (dB)	Receive Level(dBm)	Fade Margin (dB)	Open	Subur-ban	Urban
11.5	121.40	-76.40	11.60	132.06	138.06	152.06
12	121.77	-76.77	11.23	132.45	138.45	152.45
12.5	122.12	-77.12	10.88	132.82	138.82	152.82
13	122.46	-77.46	10.54	133.18	139.18	153.18
13.5	122.79	-77.79	10.21	133.52	139.52	153.52
14	123.11	-78.11	9.89	133.86	139.86	153.86
14.5	123.41	-78.41	9.59	134.18	140.18	154.18
15	123.71	-78.71	9.29	134.49	140.49	154.49
15.5	123.99	-78.99	9.01	134.78	140.78	154.78
16	124.27	-79.27	8.73	135.07	141.07	155.07
16.5	124.53	-79.53	8.47	135.35	141.35	155.35
17	124.79	-79.79	8.21	135.63	141.63	155.63
17.5	125.04	-80.04	7.96	135.89	141.89	155.89
18	125.29	-80.29	7.71	136.15	142.15	156.15
18.5	125.53	-80.53	7.47	136.40	142.40	156.40
19	125.76	-80.76	7.24	136.64	142.64	156.64
19.5	125.98	-80.98	7.02	136.88	142.88	156.88
20	126.20	-81.20	6.80	137.11	143.11	157.11

Table 21-4: Receive Levels as Function of Distance

		Receiver Levels			Simple Margin 10 dB		
	Path	open	subur-ban	urban	open	subur-ban	urban
Distance (Km)	Km	dBm	dBm	dBm	dB	dB	dB
0.05	0.05	-37.47	-43.47	-57.47	50.53	44.53	30.53
0.1	0.1	-43.79	-49.79	-63.79	44.21	38.21	24.21
0.25	0.25	-52.14	-58.14	-72.14	35.86	29.86	15.86
0.5	0.5	-58.47	-64.47	-78.47	29.53	23.53	9.53
0.75	0.75	-62.16	-68.16	-82.16	25.84	19.84	5.84
1	1	-64.79	-70.79	-84.79	23.21	17.21	3.21
1.5	1.5	-68.49	-74.49	-88.49	19.51	13.51	-0.49
2	2	-71.11	-77.11	-91.11	16.89	10.89	-3.11
2.5	2.5	-73.14	-79.14	-93.14	14.86	8.86	-5.14
3	3	-74.81	-80.81	-94.81	13.19	7.19	-6.81
3.5	3.5	-76.21	-82.21	-96.21	11.79	5.79	-8.21
4	4	-77.43	-83.43	-97.43	10.57	4.57	-9.43
4.5	4.5	-78.51	-84.51	-98.51	9.49	3.49	-10.51
5	5	-79.47	-85.47	-99.47	8.53	2.53	-11.47
5.5	5.5	-80.34	-86.34	-100.34	7.66	1.66	-12.34
6	6	-81.13	-87.13	-101.13	6.87	0.87	-13.13
6.5	6.5	-81.86	-87.86	-101.86	6.14	0.14	-13.86
7	7	-82.53	-88.53	-102.53	5.47	-0.53	-14.53
7.5	7.5	-83.16	-89.16	-103.16	4.84	-1.16	-15.16
8	8	-83.75	-89.75	-103.75	4.25	-1.75	-15.75
8.5	8.5	-84.31	-90.31	-104.31	3.69	-2.31	-16.31
9	9	-84.83	-90.83	-104.83	3.17	-2.83	-16.83

Good 54g & 11b
Fair 11b, 11Mb/s
Marginal 5.5 to 2 Mb/s
Unusable 1 - 0 Mb/s

Protocol Limit for 802.11g
Conservative Protocol Limit for 802.11b 11 Mb/s

The above is where radio MAC timing cannot cope with the transmission roundtrip delay. Within the limit distance range, inadequate RF level will drive the bit rate down.

		Receiver Levels			Simple Margin 10 dB		
	Path	open	subur-ban	urban	open	subur-ban	urban
Distance (Km)	Km	dBm	dBm	dBm	dB	dB	dB
9.5	9.5	-85.32	-91.32	-105.32	2.68	-3.32	-17.32
10	10	-85.79	-91.79	-105.79	2.21	-3.79	-17.79
10.5	10.5	-86.23	-92.23	-106.23	1.77	-4.23	-18.23
11	11	-86.66	-92.66	-106.66	1.34	-4.66	-18.66
11.5	11.5	-87.06	-93.06	-107.06	0.94	-5.06	-19.06
12	12	-87.45	-93.45	-107.45	0.55	-5.45	-19.45
12.5	12.5	-87.82	-93.82	-107.82	0.18	-5.82	-19.82
13	13	-88.18	-94.18	-108.18	-0.18	-6.18	-20.18
13.5	13.5	-88.52	-94.52	-108.52	-0.52	-6.52	-20.52
14	14	-88.86	-94.86	-108.86	-0.86	-6.86	-20.86
14.5	14.5	-89.18	-95.18	-109.18	-1.18	-7.18	-21.18
15	15	-89.49	-95.49	-109.49	-1.49	-7.49	-21.49
15.5	15.5	-89.78	-95.78	-109.78	-1.78	-7.78	-21.78
16	16	-90.07	-96.07	-110.07	-2.07	-8.07	-22.07
16.5	16.5	-90.35	-96.35	-110.35	-2.35	-8.35	-22.35
17	17	-90.63	-96.63	-110.63	-2.63	-8.63	-22.63
17.5	17.5	-90.89	-96.89	-110.89	-2.89	-8.89	-22.89
18	18	-91.15	-97.15	-111.15	-3.15	-9.15	-23.15
18.5	18.5	-91.40	-97.40	-111.40	-3.40	-9.40	-23.40
19	19	-91.64	-97.64	-111.64	-3.64	-9.64	-23.64
19.5	19.5	-91.88	-97.88	-111.88	-3.88	-9.88	-23.88
20	20	-92.11	-98.11	-112.11	-4.11	-10.11	-24.11

22. Appendix H: Wi-Fi Research Equipment for Project

Note: all prices in Canadian dollars, rounded to nearest full dollar, before taxes.

Table 22-1: Computer Equipment Purchased for Project

Number of Items	Description	Details	Purchased From	Unit price	Total price
2	Desktop PC's with Wi-Fi Cards	Northern Micro (Desk-top PC's –College standard – P4 -1.7 GHz with CD-RW and IEEE Cards (PCI cards-802.11b/g for desktops) (DWL-520+D-Link 2.4 GHz 802.11B/G enhanced wireless PCI adapter)	Through Algonquin	$888	$1776
1	Laptop Computer	IBM Mobile – Think-Pad T41 Pentium M at 1.4GHz Centrino with CD-RW/DVD Combo Drive, Disc Capacity: 30 – 40GB Graphic subsystem: ATI Mobility M/T Model: 2378-DLU	College Computer Store	$2545	$2545
2	Used Lap-top Com-puters	IBM ThinkPad Note-books A22e) Proces-sor x86 Family 6 Model 8 Stepping 10 Genuine Intel ~797 MHz System Model 265528U	College Surplus Inventory	$500	$1000
Subtotal	Computers				$5321

Table 22-2: AP's, Routers, and Accessories Purchased for Project

Number of Items	Descrip-tion	Details	Purchased From	Unit price	Total price
3	AP: Link-Sys®, WRT54G Wireless Router/Ac cess Point	54Mbps, All-in-one Internet-sharing Router, 4-port Switch, and Wireless-G (draft 802.11g). Access Point Wireless data rates up to 54Mbps	College Computer Store	$130	$390
3	IEEE Cards (Mini PCI cards-802.11b/g for lap-tops)	D-Link AirPlus DWL-G650 Cardbus Adapter	College Computer Store	$100	$300
3	IEEE Cards USB	D-Link DWL-120+Enhanced 2.4 GHz Wireless USB Adapter	College Computer Store	$100	$300

			College Computer Store		
Subtotal	APs and Routers				$1320

Table 22-3: Antennas and Accessories Purchased for Project

Number of Items	Descrip-tion	Details	Purchased From	Unit price	Total price
1	2.4 GHz, Maxrad Yagi An-tenna	MYP24013 with 13.5 dBi gain	Alpha Beta Ltd -	$362	$362
2	High Gain Directional Panel In-door/Outd oor An-tenna	2400-2500 MHz / 14 dBi / 30 deg / N-type female, Model: HD20677	Alpha Beta	$210	$420
1	Quasi Log Periodic End Fire Array Feed horn	2300-2500 MHz / 24 dBi / N-Type Female /VSWR 1.3:1 Max Po-larization Vertical or Horizontal. Model: HD18035	Alpha Beta	$213	$213
2	Yagi An-tenna	2300-2500 MHz / 18 dBi / 15 deg / N-Type Female connector Model: HD20691	Alpha Beta	$352	$704
4	Lightning arrestor kits for all outdoor antennas	LIGHTNING ARRESTER, IN LINE","AIR GAP,COAX CUSHCRAFT, Type N Connectors LTNG2400-QW. Lightning Arrestor 2.4 GHz (Quarter-wave)	Alpha Beta	$154	$308
1	75 ft Cable	LMR400 with 2 N-type male connectors at-tached	Alpha Beta	$162	$162
1	50 ft Cable	LMR400 with 2 N-type male connectors at-tached	Alpha Beta	$137	$137
1	30 ft Cable	LMR400 with 2 N-type male connectors at-tached, plus miscella-neous fittings and adapters	Alpha Beta	$122	$122
3	Wi-Fi Finder handheld signal de-tector	Model: HD21350	Alpha Beta	$48	$144

1	Til-Tek Omni Antenna	TilTek (*8 dBi Omni* – type: TA-2450 at 10 dBi gain)	Alpha Beta	$570	$570
Subtotal	Antennas and Accessories				$3700

Table 22-4: Miscellaneous Items Purchased for Project

Number of Items	Description	Details	Purchased From	Unit price	Total price
1	70 watt BP Solar Panel		Local Ottawa	$400	$400
1	6 amp charge controller to regulate the voltage at the battery		Local Ottawa	$80	$80
4	6 volt 220 amp-hr batteries		Local Ottawa	$280	$920
4	Interconnect cables	For a series parallel connection		$20	$80
2	Antenna tower(s) and accessories	10’ Tower sections Delphi	Radio Shack	$80	$160.0
1	Antenna Top tower section	Part of Delphi tower 10 ‘ with mast mount and 10’ pole	Radio Shack	$100	$100
1	Guy wire Pegs Turnbuckles. Tower Stabilizers	Misc Items for mounting the tower	Home Depot	$100	$100

For more information contact:

Algonquin College

Applied Research and Development

Tel: (613)727-4723 ext. 5278 /5040, Fax: (613)727-7633

School of Advanced Technology, Electronics and Elector-Mechanical Studies

Tel: (613)727-4723 ext. 3403, Fax: (613)727-7663

http://www.algonquincollege.com

Network Planning Systems Inc.

Main Quebec Office:

75 Rue Jean Proulx

Hull, Quebec, Canada J8Z 1W2

Ontario Office:

2353 Georgina Drive

Ottawa, Ontario, Canada K2B 7M6

Tel: (613) 721-1778, Fax: (613) 721-1778

http://www.netplansys.com