



Asia-Pacific  
Economic Cooperation

# **Designing and Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook**

Adapted for  
**APEC Telecommunications and Information  
Working Group**

**April 2005**

Algonquin College of Applied Arts and Technology  
Ottawa, Ontario Canada

## Designing and Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Copyright © 2005 APEC SECRETARIAT

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS BOOK. THE PUBLISHER AND AUTHORS MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS AND SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THERE ARE NO WARRANTIES WHICH EXTEND BEYOND THE DESCRIPTIONS CONTAINED IN THIS PARAGRAPH. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. THE ACCURACY AND COMPLETENESS OF THE INFORMATION PROVIDED HEREIN AND THE OPINIONS STATED HEREIN ARE NOT GUARANTEED OR WARRANTED TO PRODUCE ANY PARTICULAR RESULTS, AND THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY INDIVIDUAL. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

**Trademarks.** Any other trademarks are the properties of their respective owners.

Prepared by:  
Algonquin College  
1385 Woodroffe Ave  
Ottawa, Ontario Canada  
[www.algonquincollege.com](http://www.algonquincollege.com)

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION  
SECRETARIAT  
35 Heng Mui Keng Terrace Singapore 119616  
Tel: (65) 6775-6012 Fax: (65) 6775-6013  
Email: [info@apcc.org](mailto:info@apcc.org)  
Website: [www.apcc.org](http://www.apcc.org)

© [2005] APEC Secretariat

APEC#205-TC-01.3

# Acknowledgements

This “Cookbook” on how to build reliable Wi-Fi networks for rural or remote areas in both developed and developing countries is the result of a collaboration involving many Canadian institutions and people. The book was adapted from the original Cookbook which funded by the Canadian International Development Agency, Industry Canada, and the National Capital Institute for Telecommunications of Canada. The research was carried out by faculty and students of Algonquin College, along with researchers from Network Planning Systems Inc. It focused on Canadian and international Wireless Internet technology and expertise, as applied to the developing countries and to rural and remote Canadian locales. The full text contains additional technical material.

Thanks also to Roland Reeb and Alpha-Beta Communications Group for assistance with procurement and installation of equipment, as well as technical advice.

## Research and Project Team

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

## Supporting Organizations and Contact Persons

Name	Organization	E-Mail	Phone
Les Breiner	Science And Technology Group, Canadian International Development Agency	les_breiner@acdi-cida.gc.ca	(819) 994-4656
Gerry Briggs	Broadband For Rural And Northern Development, Industry Canada	briggs.gerry@lc.gc.ca	(613) 948-5045
Mohamed Zaid	Senior Research Consultant, NCIT	mzaid@ncit.ca	(613) 993 1161
Edward Bebee	Managing Director, Genstar Consulting Group Inc.	edbebee@genstarconsultinggroup.com	(613) 741-7838
Ian Easson	CEO And President, Network Planning Systems Inc.	easson@netplansys.com	(613) 721-1778
Doug Reid	CTO, Network Planning Systems Inc.	dougr@netplansys.Com	(613) 721-1778
Jack Treuhaft	Director, Applied Research And Development, Algonquin	treuhaj@algonquincollege.com	(613)727-4723 Ext. 5278
Nelson Rogers	Project Manager, Applied Research And Development, Algonquin	rogersn@algonquincollege.com	(613)727-4723 Ext. 5040
Wahab Almuhtadi	Professor, Electronics And Electro-Mechanical Studies, Algonquin	almuhtw@algonquincollege.com	(613)727-4723 Ext. 3403

## Special Thanks

---

We would like to thank Dr. Onno W. Purbo, whose work in building practical Wi-Fi networks in urban third world locations has served as an inspiration to us, as it has to many others.

# Table of Contents

1.	<b>Introduction .....</b>	<b>1</b>
	Need for Inexpensive Rural or Remote Internet Access .....	4
	What is the Cookbook About? .....	5
	Whom is This Cookbook For? .....	6
	How This Book is Organized .....	7
	Specific Benefits of the Cookbook.....	9
	Limitations of the Cookbook .....	9
	Combining Cookbook Approaches with Commercial Ones.....	10
	A Note about Jargon .....	11
	Other Icons Used in This Book.....	11
	Where to Go From Here .....	12
	<b>Part I: Planning Your Rural Wi-Fi Wide Area Network .....</b>	<b>15</b>
2.	<b>Wi-Fi Local and Wide-Area Networks .....</b>	<b>17</b>
	A Basic Wi-Fi Wireless Wide Area Network .....	20
	Types of Users .....	21
	Local Access Point Antennas for Coverage .....	28
	Access Point Equipment .....	31
	Optional Local Community Server.....	32
	What is the Backhaul?.....	33
	802.11 Wireless Bridge in Field.....	33
	Directional Antennas for Backhaul .....	35
	802.11 Wireless Bridge at Point of Presence.....	35
	Network Gateway/Router/Firewall.....	36
	Optional RADIUS Server .....	36
3.	<b>Community Services for Your Wi-Fi Network.....</b>	<b>37</b>
	Community Services .....	39
	Voice over IP .....	40
	Virtual Private Networks .....	42
	Internet Radio Station.....	43
	Internet TV Station .....	43
4.	<b>Introduction to Wireless Propagation and Coverage.....</b>	<b>45</b>
	Reach .....	47
	Factors Affecting Reach .....	48
	Throughput.....	50
	Coverage Zones.....	51
5.	<b>Creating a Wi-Fi WWAN and Connecting it to the Internet.....</b>	<b>55</b>
	Connecting the AP to the WAN or Backhaul Facility.....	58
	Local LAN Access and AP Interconnection.....	58
	The POP Gateway .....	60
	Satellite Systems.....	62
	Backhaul Terrestrial Microwave Radio Link Choices .....	64

	Point-to-Point Microwave Radio Repeaters for Backhaul.....	67
	Estimating Numbers and Locations of Relay Nodes .....	68
	Providing Secondary Paths .....	69
<b>6.</b>	<b>Serving Outlying Groups of People.....</b>	<b>69</b>
	Serving a Small Cluster of Buildings Outside of Town .....	72
	Serving Isolated Buildings Which Are Widely Spread Out .....	74
<b>7.</b>	<b>Powering Your Access Points.....</b>	<b>77</b>
	Power Budget.....	79
	Battery Backup .....	80
	Mains .....	82
	Propane (Natural Gas) .....	83
	Wind Turbine .....	83
	Solar .....	85
	Small Hydro Dam .....	87
	Stream Turbine.....	88
	Cycle Power .....	89
	Commercial Power Control Systems.....	89
<b>8.</b>	<b>Planning Your Network Security.....</b>	<b>91</b>
	Types of Wi-Fi Security Threats .....	93
	Wi-Fi Network Security Recommendations .....	94
	Checking Your Security .....	95
	Going Beyond the Security Solutions in This Cookbook .....	96
	Further Wi-Fi Security References .....	97
	Physical Security Plan .....	97
<b>9.</b>	<b>Identifying What Equipment You Need and Costing it Out .....</b>	<b>101</b>
	Wi-Fi Equipment Types .....	103
	Avoiding Incompatibility Issues.....	106
	Auxiliary Equipment.....	107
	A Simple Network Budget.....	110
<b>Part II: Assembling and Customizing Your Equipment .....</b>		<b>113</b>
<b>10.</b>	<b>Setting up Your Radio Equipment .....</b>	<b>115</b>
	Long Distance 802.11b Timing Issues .....	117
	The Solution .....	118
	Going Even Farther Distances .....	119
	Disabling Antenna Diversity.....	120
	Disable Automatic Power Setting .....	121
	Channel Settings .....	121
<b>11.</b>	<b>Setting up Your Network Equipment .....</b>	<b>123</b>
	User Interfaces for Administering Wi-Fi Equipment .....	125
	Setting up Your PCs .....	126
	Setting up the Gateway/Firewall.....	127
	Setting up the AP and Layer 2 Bridge .....	129
	Setting up the Wireless Bridges .....	131
	Testing Connectivity .....	136

	Storing Configuration Information in Flash Memory .....	137
<b>12.</b>	<b>Packaging Your Equipment.....</b>	<b>139</b>
	Repackaging for Ruggedness .....	141
	NEMA Enclosures .....	144
	Weatherproofing and Humidity .....	145
	Overheating.....	145
	Freezing .....	145
	Fireproofing .....	146
	Corrosion Resistance .....	146
	Connectors .....	146
	Coaxial Cables .....	147
	Adding Lightning Protection .....	148
	Adding an Uninterruptible Power Supply.....	151
	Improving RF Shielding .....	151
	Mounting Options .....	151
	Antenna - Cable VSWR.....	154
	<b>Part III: Installing Your Wi-Fi Network .....</b>	<b>155</b>
<b>13.</b>	<b>Putting up Your Towers .....</b>	<b>157</b>
	Towers versus Masts or Poles .....	159
	Tower Location and Placement.....	159
	Safety First .....	160
	Grounding and Lightning Protection.....	160
	Cable Runs and Equipment Placement .....	160
	Making it Sturdy.....	161
	Raising the Tower .....	165
	Final Tower Alignment.....	169
<b>14.</b>	<b>Aligning Your Antennas .....</b>	<b>171</b>
	Why Align Antennas? .....	173
	Equipment for Alignment.....	174
	Preparing for Initial Antenna Alignment.....	175
	Doing the Initial Antenna Alignment .....	178
	Antenna Tilt .....	181
	Different Approaches to Fine Antenna Adjustments .....	181
	Fine Adjustment of the Antenna Orientation and Tilt.....	182
	Final Steps .....	184
	<b>Part V: Appendices .....</b>	<b>187</b>
	<b>Appendix A: Acronyms .....</b>	<b>189</b>
	<b>Appendix B: Technical Terminology.....</b>	<b>199</b>
	<b>Appendix C: References.....</b>	<b>219</b>
	Specific.....	219
	General.....	219



# List of Figures

Figure 1-1: How the Cookbook Can Help You .....	6
Figure 1-2: Network Complexity Rises Faster than Network Size .....	10
Figure 1-3: Cookbook Solutions on Outskirts of Commercial Ones .....	11
Figure 2-1: A Basic Wi-Fi Wide Area Network for Rural Coverage .....	20
Figure 2-2: Communicating between the Local AP and the Fixed Users .....	27
Figure 2-3: Coverage of Island Community using a Sectored Antenna .....	30
Figure 2-4: Relationships between Local APs, Backhaul, and POP .....	34
Figure 3-1: Example of Large VoIP Service (Skype) .....	42
Figure 3-2: Local Community Internet TV Station (Indian Head, Canada) .....	44
Figure 4-1: Definition of Reach .....	47
Figure 4-2: How Received Signal Strength Can Affect Total Throughput .....	50
Figure 4-3: Effect of Numbers of Users on Coverage Radius .....	52
Figure 4-4: User Antennas have Higher Gains and Heights in Further Zones .....	52
Figure 4-5: Dividing the Coverage Area into Zones Solves the Coverage Radius Problem .....	53
Figure 5-1: Using Replication and Backhaul Interlinking to Extend Wi-Fi Coverage .....	59
Figure 5-2: Centrally Located Village with Satellite Link becomes POP for five APs .....	63
Figure 5-3: Duplex Inter-nodal Repeater for AP Coverage Extension .....	67
Figure 6-1: Proxy AP to Serve an Isolated Cluster of Buildings .....	72
Figure 6-2: Omnidirectional Store and Forward .....	73
Figure 6-3: Directional Store and Forward .....	74
Figure 7-1: Power Configuration Example for AP Powering .....	82
Figure 7-2: Some Alternative Power Source Options .....	83
Figure 7-3: Projected Wind Turbine Output for Arctic Bay, Northwest Territories, Canada .....	85
Figure 7-4: Example Solar Power Output for Abong Mbang, Cameroon .....	86
Figure 7-5: Example of Small Hydro Dam Installation .....	88
Figure 8-1: RADIUS Server in Action .....	96
Figure 10-1: Giving up Too Early Limits How Far Two APs can be Apart ....	118
Figure 10-2: Example of Channel Co-Ordination .....	122
Figure 11-1: One Possible Relay Node Bridge Configuration .....	132
Figure 11-2: Another Configuration of Bridges at Relay Sites .....	133
Figure 11-3: Disabling Antenna Diversity and Setting Other Parameters .....	134
Figure 12-1: Mounting in a Building .....	152
Figure 12-2: Mounting Near the Tower Base .....	153
Figure 13-1: Guy Wire Anchoring Approaches .....	162
Figure 13-2: Anchoring Parts .....	163
Figure 13-3: More Secure Tower Connection Approaches .....	165
Figure 14-1: Explaining (Mis)alignment of Directional Antennas .....	173
Figure 14-2: Antenna Tilt Versus Path Reach .....	181

# List of Tables

Table 1-1: Three Audiences for the Cookbook .....	7
Table 1-2: Organization of and Audiences for the Cookbook .....	8
Table 3-1: Most Popular Services for North American WISP Entrepreneurs..	39
Table 7-1: Example Power Requirements and Supply for AP Site .....	79
Table 7-2: Power Generation Capacity of a Solar panel.....	86
Table 7-3: Some Companies Making Small Electrical Power Control Systems .....	90
Table 9-1: Example of a Simple Budget for a Commercial Wi-Fi Network (2004 prices) .....	111
Table 10-1: Wait Intervals for Wi-Fi .....	119
Table 10-2: Firmware Modifications for Very Extended Reach (example)....	120

# List of Procedures

Procedure 11-1: Configuring Your Test PC .....	126
Procedure 11-2: Configuring Your Wi-Fi Gateway/Firewall .....	127
Procedure 11-3: Configuring Your AP and Layer 2 Bridge .....	129
Procedure 11-4: Configuring Your Wireless Bridge .....	135
Procedure 14-1: Setting up the RF for Antenna Alignment.....	176
Procedure 14-2: Initial Coarse Antenna Alignment.....	178
Procedure 14-3: Fine-tuning the Antenna Alignment.....	183

# List of Photographs

Photo 2-1: Wi-Fi Card for a Notebook and Plug-in Wi-Fi Board for a PC .....	22
Photo 2-2: Example of Consumer AP (D-Link) .....	22
Photo 2-3: Coaxial Cable .....	23
Photo 2-4: N-Connector .....	23
Photo 2-5: Antenna on Residential Window .....	23
Photo 2-6: Coverage and Backhaul Antennas on Top of a Local AP .....	24
Photo 2-7: A Variety of SMC Adaptors for Wi-Fi Cards .....	24
Photo 2-8: Yagi Antenna .....	26
Photo 2-9: Parabolic Dish Antenna Ready for Installation .....	26
Photo 2-10: Omnidirectional (“Omni”) Antenna .....	29
Photo 2-11: Two Views of a Sectored Wi-Fi Antenna (14 dBi Gain, 60 Degree Beam) .....	30
Photo 3-1: Parts of a Portable Wi-Fi-based TV Studio .....	44
Photo 7-1: Example of Small Wind Turbine .....	84
Photo 7-2: Example of Stream Turbine .....	88
Photo 8-1: Small Network Operations Centre .....	98
Photo 11-1: Main LinkSys Setup Screen .....	125
Photo 11-2: Telnet User Interface .....	126
Photo 12-1: Do-it-yourself Enclosure (Outside) .....	141
Photo 12-2: Do-it-yourself Enclosure (Top View of Inside) .....	142
Photo 12-3: Details of AP Connections inside Enclosure .....	142
Photo 12-4: Details of Wireless Bridge Connections inside Enclosure .....	143
Photo 12-5: Inside the NEMA Boxes for the AP and Wireless Bridge .....	143
Photo 12-6: Enclosing an AP within a NEMA Box .....	144
Photo 12-7: Enclosing a Bridge within a NEMA Box .....	144
Photo 12-8: Rugged Antenna Connector .....	147
Photo 12-9: LNR 400 Coax Cable .....	148
Photo 12-10: Types of Lightning Arrestors .....	149
Photo 12-11: Copper Grounding Cable Attached to Antenna .....	150
Photo 12-12: Thick Copper Grounding Cable .....	150
Photo 13-1: Guy Wires and Turnbuckle .....	163
Photo 13-2: Simple Attachment of Guy Wires to Tower .....	164
Photo 13-3: Arrow on Antenna to Help Set Polarization .....	166
Photo 13-4: Tower Ready for Raising .....	168
Photo 13-5: View up the Raised Tower .....	168
Photo 14-1: Highly Flexible Professional Signal Analyzer for Wi-Fi .....	174
Photo 14-2: Professional Antenna Alignment Kit for Wi-Fi .....	175

# 1. Introduction

In sparsely settled rural and remote areas, commercial telecommunication services are often marginal if non-existent. Many of these areas are cut off from essential communications services such as voice and basic data. The low-cost answer to this problem may lie in a relatively new wireless technology called *Wi-Fi*.

Wi-Fi was invented to deal with what are called *Wireless Local Area Networks* (WLANs). WLANs are found in homes and businesses. However, we will show you in this book how to adapt Wi-Fi to be a low-cost, high-performing, and reasonably reliable solution to providing entire smaller rural towns and villages with Internet access. This is what is called a *Wireless Wide Area Network* (WWAN).



Some of the important terms and acronyms in this chapter include:

Access Point (AP)	A radio access point (wireless data base station) that is used to connect wireless data devices (stations) to a wireless local area network (WLAN). In this Cookbook, we extend the use of the term to include similar equipment for connection to a Wireless Wide Area Network (WWAN).
Availability	The average per cent of time a system such as a network is running during the day.
Broadband	A communications network in which a frequency range is divided into multiple independent channels for simultaneous transmission of signals (as voice, data, or video). Often informally used in the much looser sense of a high-speed network.
Cable network	<p>Networks that use existing cable TV infrastructure that your cable company uses for TV signals, to transmit data to and from the Internet.</p> <p>Since cable TV was designed as a broadcast system, the cable is shared amongst the users in your neighbourhood and is considered high speed or broadband Internet access.</p>
Channel	<p>A general term used to describe a communications path between two systems.</p> <p>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.</p>
Dial-up	Internet access services that use a telephone line and modem attached to a PC, to connect users to the Internet. This is the most basic form of service for consumers, primarily to access the Internet and World Wide Web.
Digital Subscriber Line (DSL)	A means of accessing the Internet at very high speed using standard phone lines.
Frequency	<p>The number of back-and-forth cycles per second, in a wave or wave-like process. Expressed this way, the frequency is given in units of Hertz (Hz), named after the scientist who first produced and observed radio waves in the lab.</p> <p>Other units are:</p> <ul style="list-style-type: none"> <li>• Kilohertz (thousands of Hz, abbreviated KHz)</li> <li>• Megahertz (millions of Hz, abbreviated MHz)</li> <li>• Gigahertz (billions of Hz, abbreviated GHz)</li> </ul>
Hybrid solution	A mix of different network technologies (e.g., Wi-Fi and fibre) to

---

	achieve a stated objective
Internet Service Provider (ISP)	Companies or organizations that provide access to the Internet
Optical network	A network that carries digitized voice or data at very high rates on multiple channels of light.
Packet	A piece of data transmitted over a packet-switching network such as the Internet
Point of Presence (POP)	A place where there is a major connection to the Internet
Range	The space or extent included or covered by a wireless system.
Router	A device that forwards data packets along networks.
Wi-Fi	Short for wireless fidelity, and trademarked by the Wireless Ethernet Compatibility Alliance. It stands for the IEEE 802.11 standard.
Wireless Local Area Network (WLAN)	Local area networks (LANs) that transmit and receive data over the air, usually in the unlicensed sector of the spectrum, using either radio or infrared technologies, providing users with both access and mobility.
Wireless Wide Area Network (WWAN)	Wireless networks that cover a large geographic area.

---

## Need for Inexpensive Rural or Remote Internet Access

---

Characteristics of a WiFi Network include:

- Minimum *bandwidth* to provide speed equal to or better than dial-up
- Minimal costs
- All-weather operation
- Low electrical power consumption
- High system *availability*
- Ease of local user intercommunication
- Easy and quick installation and expansion
- Ability to restore operations automatically after the network goes down
- Ability to be remotely maintained and monitored
- Self-contained, with no few or no dependencies on other systems
- Flexible enough to serve as the basis for a number of community communications services such as voice, emergency services, radio, TV, etc.

### **Wireless**

In a wireless network, your computer (or computer network) is connected to a wireless modem that either includes a small antenna or can be connected to an external antenna. The antenna is then pointed at a much larger antenna that serves your region, community, or neighbourhood.

There are many possible wireless technologies. Each uses a specific *frequency* (like the *channel* on a TV), and uses different means to encode the signal on a radio transmission.

Typically, each type of wireless technology was developed with a certain application in mind. For example, there are a number of wireless technologies aimed at serving a Wide Area Network (WAN) such as an entire city. One such example is LMDS (Local Multipoint Distribution Service).

If there is little communications infrastructure in place (DSL, cable, optical fibre), then wireless is typically a lot less expensive. Why? Simply because you do not have to dig up the ground.



## **Wi-Fi**

Wi-Fi (Wireless Fidelity) is a set of wireless technologies that was originally designed for application to a Local Area Network (LAN). A LAN typically inter-connects computers within a building. For example, you can use Wi-Fi to connect wirelessly the computers within a house or a small office.

In Wi-Fi, your computer has a Wi-Fi card that has an antenna built into it. Some types also allow you to connect a more powerful external antenna. Your antenna “talks” wirelessly to what is called an *Access Point*, abbreviated AP. An AP includes its own antenna. We will talk a lot about APs in this book. The AP is connected, directly or indirectly, to the Internet at what is called a *Point of Presence*, abbreviated POP. We will also talk a lot about POPs in this book.

There are three varieties of Wi-Fi, with varying characteristics. The variety we will be speaking about mostly in this book allows you to communicate wirelessly at up to 11 Mb/s (millions of bits per second). There is a catch, though. If there are 11 people on the same Wi-Fi frequency at one time, they get only up to an average of 1 Mb/s each. To compensate for this effect, there are several frequencies available.

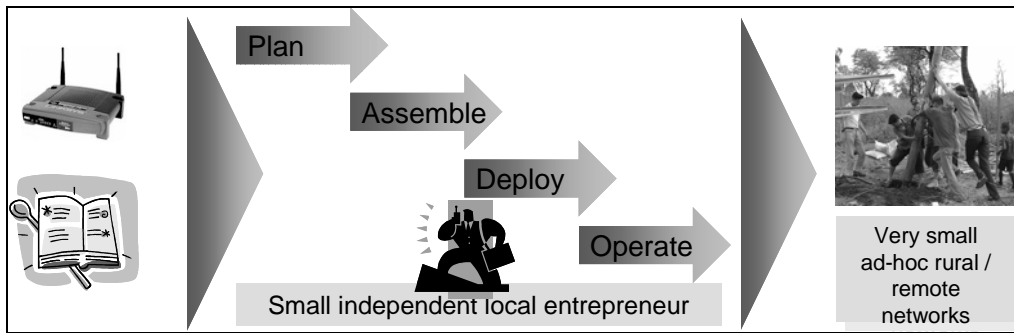
## **What is the Cookbook About?**

---

This book is a set of systematic instructions – a Cookbook of recipes – showing how you can on your own develop and deploy a rural or remote Wi-Fi network using inexpensive off-the-shelf equipment. The network will be a practical way to meet your unique set of conditions of climate, power, terrain, special service needs, and other factors. The cookbook covers recommended approaches, technologies to employ, and system solutions that should meet these challenges. Figure 1-1 shows how the Cookbook helps you plan, assemble, install, and maintain such small networks.

The development of the Cookbook was a joint project sponsored by Algonquin College in Ottawa, Canada, the Canadian International Development Agency (CIDA), Industry Canada (IC), and the National Capital Institute of Telecommunications (NCIT). The research was carried out by Algonquin College and researchers from Network Planning Systems Inc.. This book was specifically adapted for the APEC Telecommunications and Information Working Group.

Figure 1-1: How the Cookbook Can Help You



All of the types of systems and techniques described in the book were validated in the field as part of this project.

### Whom is This Cookbook For?

This book is aimed at three types of people:

- Local community leaders with little technical expertise,
- Entrepreneurs and business people, and
- Technically-oriented people such as engineers or networking specialists,




who wish to:

- Assess whether a Wi-Fi system is a valid option for their rural or remote community
- Assess whether it is the best approach to use, and if it is,
- Plan their Wi-Fi network
- Install it, and
- Operate it.

This book covers a great deal of ground. So, we have introduced icons representing three types of people who might want to read it.

Each of the major parts of the book and each chapter is labelled by one or more icons representing the type of person that would best benefit by reading that chapter or part.

Table 1-1: Three Audiences for the Cookbook

Icon	Type of Person
	Community leader
	Entrepreneur or business person
	Technically-oriented person such as an engineer or networking specialist




























### How This Book is Organized

The book is divided into parts, each of which has several chapters. The five main parts of the book are given in Table 1-2 below, along with their respective chapter headings.

Also listed are the suggested audience for each chapter. You can use these icons to help plan your reading of the book. For example:

- Community leaders without much technical background  
We recommend that such people focus on the first six chapters, with occasional references to the appendices.
- Business people and entrepreneurs  
We recommend that most of their reading focus should be on Part I, with selected chapters from Parts III and IV.
- Technically-oriented people  
We recommend that such people read the entire cookbook.

**Table 1-2: Organization of and Audiences for the Cookbook**

Chapter 1	Introduction			
<b>Part I</b>	<b>Planning Your Network</b>			
Chapter 2	Wi-Fi Local and Wide Area Networks			
Chapter 3	Community Services for You Wi-Fi Network			
Chapter 4	Introduction to Wireless propagation and Coverage			
Chapter 5	Creating a Wi-Fi WWAN and Connecting it to the Internet			
Chapter 6	Serving Outlying Groups of People			
Chapter 7	Powering Your Access Points			
Chapter 8	Planning Your Network Security			
Chapter 9	Identifying What Equipment You Need and Costing it Out			
<b>Part II</b>	<b>Assembling and Customizing the Equipment</b>			
Chapter 10	Setting Up Your Radio Equipment			
Chapter 11	Setting Up Your Network Equipment			
Chapter 12	Packaging Your Equipment			
<b>Part III</b>	<b>Installing Your Network</b>			
Chapter 13	Putting Up your Towers			
Chapter 14	Aligning Your Antennas			
<b>Part V</b>	<b>Appendices</b>			
Appendix A	Acronyms			

Appendix B Technical Terminology



Appendix C References



## Specific Benefits of the Cookbook

Some of the ways this Cookbook can help you in your rural or remote wireless deployment projects are:

- Summarizing for you the knowledge of how to plan, design, build, and maintain such systems in a very practical and low-cost way
- Reducing the level of technical competence needed to successfully plan, deploy, and operate the system
- Reducing the start-up time for your Wi-Fi network
- Helping you to avoid common errors
- Helping you plan Wi-Fi networks that are better suited to your needs.
- Helping you build a communications network that can serve as a good foundation for community services that go well beyond Internet access. Such services could include voice communications, radio, television, emergency services, location services, etc.  
→ See Chapter 3 for more information on community services.

## Limitations of the Cookbook

The Cookbook will help you modify and connect consumer Wi-Fi equipment to create small networks suitable for rural or remote applications. By “small”, we mean a network that has at most several wireless Access Points (APs) which are fairly close to the Internet Point of Presence (POP). Depending on the population density, this might be enough for up to a thousand people, but more likely the limitation is about half of that amount.

However, if your needs go beyond this, you will need the help of professionals or companies who know the types of techniques covered in this Cookbook. Some of these needs include:

- More than a few Access Points
- More than a couple of “hops” between these APs and the POP
- Particularly harsh environmental conditions

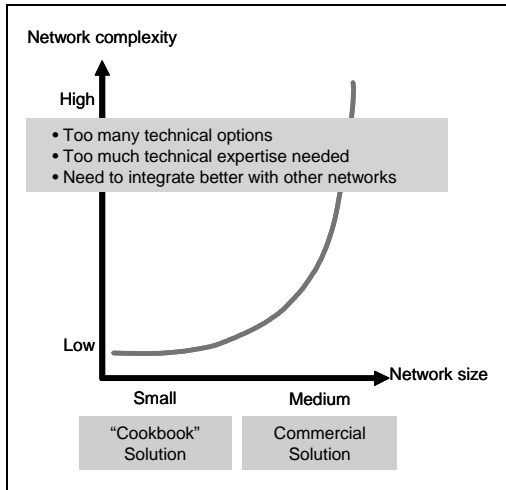
- Specific electrical power needs (e.g., solar power).

The basic reason for turning to professional solutions is increasing complexity; see Figure 1-2.

---

**Figure 1-2: Network Complexity Rises Faster than Network Size**

---



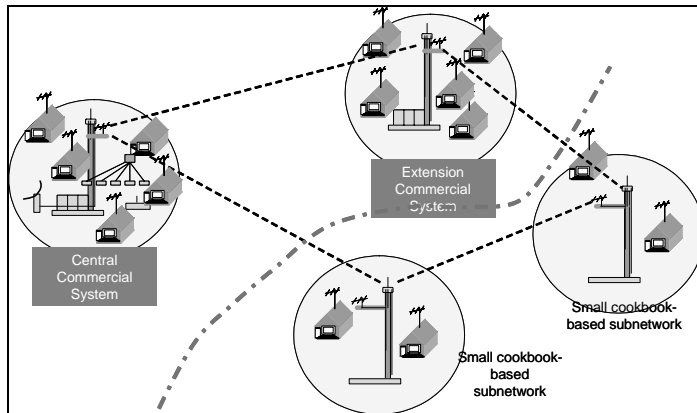
➔To help you in this case, we have made a short list of some of these companies..

## Combining Cookbook Approaches with Commercial Ones

---

The approaches to providing Internet access discussed in this Cookbook are usually complementary to commercial ones. See Figure 1-3.

Figure 1-3: Cookbook Solutions on Outskirts of Commercial Ones



## A Note about Jargon

Jargon is the use of specialized terms, phrases, or acronyms. In any technical discussion, the use of jargon is essential. However, jargon can be confusing if you do not know what it means. Therefore, our approach to jargon in this Cookbook is:

- Avoid it if possible
- Define it the first time it is used
- Start each Chapter with a list of the most important jargon you will encounter in that chapter.
- Provide reference appendices (A and B) defining all technical terms and acronyms used in the book, or in the general field. Thus, if in your other reading about the subject you encounter a strange piece of jargon, you may find its definition in the appendices.

## Other Icons Used in This Book

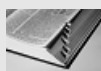
We use the following icons throughout the Cookbook. They are used to point out particularly important information.



Helps you avoid common pitfalls or dangerous situations



Cross-references to point you to other locations in this Cookbook that will provide supplemental or supporting information.



Demystifies wireless and telecommunications jargon.



Gives addresses, phone numbers, and/or web site information. Information next to this icon may help you find small useful pieces of information for your Wi-Fi network.



A note with additional information.



Flags useful information that even some experienced wireless network engineers might not know.

---

## Where to Go From Here

---

We cannot possibly cover all aspects of Wi-Fi here. So, below is a very short list of sources of further information.

### **Books**

Wi-Fi Handbook: Building 802.11b Wireless Networks	Frank Ohtman and Konrad Roeder	Publisher: McGraw-Hill Professional; 1st edition (April 10, 2003) ISBN: 0071412514
Deploying License-Free Wireless Wide-Area Networks	Jack Unger	Publisher: Cisco Press; 1st edition (February 26, 2003) ISBN: 1587050692
How Wireless Works	Preston Gralla	Que Publishers
Building Wireless Community Networks	Rob Fleckinger	2nd Ed, O'Reilly Media

---

### **Web Sites**

802.11 news	<a href="http://www.80211-news.com/default.asp">http://www.80211-news.com/default.asp</a>
Unstrung	<a href="http://www.unstrung.com/">http://www.unstrung.com/</a>
Broadband Wireless Exchange Magazine	<a href="http://www bbwexchange.com/">http://www bbwexchange.com/</a>

---

### **Consulting Companies**

Instead of doing it all yourself, you might consider hiring a company to do it for you. The types of companies include Consultants, System Integrators (SIs) and Value-Added Resellers (VARs). Depending on the type of com-



pany, they may include various services as part of the package they sell you. Such services may include:

- Broadband franchise
- *Turnkey systems*
- Installation
- *Network planning*

A list of general wireless consultants, SIs, and VARs is at the website:

<http://www bbwexchange.com/news/2004/jan/bwe010204.asp>.



The vast majority of consultants, SIs, or VARs do not specialize in rural wireless. Ones that we know about are:

BTPGroup LLC	<a href="http://www.btpgroup.net/">http://www.btpgroup.net/</a>
FDM Broadband	<a href="http://www.fdm broadband.net/">http://www.fdm broadband.net/</a>
Remote Wireless Access Systems Inc	<a href="http://www.rwas.com">http://www.rwas.com</a>

### ***Equipment Manufacturers***

These can also be a source of information. Some of the major manufacturers of consumer Wi-Fi gear are:

Linksys (part of Cisco)	<a href="http://www.LinkSys.com">http://www.LinkSys.com</a>
D-Link	<a href="http://www.Dlink.com">http://www.Dlink.com</a>
SMC Networks	<a href="http://www.smc.com">http://www.smc.com</a>





**Part I:  
Planning Your  
Rural Wi-Fi  
Wide Area  
Network**

# In this part...

- Chapter 2 introduces you for the first time to the types of Wi-Fi equipment in wide-area networks, their functions, and how they fit together into a network. Unlike most books on Wi-Fi, we avoid at this point any detailed technical discussion of Wi-Fi, and instead focus on the networking aspect.



- Chapter 3 helps you plan for adding community services that you want to deliver on your Wi-Fi network.



- Chapter 4 is a simple tutorial on how wireless signals propagate and how to achieve wireless coverage, with an emphasis on Wi-Fi.



- Chapter 5 looks at how to hook up your APs to the Internet Point of Presence (POP) in your community, or to each other. This allows you to form a WWAN to cover a single community or several close by communities.



- Chapter 6 looks at extending a community's coverage to include nearby small clusters of people outside of the main communities.



- Chapter 7 deals with electrical powering issues for your AP. A prime consideration in making your Wi-Fi network reliable is making sure you have a reliable source of clean power.



- Chapter 8 guides you through developing a security plan for your Wi-Fi network. Even a small network can benefit from working through security issues before you install the network.



- Chapter 9 helps you make a detailed list of equipment you will need to purchase. It also gives a simple network budget example for you to customize.



## 2. Wi-Fi Local and Wide-Area Networks

In this chapter, we are going to take our first look at Wi-Fi local and wide area networks – the types of equipment used, what they do, and how they fit together. We will use a small but representative type of Wi-Fi network suited for rural coverage as our means of illustrating all this.

**Suggested audience for this chapter:**





Important terms in this chapter include:

Bridge (noun)	A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol.
Directional antenna	An antenna that focuses its energy into a limited beam width.
Ethernet	A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976.
Firewall	A system designed to prevent unauthorized access to or from a private network.
Gain	The amount of increase in signal power or voltage or current expressed as the ratio of output to input.
High-gain antenna	An antenna whose maximum gain is very large.
Hub	A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN.
Microwave	The subset of the Electromagnetic Spectrum encompassing wavelengths between .03 and 30 centimetres, corresponding to frequencies of 1-100 Gigahertz.
Port	An interface through which data is sent and received.
Protocol	An agreed-upon format for transmitting data between two devices.  The protocol determines the following: <ul style="list-style-type: none"> <li>• The type of error checking to be used</li> <li>• Data compression method, if any</li> </ul>
RADIUS server	Remote Authentication Dial-In User Server / Service. A server for authentication, authorization, and accounting of endpoints and endpoint aliases.
Reach	The distance an antenna of a certain type and height above average ground level can transmit with adequate power over a certain type of terrain, given a receive antenna of a certain type and height.
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.
SMC Connector	A type of connector, used in Wi-Fi client cards, amongst other uses.  The SMC name derives from SubMiniature C (the third sub-

## Chapter 2: Wi-Fi Local and Wide-Area Networks

---

miniature design). The SMC design was developed in the 1960's. SMC has threaded coupling, with 10-32 threads. It is available in 50 and 75-Ohm impedances.

Stub antenna	The stubby antenna on most Wi-Fi cards
Wireless Bridge	A bridge that operates wirelessly.
Yagi antenna	A highly directional type of antenna.

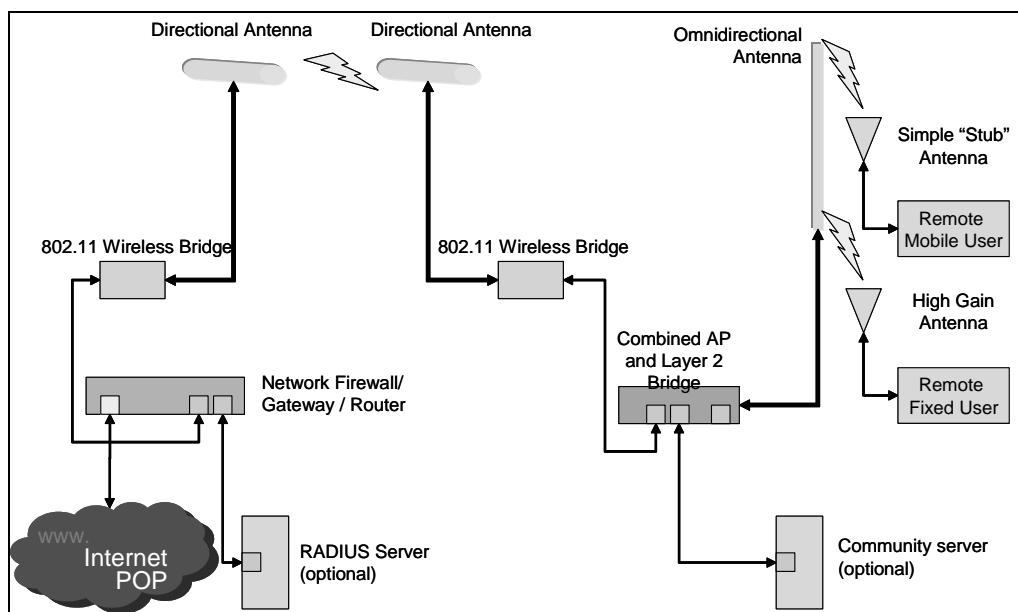
## A Basic Wi-Fi Wireless Wide Area Network

In order for your network to work correctly and provide good performance, you have to start by specifying:

- What types of equipment are to be used,
- What their main functions or capabilities are, and
- How they are interconnected so they can work together.

This is all at a very high level. This specification is usually documented by means of a simple diagram such as Figure 2-1, with few if any details. (Many details will come later in this Cookbook.)

**Figure 2-1: A Basic Wi-Fi Wide Area Network for Rural Coverage**



We are going to go through the parts of this diagram, from right to left. We will start from the “user” end and work our way up to the Internet, so you can see how things fit together. At each stage, we will first look at the types of equipment used and what they do (their functions). Then we will look at how that type of equipment is connected up to others so that everything works together to form a workable WWAN.



Before we leave this diagram, though, it is well worth pointing out that this type of setup was not pulled out of the air. We designed it specifically to meet the following objectives:

- Ease of set-up of wireless APs and supporting network equipment, using a mix of auto configuration and manual setups
- Stability under highly variable traffic loads and varying channel quality
- Scalability: can be enlarged easily to larger networks
- Performance: good throughput, etc.
- Facilities management, including system monitoring, updating of software, or change in configuration.
- Security of the wireless services (AP and backhaul) from unauthorized access
- Ease of adding new users by the local network maintainer.

### Types of Users

---

In a typical rural coverage situation, users will fall into different types that determine the appropriate approach to use. We suggest that your design take into account the differences between three main types of users, and which type your WLAN/WAN will be primarily for.

#### **Fixed users**

These are homes, schools, businesses, or public or government buildings that are each connected to the Wi-Fi network at one location that does not move around. They are likely the main types of users for which you will be designing your WLAN/WAN.

Fixed users need the following equipment:

- A Wi-Fi card or plug-in board for a PC (Photo 2-1), or a consumer Wi-Fi Access Point of their own (Photo 2-2).

For reasons that will be explained later, the Wi-Fi equipment should support what is called the “b” version of the 802.11 standard.

- The Wi-Fi card, board, or AP is then connected via
  - A coaxial cable (Photo 2-3) using an N-connector (Photo 2-4) to
  - An antenna mounted in a window or on the outside of their building (Photo 2-5) and pointing at their local community Access Point (Photo 2-6).

Photo 2-1: Wi-Fi Card for a Notebook and Plug-in Wi-Fi Board for a PC



Photo 2-2: Example of Consumer AP (D-Link)

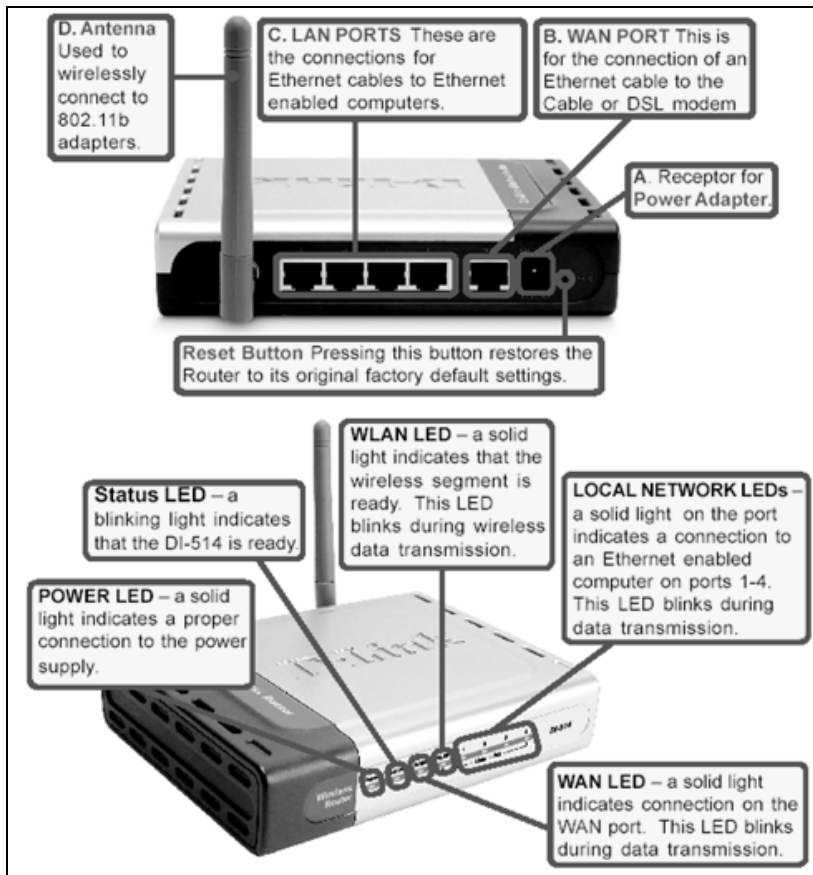


Photo 2-3: Coaxial Cable

---



Photo 2-4: N-Connector

---



Photo 2-5: Antenna on Residential Window

---



This is a simple sectored antenna

## Photo 2-6: Coverage and Backhaul Antennas on Top of a Local AP

---



The antenna on top is the omnidirectional antenna ("Omni").

Below it is the backhaul antenna, pointing horizontally.

You can see the coaxial cables connected to each antenna.

The user's Wi-Fi equipment *must* be of a type that has a detachable antenna. If you have a Wi-Fi card like that depicted in Photo 2-1, you will first need an SMC to N-type adapter (Photo 2-7). The SMC part goes in your card; the N-type adapter goes to the coax cable.

## Photo 2-7: A Variety of SMC Adaptors for Wi-Fi Cards

---



The further away the user is from the local AP, the higher *gain* their antenna must be. This enables further distances as well as higher transmission stability on shorter paths.

---

**An antenna's gain is measured in dBi. Three dBi corresponds to a doubling of power. Therefore, an antenna with 9 dBi of gain can pick up signals 8 times smaller. The math works out this way: 9 dBi = 3 dBi + 3 dBi +3 dBi, so the power is doubled, doubled again, and then doubled a third time, which gives 8 times overall.**

---

Modest elevation of the user's antenna can also be used in addition to antenna gain to achieve a better path clearance between the antennas. The type of antenna needed and how high it needs to be mounted is mostly determined by how far away the user is from the local AP:

- For distances of 1 km or less away from the local AP, the simple antennas supplied with the user's Wi-Fi cards or APs might work acceptably. However, a simple directional antenna such as shown in Photo 2-5 would be better.
- For distances of 3 to 6 km, antennas of up to 14 dBi gain (such as a Yagi or flat panel) along with 2 to 4 metres elevation are likely to be needed. Photo 2-8 shows a Yagi. The horizontal antenna in Photo 2-6 is also a Yagi.
- For very remote users, you should use a 25 dBi gain parabolic dish antenna. Here, elevation of the antenna must be higher to achieve a reasonable line of sight with the AP. Photo 2-9 shows such a dish on the ground, about to be installed.

→ A more detailed discussion of antenna gain and height needed is given in Chapter 3, after we have covered the basics of how wireless signals propagate.

## Photo 2-8: Yagi Antenna

---

Photo courtesy Harvard University



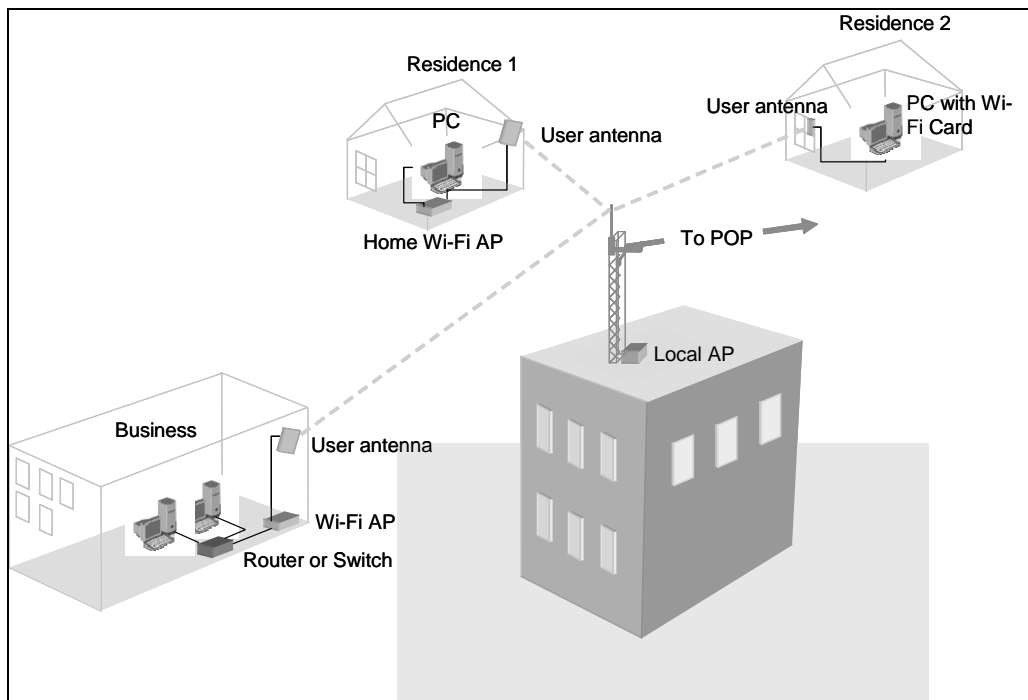
## Photo 2-9: Parabolic Dish Antenna Ready for Installation

---



Wireless communications flow between the user's antenna and the antenna for the local AP, as shown in Figure 2-2. Wi-Fi signals are at a frequency near either 2.5 GHz or 5 GHz. These frequencies are unlicensed. That means they can be used by all sorts of equipment such as cordless phones or microwave ovens without regard for how they interfere with each other. One of the main reasons for preferring to use a high-gain user antenna is that such antennas are usually directional. Therefore, interference is cut down considerably.

Figure 2-2: Communicating between the Local AP and the Fixed Users



**Fixed/mobile users**

These are users that may set up temporary portable directional antennas that will not move around while set up. An example might be a local group that wants to use the Wi-Fi network to do a community broadcast of a sports event.

Such users are likely to be rare in the next couple of years. However, it is already technically feasible and economical to set up temporary Wi-Fi equipment to:

- Provide Internet coverage at an event
- Broadcast radio from an event over the Wi-Fi network
- Broadcast television from an event over the network.

### **Mobile users**

This includes anyone who is outdoors and uses Wi-Fi enabled laptop computers, *Personal Digital Assistants (PDAs)* such as Palm Pilots or Pocket PCs, or portable IP phones. Serving outdoor mobile users will only be practical in the immediate vicinity of the AP.

As of today, there are not that many outdoor mobile users, even in developed urban areas. Therefore, generally you do not want to design a rural wide-area network around this type of user. An exception might be if you want to provide supplementary coverage for situations like schoolyards or outdoor businesses.

You do not really see many people wandering about using portable Wi-Fi equipment yet, especially in rural areas. An exception might be people who work mostly outdoors and whose job requires them to have constant wireless access to data. By the very nature of their mobility, they will be forced to use the built-in *stub* antenna in their Wi-Fi equipment. That implies they must not be more than 1 km away from the local AP. You might have to install an additional local AP just to serve such a mobile group of people with low-gain antennas.

## **Local Access Point Antennas for Coverage**

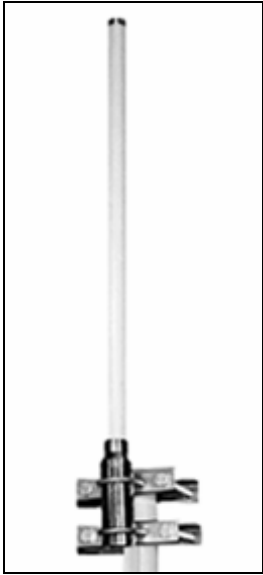
---

### **Omnidirectional Antennas**

Local APs will typically use high-gain omni-directional antennas (8 or 9 dBi) for a roughly circular coverage footprint. Omnis, as they are often called, pick up or radiate signals from all horizontal directions equally, in a 360° pattern. They stick up vertically in the air. Photo 2-10 shows one.



Photo 2-10: Omnidirectional (“Omni”) Antenna



High-gain AP omni-directional antennas are usually mounted on a tower at a significant elevation (10 m to 15 m). This elevation dictates the direct line-of-sight *reach*. When combined with the high gain, elevation helps in two ways:

- It increases the coverage, by providing a very usable coverage radius of several kilometres or more with simple user antenna installations.
- It improves the reliability of the signal to the user’s antenna.

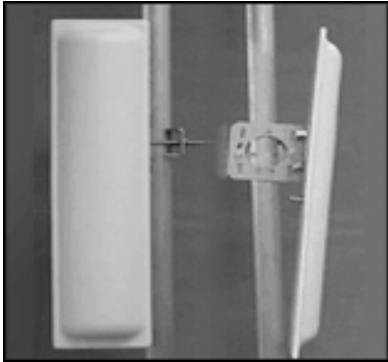
To improve the Omni’s reach further, you can place the tower on top of a building, like in Figure 2-2, or on top of a local hill or other rise in elevation.

The Omni antenna will be on the same tower as the *backhaul* antenna. Typically, both are mounted at the same elevation above ground level. See Photo 2-6 for an example.

### **Sectored Antennas**

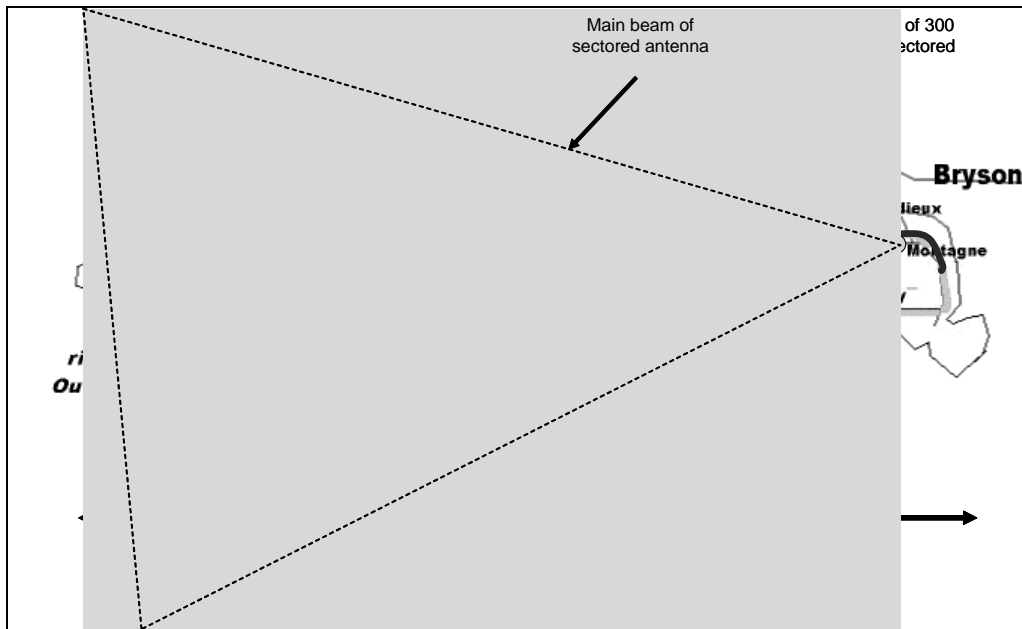
Your target coverage area may not be anything like a uniform circle. If so, the AP can employ *sectored antennas*. A sectored antenna just covers one horizontal sector (wedge) of, say, 45, 60, 90, 120, or 180° instead of the full 360° that an Omni covers. See Photo 2-11.

Photo 2-11: Two Views of a Sectored Wi-Fi Antenna (14 dBi Gain, 60 Degree Beam)



The shape and size of your target coverage area will determine how many sectors you should use, the angle each should cover, and the gain each should use. Figure 2-3 shows a simple example of how this might be done, with a single sectored antenna placed at one elevated end of a rural island community in Canada.

Figure 2-3: Coverage of Island Community using a Sectored Antenna



### **Connecting the Antenna to the AP**

The antenna that provides Wi-Fi coverage is connected to the Wi-Fi AP by means of a thick coaxial cable that carries signals between the two. Photo 2-6 shows such a cable connecting the Omni (pointing up) to the AP at the base of the tower. Photo 2-3 shows the type of cable to use.

## **Access Point Equipment**

---

### **The Basics**

There are two potentially confusing aspects of Wi-Fi equipment that we had better consider now.

*First*, such equipment can run in a number of *modes*, with the mode determining the function of that Wi-Fi equipment in the network. These modes are:

- *Ad-hoc*  
This is a mode for two users to communicate directly, without a Wi-Fi AP. We will not be saying anything more about this mode, because it is not relevant to creating a Wi-Fi WWAN.
- AP  
This is the mode used when the Wi-Fi equipment acts as an access point.
- Gateway/bridge  
This is the mode when the equipment is used to relay traffic between two parts of the Wi-Fi network. This is more specifically called a *wireless bridge* in this Cookbook. It is not to be confused with a bridge, discussed below.

*Second*, Wi-Fi equipment can be combined with other networking equipment in the *same* box. For example, consumer Wi-Fi APs often include a *switch* or a *router*, which are used to control traffic flow in various ways and to help in maintaining the network. The switch may also be called a *hub* or a *bridge*, just to confuse terminology further. Figure 2-1 shows such a combination box, which has both an AP function and a bridge.

### **Combined AP and Layer 2 Bridge**

The network layout shown in Figure 2-1 is based on what is called “Layer 2 bridging”. All you need to know about this jargon right now is that it is de-

signed to enable a simple as possible connection to the Internet by the user.

This connection requires several key elements in addition to the 802.11 radio equipment, such as a *firewall/gateway/router* (on the left of Figure 2-1) and a layer 2 switching hub (near the right). These networking elements provide the following benefits:

- They provide the necessary isolation from Internet traffic that is not intended for our Wi-Fi users
- They allow efficient use of the radio resources (bandwidth, channels, etc.)
- They allow easy scaling up of the network to cover more users or deploy more APs.
- They permit straightforward management of the facilities.

If there are two users on the same AP, the traffic between them will go only as far as the AP. It will not flow up the backhaul to the POP and then back down again. There are two benefits of this arrangement:

- Unnecessary traffic is kept off the backhaul
- The users on the same AP can still communicate with one another even if the backhaul is temporarily out of service.

In our own test network, we used a LinkSys Router AP to serve the functions of the combined AP and Layer 2 Bridge and another identical LinkSys Router AP to serve the firewall/gateway/router functions. This type of equipment features a 4-*port* Layer 2 switching hub along with a router / gateway port for direct interface to the Internet. We selected the LinkSys AP primarily due to its layer 2 hub functions, which eliminate the need for a separate piece of equipment to provide a bridging function.

Because of its *Ethernet* ports, this equipment can easily interface to other equipment. For example, one 100 Mb/s Ethernet cable with RJ-45 connectors goes to the 802.11 Wireless Bridge. If you have other, Ethernet-based equipment in the field such as the local community server mentioned immediately below, these could also be easily connected via Ethernet.

## Optional Local Community Server

---

Suppose you want to allow community members served by the AP to access some community resource, such as information from a local library or

health facility. Also, suppose that resource is not to be shared with communities on other APs (or if there are no other APs in your network). Then the best place to put a server with that information is directly on the local AP shown in Figure 2-1, through one of its Ethernet ports.

On the other hand, if you have a network of several APs and you want to share some resource amongst all of them, you should connect the server to the gateway/firewall shown in Figure 2-1.

### What is the Backhaul?

---

The connection to the “outside” world and the Internet requires the linking of your wireless LAN to a POP or point of presence that provides a gateway into the main public IP networks. This is a standard approach for all wired or wireless LANS as well as private wide area networks or WANs that must also link into the public IP.

The POP is often not located where your WLAN/WAN will be. As a result, you will need a transmission facility to connect your WLAN/WAN via a gateway router to the POP. This link is also known as a backhaul facility. Its main purpose is to provide a two-way channel with enough capacity to handle the total traffic demand from the users of the WLAN to the public IP networks. The link can be via satellite, fibre optics, wired such as coax cable or DSL, or perhaps point-to-point digital microwave radio. The latter can be a Wi-Fi system or a commercial digital radio service.

For most rural and remote situations, satellite or terrestrial microwave links spanning tens of kilometres between towers are required to reach a portal to the public IP network. The POP can be provided by a commercial Internet Service Provider or by a telephone company.

You can also use backhaul facilities to link a number of APs together in a daisy chain or even in a mesh-like network that connects to the public networks.

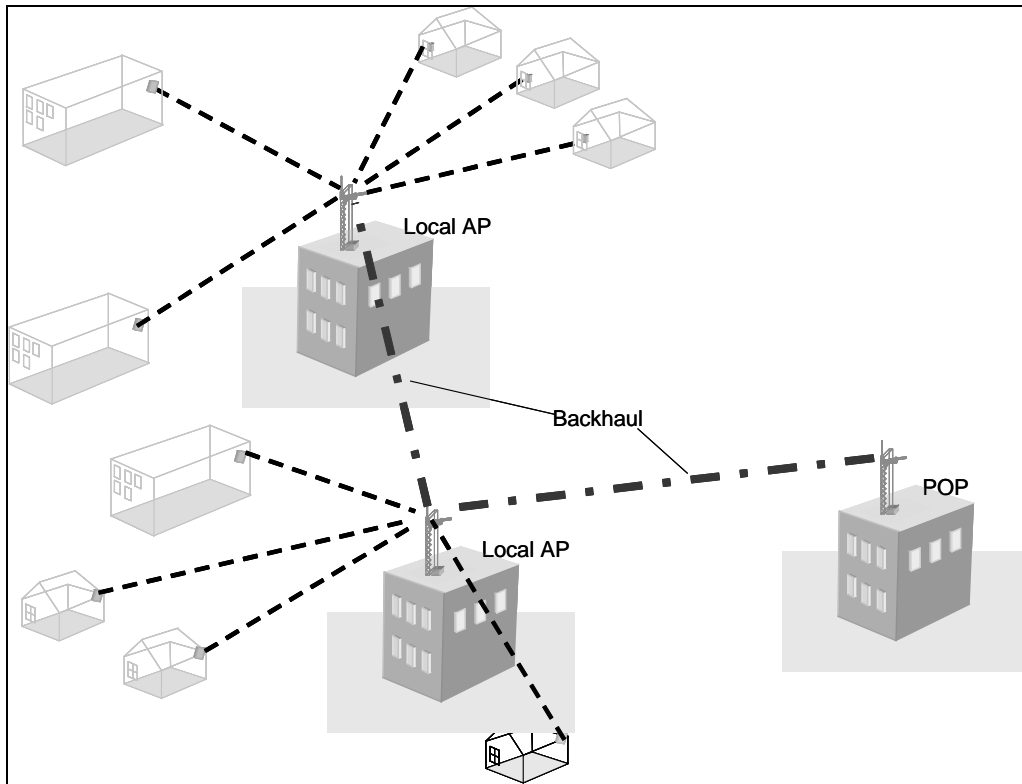
➔ As discussed in Chapter 5, this is how to expand coverage of your WLAN/WAN.

### 802.11 Wireless Bridge in Field

---

See Figure 2-4 for a view of how the local AP and POP are connected via the backhaul. The backhaul is a set of links carrying traffic between the POP and all the local APs.

Figure 2-4: Relationships between Local APs, Backhaul, and POP



The next link in the equipment chain is the Wi-Fi box in the field that bridges between the local AP and the equipment near the POP. This box is used for the backhaul. There are two important things in setting up this equipment<sup>1</sup>:

- It must be set up in wireless bridge mode.
- Its radio should be set to operate on a non-overlapping frequency (channel) with respect to the AP and the users. This helps ensure that radio interference between the backhaul and the AP will not be a problem.

<sup>1</sup> Chapter 10 tells you the details of how to set this up.

In our own test network, we used two D-link 2100 APs as wireless bridges, one in the field, and one near the POP. This type of equipment is known for its good support of bridge mode operation<sup>2</sup>.

The wireless bridge is connected to its antenna by the same type of coaxial cable mentioned earlier in this chapter. This cable carries the traffic between the box and its antenna. Photo 2-6 shows the cable from the bridge at the base of the tower to the horizontally mounted backhaul antenna.

### Directional Antennas for Backhaul

---

We have already mentioned directional antennas. They are used in the backhaul, for several reasons:

- To allow longer radio hops on the backhaul.  
These hops can be as long as 10 km or more, depending on terrain and climate.
- To reduce interference from radio sources outside the main beam of the directional antenna.
- To improve the radio link reliability against fading, e.g., due to rain.

There is one directional antenna in Figure 2-1 which points up the backhaul, and another that points down it. For the radio link between them to work, these two antennas need to point at each other with a fair degree of accuracy.

→ Chapter 9 gives you the details of how to do this alignment.

You should select directional antennas that are high-gain, perhaps 15 to 28 dBi. They also usually need to be mounted fairly high to avoid obstacles that interfere with radio propagation.

→ Chapter 3 covers the details of what gains and heights to use.

### 802.11 Wireless Bridge at Point of Presence

---

This equipment is set up very much like the similar bridge out at the local AP in the field. It is connected by coax cable to the directional antenna, and is set up in bridge mode. Then, it is connected via Ethernet to the Wi-Fi gateway.

---

<sup>2</sup> Initially, we used older model 900's, but they proved to have trouble bridging consistently, and had a radio design that did not optimally match external antennas. These problems were fixed in the 2100s.

## Network Gateway/Router/Firewall

---

This is a Wi-Fi box that can also serve as a router. There is a variety of consumer Wi-Fi equipment that can do this, but it needs to be set up properly.

→ Chapter 11 tells you how to do it.

If you cannot find Wi-Fi equipment that does routing, you will have to buy a router in a separate box and connect it via Ethernet to the Wi-Fi box. This arrangement has two disadvantages:

- It is more expensive to buy
- It is more complex and expensive to maintain.

## Optional RADIUS Server

---

*RADIUS* is an acronym for Remote Access Dial-In User Service. The name survives from the days when remote users accessed networks almost exclusively via dial-up. It is used to enforce security in the network.

→ Chapter 8 describes RADIUS servers in more detail.

The main things you need to know here are that:

- Such a server is optional
- Without it, there still are fairly strong security measures for your network
- It provides the highest level of security.



# 3. Community Services for Your Wi-Fi Network

The main reason you are probably thinking of setting up a community Wi-Fi network is Internet access. However, you should be aware that there are a variety of community services that you could carry on your Wi-Fi network that go beyond Internet access. Some of these are quite straightforward, such as e-mail. Others are more complex, such as setting up virtual private networks or local TV stations.

This chapter is intended to give you some inspiration about what you might deliver. It does not provide a great amount of detail about setting up these kinds of services.

## **Suggested audience for this chapter:**





Important terms in this chapter include:

Encryption	A method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data.
Quality of Service (QoS)	The ability to define a level of performance in a data communications system.
Virtual Private Network (VPN)	A means of establishing secure communication channels on the Internet using various forms of encryption.
Voice Over IP (VoIP)	A technology for transmitting ordinary telephone calls over the Internet using packet-linked routes.
Wireless Internet Service Provider (WISP)	An Internet Service provider whose network delivers the service wirelessly.

## Community Services

If you are setting up your own POP(s) for the community, you are in effect becoming a Wireless Internet Service provider (WISP). An online survey of entrepreneurs who want to become a WISP is available on the web site:

<http://www.bbwexchange.com/>

From the results of this survey (which is likely North American-oriented), we have calculated in Table 3-1 the percentage of respondents who wish to serve their customers with different types of services.

**Table 3-1: Most Popular Services for North American WISP Entrepreneurs**

Service	% of Respondents Who Wish to Provide This Service
Residential Service	77%
Business Service	73%
Email Hosting	69%
Wired LAN Installation	64%
Wireless LAN Installation	64%
In-Home Wireless Networks	55%
Hot Spot Access Point Service	53%
Voice over IP	53%
Virtual Private Networks (VPN)	47%
Point-to-Multipoint Links	46%
Web Hosting / Collocation	44%
Point-to-Point Backbone Links	41%
Network Planning and Installation Services	37%
Network Management Services	37%
Web Site Design	36%
Application Hosting	30%

Most of these services are common to any ISP, such as:

- Residential service
- Business service
- Web hosting
- Web site design
- Email hosting
- Application hosting.

Others are outside the scope of this book, because they relate to inside networks:

- In-home wireless networks
- Wireless LAN installation
- Wired LAN installation
- Network planning and installation services
- Network management services.

Others are just enabling capabilities that are provided by the Wi-Fi WAN anyway, such as:

- Point-to-multipoint links
- Point-to-point backbone links.

That leaves us with a couple of Wi-Fi-based *network* services, which we will discuss a bit further below:

- Voice over IP
- Virtual private networks

We will also be covering two more possibilities:

- Internet radio station
- Internet TV station.

## Voice over IP

---

### **Overview**

Voice over IP (VoIP – pronounced “*voypp*”) is one of those technologies that always seem to be on the verge of becoming widespread. VoIP can provide person-to-person calls within the community, between nearby isolated communities in the same region, or between the community and the outside world.

By its name, you can see that VoIP can “run” over any IP-based network, and that includes Wi-Fi networks. However, with current Wi-Fi networks, there is *no guarantee* that there will be good voice quality, or to use the technical term, *Quality of Service (QoS)*. The reason is that basic IP networks are designed for data transmission, not voice transmission. Without some QoS mechanism, an IP network could scramble the voice signal, cause unacceptable delays, etc.

### ***VoIP Standards for Wi-Fi***

The IEEE standards organization is also expected to ratify, at the earliest the end of 2004, a Quality of Service specification for Wi-Fi networks called IEEE 802.11e. The specification will have two components:

- WME (Wi-Fi Multimedia Extensions)  
Developers can use this to assign priority to packets.
- WSM, (Wi-Fi Scheduled MultiMedia)  
This will control resource management for bandwidth.

On the business side, QoS will be mainly targeted in voice over Wi-Fi applications. Eventually, it might manage cell phones that include Wi-Fi and switch between networks as appropriate.

### ***What you can do now with VoIP on Wi-Fi***

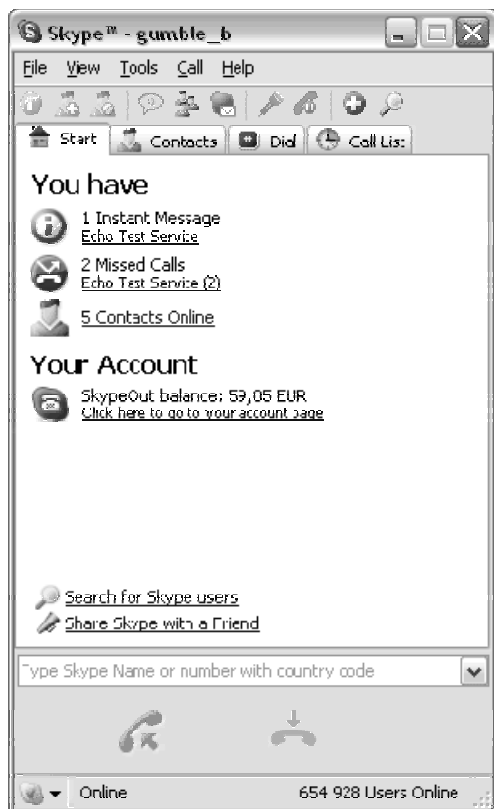
Fortunately, you do not have to wait for these standards to take advantage of VoIP on your Wi-Fi network:

- For calls within your own community  
Each user will need a microphone and speaker for their PC, plus simple free point-to-point conferencing software such as NetMeeting<sup>3</sup>. If you have designed the Wi-Fi network the way we advised, such person-to-person voice calls will stay entirely within the community Wi-Fi network, with few voice problems as a result.
- For calls from your community to the world outside  
There are free services that allow you to make a call from your PC to anyone else in the world who has signed up for the service. For example, one of the largest is Skype (see Figure 3-1). Such services do charge if you call a regular phone number, however, rather than a PC.

---

<sup>3</sup> Other conferencing software such as MSN or Windows Messenger needs to be routed via a server on the Internet. The result is lower voice quality.

Figure 3-1: Example of Large VoIP Service (Skype)



## Virtual Private Networks

VPNs are intended for local businesses, government, or other organizations with more than one location, who need secure communications between those locations.

Companies have used private data networks for many years with technologies such as private lines and Frame Relay. These solutions offered secure connections between enterprise locations enabling the transfer of company information/data. IP VPNs extend this capability to medium and small businesses by leveraging the public IP network infrastructure as a transport vehicle and placing services such as security (firewalls, intrusion detection, and authentication), virtual routers, and bandwidth management into the network.

Today, the equipment needed to establish a VPN for an organization is a single router with VPN capabilities at each location where the VPN will ex-

tend. Most commercial (non-consumer) routers today have such VPN capabilities. Such VPN routers lie between the location's LAN and its connection to the Wi-Fi network.

Be aware, though, that configuring IP equipment to interconnect multiple locations securely can be a daunting task.

## Internet Radio Station

---

Setting up a community radio station can involve no more than getting a plug-in PC card, a microphone, and audio sources.

## Internet TV Station

---

### ***Equipment***

Today, it is possible to set up a sophisticated Internet TV station for your community with an equipment budget measuring only in the few thousands of dollars. You can buy such equipment off-the-shelf or you can assemble it yourself. Here are some equipment options, going from least to most sophisticated:

- A plug-in PC card, microphone, camera, and other video sources
- Windows streaming media server software, running on a PC server  
Such a media server makes all sorts of advanced capabilities possible (hi-definition TV, 7-channel surround sound, etc.)
- A self-contained video box, which combines hardware for video processing and the media server software. See Photo 3-1 for an example.

### ***What you can do With It***

You can use your Internet TV station to distribute (locally or across province or territory):

- Locally-made shows
- On-demand video community news and public announcements
- Community-based E-learning

See Figure 3-2 for an example.

### Photo 3-1: Parts of a Portable Wi-Fi-based TV Studio

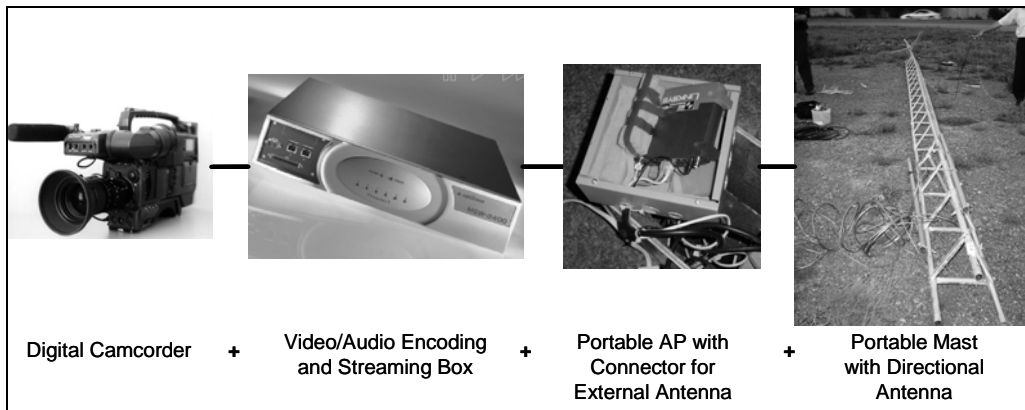
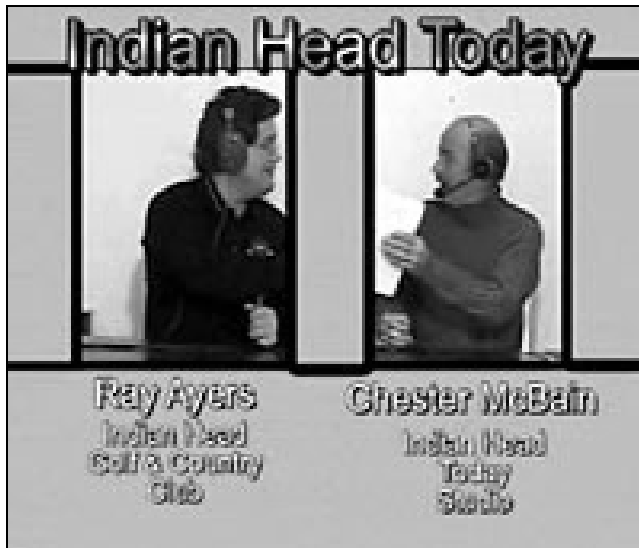


Figure 3-2: Local Community Internet TV Station (Indian Head, Canada)



*"... when the Internet started really blooming, we found out that, hey, we can actually have our own television station and give people the information that way."*

CBC Newsworld March 2004.



# 4. Introduction to Wireless Propagation and Coverage

Even if you are a non-technical person, it is important to understand some of the basic concepts behind how wireless signals propagate. The main reason is that wireless propagation directly affects the coverage question: how many APs are needed to cover a given community.

That in turn affects the budget needed for the Wi-Fi network and the degree of technical expertise needed.

Wireless propagation has two main aspects:

- An AP's *reach* (essentially, how far it can go), and
- The average *throughput* per user (essentially, how good the performance is).
- This chapter gives a *non-technical overview* of these aspects and what determines them. .

**Suggested audience for this chapter:**





Important terms you will learn in this chapter include:

Amplifier	A device for converting an input signal (usually low level) into a larger version of itself.
Clearance	The amount of additional height you have to account for above obstacles in order to transmit a good wireless signal
Digital	Describes when information - speech, for example - is encoded before transmission using a binary code — discrete, non-continuous values.
Reach	The distance an antenna of a certain type and height above average ground level can transmit with adequate power over a certain type of terrain, given a receive antenna of a certain type and height
Receiver Sensitivity	
Throughput	The amount of data that can be sent from one location to another in a specific amount of time. Usually measured in Kb/s, Mb/s, or Gb/s.

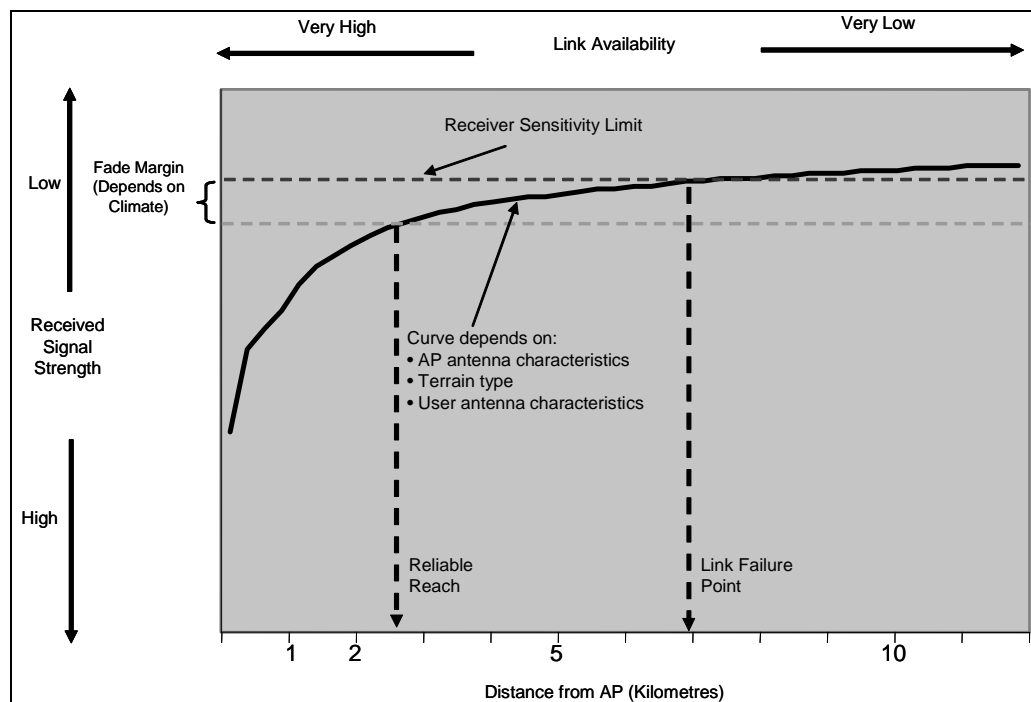
---

## Reach

Reach is how far an AP wireless signal can go without a user experiencing an unacceptable level of performance. The performance level is measured by the percentage of time that the link is “up” (i.e., available). The farther the user is away from the AP, the lower the availability. Due to weather, wireless link availabilities 100% of the time are just not possible.

We will start by presenting Figure 4-1 which puts everything together. Then we will discuss each of the various factors that affect reach in more detail.

Figure 4-1: Definition of Reach



In this figure:

- The distance the user is from the AP is shown at the bottom, with distance increasing towards the right.
- The signal strength that the user receives is on the vertical axis. Strength *decreases* as we move up the axis.

- The solid curve represents the received signal strength at different distances from the AP. The curve depends on a number of characteristics that we will discuss below. For example, if you increase the height of the AP antenna, the curve will shift down.
- The percentage of the time that the link is functioning (the availability) is shown at the top. The further the user is away from the AP, the lower the link availability. Typically, you would like the link to be available 95% or more of the time for users.
- The top dashed horizontal line represents how low a signal strength the user's receiver can detect. Signals whose strength is below the *receiver sensitivity* are so low they are drowned out in the noise.
- The point at which the solid curve meets the receiver sensitivity line occurs at a distance away from the AP that we will call the link failure point. At that distance, the signal is so low it cannot be detected and the link availability drops to nearly 0%. Clearly, you cannot serve users beyond this point without changing something like antenna heights or gains.
- It is therefore prudent to introduce a certain margin to how low a signal strength you take things, to reduce the effect of signal fading. This fade margin reflects:
  - Your preferences on what is an acceptable link availability
  - The influence of climate. Climates that involve a lot of rain or humidity will need additional margin.
- The horizontal line below the receiver sensitivity line is the sensitivity plus the fade margin. You can see that it intersects the curve at a distance from the AP called the reliable reach, or just reach for short. Because the curve can be fairly flat there, allowing for the fade margin can make the reach point much closer in than the link failure point.

## Factors Affecting Reach

---

Reach primarily depends on four sets of characteristics, those of the AP antenna, the terrain, the climate, and the user's antenna.

### ***AP Antenna Characteristics Affecting Reach***

The two primary characteristics are antenna gain and height.

The gain you can use is normally dictated by the fact that these coverage APs are usually omnidirectional. You can add amplifiers if needed. How-

ever, the total power output of the antenna (measured in Watts) should not exceed the limits usually set by governments<sup>4</sup>. For example, in the US and Canada, the limit is 1.0 Watts. You will need to know what these limits are in your country.

Height matters because it helps you overcome two things: the curvature of the earth, and obstacles such as a stand of trees or a set of office buildings. It is not sufficient to just clear obstacles or just clear the earth's curvature. You also have to allow for a certain amount of *clearance* too. Later on, we will show you how to calculate the amount of clearance needed.

The antenna height is usually more under your control, because you can select a higher location or install a higher tower. There are limits to what you can do, though, at a reasonable price. Very high towers (say, 50 m or more) can cost a lot of money.

### ***Terrain Characteristics Affecting Reach***

The type of terrain you are trying to cover is fixed.

### ***Climate Characteristics Affecting Reach: The Fade Margin***

A typical fade margin for temperate climate regions is 10 dB. In the other climate regions, you will need to add a further correction to the fade margin to account for the probability of rain or high humidity.

### ***User's Antenna Characteristics Affecting Reach***

The gain of a user's antenna and its height need to be selected so the received signal strength is adequate. Your aim as the network designer should be to provide roughly as equal a received signal strength as possible within the coverage area. There are practical and economic limits to antenna heights and gains for user's antennas. For a residence, a typical set of limits is for a 28 dBi parabolic antenna on a mast about as high as a residential TV mast. For an office building, the height above average ground level could be much higher.

---

<sup>4</sup> It is sometimes possible to get waivers to these power output limits.

## Throughput

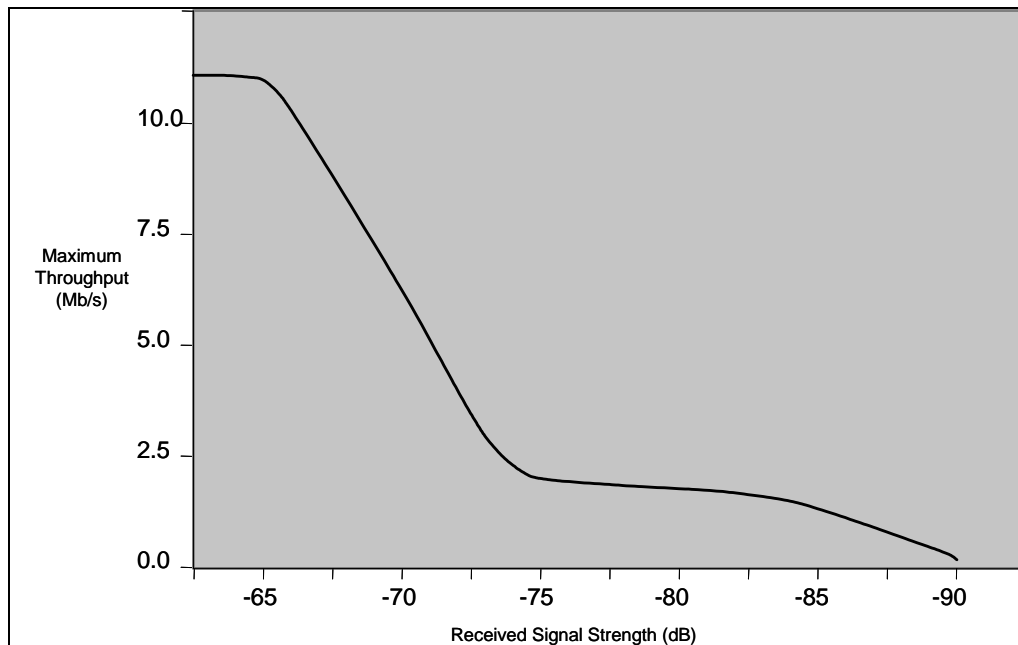
### **Maximum Total Throughput**

Signal strength or equivalently distance from the AP also affects total *throughput*. Throughput tends to drop as the distance from the AP increases, because the received signal strength decreases, amongst other factors. Thus, more and more errors occur due to interference and noise.

These errors have to be dealt with by the system signalling back and forth and re-transmitting data. All that re-transmitting and signalling takes up bandwidth, which is then not available for transmitting other data.

The details of how throughput falls as received signal strength falls depends on the specifics of the Wi-Fi product used. To give you an idea of how the fall occurs, we have created a hypothetical example in Figure 4-2.

**Figure 4-2: How Received Signal Strength Can Affect Total Throughput**



### **Average Throughput per User**

Your AP can provide great signal strength to its users and yet provide poor performance. This situation can happen because there are simply too

many users trying to share a fixed total amount of bandwidth. The result is poor throughput *per user*.

Throughput is the rate of transfer of a *digital* signal. For example, the maximum throughput of 802.11b Wi-Fi is 11 Mb/s, although actual Ethernet throughput can be half of this, say 6 Mb/s. Since a Wi-Fi channel is a shared medium, if there are 6 users simultaneously and actively using a single channel, they each have an average throughput of about  $6/6 = 1$  Mb/s. This calculation oversimplifies things because each user is not actually allocated a fixed amount of bandwidth, but it is good enough to make our point.

Suppose the community you are trying to cover has roughly equal population density throughout the coverage area. Then, the number of users that can be covered increases as the square of the distance from the AP. To understand this, think of a circle surrounding the AP. The area of the circle (the coverage area) is proportional to the square of its radius.

Therefore, if the population density is high enough, it is possible for the effective coverage radius of an AP to be less than its reach. This is illustrated in Figure 4-3, which shows:

- The maximum throughput dropping with distance from the AP
- The average throughput per user dropping at a much faster rate, simply because the number of covered users grows much more rapidly with distance from the AP.
- The minimum acceptable average throughput per user being reached at a distance we will call the coverage radius. The latter in this hypothetical example is *far less than the reach*.

### Coverage Zones

---

This problem can be simply solved, however. Divide the AP coverage area up into concentric zones and use higher gain user antennas and higher masts the further away a zone is from the AP. Figure 4-4 shows this solution. The result is that as you move from a zone to the next zone out, the received signal strength and the average throughput both jump. Figure 4-5 shows these jumps and how they result in a coverage radius which can be much further out than if every user had the same antenna setup (as was the case in Figure 4-3).

Figure 4-3: Effect of Numbers of Users on Coverage Radius

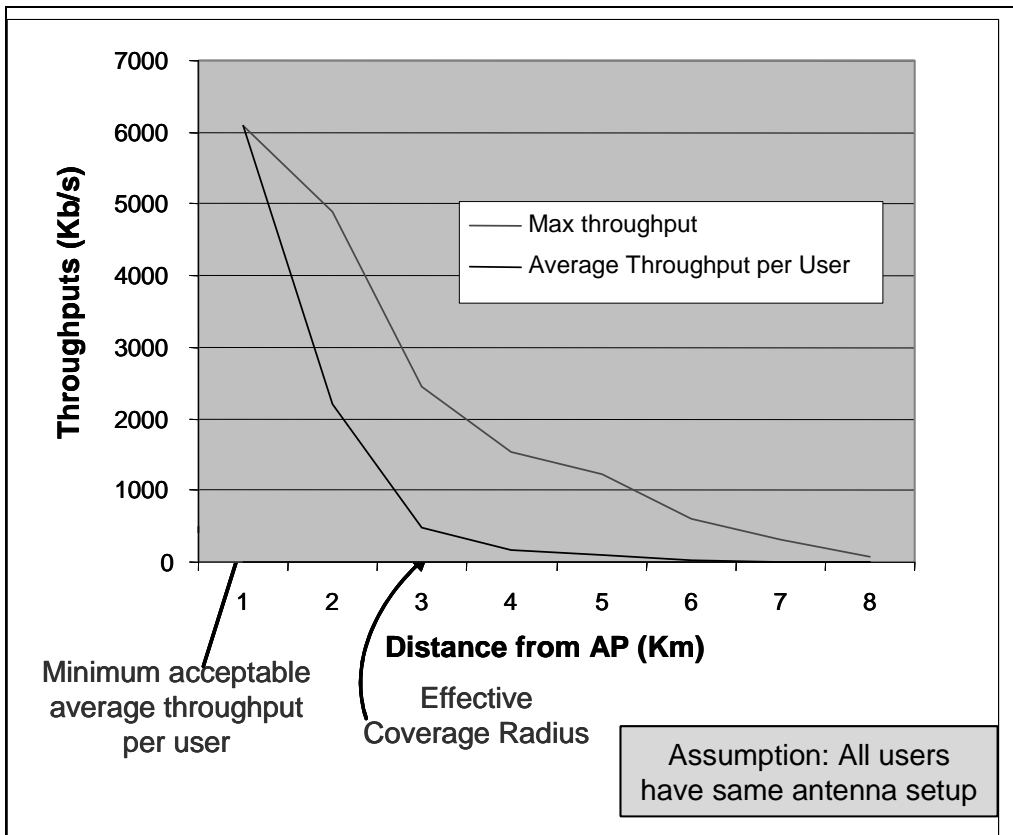


Figure 4-4: User Antennas have Higher Gains and Heights in Further Zones

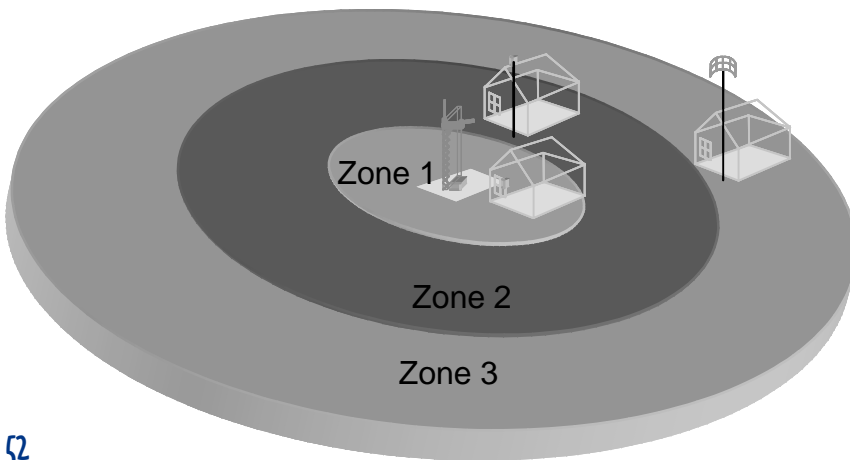
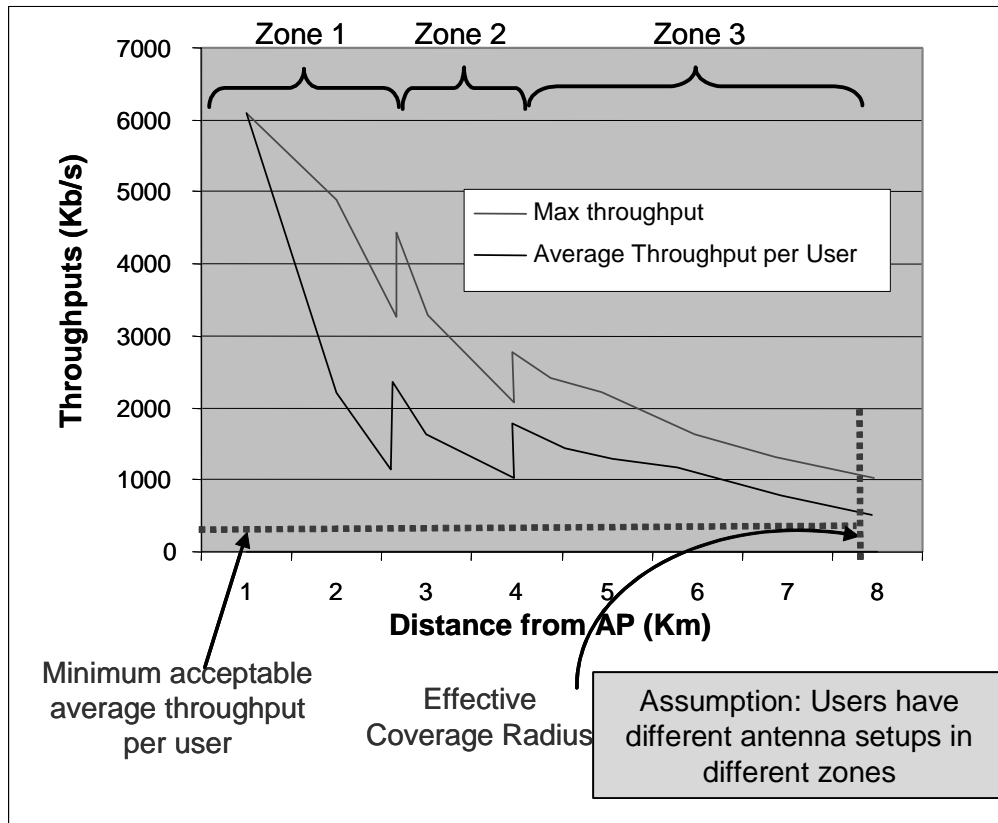




Figure 4-5: Dividing the Coverage Area into Zones Solves the Coverage Radius Problem





# 5. Creating a Wi-Fi WWAN and Connecting it to the Internet

Once you have planned out your basic WLAN/WAN, you now have to consider how it will be connected into the public IP networks such as the Internet. The connection consists of a backhaul facility along with the POP – WWAN/LAN gateway. In Chapter 2, we described what a backhaul link is, along with the need for a gateway into the public network.

The establishment of the connection into the Public IP network is where it can get challenging if there are no local existing broadband services offered by commercial or governmental organizations. In this chapter, we show you the most common options to get a plan of action together to implement a backhaul system and to expand your coverage.

**Suggested audience for this chapter:**





Important terms in this chapter include:

Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Buffer	<p>An amount of memory that temporarily stores data to help compensate for differences in the transfer rate of data from one device to another.</p> <p>Data that is in a buffer is said to be "buffered".</p>
Dynamic Host Configuration Protocol (DHCP)	Protocol for automating the configuration of computers that use TCP/IP.
Duplex	A duplex communication system is one where signal can flow in both directions between connected parties
Dynamic IP Address	An IP address that changes with each connection to the Internet.
Filtering	<p>The process by which particular source or destination addresses can be prevented from crossing a bridge or router onto another portion of the network.</p> <p>Bridges and switches can reduce the level of congestion on a LAN through the process of filtering. A filtering bridge or switch forwards a packet from one LAN segment to another only as required. Packets that are not forwarded by a bridge or switch are said to be "filtered".</p>
Half-duplex	A half-duplex system allows communications in both directions, but only one direction at a time (not simultaneously).
Media Access Control (MAC)	The unique physical address of each device's network interface card.
Network Address Translation (NAT)	NAT devices translate IP addresses so that users on a private network can see the public network, but public network users cannot see the private network users.
Port Number	<p>A number identifying a certain Internet application.</p> <p>For example, the default port number for the WWW service is 80.</p>
Proxy	<p>A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.</p> <p>A software agent that acts on behalf of a user, typical proxies accept a connection from a user, makes a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then</p>

# Chapter 6: Serving Outlying Groups of People

---

	completes a connection on behalf of the user to a remote destination.
Repeater chain	Set of repeaters, connected in a single chain. Sometimes called Daisy Chain.
Spanning Tree	A method used by bridges to create a logical topology that connects all network segments, and ensures that only one path exists between any two stations.
Static IP Address	A permanently assigned address on the internet. Usually used for servers, printers, VPNs (Virtual Private Networks), etc.

---

## Connecting the AP to the WAN or Backhaul Facility

---

You have to connect the APs in a local community to a WAN or directly to a backhaul transmission link in order to access the POP as well as any community-based servers. This type of connection is in concept identical to how typical networks for companies or schools work. In that case, a set of LANs are interconnected via a WAN and then to a gateway to access the outside world. Each LAN must connect to the WAN via a bridge, also known as a layer 2 switch.

In Figure 2-1, we showed an example of this type of connection that we used in some of our own tests. The configuration duplicates the functions required to link the wireless LAN provided by the AP onto a backhaul or WAN facility to enable it to have Internet access. The bridge in this example was provided by the built-in switch that the LinkSys AP router has integrated with it. This function can also be provided by a separate Ethernet layer 2 switch or bridge to provide the capability to link the AP to the Backhaul link.

---

**→ Note: Wireless bridges and any peripheral bridges must be configured properly so that they are on the same network and reachable by the Network Administrator. See Chapter 11 for how to do this. In addition, you must record the configurations for later use in order to access the equipment.**

---

### Local LAN Access and AP Interconnection

---

Using a bridge to link the AP and backhaul facility provides the added advantage of having spare Ethernet ports to feed a local community server or other WAN links that can connect to another AP. *These connections can be wired or provided by wireless means.* In our own tests, two D-Link 2100s 802.11b wireless APs set in network bridging mode provided the backhaul link to the POP. The DWL-2100 connected directly to the LinkSys switch via an Ethernet cable.

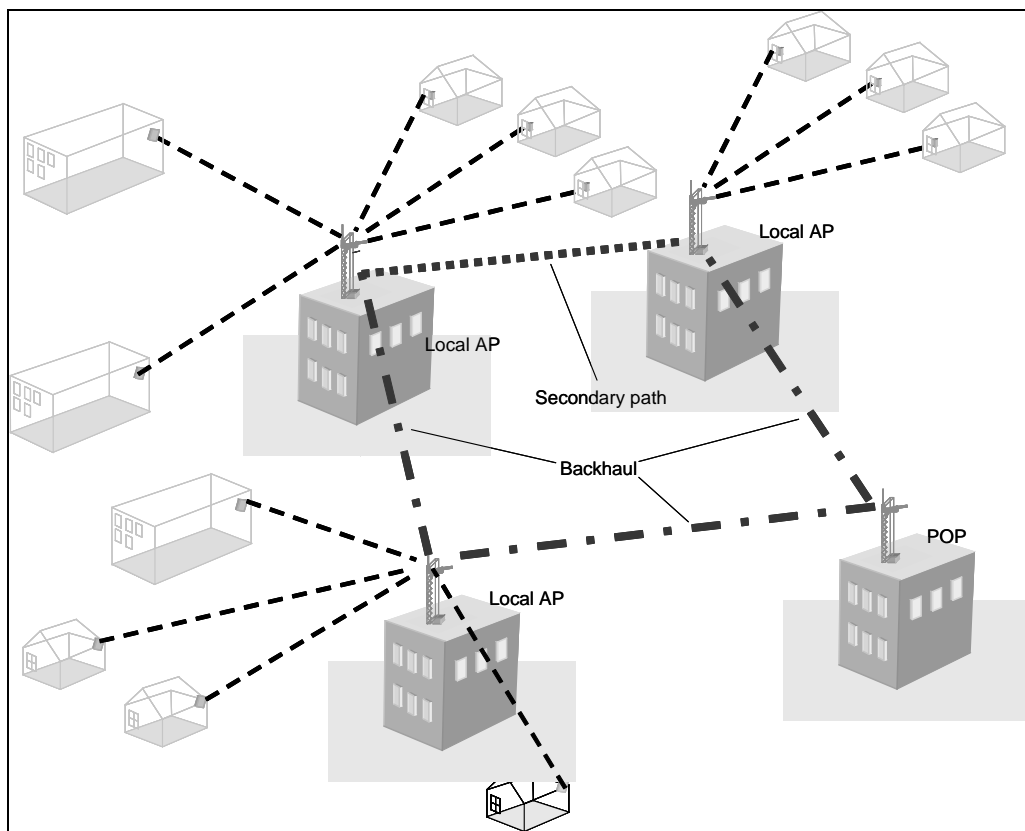
To extend the coverage to another AP, another pair of DWL-2100 APs can be used to connect to the next AP's switch, to provide again local wireless access in its' location as well as another jump point to extend the system out to another AP further out.

# Chapter 6: Serving Outlying Groups of People

Thus, a local WWAN can be formed in this way, with AP nodes that subdivide the Wireless Local Area Network coverage provided by each AP. Repetition of this linking approach thus allows a community area to be covered reliably.

Figure 5-1 depicts this interlinking and backhaul approach.

Figure 5-1: Using Replication and Backhaul Interlinking to Extend Wi-Fi Coverage



## The POP Gateway

---

→ We briefly mentioned the network gateway/firewall in Chapter 2, when we first introduced you to the basics of Wi-Fi networks.

Below, we will give you enough detail to understand what you have to do to set one up.

### **Purposes**

You will need a gateway to connect your WLAN/WAN to the public IP network. The gateway has two main purposes:

- Preventing local traffic on the WLAN/WAN from ending up on the public network.
- Preventing outside traffic that is not intended for the WLAN/WAN from entering the WLAN/WAN.

Thus, the gateway provides a firewall between the public IP network (via the ISP) and your community WLAN/WAN. This firewall provides security to prevent disruption of the community network or the IP public network by problems or deliberate hackers.

Typically, a gateway is hosted by an Internet Service Provider (ISP). The ISP will provide a port that is used to link the ISP to the WLAN/WAN. This relationship with the ISP requires that the local community network provider have a gateway (usually a router) that sits between their WLAN user and the ISP hosting their gateway.

### **IP Number Assignment, DHCP, and NAT**

In order to fulfill its firewall purposes, the gateway performs several specific functions. These are three of the essential ones.

The Wi-Fi cards used by people in your community will not have fixed (static) IP addresses. Instead, they will be assigned *dynamic IP addresses* by the gateway itself, each time they log on. In effect, the user requests an IP number for the Wi-Fi card by the very act of logging in.

Once the local user's Wi-Fi card receives its IP number, the user can connect to the Internet through the gateway.

---

**Note: The request for an IP number is done in the background. The user does not see it happening. Instead, all they see is the logging-in process.**

---



# Chapter 6: Serving Outlying Groups of People

---

The process of assigning an IP number to the user's Wi-Fi card uses a technique called *Domain Host Control Protocol* (DHCP). The gateway acts as a DHCP server. The server assigns a unique IP number within its own domain (a list of IP numbers in the 192.168.0.xxx range) to the user's card. The request for an IP number is called a DHCP request.

The IP numbers assigned by the gateway are private. By private, we mean that these numbers are internal to your community WLAN/WAN, and cannot be seen outside. Instead, there will be a common *proxy* IP address assigned to the gateway by the ISP.

One of the main reasons for using a proxy is that IP addresses are limited. By doing this renaming convention, a common set of IP numbers can be reused for LANs. A typical local number is 192.168.0.xxx. Since the numbers are only used in the LAN and blocked at the gateway, they cannot be seen by other LANs attached to the public network.

The translation between the internal IP numbers and the external IP number of the gateway proxy is called network address translation (NAT). Your local community WLAN/WAN users are identified by the IP numbers assigned to them, as well as by their *MAC* ID number that is unique hardware code assigned to their Ethernet or Wi-Fi network cards. The gateway maintains tables and ensures that traffic from the network is directed to the correct end-user.

## **Gateway Filtering**

Another function of the gateway is to act as a security node to block certain traffic, either incoming or outgoing. This filtering can be done according to several criteria. For example, filtering could be done:

- By specific IP numbers  
This criterion can be used to block traffic coming into the community network from well-known sources (IP numbers) of junk e-mail or other generally unwanted traffic.

- **By specific MAC numbers**  
Unlike IP numbers that can dynamically change, MAC numbers are fixed and unique. There is a different MAC number for each piece of IP equipment, including each individual Wi-Fi card. MAC filtering can be used to block traffic to or from users who the network administrator has decided are not allowed to belong to the network. For example, if the WLAN/WAN is a commercial one, the administrator could use MAC filtering to block all but paid subscribers.
- **By type of traffic**  
There are different types of IP traffic, each of which uses a different *port number* to identify what type it is. For example, general Internet surfing traffic uses port 80.  
Certain types of traffic such as mass file sharing of music or videos are often considered undesirable by network administrators, because they tend to hog the bandwidth. This hogging reduces the network performance for all other community Wi-Fi users. You can use traffic type filtering to block such undesirable types of traffic completely.
- **By time of day**  
For example, suppose instead of completely banning mass file sharing from your community network, you wanted instead to limit it to certain off-hours such as midnight to 4 AM. You could combine traffic type filtering with time of day filtering to achieve your objective.

### ***User Authentication***

As part of the “firewall” security functions, the gateway can be used as part of user authentication, particularly on wireless LANs. In private WLAN/WAN networks, it may be desirable to prevent non-authorized users from logging in. This authentication is done by a system called RADIUS that is part of Wi-Fi’s security strategy. The gateway can maintain a list of approved users. It can also manage the traffic flows for fairness among the user’s community.

➔ We briefly discussed RADIUS servers earlier. We will cover them in a bit more detail in the chapter on network security, Chapter 8.

## **Satellite Systems**

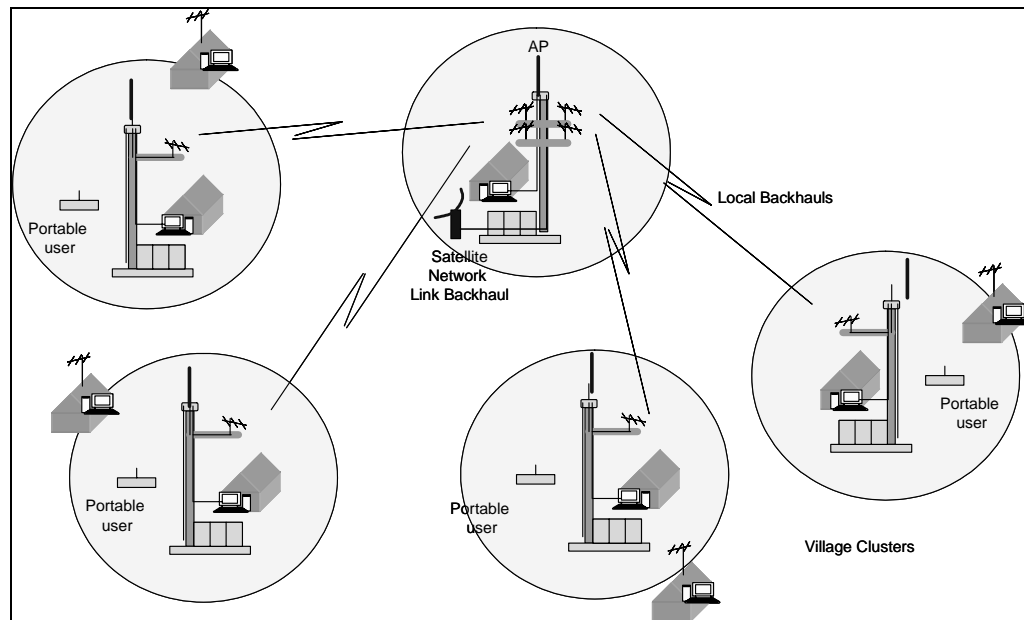
---

Satellite ground stations are a viable option if there is no POP location within a reasonable distance (say, more than 80 Km), or if there are no es-

# Chapter 6: Serving Outlying Groups of People

established microwave long-haul facilities. Figure 5-2 shows a typical backhaul configuration connecting to a ground station.

Figure 5-2: Centrally Located Village with Satellite Link becomes POP for five APs



Generally, you should consider satellite ground stations when:

- There are no established microwave radio facilities to the POP and ranges are over 80 Km.
- The POP is more than 80 Km (more than one repeater) away from putting in your own systems.
- The local area is very hilly and treed, making tower placement and line of sight links difficult even if distance is 80 Km or less. This situation will likely require more repeaters as well as higher more costly towers.

In many remote locations, satellite facilities are already used as the primary communications system. Unfortunately, the service they provide is

often not open to the general community, except possibly for telephone low-bandwidth data services (56 Kb/s or less) and television broadcast feeds. However, satellite service providers are now offering wider band Internet services of up to 10 Mb/s. These services can easily be extended through the community, using APs linked to the satellite ground station.

The cost of the satellite ground station and the monthly bandwidth charges could be quite reasonable on a per-user basis, with 20 to 30 users or more. Ground station terminals can be expensive (more than \$15,000 US) with monthly bandwidth charges of more than \$ 200-300 US. This cost is spread over a number of users so that it can become affordable.

## Backhaul Terrestrial Microwave Radio Link Choices

---

When you choose what types of wireless links to use, you should take into account several factors:

- Cost
- Capacity (bandwidth)
- Reliability
- Who is going to maintain it: you, or an outside company?

The following are the main choices.

### ***Commercial Microwave Facilities***

Typically, you can achieve ranges of over 40 Km with commercial radio equipment, given towers of over 60 meters in moderate terrain and proper line of sight clearances. For distances exceeding 40 km, repeaters are needed and costs will increase significantly. However, unless there are towers and supporting infrastructure already in place, the costs of having the repeaters can make the overall link cost excessive.

There are a number of short to long-range commercial digital radio systems that can provide bandwidth of 1 Mb/s up to 130 Mb/s per channel. Such systems are mostly designed to use licensed radio frequencies. The word “licensed” implies that:

- The service meets all regulations
- It can be placed into service by qualified personal
- An engineering brief has been submitted to the government body responsible for the country's telecommunication regulations

# Chapter 6: Serving Outlying Groups of People

---

- Annual fees are to be paid.

Equipment costs range from \$1000 US up to \$20,000 per terminal, depending on the bandwidth and features required. For an example of advanced features, you can buy radio systems with *protection* systems that provide both equipment redundancy and dual antenna systems (diversity) to overcome radio fading due to atmospheric effects.

Companies such as SR Telecom, Harris, NEC, Alcatel, Nortel Networks, Marconi Wireless, Proxim, and many others provide a wide range of system designed for backhaul use. Their solutions are routinely used for cellular radio backhaul and for access to factories, commercial enterprises, and government offices. Their use in rural or remote situations can be justified where high reliability is needed and reasonable usage will occur. In situations where there will be many end users, the costs can be justified.

Depending on your community's location, there may be existing microwave facilities that you can lease. You either lease capacity or the towers and infrastructure itself to support your own radio equipment.

## **802.11 Technologies for Shorter Link Backhaul**

If a POP is reasonably close (less than 40 km) and terrain features are gentle, the use of Wi-Fi 802.11, 802.11a, or 802.11b solutions can be used successfully. Here, equipment costs are low and the costs of establishing one to three repeaters to provide a backhaul link can be reasonable. The drawback with the unlicensed bands (2.4 GHz and 5 GHz) is that power is restricted in most regions and thus shorter hops at 11-54mb/s (less than 2Km) 2-11 Mb/s (less than 10 Km) or lower bandwidth with longer hops (1 to 2 Mb/s using 802.11) will be typically realized. This is still very usable depending on the needs of the community.

Therefore, to link peripheral communities within 40 km (terrain dependent), use of 802.11 technologies should definitely be considered. The range testing done by our research team as well as published literature from many other groups show that for spans of 2 to 10 Km, reliable throughput of 2 up to 11 Mb/s can be obtained with moderate gain antennas and less

then ideal obstacle clearance. Of course, even better results can be obtained in terrain that is more open.

The use of 802.11 technologies for providing backhaul services is also very viable. Companies such as Linksys, Proxim, D-link, NETGEAR, BelAir Networks, and others offer WLAN/WAN bridges and repeaters to be used to link LANs and WANs to each other at LOS distances exceeding 35 km.

Typically, ranges between 5 to 20 km are achieved on a regular basis using commercial-grade 802.11a and 802.11b AP nodes with power of up to 1 watt (30 dBm). These systems are currently on the market for less than \$700 USD and are falling rapidly in price.

Lower cost Wi-Fi equipment (less than \$130 US) such as we used in our own research (D-link 2100, 900 and Linksys WG54 and others) have bridge features as well. At lower power, reliable range is more restricted to less than 10 km depending on the radio path clearance and local conditions.

→ The expected throughputs provided by this equipment are described in Chapter 3 as well as later on in this chapter on range considerations.

The use of lower cost Wi-Fi consumer equipment does restrict the way in which the equipment can be used for backhaul and as repeaters. This requires that the equipment be appropriately packaged for outdoor use. In addition, longer cable run will be needed to the external high gain antennas.

→ See Chapter 12 for details of outdoor packaging.

However, despite these restrictions, 802.11 can be reliably used for shorter links to connect APs in chains or for other backhaul solutions.

### ***Combination of Satellite and Local Microwave Radio Backhaul***

The satellite ground station can serve as an effective POP hub for local settlements that are within a 40 km radius. This provides the opportunity to use local microwave links to join the settlements. Each settlement AP can be backhauled to the satellite “hub” ground station.

This situation reduces the cost per user very significantly. The major limitation will be the amount of total throughput the satellite ground station can provide within the spot area coverage of the serving satellite. The number

# Chapter 6: Serving Outlying Groups of People

of simultaneous users that can be supported will depend very much on the type of Internet usage on average and uplink capacity available.

## Point-to-Point Microwave Radio Repeaters for Backhaul

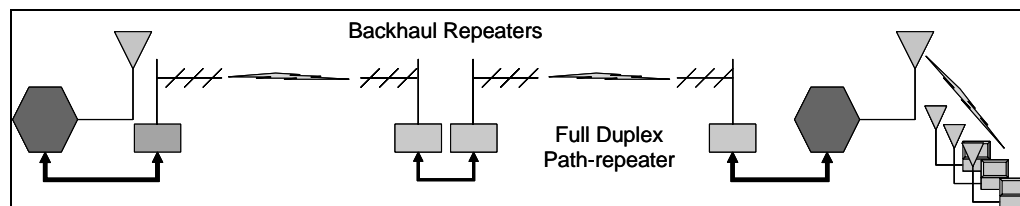
### ***What Are Repeater / Relay Nodes?***

The distances between the POP and the APs or between pairs of APs may be too far to span with a single wireless link. If satellite is not an option, then you should use a relay node to receive and transmit signals between the between the APs or between an AP and the POP. Your backhaul then becomes a multi-hop system (hop refers to spans between each node). The relay node regenerates or “repeats” the weakened signals and sends them on to their destination. In cases where significant distances are involved, a chain of repeater nodes may be required to link the sites together.

### ***How to Set Up a Repeater Node***

This configuration is the classic full-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 are retransmitted to the next repeater station or end terminal. You use this type of repeater configuration for backhauling an AP to a POP or interconnecting APs in a daisy chain. See Figure 5-3.

**Figure 5-3: Duplex Inter-nodal Repeater for AP Coverage Extension**



To establish your own repeater, two APs are set up as wireless layer 2 bridges, as is the case of 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 an 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.

You will need to do channel (frequency) planning to prevent excessive system self-interference.

➔ See the section "Channel Settings" of Chapter 10 for further details on channel planning for repeater links.

## Estimating Numbers and Locations of Relay Nodes

---

The required number of repeaters depends a lot on your local terrain features and climate. You can estimate the numbers needed as follows:

- Decide the approximate path the radio links will need to take on a topographic map. As you do this, note what the terrain is and try to avoid obstructions. The idea is to find the shortest most direct feasible path without incurring high costs.
- Looking at the height of the terrain on your selected path, try to locate what locations have some elevation over other points on the path. Tentatively locate a potential site there.
- From these locations, determine if a line of sight path exists to the next up and down the path.
- Determine the distance between sites. Compare to the maximum range possible given the terrain and type of wireless technology you have chosen. If necessary, add other relay sites.
- Determine a cost for the links. Compare this cost to the cost of alternatives such as using satellite.



# Chapter 6: Serving Outlying Groups of People

---

## Providing Secondary Paths

---

### ***Redundancy and Survivability***

In using the bridging layer 2 networking we described in this chapter, you will need to use what is called a *spanning tree* across the network. A spanning tree connects all nodes in a way that there is only one path between any two nodes. Spanning trees are supported in most low-cost Ethernet switches that are built into many of the AP router now on the market.

You can improve the reliability of your community WLAN/WAN by going beyond the single path between any two nodes. You create a secondary path to provide more than one way to reach the POP or hub location. An example of a secondary link between two APs is shown in Figure 5-1.

Using this approach, ring-like network structures can be established to link the APs back to the POP. This can be called a minimum mesh approach. You can evolve it into a full mesh networking operation by adding more links, but that can be costly.

## 6. Serving Outlying Groups of People

In many rural or remote regions, 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 may also be needed to inter-link communities, as well as reach POP locations.

Our own work has shown that you can use several types of repeater approaches with reasonable results.

As of the time when we are writing this book, 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. Other companies may follow with similar capabilities.

**Suggested audience for this chapter:**



# Chapter 6: Serving Outlying Groups of People

---



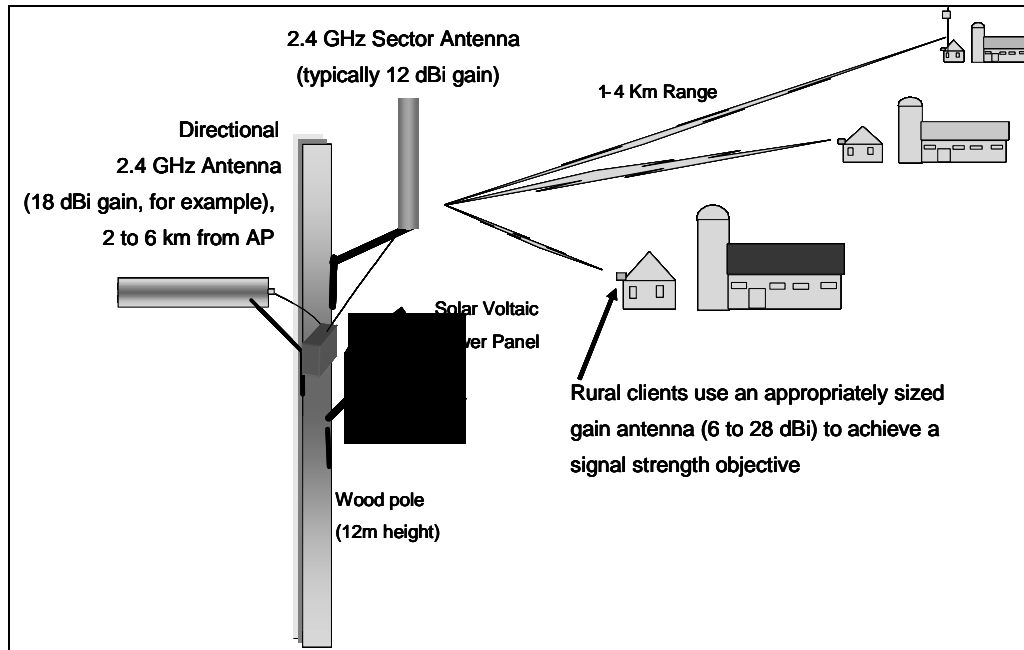
Important terms in this chapter include:

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.
Firmware	Software that is embedded in a hardware device that allows reading and executing the software, but does not allow modification, e.g., writing or deleting data by an end user.
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.
Range Extension	Methods to extend the range of a wireless system
Transceiver	A radio transmitter-receiver that uses many of the same components for both transmission and reception.

## Serving a Small Cluster of Buildings Outside of Town

Figure 6-1 shows a cluster of buildings which are well outside a town and well outside the reach of any AP in town. How do you extend Internet coverage from the town to the cluster in such situations?

Figure 6-1: Proxy AP to Serve an Isolated Cluster of Buildings



The name for our problem is *range extension*. Clearly, to solve the problem we are going to have to set up some sort of *repeater chain* going from an AP in town out to the cluster. There are a couple of ways to do this. In our own field tests, we have verified that these approaches work.

### **Store-and-Forward Repeaters**

Some Wi-Fi manufacturers such as D-Link have 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 (in this case, the one in town) and a more remote client (in the isolated cluster). Here the repeater at the end of the chain nearest the cluster is acting as an AP *proxy*. In this type of setup, the end-client “sees” the originating

# Chapter 6: Serving Outlying Groups of People

AP. It does not “see” the proxy or any other “transparent” repeater. By “see”, we mean that if someone in one of the buildings asked their Wi-Fi software what AP they were connected to, it would list the AP in town and *not* the AP that is actually nearest to them!

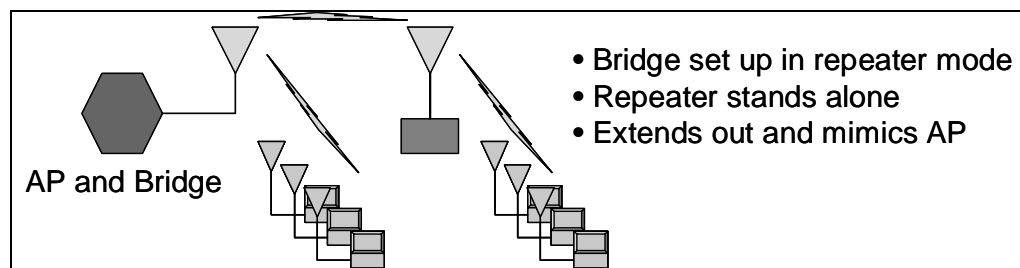
Classical microwave radio links use two complete radio transceivers for the repeater to serve either direction (*duplex*) of the radio link. By contrast, the 802.11 repeater runs in *half duplex*, with one transceiver. Packets from the originating AP are received, stored, and then retransmitted to the 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 affected 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 less than 100  $\mu$ s per hop. See Figure 6-2.

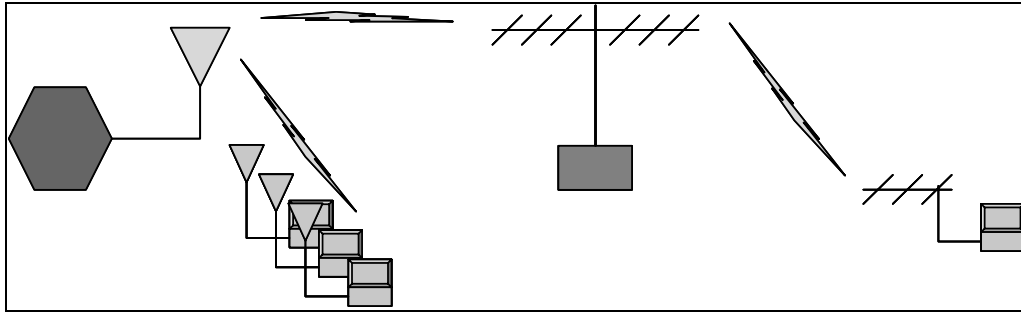
**Figure 6-2: Omnidirectional Store and Forward**



### Using dual repeater nodes with directional antennas

In this approach, you use directional antennas to extend the reach to remote clients. You do this 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 6-3.

Figure 6-3: 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 select automatically 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.

→ See “Disabling Antenna Diversity” in Chapter 10 on how to do this.

## Serving Isolated Buildings Which Are Widely Spread Out

This is probably the toughest layout to try to cover. What we recommend is to mark up a map with the locations of the isolated buildings. Based upon the distribution of buildings, choose one of two approaches:

- Omnidirectional coverage  
Use this coverage approach if the buildings are fairly evenly distributed around the AP, which should be located near the centroid of the distribution.
- Sector coverage

## Chapter 6: **Serving Outlying Groups of People**

---

Use this approach if the distribution of buildings is notably uneven. Based on this distribution, you will need to decide how many sectors you will need and what angle each of the sectors should cover.

Because of the large average distance between buildings, it is likely that you will have to mount the antenna on quite a high tower. You can use the spreadsheet accompanying this book to determine the appropriate tower height.





# 7. Powering Your Access Points

This chapter deals with electrical powering issues for your AP. A prime consideration in making your Wi-Fi network reliable is making sure you have a reliable source of clean power. However, a common problem in many places is having reliable power available. In many locations, you must generate power locally, since there are no nearby power grids. In this chapter, we discuss how you can use alternative power sources to back up local power or be the prime source for the radio system. The goal is a solution that will provide electricity on a continuous basis.

The chapter begins with sections that help you calculate:

- The electrical power requirements for a single AP site
- The amount of battery backup you will need.

We will then cover the basics of different types of power sources, including:

- Electrical mains
- Solar power
- Wind (turbine) power
- Propane (natural gas)
- Small hydro dams
- Steam turbines
- “Bicycle” power.

In many cases, you will have to combine power from two or more of these sources. So, the chapter concludes with pointers to commercial systems for managing power from multiple sources.

**Suggested audience for this chapter:**





Important terms in this chapter include:

Charge controller	A component of a photovoltaic system that controls the flow of current to and from the battery subsystem to protect batteries from overcharge, over-discharge, or other control functions. The charge controller may also monitor system operational status.
DC-to-DC converter	A circuit that converts DC power from one voltage to another. It is a special class of power converter.
Float charged	The charging of a battery, taking into account a minimum "float" or reserve charge.
Head	The pressure exerted by a fluid; "a head of steam"
Mains	The AC power distribution lines provided by a power utility.
Memory effect	An effect seen in some rechargeable batteries that causes them to hold less charge. Also known as the lazy battery effect.
Pelton wheel	A turbine with many small fans arranged in a wheel.
Penstock	A large pipe or conduit to carry the water from the reservoir or dam to a turbine or water wheel
Power budget	The allocation, within a system, of available electrical power, among the various functions that need to be performed.
Power inverter	A circuit for converting direct current electrical power to alternating current.
Solar panel	An electrical device consisting of a large array of connected solar cells.
Stepped pseudo-sine wave	An electrical waveform that looks like a square wave with some steps in it.
Turbine	A device for converting the flow of a fluid (air, steam, water, or hot gases) into mechanical motion that in turn produces electricity.
Uninterruptible Power Supply (UPS)	A battery backed-up power supply.

---

## Power Budget

You can use the *power budget* in Table 7-1 to estimate the electrical budget needed to maintain continuous electrical power to a single AP site.

**Table 7-1: Example Power Requirements and Supply for AP Site**

Item	Power Need per unit	Number of Units	Duty Cycle 24 hours	Amp Hours	Daily Amp Hours
Backhaul Radios	<b>7.2 Watts</b> (0.6 Amps @12 V)	2 (max)	80%	2 x 0.6 Amps x 1 hr x 0.8= <b>0.96 Amp-hours</b>	24 x 0.96 = <b>23.04 Amp-hours</b>
AP / Switch	<b>11.0 Watts</b> (0.92 Amps @12 V)	1	90%	1 x 0.92 x 1hr x 0.9 = <b>0.83 Amp-hours</b>	24 x 0.825 = <b>19.80 Amp-hours</b>
Inverter Power Draw (idle)	<b>2.4 Watts</b> (0.2 Amps @12 V)	1	100%	1 x 0.2 x 1hr x 1.0 = <b>0.20 Amp-hours</b>	24 x 0.2 = <b>4.80 Amp-hours</b>
Inverter dissipation with load (10% loss)	Load total = 16 Watts @12 Volts 1.333 Amps 1.333 x 0.1 = 0.133 Amps (dissipation) 0.133 *12 V = <b>1.6 Watts</b>	1	85%	1 x 0.133 x 1hr x 0.85 = <b>0.11 Amp-hours</b>	24 x 0.113 = <b>2.72 Amp-hours</b>
<b>Totals</b>	<b>22.2 Watts</b>			<b>2.10 Amp-hours</b>	<b>50.43 Amp-hours</b>

## Battery Backup

---

### **Objectives**

Battery backup is necessary even with the most reliable power system since equipment failure, human error, or disruption due to weather can occur. 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. It is *very important* that the battery be the correct size to span these gaps in power.

In order to power the AP with solar or other alternative power sources, you should consider several factors to determine:

- How much power the power source can deliver over time, and
- The amount of time the source will be unavailable.

The most common objective is to span power failures of up to 24 hours. This time usually allows repairs to be completed and power restored before the batteries run out of power.

### **Sizing the Power Supply**

In sizing the electrical 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 also be powerful enough to provide sufficient capacity to supply during the down time of the power sources.

The required battery size is determined by the total load of the AP to be powered plus the need for powering any extra hardware. The following calculation outlines how you can calculate the battery size needed to cover the span. For an example configuration:

Power required	= AP	+ Backhaul Bridge	+ RF Amplifier
	= 14 Watts	+ 12 Watts	+ 10 Watts
	= 36 Watts total demand.		

In terms of Amps, this is  $(36 \text{ Watts}) / (12 \text{ Volts}) = 3 \text{ Amps}$ . On an hourly basis, this is termed 3 Amp-hours. For a 24-hour period, the total battery capacity =  $3 \text{ Amp-hours} \times 24 \text{ hours} = 72 \text{ Amp-hours}$ . Thus, the minimal battery that is required for this case has a capacity of 72 Amp-hours.

Since batteries deteriorate over time, thus reducing the storage capacity, the installed capacity should be 25% or more than this:

$$\begin{aligned}\text{Required battery size} &= 75 \text{ Amp-hours} + (75 \text{ Amp-hours} \times 25\%) \\ &= (75 + 18.75) \text{ Amp-hours} \\ &= 93.75 \text{ Amp-hours.}\end{aligned}$$

### ***Types of Batteries***

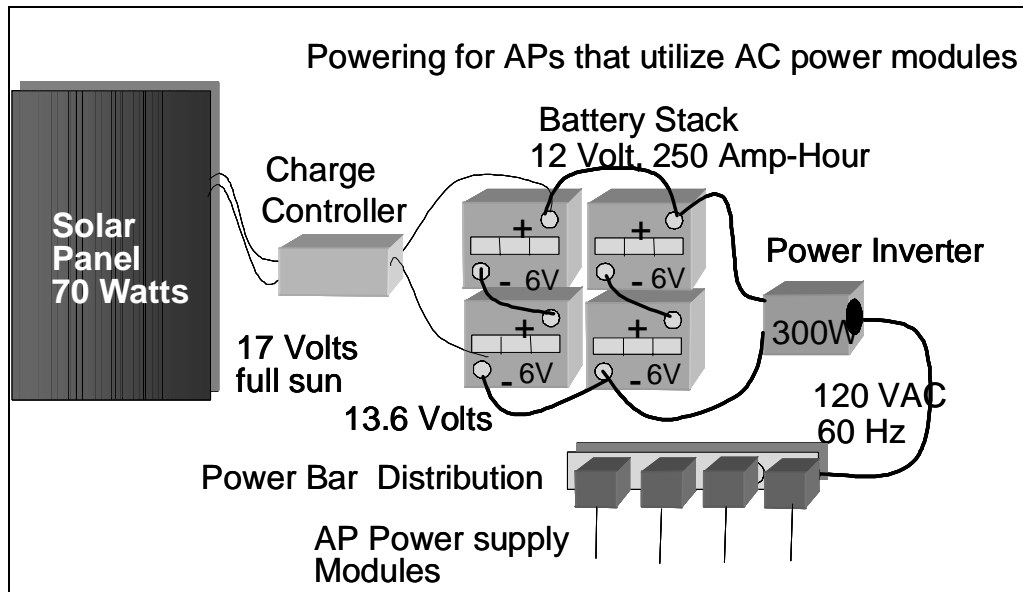
The batteries used for supplying power should be of the deep discharge variety used for marine and recreational vehicle (RV) applications. There are also gel-cell lead acid batteries built for use in enclosures that do not outgas significantly. Conventional car batteries can pose problems since they release hydrogen gas and SO<sub>2</sub>, which can be dangerous in an enclosed space.

### ***Battery Backup Systems***

In our own work, we normally use four 6-Volt batteries arranged in a series / parallel configuration. Figure 7-1 shows this type of arrangement. It provides about 125 Amp-hours per 12 Volt set or 250 Amp-hours at 12 Volts. A photograph of a two-battery reduced version in the back of a van is shown in **Error! Reference source not found..**

The four-battery system uses 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, you can use a lower *power inverter* to save on power losses and costs. For a three-transceiver node, a 150 to 300 watt inverter will suffice. The panel and a small battery charger maintain the battery charge. This arrangement provides 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 puts out quite a bit of radio frequency interference.

Figure 7-1: Power Configuration Example for AP Powering



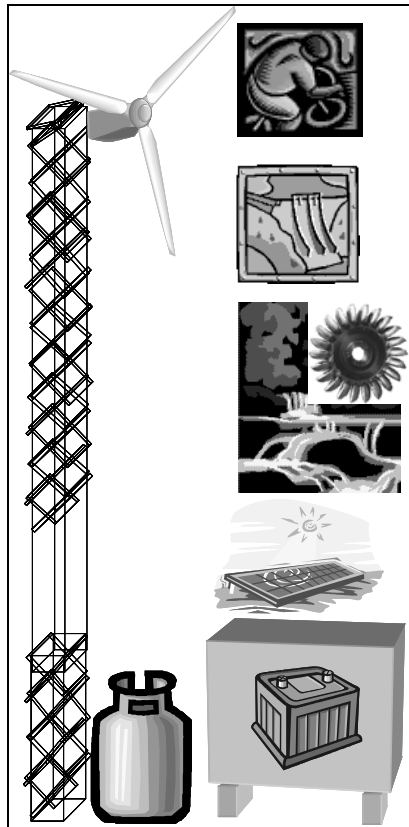
## Mains

If local power is available, it should be the primary source of power for your radio system. However, the following aspects are important to ensure reliability of the system:

- **Electrical standards**  
Before plugging in your equipment, make sure that the electrical specifications of the equipment match that of your local power utility. Common examples are (120 VAC, 60 Hz) or (240 VAC, 50 Hz).
- **Reliability**  
You should consider the reliability of the locally supplied power when you determine what back-up power you need. An Uninterruptible Power Supply (UPS) that can provide power for 15 to 20 minutes can back up highly reliable mains where there are only short and infrequent power disruptions.

As we have just seen, the power needs for wireless LAN equipment are very modest — in the order of 20 Watts for many APs. The cost of providing power in most situations will therefore be reasonable. Figure 7-2 shows some of the alternatives or supplements to mains power.

Figure 7-2: Some Alternative Power Source Options



On the left:

- Small wind turbine located on same tower as AP antenna

Middle:

- Propane

On the right, from top to bottom:

- Bicycle power, for battery charging during off-hours or power failures
- Small dam
- Micro water turbine for streams
- Solar power
- Battery backup system, housed in protective enclosure

## Propane (Natural Gas)

In areas where there is no community power available at all, you must look at alternative means. Propane-fuelled generators or thermo-electric generators can be used. You should consider propane systems as a *supplemental* power source, to be used along with another principal power source.

## Wind Turbine

The use of wind power is quite common in remote areas where there are no other significant sources for electrical power. The best way to use wind power is in conjunction with other alternative sources such as solar or propane.

The approach here is to have the sources power back each other up to ensure that ample total power is available. Typically, wind will be more prevalent during periods of bad weather and cloudiness. Thus, solar and wind are somewhat complementary. In some cases, both are deployed together to form a hybrid system.

Photo 7-1 shows an example of a small wind turbine that was developed to meet the needs of rural electrification in developing countries.

---

### Photo 7-1: Example of Small Wind Turbine

---



Bergey XL.1 small wind turbine.

Rotor diameter: 2.5 meters

Peak output: 1.6 kW

Photo courtesy of:

<http://www.ecobusinesslinks.com/>

A useful web site that has online calculators to help you determine your wind turbine or other powering system needs specific to your region, environment, and terrain is:

<http://www.odysen.com/calculators/main.php>

As an example of how to use the calculator, we asked it for a wind turbine design for Arctic Bay, North-West Territories, Canada. We specified that the ground was smooth, there were no trees, and no object within 500 ft (170 m) of the wind turbine. We asked for 500 kW of power per month.

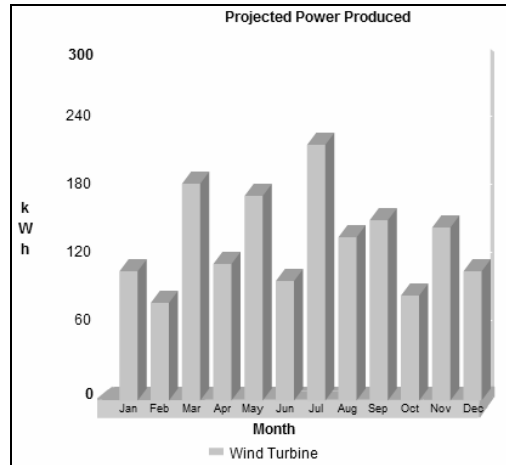
Figure 7-3 shows a graph of the projected monthly power outputs. Other outputs from the online calculator included:

- 1 kW wind turbine on a 64 ft. (30 m) tower with 5.3 kWh of backup.
- Average power produced per month: 128 kWh
- Percent of needed: 26%



- Backup power available: 5 kWh. Based upon a usage of 500 kWh per month, this will last for 8 hours.

Figure 7-3: Projected Wind Turbine Output for Arctic Bay, Northwest Territories, Canada



## Solar

Solar power is commonly used for remote radio and in conjunction with other applications such as irrigation. The modest power demands of Wi-Fi equipment make solar a good choice. With solar, the intent is to provide power for the system to operate and at the same time charge batteries sufficiently to keep the equipment operating during the nighttime or on cloudy days. The requirements of the equipment must be determined for 24 x 7 operations.

The efficiency of a solar power solution will depend primarily on two environmental factors:

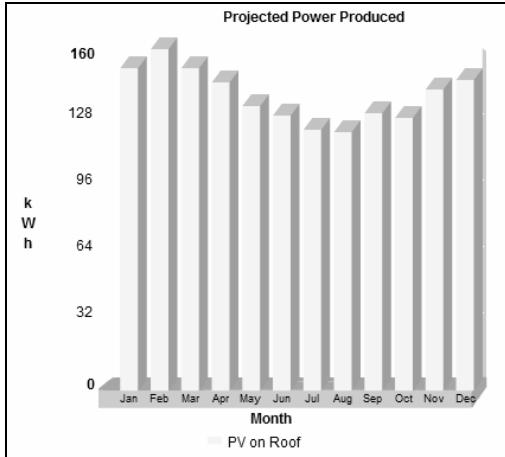
- The average amount of sunlight in your region
- The average ambient air temperature.

Do not make the mistake of assuming that only the first factor counts. The efficiency of a solar cell increases as ambient air temperature drops. There can be as much as 30% efficiency boost due to lower air temperature!

Using the online calculator at [www.odysen.com](http://www.odysen.com), we generated the projected monthly power output of a solar system for Abong Mbang, Camer-

oon. We specified that we wanted 660 Watts output each month. That is enough to power a simple AP with battery backup, according to Table 7-1. The results are shown in Figure 7-4.

**Figure 7-4: Example Solar Power Output for Abong Mbang, Cameroon**



You can do your own calculation of solar panel output using Table 7-2.

**Table 7-2: Power Generation Capacity of a Solar panel**

Item	Power Need per unit	Number of Units	Duty Cycle 24 hours	Amp Hours	Daily Amp Hours
Solar Generation Per Panel	<b>70 Watts</b> 5.15 Amps @ 13.6 Volts Full Sun	2 panels	10 hours average (year round) Canada mid-latitudes		<b>103 Amp-hours</b>

For a basic AP node, the package consists of one backhaul module and one AP *transceiver* module. The power draw is about 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 one to two Watts power saving should provide better reserve margins when there are poor solar conditions.

The batteries used with solar powered installations must be deep discharge lead-acid types used for Recreational Vehicle (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 provide for 24 hours of full system operation. This is the type of duration objective used by telephone companies to maintain system availability. After 24 hours with no power, you must implement a power contingency mode to stretch remaining power another 6 hours, if possible.

### Small Hydro Dam

---

There are locations where a small penstock and turbine can be installed to generate a modest amount of power. Here the power is available on a continuous basis and can be quite significant (1 kW).

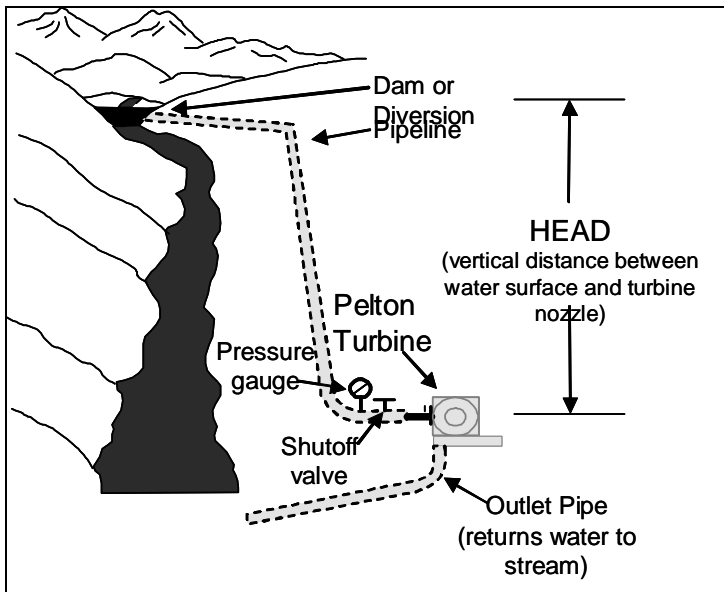
This type of solution can be quite expensive to build and can be subject to local regulations. In addition, such facilities can require construction of supporting structures such as flow-ways, pipes, etc. An example of an installation is shown in Figure 7-5.

Turbines such as this can operate over a wide range of vertical head, but narrow flow range.

We cannot cover all aspects of such systems in detail here. Your best bet is to look for information on the web. To get you started, here is a web address:

<http://www.absak.com/design/hydro.html>

## Figure 7-5: Example of Small Hydro Dam Installation



Based on a diagram at:  
<http://www.absak.com/design/hydro.html/>

## Stream Turbine

If there is a fast running stream that has some depth (1.5 meters), you can install a small stream turbine. These units can supply 60 to 200 Watts of power at 12 Volts each. This is quite adequate to power several APs and charge backup batteries at the same time. An example of such a stream turbine is given in Photo 7-2. Reaction turbines such as this operate over a wide range of high flow, but low head.

## Photo 7-2: Example of Stream Turbine



Aquair UW stream turbine, with 4m of cable, heat sink, and manual.

Rotor diameter: 2.5 meters

Peak output: 60 W

Photo courtesy of:

<http://www.ecobusinesslinks.com/>

## Cycle Power

---

On a sustained basis, a person on a bicycle or foot crank can generate up to about 100 Watts of power. This is about four or five times the power requirements of a Wi-Fi AP and its supporting equipment. Therefore, sustained pedalling for about three hours each day should charge up the batteries enough to provide electrical power for most of the active hours in a day. Cycle power can be especially useful as a backup in case of power failure, but it can be the only choice if there is no other source of electricity.

For an example of this approach in action, see the Jhai foundation web site at:

[http://www.jhai.org/jhai\\_remotelT.htm](http://www.jhai.org/jhai_remotelT.htm)

## Commercial Power Control Systems

---

You can buy power control systems designed to manage power generated from several sources. An example would be combining solar with wind along with a conventional gas or propane fuelled generator coupled to a battery reserve system.

The functions of the power management systems are to:

- Manage the power loads and source selections  
e.g., a mix of wind and solar
- Control the battery charging
- Supervise the battery condition
- Select power source combinations  
e.g., a mix of wind and solar
- Provide survival modes in a contingency  
e.g., cycling power to prevent complete system outage
- Provide remote telemetry and control via an Ethernet Interface.

Table 7-3 below lists two examples of companies making such control systems.

**Table 7-3: Some Companies Making Small Electrical Power Control Systems**

Company	URL	Product Types	Address	Phone/fax
Dyane Systems Inc.	<a href="http://solarwindworks.com/Products/Power_Centers/power_centers.htm">http://solarwindworks.com/Products/Power_Centers/power_centers.htm</a>	<ul style="list-style-type: none"> <li>• Backup power systems</li> <li>• Telecommunications power systems</li> <li>• Wind energy system components (small)</li> <li>• Fuel powered electric generators</li> </ul>	19 Marlborough Drive, Sydney, Nova Scotia, Canada B1S 1W7	<ul style="list-style-type: none"> <li>• Telephone: +1 (902) 562-0133</li> <li>• Fax: +1 (902) 567-0633</li> </ul>
Denon Technologies Ltd		<ul style="list-style-type: none"> <li>• Hybrid power systems</li> <li>• Packaged power systems</li> <li>• Solar Panels &amp; accessories</li> <li>• Hydro power controllers</li> <li>• Induction generator controllers</li> <li>• Turbines and Generators for micro/mini hydro systems</li> </ul>	7002 MacPherson Avenue, Burnaby, BC, Canada V5J 4N3	<ul style="list-style-type: none"> <li>• Telephone: +1 (604) 677-3231</li> <li>• Fax: +1 (604) 677-3231</li> </ul>

# 8. Planning Your Network Security

**W**i-Fi has developed a reputation for being insecure. This reputation likely arose due to two things:

- Almost all consumer Wi-Fi equipment is shipped with security turned off.

As a result, perhaps half of all home Wi-Fi networks are completely open. The owners never bothered to turn the security on. Anyone with basic Wi-Fi equipment and an inexpensive antenna can easily freeload onto such an open network. In our own experiments driving around urban areas, we found there were some neighbourhoods where we could have connected to a few dozen home Wi-Fi networks.

- Standards for Wi-Fi security are an ongoing story.

The very earliest Wi-Fi standards lacked security. In the last year, we entered the second generation of security standards for Wi-Fi. As this book goes to press, equipment supporting the third generation is about to appear. However, there is a lot of equipment out there that uses the first, and weaker, generation of security standards.

We do not want to give the impression that Wi-Fi is inherently insecure. You can achieve an extremely secure network by using equipment that supports the latest standards and by turning security on.

The very highest levels of Wi-Fi security require you to buy additional equipment and get it configured by an expert. Later in this Chapter, we give a brief overview of what is required, along with references.

**Suggested audience for this chapter:**





Important terms in this chapter include:

Denial of Service (DoS)	<p>A form of network attack in which a network is flooded with traffic. The system cannot then respond normally, so service is curtailed or denied.</p> <p>This is a favourite technique of network saboteurs.</p>
Encryption	<p>A method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data.</p> <p>Only individuals with access to a password or key can decrypt and use the data. The data can include messages, files, folders, or disks.</p>
Service Set Identifier (SSID)	<p>A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.</p>
Virus	<p>A parasitic program written intentionally to enter a computer without the user's permission or knowledge.</p>
Wired Equivalent Privacy (WEP)	<p>A security protocol for wireless local area networks.</p> <p>WEP was intended to provide the same level of security as that of a wired LAN. However, it has been found that WEP is not as secure as once believed. It does not offer end-to-end security.</p>
Wi-Fi Protected Access (WPA)	<p>The successor to WEP. Considerably more secure than WEP.</p>
WPA2	<p>The successor to WPA. More secure than WPA.</p>



## Types of Wi-Fi Security Threats

---

Threats are either deliberate or incidental.

### ***Deliberate***

The main kinds of deliberate threats are:

- **Freeloading**  
Someone may want to use your network for free Internet access. This will lower the available level of service for legitimate users.
- **Eavesdropping**  
This can result in disclosure of confidential data.
- ***Spoofing***  
A malicious user could send data (e.g., e-mail) that may appear to come from a legitimate user.
- **Intercepting and changing data**  
If an attacker can gain access to the network, they can insert a computer to intercept and change communications between two legitimate parties.
- ***Denial of service (DoS)***  
DoS is a deliberate attempt to deny your users access to your network. There are many ways to do this. For example, simply using a microwave oven or flooding the network with random traffic will do it.

### ***Incidental***

There are two types of incidental threat:

- **Accidental threats**  
A legitimate visitor may start up their PC with no intention of connecting to your Wi-Fi network. However, they can then be automatically connected to it. The visitor's PC is now a potential entry point for *viruses* onto your network.
- **Rogue Wi-Fi Networks**  
You may be at threat from people installing unauthorized networks onto yours.

## Wi-Fi Network Security Recommendations

---

### ***Type of Security***

Wi-Fi security comes in three major flavours today:

- **Wired Equivalent Privacy (WEP)**  
WEP, like the other two security schemes below, provides methods to *encrypt* traffic between wireless clients and APs, and a strategy for restricting network access. WEP has been included in 802.11-based products for some time. However, WEP has some recognized security weaknesses.
- **Wi-Fi Protected Access (WPA)**  
WPA provides enhancements to WEP, in both encryption and access control. WPA-compliant APs and client PC cards have been available since mid-2003.
- **Wi-Fi Protected Access generation 2 (WPA2)**  
The primary difference between WPA and WPA2 is that WPA2 uses a more advanced encryption technique called AES (Advanced Encryption Standard), allowing for compliance with US government security requirements. The first products supporting WPA2, both APs and client air cards, were entering the market as we wrote this chapter<sup>5</sup>.



**Recommendation: If security is an important concern to you, the wireless equipment you buy should at least support WPA, and if possible WPA2. You should also enable it on your network. You should also strongly advise your Wi-Fi users to purchase WPA or preferably WPA2-compliant equipment such as PC cards.**

---

### ***Configuring Your Wi-Fi Equipment for Better Security***

Wi-Fi APs come with a bewildering variety of configuration choices. We list the *minimum* things you should do for security reasons in *any* Wi-Fi WLAN/WAN.

→ Configuration choices in general are covered in Chapter 11.

**Recommendation: Change the default password for the Administrator account when you first install your network, and change the password regularly. Also, do not ever use simple passwords.**

---



---

<sup>5</sup> WPA2 is the marketing designation for the IEEE 802.11i standard.

---

The administrator is the only person who can change network settings. If a hacker gets hold of the administrator's password, they can also change those settings. Make it harder for a hacker to get that information.

---

**Recommendation: Change the default SSID, disable SSID Broadcast, and change the SSID periodically.**

---



The SSID is a name you can create for each Wi-Fi piece of equipment. Most wireless networking devices will give you the option of broadcasting the SSID. That option allows *anyone* to log into your wireless network. Do not broadcast the SSID.

Wireless products come with a simple default SSID set by the manufacturer. For example, the default SSID for Linksys wireless equipment is "linksys". Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use. Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start all over in trying to break in.

---

**Recommendation: Enable MAC Address Filtering.**

---



A MAC uniquely identifies a piece of network equipment. Even the equipment used by people to access your WWAN such as Wi-Fi cards has unique MACs. MAC address filtering will allow you to limit access to *only* those wireless nodes with certain MAC addresses. This makes it harder for a hacker to access your network with a random MAC address.

---

**Recommendation: Change the encryption keys periodically.**

---



The encryption keys are the "keys to the kingdom". Just as you need to change locks regularly on a building containing valuable articles, you should regularly change your Wi-Fi encryption keys.

## Checking Your Security

---

If you have followed all our recommendations, your Wi-Fi WWAN should be reasonably secure. Nevertheless, you should still install NetStumbler on one of your wireless PCs, and see if any of your APs show up. NetStumbler is the most common Wi-Fi network *sniffer*. Most likely, it is what someone will use to hack your network. If you configured everything correctly, none of your APs should show up in NetStumbler's window.



## Going Beyond the Security Solutions in This Cookbook

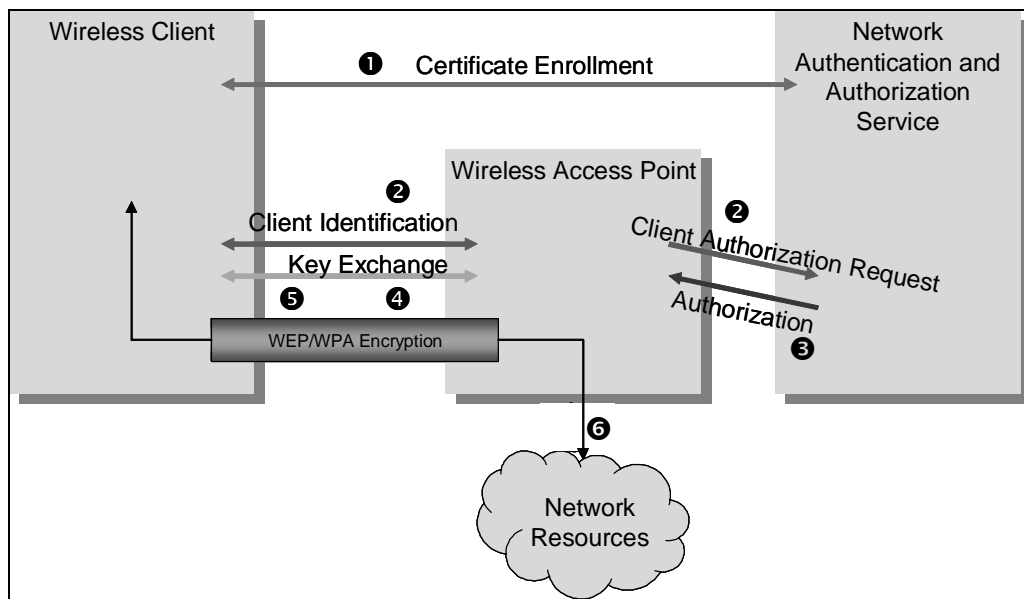
If you want to go to the highest level of Wi-Fi security, you will have to make some additional investment in equipment and Information Systems, for rigorous access control. This enhanced security approach requires an authentication infrastructure of RADIUS servers and a centralized account database. RADIUS servers were briefly covered earlier.

A RADIUS server is a computer that does three things for potential users of a network:

- Administration
- Authentication
- Authorization

You can use RADIUS servers for securing both wireless and non-wireless networks. The way that a RADIUS server works in conjunction with this WEP/WPA encryption is shown in Figure 8-1.

**Figure 8-1: RADIUS Server in Action**




---

**Recommendation:** For the very highest level of network security, use a RADIUS server in conjunction with the security techniques we described earlier.

---

## Further Wi-Fi Security References

---

Securing Wi-Fi networks is a complex subject. Therefore, this Cookbook cannot provide a complete guide. For further reading, here are some references to more detailed discussions of Wi-Fi security: 

- *Planning Guide for Securing Wireless LANs. A Windows Server 2003 Certificate Services Solution.* Microsoft.
- *Security for Next Generation Wireless LANs,* Cisco
- *Wireless Security End to End,* by Brian Carter and Russell Shumway. John Wiley & Sons; 1st edition (August 15, 2002).

## Physical Security Plan

---

### **Network Operations Center Physical Security**

If you have dedicated computers that are used as servers and management centers, you should take precautions to prevent the loss of the equipment.

- **Anti-theft kits**  
You should lock computers and peripheral equipment with security steel cables to secure mounts on a wall or floor. Most computer vendors sell complete kits to secure equipment. These cables can be defeated. However, it will take time to break them, which makes a theft more risky and provides time to respond to an alarm if installed.  
If there are APs or other wireless devices external to the computer, they should be placed in a locked ventilated small cabinet to prevent them being tampered with. An ideal indoor enclosure is a box made with perforated metal walls to allow you to see status lights and allow ample airflow so the equipment does not heat up.
- **Inexpensive break-in alarms**  
You can purchase inexpensive alarm systems that can detect motion, door or window entries, as well as smoke detectors. These can be directly purchased or installed by an alarm monitoring company, if one is available in your area. If you are located where these services are un-

available, you can mount an electronic siren and other indicators such as a strobe light in a location where you will hear or see it. This will also tend to make the intruder leave for fear of being caught in the act.

- **Building physical security**

To prevent grab and run thefts, you should install adequate door and window locks, bars on windows and measures to control who has access to the location. Depending on your situation, this may not always be possible. However, you should make some effort to prevent unauthorized access to the equipment. Simple “finger problems” such as often experienced with children or paws of pets could cause some interesting problems in your network.

Photo 8-1 shows the simple network operations centre we set up for our own experiments.

---

### Photo 8-1: Small Network Operations Centre

---



Dr. Onno W. Purbo at the controls

### ***Outside Equipment Physical Security***

- **Towers**

External towers can be an attraction for children or animals to climb up. A simple chain-link fence about two meters high will deter this from happening. You should also post signs to warn people that the tower is dangerous and that it is not designed to be climbed safely without appropriate safety equipment. Also, if there is any electrical equipment at the tower. You should post a sign warning of danger of electrocution.

A fence will deter but not stop someone who is determined to damage or climb the tower. Therefore, the tower should be placed in locations where people in the area can see it. Vegetation or brush should be cut back from the tower so it can be seen and easily accessed.

If problems are encountered, a simple intrusion alarm can be set up using a motion detector and siren. This can also be monitored remotely via a wire link or through the wireless equipment.

- AP equipment and power systems

We have covered options to mount AP equipment at the top of the tower, at its base, or indoors. External cases require that enclosures if near the ground should be mounted to make removal and opening of the enclosure difficult for people without proper tools. Security bolts and padlocks are typical approaches that prevent vandalism.

Ideally, enclosures should also be mounted at least a metre off the ground to prevent animals, water and insects from getting into the enclosure,

You should screen and orient any ventilation ports so that precipitation does not get into the equipment enclosures.

NEMA enclosures incorporate many of these features. They provide cover seals to prevent moisture and insects from getting inside.

Manufacturers offer APs at approximately two to three times the cost of indoor units that can be mounted easily on a tower or wall. These units already incorporate the features spoken about above. If you can afford them, they make your installation and security measures much easier to do. The added benefit with these ready-made units is that they are warranted for use outdoors.

Outdoor units operate in temperature ranges from -20 C to +40 to 50 C, whereas indoor units must be kept in temperatures from 0 to +5 C and no higher than 40 C. If indoor equipment is being used outside in warmer climates, any enclosures must provide venting to prevent overheating. Insulated (2 cm or thicker foam) enclosures must be used where temperatures go below 0 C. This will extend the operating temperatures to approximately the same range as a commercial unit.

In very cold locations, we recommend that outdoor AP units be used along with an additional cabinet around the enclosures. This cabinet acts as a thermal shell and windbreak around the AP enclosures. This

will extend the operating range to - 40 C or lower. In the warm season, you can open up the cabinet to prevent overheating. This cabinet / enclosure approach offers improved security against weather or vandalism.



# 9. Identifying What Equipment You Need and Costing it Out

In this chapter, the essential types of equipment that are needed in various extents to implement a community WLAN/WAN network is presented. Guidance is also given as to where to best procure equipment and to how to deal with typical problems that are often encountered such as poor equipment quality.

It should almost be understood, but the best way to get good prices nowadays is to make use of the Internet to:

- Locate vendors and their prices
- Locate freeware or shareware software that is adequate, instead of commercial software.

**Suggested audience for this chapter:**



Important terms in this chapter include:

Guy wire	A wire used to attach a tower to a guy anchor and the ground.
Rated	Assigned a normal capacity or power.
Sectional tower	A tower that consists of various sections.

## Wi-Fi Equipment Types

---

The types of wireless equipment needed to provide the functions of a Wi-Fi WLAN/WAN network vary with the network size and unique area being served.

Lower-cost Wi-Fi equipment on the market today offer features mostly aimed at the residential and small business user. Typically, these features include small routers, hub, bridges, packet switches, and print servers integrated with the basic AP unit. In selecting this equipment, you can end up paying for these additional capabilities when they are not needed for the network that will be put together.

### ***Basic APs***

Basic APs that do not have any additional routing or switching features are not as plentiful as the more integrated APs used by most consumers. In many retail outlets, these units are often not carried and have to be specially ordered from the supplier.

Such units are useful in providing local AP coverage at low cost. They are also very straightforward to set up. The areas for their application include:

- Single AP node networks with no linking to another AP in a chain
- Providing additional capacity to an established AP location by assigning the second AP to another frequency to serve more users.

### ***APs with Bridging and Repeater Modes***

As with basic APs, these are not commonly found in retail outlets. Instead, they are available from Internet suppliers and distributors. These offer all the features of an AP with the additional ability to act as point-to-point radio terminals, point-to-multipoint terminals, and single-ended and double-ended repeaters.

Such units cost 20 to 30% more than basic APs. However, the units can be deployed as APs, bridges, and repeaters, making them very flexible and re-deployable to deal with changing demands.

### ***Wireless Bridging (point-to-point links)***

This function is extremely useful in setting up a local wireless service, allowing traffic to be carried from a broadband POP out to the AP. These units only “talk” to each other. Thus, they provide a transparent data channel from the AP back to the broadband POP. The other key use is a way

of interconnecting APs to extend out a network to cover a wider area. This can be extended to form a “backhaul” network made up of all the individual bridge links between the APs as well as back to the POP. This is very similar to the meshing used in high-density WLAN urban networks.

### ***Repeater Functions***

The use of these types of APs as repeaters is another way of extended the reach to a POP or enlarging the coverage area provided by a single AP.

The repeater operation is very effective as long as it has a reasonable signal levels to do regeneration of the signal.

### ***Routing APs***

In setting up an AP to serve a small town or village, using a routing AP provides the needed flexibility to set up network with equivalency of a wired Network

These are very common in shops and come with a widely varying range of extra features and special high-speed turbo modes to provide up to 108 Mb/s over short wireless links, These APs are oriented at providing the home user the same or better networking while for their home network. Typically, the AP is connected to a cable or DSL modem via its WAN port. The unit provides firewall, NAT and DHCP server functions. Often the units also include a print server port as well. The majority of these APs incorporate multiple port switching hubs to allow multiple wired Ethernet devices to such as a local computer to have access to the Internet gateway besides the AP itself.

### ***Hubbing Features to Connect to Other APs***

Routing APs that have multiple port Ethernet bridges are the most versatile in situations where you need to link up a chain of APs. Here, the AP hub can connect to a wireless bridge to link to a remote AP or feed a close-by AP via an Ethernet cable to provide more local capacity by operating several APs on different channels. This illustrated in Figure xxx.

Depending on the manufacturer, there is firmware being offered to provide VLAN and other LAN options to improve security and resource utilisation. This is seen in more expensive APs. However, low cost units such as the LinkSys can have third-party firmware with these capabilities.

### ***Amplifiers***

In certain areas, amplifiers can be used to boost signal levels and overcome excessive fading problems, or to extend the range of a backhaul link or AP coverage area.

---

**Note: Amplifiers can only be used where regulations permit them, since the radiated power of the AP is boosted as well as the receiver sensitivity. Amplifiers can raise a systems output from 50 mW to 1000 mW (1 Watt) or more. In many jurisdictions, this far exceeds allowed maximums especially when the amplifier is then fed in to an antenna with gain.**

---

Amplifier costs are somewhat proportional to their power and features. Some units can be adjusted to a selected value. The price range is \$200 to \$400 US.

### ***Wi-Fi Adapter Cards***

There is a very wide range of Wi-Fi adapters available for laptops, desktops, and PDAs.

#### ***Desktop Computers***

Desktop computers have several options available to incorporate a wireless capability:

- PCI  
This is an internal card that usually features an antenna that can be removed to allow connection of a higher gain external antenna. Some cards also have an internal antenna for diversity. The cards come with a CDROM to allow the installation of the required drivers, help files, and user instructions as well as a configuration interface. The configuration is straightforward and installation is mainly self-directed.
- USB Adapter Cards  
In the event that the desktop PC does not have a spare port for a PCI card, a USB connected Wi-Fi unit can be used. Here, the unit is powered via the USB line and is set up in the same way as the PCI card. Most of the USB devices have fixed non-removable antennas that make them useful when the signal strengths are sufficient to have service without need of an external antenna. USB units can be modified to allow the connection of an external antenna with satisfactory results.

(Our own field testing used a US Robotics USB unit with good results). This approach can be used with laptops as well.

- Ethernet Connection

If the desktop computer has only has Ethernet connections, several AP manufacturers such as NETGEAR offer simple wireless bridge APs that act as a simple Ethernet service extension on a port-to-port basis. This can also be done with Basic APs that can be operated in “client” mode and provide an Ethernet feed to the desktop. This can be done with laptops as well. The hardware available now allows a lot more flexibility on where equipment can be mounted.

### ***Laptop Options***

Laptops also offer a range of possible ways to get WI-FI service using built-in wireless capabilities, plug-in cards or externally connected units.

- Internal Wi-Fi systems and Antennas

Many current laptop manufacturers are incorporating full wireless capabilities into their products. This wireless ready capability is good. However, it is not well suited to situations where external antennas are needed. The laptops incorporate antennas in the computer case which provide 2to 4dB of gain. These laptops can also support cards or externally connected adapter cards.

- PCMCIA cards

The most common adapter card for laptops is the PCMCIA card. Most of these cards do not have external antenna connectors. Like the internal systems mentioned above, they have low gain antennas that are typically 2 dB. These are quite good for local use within 500 meters of an outdoor AP site. Beyond that, external USB or Ethernet adapters with higher gain antennas must be used.

## **Avoiding Incompatibility Issues**

---

You must beware of buying long outdated models of Wi-Fi equipment, because there can be incompatibility problems.

For example, in our own testing of several D-Link client adapter cards, we found a compatibility problem between the LinkSys and the D-Link PC USB Adapter DWL-120. The cards failed to connect to the LinkSys AP on most attempts. If a connection were 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. How-

ever, 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 equipment that is more recent.

### Auxiliary Equipment

---

#### **Towers**

For our own work, we used a sectional tower manufactured by Delphi Inc. This tower comes in 3-metre 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 26 m. At lower heights, the tower can be supported by a building using a special mounting bracket, thus eliminating the need for guy wires. The tower is very durable, *rated* at winds over 160 kph.

Three people can set up a 10-metre tower in less than an hour, complete with antennas and cabling. Standard carriage bolt hardware is required along with simple tools (wrenches, pliers etc).

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 affect the link performance due to misalignment of the antenna's field patterns.

#### **Tower Lightning Protection Accessories**

To go along with the tower, the following lightning protection items are also required.

- Lightning arrestors
- Grounding rods
- Heavy gauge copper wire
- Wire ground clamps.

These items are required to protect the equipment and any local buildings from lightning strikes. Strikes can be quite damaging and thus, suitable grounding must be provided for the antenna as well as the tower. Typical installations require:

- Inline lightning arrestor per antenna

- Tower ground with grounding clamps to connect copper cable
- Several grounding rods (one for the tower and each antenna)
- Suitable lengths of heavy copper wire

### ***Tower lights***

If a tower high enough and is in an area where there is an airport or helicopter pad operations, tower lights may be required. In this case, only lights meeting the country's transport regulations can be used. The expense of the lights can be offset by government support.

### ***Guy wires***

In the budget for putting up your main AP tower, guy wires, turnbuckles, ground pegs, and other miscellaneous hardware must be included. Towers will involve at least one set of three guy wires. In higher freestanding towers (over 15 meters), two sets are needed. One set is mounted mid-way, with the other mounted near the top of the tower below the antennas.

→ Details of antenna installation are presented later in Chapter 13.

### ***NEMA Boxes***

If the Wi-Fi equipment is to be operated outside, suitable enclosures must be bought to place the equipment in. There are APs available that are already packaged and range in cost between \$500 and up. Doing it yourself will cost about \$100 dollars for the AP and \$70 and up for the NEMA enclosure. These enclosures are thick aluminium clamshell boxes with waterproof conductive gaskets. They provide thermal dissipation and are reasonably waterproof. They can extend the cold operating range of the AP if the NEMA box is also placed in a box to reduce cooling by radiation and wind.

For external equipment, the NEMA or equivalent box is necessary. Low cost APs are not designed to take outdoor weather and will fail quickly.

### ***Antennas***

The costs and quality of antennas can vary a lot. There are two main classes of antennas: indoor units and those designed to be mounted on outdoor towers or building walls.

#### ***Internal antennas (Planar Antennas or Patch Antennas)***

These types of antennas are suitable if the user is reasonably close to an AP and there is not too much obstruction (line of sight radio path). Typi-



cally, these types of antennas connect to adapter cards via a lightweight coaxial cable. They provide up to 9 dB gain, and can be placed in windows or higher locations to help bring in the signal better. They typically cost under \$40 US.

### ***External Antennas***

These have a very wide range in costs and quality.

Commercial grade<sup>1</sup> antennas are typically over \$400 US. These are usually planar or radome dish types meant for point-to-point microwave links. They are available for 2.4 and 5 GHz 802.11b and 802.11a bands. In certain case such as extended range links to access a POP, these can be justified if they are carrying the traffic of many users.

These commercial antennas also include specialized high gain units omnidirectional and sectional antennas between 6 and 10 dB to provide cellular like coverage over a wider area. These units are quite expensive at \$300 to \$500 US. The costs can be justified in cases where a fair number of users are served by it. Such antennas can serve multiple APs by using combiners.

### ***Lower cost WI-Fi oriented Antennas***

These have gains from 12 dB up to 28 dB and higher. They are designed for specific Wi-Fi and short-range microwave links. These come in a variety of forms:

- Wall mounted patch or planar directional Antennas
- Small Yagi multi-element antennas (housed or un-housed)
- Parabolic open grid type antennas
- Lower-gain omnidirectional and sectional antennas (up to 6 dB).

The costs of the above antennas range fro \$50 up to \$200 US. The retail cost varies from supplier to supplier and good deals can be had. Many of these units are made by reputable antenna companies and are quite durable. We have found no significant problems with the performance or the hardware of such units.

These antennas are lightweight and can be used for portable testing operations quite successfully.

### **Coaxial Cables and Connectors**

The connecting of tower-mounted antennas requires suitable cables and connectors that have low loss at 2.5 GHz. High quality cable such as LMR 400 provides very acceptable loss at 0.2 dB/ m. Other higher loss cables can be used as long as runs are short. Common RG8U 50 ohm cable is an example. Note that coax used for cable TV is 75 Ohm impedance and cannot be used. The cable can be \$4 and up a meter.

Connectors used for microwave use are Type N, at several dollars each. Again only units designed for weather exposure should be used. Waterproofing tape must be used to ensure connectors do not get water in them. Cheaper substitutes should be avoided since it may be difficult to access the connectors up on a tall tower,

### **Solar Power**

Solar panels can be used in situations where the AP or local user's computer cannot access commercial power. Solar electrical systems can be expensive, however this is dependent on the degree of usage that the system will have.

For users, modest systems can be used to provide power on an on and off basis. For main APs, the power supplies must be much higher capacity to maintain continuous basis. Here, the cost can typically be around \$600 USD and up depending on the power demands (multiple APs).

A complete solar system includes:

- A solar voltaic panel and Mount, 60 Watts Minimum
- Batteries heavy duty (\$100 each)
- Charge controller (\$50)
- Hardware and housing (\$60)
- Power inverter (for AC power supplies) (\$45)

## **A Simple Network Budget**

---

Now that you know what network equipment and other equipment you need to buy, you can start to make up a network budget. Table 9-1 is a snapshot of one of the spreadsheets available for the Cookbook; see Appendix F for more details. You will need to customize the budget to suit your own needs, to include:

- Your own estimates of the adjustable parameters (in ***bold blue italic*** font)
- Non-network capital expenditures (e.g., testing equipment and tools)
- Backhaul costs
- More than one base station
- Financial expenses such as interest on loans
- Breakeven or Net Present Value calculations
- Making it non-profit if you will be providing a non-commercial network, etc.

**Table 9-1: Example of a Simple Budget for a Commercial Wi-Fi Network (2004 prices)**

<b>Basic Assumptions</b>	
Customer Premises Equipment Cost	<b>\$100.00</b> per subscriber
Base Station Cost	<b>\$1,000.00</b> per radio
Subscription Rate	<b>\$25.00</b> per month
On - Air Base Station Capacity	11.0 Mb/s
On - Air Overhead	<b>30%</b>
Actual Base Station Capacity	7.7 Mb/s
Subscribers	<b>200</b> per Base Station radio
Oversubscription Ratio	<b>10</b> to 1
Throughput per Active User	385 Kb/s
Management Software Cost	<b>\$100.00</b> per Base Station
<b>Annual Capital and Operating Costs</b>	
Number of Base Station Radios	<b>2</b> <b>4</b> <b>6</b>
Base Station Capital Cost	\$2,000.00              \$4,000.00              \$6,000.00
Capital Cost of New Radios	\$2,000.00              \$2,000.00              \$2,000.00
Total Customers	400                      800                      1200
New Customers Each Year	400                      400                      400
New Base Station Cost per New Customer	\$5.00                      \$5.00                      \$5.00
CPE Cost per New Customer	\$100.00                      \$100.00                      \$100.00

## Building Rural Wi-Fi Networks: A Beginner's Cookbook

Management Software Cost per Customer	\$0.25	\$0.13	\$0.08
One Year Operating Costs Per Customer	<b>\$200.00</b>	<b>\$180.00</b>	<b>\$160.00</b>
Capital Cost per New Customer	\$105.25	\$105.13	\$105.08
Total Capital and Operating Costs per New Customer	\$305.25	\$285.13	\$265.08
Total Capital and Operating Costs	\$122,100	\$186,050	\$234,033
<b>Total Costs per Customer</b>	<b>\$305.25</b>	<b>\$232.56</b>	<b>\$195.03</b>
<b>Annual Revenues</b>			
Installation Fee for New Customer	\$100.00	\$100.00	\$100.00
Annual Subscription Fees (all customers)	\$300.00	\$300.00	\$300.00
Revenues for Existing Customers	\$0.00	\$120,000	\$240,000.
Revenues for New Customers	\$160,000.	\$160,000	\$160,000
Total Revenues	\$160,000	\$280,000	\$400,000
<b>Total Revenues per Customer</b>	<b>\$400.00</b>	<b>\$350.00</b>	<b>\$333.33</b>
<b>Gross Revenue per Customer</b>	<b>\$94.75</b>	<b>\$117.44</b>	<b>\$138.31</b>

**Part II:  
Assembling  
and  
Customizing  
Your  
Equipment**

# In this part...

Off-the-shelf consumer equipment is not usable out of the box for WWANs using the supplied information from the manufacturer. However, once configured according to the rules we document below, the WLAN/WAN 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.

We also found that the typical *firmware* supplied with the consumer AP does not support the needed features out of the box. However, alternative third party firmware is available and works well.

---

## **This entire part of the Cookbook is technically oriented.**

---

- Chapter 10 deals with how to set up the radio aspects of your Wi-Fi equipment. For example, we will show you how to achieve much greater ranges than you may have thought possible.
- Chapter 11 deals with the network side of things. Here, we are concerned with aspects like those that you will run into with any data network.
- Chapter 12 deals with the issue of physically adapting your equipment for outdoor use in your environment.



# 10. Setting up Your Radio Equipment

Off the shelf, the features, documentation, and firmware of consumer APs are tailored for residential and office use. They are thus nearly a plug and play experience for the user. Using 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 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 have found many third 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.

Information supplied in the box by manufacturers of consumer Wi-Fi equipment is generally inadequate to configure the equipment for rural or remote applications. However, once configured according to rules we have discovered, 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 any need for you to intervene.

**Suggested audience for this chapter:**



## Part II: Assembling and Customizing Your Equipment

---



Important terms in this chapter include:

Institute of Electrical and Electronics Engineers (IEEE)	A standards-setting body for North America.
--	---

$\mu\text{sec}$	Millionths of a second
-----------------	------------------------

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
-------------------	--

---



## Long Distance 802.11b Timing Issues

---

### ***The Problem***

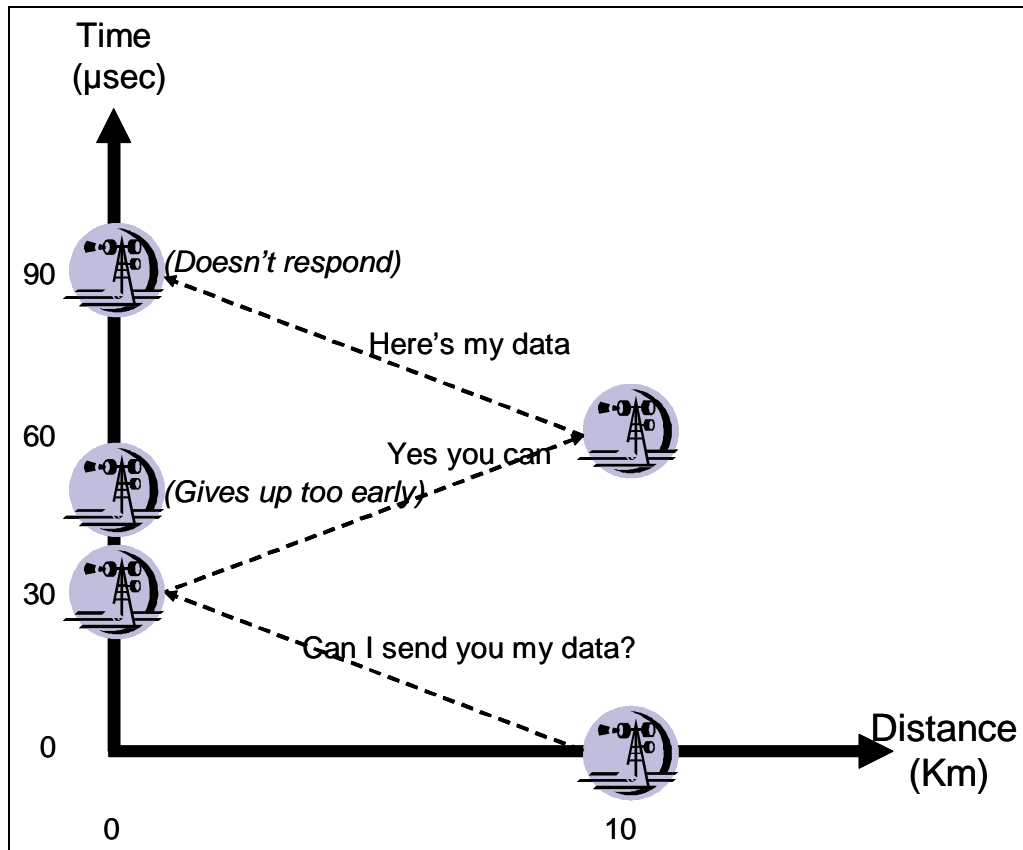
Light does not travel instantaneously. This fact sets a limit on how far two APs or relays can be spaced apart. The reason for the limitation is that the Wi-Fi standard sets limits on how patient an AP can be in waiting for a response from another AP.

You can change those limits. If you have configured an AP to be too “impatient”, then data from the other AP will be ignored. Figure 10-1 shows two APs about 10 km apart. Starting at the bottom right and following the arrows, you can see the following events:

- The AP on the right sends a message to the left one that it has some data to transmit to it
- About 30 millionths of a second ( $\mu\text{s}$ ) later, the left AP gets the message (due to the light travel time).
- The left AP sends a message to the right AP saying that it is allowed to send data.
- The left AP starts a timer. If that timer goes beyond its limit, then it will ignore data transmission from the right AP (but not messages).
- The left AP gives up, perhaps after 10  $\mu\text{s}$ , or however long it was configured to wait.
- About 20  $\mu\text{s}$  later, the right AP gets the message that it can start transmitting data.
- The right AP starts transmitting.
- About 30  $\mu\text{s}$  later, the data arrives at the left AP, but is ignored.

If you set the interval to be 10  $\mu\text{s}$ , which is the shortest possible interval according to the technical standard, the furthest the two APs can be apart is about 3 km. This is not surprising since the 802.11 specification was designed with Local Area Networks in mind, where distances are less than several hundred metres.

Figure 10-1: Giving up Too Early Limits How Far Two APs can be Apart



### The Solution

Obviously, that is not very far for covering a wide area such as a rural community.

The fact that we and many other people have been able to maintain 11 Mb/s connections over much longer distances implies you have to set the wait interval to be longer than this.

So far, we have talked about a waiting interval. Actually, there are three parts to it. Table 10-1 gives you details of what they are called.

Table 10-1: Wait Intervals for Wi-Fi

Name of Timing Interval	Acronym	Note	Example Values ( $\mu$ Sec)
Short Inter-Frame Spacing	SIFS	Should not change this.	10
Distributed Point Coordination Function Inter-Frame Space	DIFS	Set it to at least the SIFS	10
“Contention window”		Set it to several times the SIFS	50
Total wait ( $\mu$ s)			70
Distance corresponding to this wait time (km)			21

The important thing for you to do is to use the following formula to set the total waiting interval:

$$\text{Total wait interval } (\mu\text{s}) = 10 \times \text{AP distance (km)} / 3.$$

## Going Even Farther Distances

In order to go over single hop distances of 25 – 40 km, a Lucent/Orinoco demonstration ad-hoc mode can be used. This was implemented by Lucent before the IEEE had standardized the mode of operation for wireless bridging that wireless bridge products now incorporate.

This special mode does not send acknowledgement signals (ACKs) and is thus will prevent messages from being timed. This solution will work for long point-to-point links as well as for long-range point-to-multipoint configurations with low user density (about 10 active users).

You can still access this mode via any Prism or Hermes chipset under Linux with the right wireless tool commands. In Table 10-2 below are listed 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 11 Mb/s at a decent distance.

Table 10-2: Firmware Modifications for Very Extended Reach (example)

Command	Notes
<code>dev=eth0</code>	Put card in ad-hoc mode
<code>iwconfig \$dev mode ad-hoc</code>	Disable RTS as this is a point-to-point link - probably not needed
<code>iwconfig \$dev rts off</code>	Place a fragmentation threshold — more loss on precarious point-to-point links. If you are using point-to-multipoint, setting this lower would be a good idea.
<code>iwconfig \$dev frag 1024</code>	Fix the rate at 11 Mb/s
<code>iwconfig \$dev rate 11M</code>	Turn on the old ad-hoc "demo" mode for peer to peer
<code>iwpriv \$dev set_port3 1</code>	You can verify that you are using the ad-hoc mode if the Access Point BSSID/MAC in <code>iwconfig</code> is reported as all zeros. If it is your MAC or the peer's MAC, you are using IBSS ad-hoc.

### Disabling Antenna Diversity

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*. Such AP units 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 *stub antennas*.

In outdoor applications involving external *high-gain antennas*, the diversity operation *must be turned off*. The AP must be set to use the same single antenna at all times. If left in diversity mode, 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 miss them if there are strong signals very close by being received on the other low gain antenna.

In our own backhaul field experiments, we found intermittent operation and low power with the wireless bridges (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. Our local Link-Sys 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 antenna caused switching from the external antenna to the internal antenna whenever the local APs did a transmission burst.

Unfortunately, not all Wi-Fi equipment makes it easy to configure them to disable the diversity operation. 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.

### Disable Automatic Power Setting

---

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, *you should adjust the power level.*

**Unfortunately, not all APs make it straightforward to configure them to disable the diversity operation and have the power level fixed. For example, the documentation supplied with consumer units may 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.**



### Channel Settings

---

The Wi-Fi frequency band has up to 14 overlapping channels, numbered 1 through 14. Three of these channels (1, 6, and 11) are non-overlapping and are thus commonly used. When you set up a Wi-Fi network, you must select a channel for each AP or relay node.

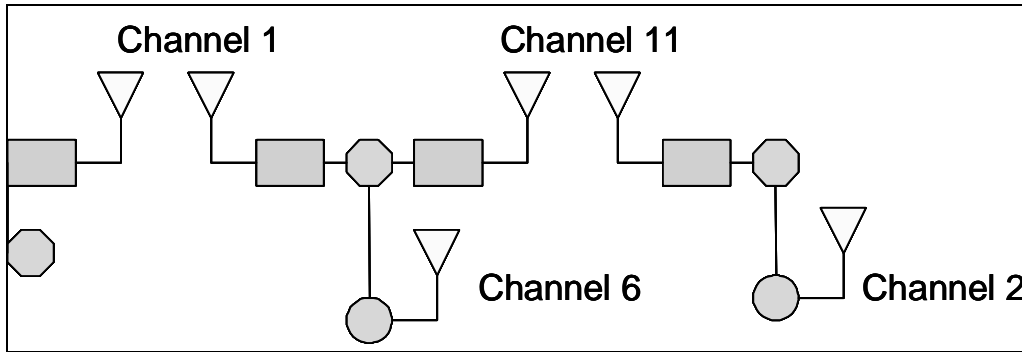
For remote applications where APs and relay nodes will be using the same frequency band, you need to do the channel assignments to provide as

## Part II: Assembling and Customizing Your Equipment

much isolation as possible between APs or wireless bridges that are within 100 – 200 metres of each other. Otherwise, you might get interference.

For example, you might use channel 1 for the backhaul radio link and channel 11 for the AP. If another backhaul were being used, Channel 6 would be used. See Figure 10-2 for an example of how you can do this.

**Figure 10-2: Example of Channel Co-Ordination**



# 11. Setting up Your Network Equipment

etting computer equipment set up so that it all works together is still something of an art. The process involves setting a sometimes-bewildering group of networking “parameters” for each piece of equipment. If one of them is wrongly set, your whole network might simply not work at all!

**G** Fortunately, we have gone through the pain of figuring out how to do this for a Wi-Fi WLAN or WWAN. This chapter gives you the benefit of our experience.

Before you read the chapter, have a look again at Figure 2-1. In it, you will see the main Wi-Fi equipment whose network configuration you have to set up:

- The AP used to provide coverage.  
This AP has a built-in Ethernet bridge that is connected via Ethernet cable to the wireless bridge.
- The wireless bridge in the field
- The gateway (if not already provided).

**Suggested audience for this chapter:**



## Part II: Assembling and Customizing Your Equipment

---



Important terms in this chapter include:

Baud rate	The speed at which data is transmitted
Beacon interval	Time between attempts to locate a Wi-Fi source when the scanner is in scan mode
Gateway router	A router that performs conversions between different coding and transmission formats.
RIP	Routing Information Protocol

---



# Chapter 11: Setting up Your Network Equipment

## User Interfaces for Administering Wi-Fi Equipment

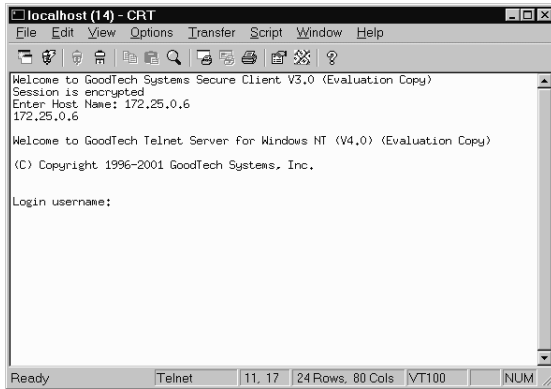
Both consumer and commercial Wi-Fi equipment are administered through a browser. Photo 11-1 below shows a screen shot of the main configuration screens for LinkSys equipment. Screens such as these are used for setting the network configuration of the equipment.

Photo 11-1: Main LinkSys Setup Screen



Most commercial Wi-Fi vendors also offer a Telnet interface to their equipment. At least one consumer AP also has a Telnet interface, the D-Link DWL-2100. Such an interface is like logging into a mainframe computer in which you issue commands line-by-line. See Photo 11-2 for an example.

### Photo 11-2: Telnet User Interface



## Setting up Your PCs

You will need a portable PC or notebook in order to configure the Wi-Fi equipment. The PC or notebook itself first needs to be properly configured for communication, though. Procedure 11-1 shows how to do it.

### Procedure 11-1: Configuring Your Test PC

Step	Step Description	Notes	Done?
1. Configure static TCP/IP properties of the PC to communicate with AP and the wireless bridge.	The IP address and subnet mask must have same the network address as the AP and wireless bridge in order to access each device's configuration settings.	Static addresses are essential for testing. If at any time the RF link is unable to connect, any computers with dynamic DHCP addresses will lose connection to DHCP server and be unable to receive DHCP-served TCP/IP properties.  Also, double check the factory default TCP/IP properties of each device.	<input type="checkbox"/> Yes <input type="checkbox"/> No
2. Configure the PC have the static network address 192.168.0.0.		This will enable communication with both the LinkSys and the D-Link.	<input type="checkbox"/> Yes <input type="checkbox"/> No

# Chapter 11: Setting up Your Network Equipment

Step	Step Description	Notes	Done?
3.	Ensure that the correct DNS servers and suffix search list parameters are entered.	This will allow access to the Internet.	<input type="checkbox"/> Yes <input type="checkbox"/> No

In addition, you will likely have a PC directly connected to the gateway for monitoring purposes. If so, set the monitor PC to receive DHCP address, to be able to test DHCP functionality.

## Setting up the Gateway/Firewall

Procedure 11-2 gives the instructions for setting up a Wi-Fi router as a gateway. If you have a router that is separate from your Wi-Fi equipment near the POP, you may have to change this procedure a bit.

### Procedure 11-2: Configuring Your Wi-Fi Gateway/Firewall

Step	Step Description	Notes	Done?
1.	Connect the Ethernet cable from the PC to any of the "LAN" ports on the gateway.	The labels may be different of your gateway.	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.	Connect the gateway's Internet WAN port to the Internet connection.		<input type="checkbox"/> Yes <input type="checkbox"/> No

## Part II: Assembling and Customizing Your Equipment

Step	Step Description	Notes	Done?
3. Configure that Internet WAN port to receive DHCP addresses.			<input type="checkbox"/> Yes <input type="checkbox"/> No
4. Configure the equipment's mode to be Gateway.		It will act as an Internet firewall.	<input type="checkbox"/> Yes <input type="checkbox"/> No
5. Configure the Wi-Fi gateway's wireless connection.	<ul style="list-style-type: none"><li>• Set its SSID name.</li><li>• Select the broadcast channel. Ensure that the channel does not conflict with any other devices on network.</li></ul>		<input type="checkbox"/> Yes <input type="checkbox"/> No
6. Configure the Wi-Fi gateway to act as a DHCP server.	Set the start and end IP addresses of the DHCP range.		<input type="checkbox"/> Yes <input type="checkbox"/> No
7. Configure the TCP/IP properties of the LAN ports.	Assign the same IP address to all LAN ports.	If you set the IP address and subnet mask on the gateway to have a different network address from that of the PC used to configure it, communication will be lost. You will have to change the PC's TCP/IP properties again to match the network address of the gateway.	<input type="checkbox"/> Yes <input type="checkbox"/> No

# Chapter 11: Setting up Your Network Equipment

Step	Step Description	Notes	Done?
8. Turn off antenna diversity.	Select one antenna for both transmit and receive.	See the section “Disabling Antenna Diversity” in Chapter 10.  This option may not be available with the factory firmware version, or may only be reachable via Telnet. Firmware capable of adjusting the antenna characteristics must be loaded.	<input type="checkbox"/> Yes <input type="checkbox"/> No

## Setting up the AP and Layer 2 Bridge

In the network configuration of Figure 2-1, we use a single box that combines the features of an AP and a layer 2 bridge. This simplifies the network architecture considerably. In addition, it provides additional Ethernet ports for a local test computer and a connection for another backhaul link if desired.

If instead you have two separate boxes to do these two functions, you will have to adjust Procedure 11-3 somewhat.

### Procedure 11-3: Configuring Your AP and Layer 2 Bridge

Step	Step Description	Notes	Done?
1. Connect the Ethernet cable from the PC to any of the “LAN” ports on the remote AP.		The labels may be different of your gateway.	<input type="checkbox"/> Yes <input type="checkbox"/> No

## Part II: Assembling and Customizing Your Equipment

Step	Step Description	Notes	Done?
2. Do not use the WAN port labelled "Internet".		Therefore, the operating mode of the AP does not matter, since only the LAN port switch capabilities will be used. The AP can be set to either Router or Gateway operating mode. This setting only dictates the behaviour of the WAN port.	<input type="checkbox"/> Yes <input type="checkbox"/> No
3. Configure the AP wireless connection.	<ul style="list-style-type: none"><li>• Set its SSID name.</li><li>• Select the broadcast channel. Ensure that the channel does not conflict with any other devices on network.</li></ul>		<input type="checkbox"/> Yes <input type="checkbox"/> No
4. Disable the AP DHCP server feature.		You already configured the gateway/firewall to act as a DHCP server in Procedure 11-2. It is possible to have more than one DHCP server on network. However, for simplicity, you should use only one DHCP server unless you have a very specific reason to do otherwise.	<input type="checkbox"/> Yes <input type="checkbox"/> No

# Chapter 11: Setting up Your Network Equipment

Step	Step Description	Notes	Done?
7. Configure the TCP/IP properties of the LAN ports.	Assign the same IP address to all LAN ports.	If you set the IP address and subnet mask on the AP to have a different network address from that of the PC used to configure it, communication will be lost. You will have to change the PC's TCP/IP properties again to match the network address of the AP.	<input type="checkbox"/> Yes <input type="checkbox"/> No
8. Turn off antenna diversity.	Select one antenna for both transmit and receive.	See the section "Disabling Antenna Diversity" in Chapter 10.  This option may not be available with the factory firmware version, or may only be reachable via Telnet. Firmware capable of adjusting the antenna characteristics must be loaded.	<input type="checkbox"/> Yes <input type="checkbox"/> No

## Setting up the Wireless Bridges

### **Numbers of Bridges**

In our example network configuration (Figure 2-1), there are two wireless bridges, one near the remote AP and one near the POP gateway. If you have several remote APs directly linked to the POP gateway, there will be  $n+1$  bridges, where  $n$  is the number of remote APs.

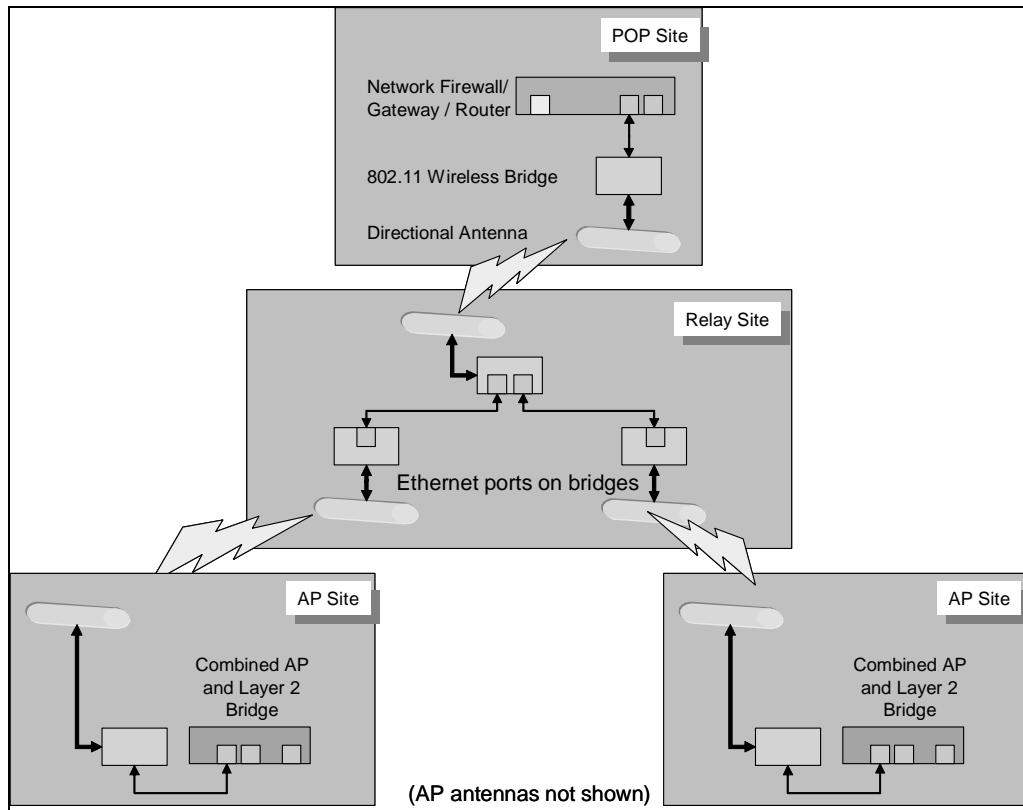
Further, if you have a more complex backhaul with relay nodes, those relay nodes will each contribute at least two bridges, one going "up" in the

## Part II: Assembling and Customizing Your Equipment

direction of the gateway, plus one or more in the “down” direction towards the remote APs.

If your wireless bridge can connect to only one bridge or AP, there as many bridges in the down direction as there are nodes to connect to, usually via directional antennas. This configuration is shown in Figure 11-1.

**Figure 11-1: One Possible Relay Node Bridge Configuration**



Note that we have not shown the relay site also serving as an AP site, which is a quite feasible and attractive configuration.

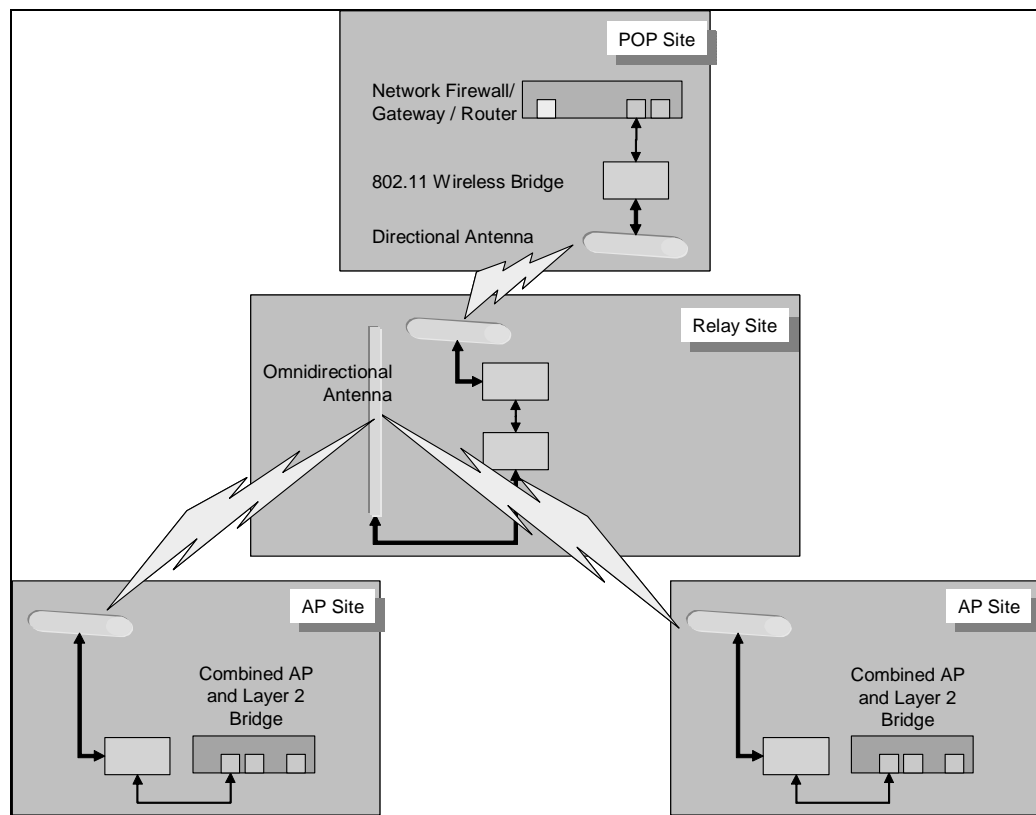
By contrast, if your equipment supports multiple APs per bridge, you will need fewer bridges at the relay nodes. An example of equipment that does just this is the D-Link DWL-2100. Figure 11-2 shows this type of bridge configurations for a relay node. An omnidirectional antenna is used.



# Chapter 11: Setting up Your Network Equipment

To make things simple, we will document the procedure for the two-bridge case shown in Figure 2-1.

Figure 11-2: Another Configuration of Bridges at Relay Sites



## General Considerations

You can find consumer APs that provide the needed configurations for use as a wireless bridge. However, the settings must be modified from the default settings in order to be able to utilize its bridging mode. In this mode, a transparent connection is set up at layer 2. This requires that the both bridges know the other's MAC addresses. This arrangement excludes

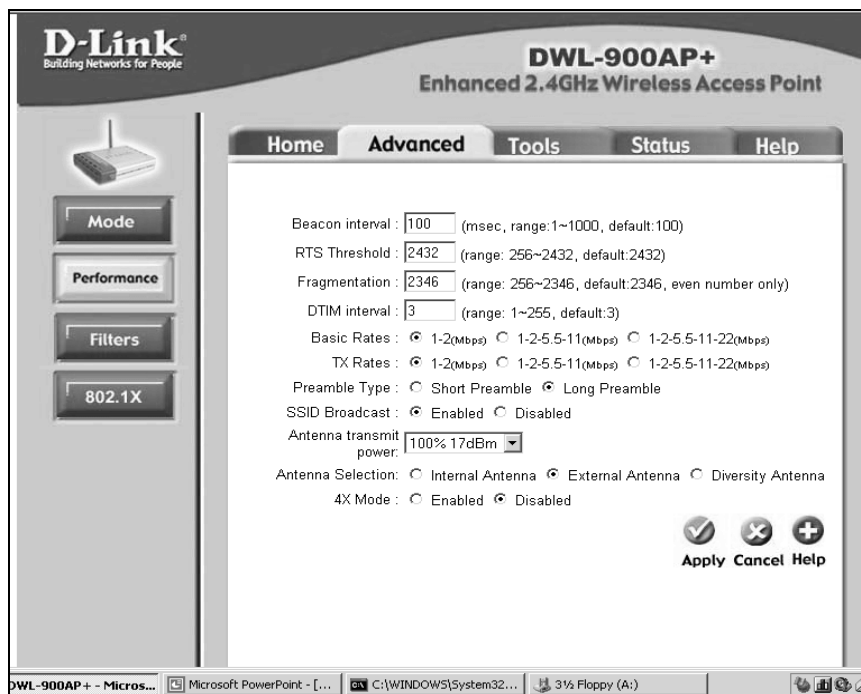
## Part II: Assembling and Customizing Your Equipment

other users from using the bridges for AP addresses, but does not guarantee immunity from deliberate Wi-Fi hackers.

In our own field tests, we used D-Links as bridges. These can be easily used as an AP or backhaul transceiver. In the browser interface, there is usually a screen in which you can set the unit's mode. Bridge mode proved to very transparent, with no significant packet legacy at the highest baud rates.

Other settings will need to be changed. You will typically find many of these under an "Advanced" tab such as shown in Figure 11-3 for the D-Link.

Figure 11-3: Disabling Antenna Diversity and Setting Other Parameters



### Wireless Bridge Configuration Procedure

See Procedure 11-4.

# Chapter 11: Setting up Your Network Equipment

## Procedure 11-4: Configuring Your Wireless Bridge

Step	Step Description	Notes	Done?
1. Connect the Ethernet cable from the PC to the Ethernet port on the wireless bridge.		The labels may be different of your gateway.	<input type="checkbox"/> Yes <input type="checkbox"/> No
2. Configure the TCP/IP properties of the Ethernet port.	The same IP address will be assigned to all LAN ports.	If you set the IP address and subnet mask on the wireless bridge to have a different network address than that of the PC used to configure the wireless bridge, communication will be lost. You will have to change PC TCP/IP properties again to match the network address of wireless bridge.	<input type="checkbox"/> Yes <input type="checkbox"/> No
3. Configure the wireless connection.	<ul style="list-style-type: none"><li>• Set its SSID name.</li><li>• Select the broadcast channel. Ensure that the channel does not conflict with any other devices in the area.</li></ul>		<input type="checkbox"/> Yes <input type="checkbox"/> No

## Part II: Assembling and Customizing Your Equipment

Step	Step Description	Notes	Done?
4. Configure the operating mode as a wireless bridge.	Enter the MAC address of the other unit that will complete the wireless bridge.	You must enter the MAC address of the Ethernet port. Do not enter the MAC address of wireless port.	<input type="checkbox"/> Yes <input type="checkbox"/> No
5. Disable the DHCP server feature.			<input type="checkbox"/> Yes <input type="checkbox"/> No
6. Turn off antenna diversity.	Select one antenna for both transmit and receive.	See the section "Disabling Antenna Diversity" in Chapter 10.	<input type="checkbox"/> Yes <input type="checkbox"/> No
7. Set the receiver to not scan in the event of a Loss of Signal (LOS).			<input type="checkbox"/> Yes <input type="checkbox"/> No
8. Set the power to the highest level (+17 dBm).			<input type="checkbox"/> Yes <input type="checkbox"/> No
9. Repeat for the other wireless bridge.			<input type="checkbox"/> Yes <input type="checkbox"/> No
10. Connect the network configuration as shown in Figure 2-1.			<input type="checkbox"/> Yes <input type="checkbox"/> No

## Testing Connectivity

Now, do a quick check to see that all the devices are reachable. From your monitor PC, ping the devices in the following order:

- Gateway LAN IP address
- Wireless bridge connected to gateway
- Wireless bridge connected to AP / Layer 2 Switch
- AP / Layer 2 Switch LAN port

# Chapter 11: Setting up Your Network Equipment

---

- Remote PC's connected to AP / Layer 2 Switch LAN port
- Internet address (i.e., www.yahoo.com) to ensure Internet connectivity.

## Storing Configuration Information in Flash Memory

---

Momentary power disruptions can result in unexpected hangs in the recovery of the units. By design, APs are supposed to refer to the firmware stored in flash ROM with the configuration data intact.

Our own experience with consumer APs is that this usually works. However, we have on occasion seen consumer APs hang or go back to default settings. Such behaviour is of concern, especially 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. After looking into this problem in more detail, we have concluded that it is likely due to inadequate testing of consumer Wi-Fi units. Such lack of testing results in a higher variability in quality compared to the norm for commercial units.

A minimum of 15-minute of Uninterruptible Power Supplies (UPS) should be used with the main units to ensure acceptable reliability and manual reset / reconfigure actions. The use of UPS units brings on some additional costs and complexity. However, the trade-off is well worth it.

Further, repeaters / relays in poorly accessible locations should have longer-term battery backup as well, if you can afford it.

### ***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. We have found this to be fairly reliable. However, as a precaution, you should:

- Document the configuration of each piece of equipment
- Take screen shots of forms you have modified
- Save any notes you used during the system's first set-up.

## Part II: Assembling and Customizing Your Equipment

---

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

### ***Recovery from Failure***

AP units recovering from a power failure will reboot their firmware. If you have custom configured them, they will reload the selected parameters set by you. 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).

We tried this 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.

We observed the behaviour 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 timeout hardware reset feature to allow an automatic reboot if the unit fails to fully come on line.

# 12. Packaging Your Equipment

ackaging for consumer APs is only suitable for indoor use, as shipped by the manufacturer. Equipment built for residential use has compromises between costs and its ability to continue to operate well in environments that are more hostile. Temperature extremes, moisture, resistance to electromagnetic interference, and resistance to mechanical shock are examples of where tradeoffs have been done. In home environments, these factors are usually benign and do not significantly affect the equipment.

For outdoor rural or remote applications, it is quite likely that one or more of these factors will be outside the consumer product's tolerance. However, you can modify such equipment to some extent to enhance their ability to provide acceptable performance without triggering high costs.

In order to upgrade the packaging for outdoor use, you need to:

- Repackage for ruggedness
- Upgrade the RF connectors
- Add lightning protection for external antennas
- Add power surge protection
- Improved the generally inadequate RF shielding.

This is especially true if there are other APs nearby. A metal box with shielding (a NEMA box) is required for outdoor operations.

Simple low-cost fixes are available to deal with these issues. You will need to mount the equipment in ways that make it more resistant to environmental extremes.

**Suggested audience for this chapter:**



## Part III: Installing Your Wi-Fi Network

---



Important terms in this chapter include:

Electromagnetic Interference (EMI)	The interference in signal transmission or reception caused by the radiation of electrical and magnetic fields.
Ground Fault Interrupter (GFI)	An electrical safety device that is able to detect a short circuit and shut off power automatically. Used as a protection against electrical shock.
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.
NEMA	North American Manufacturer's Association
Radome	A cover that protects an antenna from the extremes of climate while allowing electromagnetic signals (radio waves) to pass through without attenuation.
RG58	A type of coaxial cable. (50 Ohms)
Uninterruptible Power Supply (UPS)	A battery backed-up power supply

---



### Repackaging for Ruggedness

---

Consumer AP packages are designed to operate in partially environmentally controlled areas typical of a household. This is contrast to most commercial grade equipment, which 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 than 60% is acceptable.

If you are to base your Wi-Fi WWAN on consumer equipment as we have done in our own tests, you are going to have to repackage it to meet outdoor environmental conditions. You will have to adapt your enclosure to your region's specific environmental conditions.

Photo 12-1 shows a simple inexpensive do-it-yourself enclosure we made for our own work in southern Canada. The inside of the enclosure is shown in Photo 12-2. Inside details are shown in Photo 12-3 through Photo 12-5.

---

#### Photo 12-1: Do-it-yourself Enclosure (Outside)

---



The enclosure was originally used to carry equipment for a touring rock band.

Photo 12-2: Do-it-yourself Enclosure (Top View of Inside)

---



Upper left:  
Box containing AP

Right:  
Box containing  
bridge

Bottom:  
Electrical  
connections

Note that the  
inside of the overall  
enclosure is foam-  
lined.

Photo 12-3: Details of AP Connections inside Enclosure

---



Cable ties keep  
everything neat.

## Part III: Installing Your Wi-Fi Network

---

Photo 12-4: Details of Wireless Bridge Connections inside Enclosure



Note how nicely the cable screws into the connectors fixed to the NEMA box.

Photo 12-5: Inside the NEMA Boxes for the AP and Wireless Bridge



Note the foam used in the NEMA box.

### NEMA Enclosures

---

The best enclosures to use for outdoors follow standards for being corrosion proof, feature gaskets on lids, and are designed to use waterproof connectors. In North America, the relevant standard is that of the North American Manufacturer's Association (NEMA). Such enclosures are typically carried by electronic supply stores or web-based suppliers. For example, see:

<http://www.terra-wave.com/browse-enclosures.html>

Photo 12-6 and Photo 12-7 show how other people involved in do-it-yourself Wi-Fi have used NEMA enclosures in conjunction with consumer Wi-Fi equipment. By contrast, you will notice from Photo 12-2 that we have also used NEMA enclosures for both the AP and the bridge, but in addition, we have an outer enclosure that contains both of these NEMA boxes. The outer enclosure is then mounted at the tower base.

---

#### Photo 12-6: Enclosing an AP within a NEMA Box

---



Photo from web site:  
<http://www.sveasoft.com>

---

#### Photo 12-7: Enclosing a Bridge within a NEMA Box

---



Photo from web site:  
<http://www.sveasoft.com>

### Weatherproofing and Humidity

---

If you use the equipment in outdoor conditions, you will need to place it in a reasonably airtight and waterproof container. If the container is not airtight, condensation can build up in the box and water can leak in from rain and dew. High humidity will make the circuit board fail, especially if there is salt brine in the air in coastal areas.

You must waterproof any external connectors or equipment to prevent moisture from entering the connector. Moisture will absorb energy in the connector and lead to corrosion that will degrade RF performance.

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

---

**Antennas are usually waterproof. However, units that are enclosed within radomes have small drainage holes to allow any condensation to drain out. It is important that you mount the antenna so that one of the drain holes is facing downwards.**

---

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

### Overheating

---

A problem with enclosing the APs will be keeping the AP electronics below 40 C on hot days (up to 50 C). You can cool the AP 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 color.

### Freezing

---

Equipment in locations where outside temperatures can dip below 0 C should be protected from getting too cold. At low temperatures (0 or below), radio frequencies can drift off channel. The result? Failure of the service. This is not just theoretical – we have seen it happen.

To prevent excessively low temperatures, simple solutions such as an insulating a metal enclosure with foam padding on the outside can extend the unit's cold resistance. Such solutions retain the heat given off by the

## Part III: Installing Your Wi-Fi Network

---

hardware itself. When temperatures go above 10 C, you should take the foam padding off the enclosure so that overheating will not occur.

You can construct a small cabinet to enclose the APs and their own enclosures that can be insulated as well. The cabinet can be placed at the base of tower. In this situation, the cabinet can incorporate small low power cooling fans and vents with flap valves that allow for all-season operation. Here the APs in their own metal boxes are simply mounted in the cabinet.

In extreme situations, an indoor location may be required for the APs. This could require longer antenna lines and power feeds if the tower is not adjacent to the building or shelter.

Certain manufactures supply APs in enclosures that already have heating and cooling features. These units are specified to operate from -30 C to +40 C and still maintain proper operation. They can be 3 to 10 times more expensive than off-the-shelf APs for home use. Prices are falling monthly; thus, more rugged equipment is becoming more viable for rural Wi-Fi use.

### Fireproofing

---

If the enclosure selected is made of plastic or resin material that has metal screen or film applied for EMI shielding, it must be fire retardant. This is especially true if you plan to mount the AP unit near flammable objects. Lightning can ignite the box if the materials are flammable.

### Corrosion Resistance

---

Enclosures and well as towers should made of galvanized steel or aluminum to reduce the rate of corrosion. Rust particles can easily get into equipment causing problems. Similarly, any mounting hardware that from time to time will be adjusted such as an antenna mount should be corrosion resistant, e.g., made of plated or stainless steel.

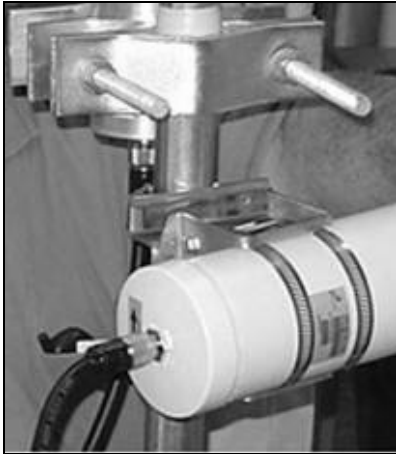
### Connectors

---

The connectors for power, RF, and local data ports (Ethernet and other for telemetry) need to be robust. See Photo 12-8. All such connectors exposed to the weather should be waterproofed to prevent moisture from getting into the connectors and causing poor electrical contacts and excessive RF loss.

### Photo 12-8: Rugged Antenna Connector

---



The usual way with connectors is to use corrosion resistant connectors and wrap the connectors with cable sealing tape, which is rubber-based tape that fuses to itself. You should check these connectors at least twice a year for any increase in loss as well as physical signs of corrosion.

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, you should take care in handling the cable connector to prevent excess stress on the mounted connector.

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

### Coaxial Cables

---

You will need coaxial cables to interconnect the 802.11b APs to mast-mounted external high-gain antennas. Such cables must be low loss and durable to take on widely varying weather. The LNR 400 coaxial cable that we selected for our own work exhibited both qualities. See Photo 12-9. Such cable is rated at a loss of 0.2 dB per metre.

Photo 12-9: LNR 400 Coax Cable

---



Less expensive cable such as *RG58* (1.0 dB/m loss) can be used for short runs under 1 to 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.

You should avoid cable not designed for UHF or microwave frequencies, since excessive loss will happen at Wi-Fi frequencies.

### Adding Lightning Protection

---

Because wireless equipment is typically located out of doors and has components located on towers and tall buildings, they are especially susceptible to damage from lightning. Therefore, it is important that a lightning protection system be designed and implemented at the same time you are designing and implementing the wireless system. Doing so will result in less down time and lower liability for people and property.

The use of lightning arrestors is mandatory for any towers or antenna structures mounted on buildings or stand-alone. You should ground the tower structure itself, along with the antenna to prevent damage to the antenna and equipment attached to it.

#### **Antenna Arrestors**

For our own work, we used an inline coaxial lightning arrestor unit. This prevents high voltage induced by the lightning strike from reaching the



## Part III: Installing Your Wi-Fi Network

---

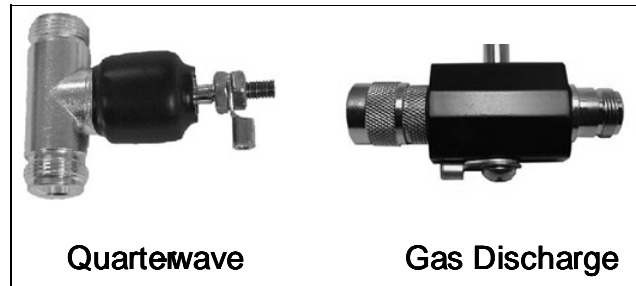
transmitter. The arrestor is grounded to the earth. Photo 12-10 shows the main types of inline arrestors.

**Antenna arrestors should not be the only protection in place since they will be inadequate to handle the discharge.**

---

Photo 12-10: Types of Lightning Arrestors

---



### ***Wooden Poles***

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

### ***Grounding Rods***

You should use grounding rods made of copper pipe or solid copper rods (more than 3 cm in diameter). Such rods should be 1.5 to 2 m in length. They need to be driven at least 1 m into the ground. 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.

### ***Grounding Cable***

For our own experiments, we used a 6# copper wire to link the tower and the coaxial lightning 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 is done to prevent any discharge between the antenna and tower itself. See Photo 12-11 and Photo 12-12.

## Part III: Installing Your Wi-Fi Network

---

Photo 12-11: Copper Grounding Cable Attached to Antenna

---

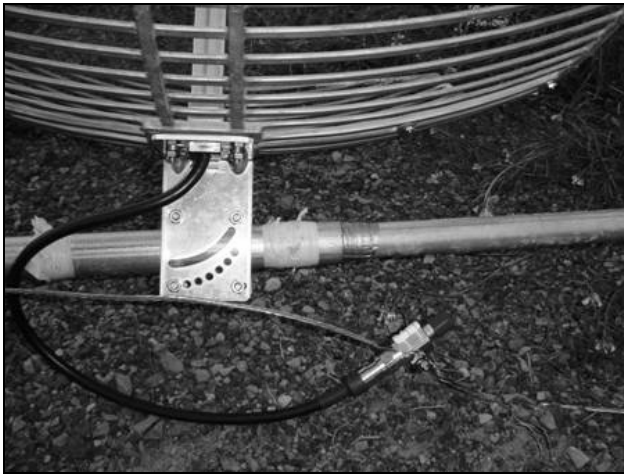
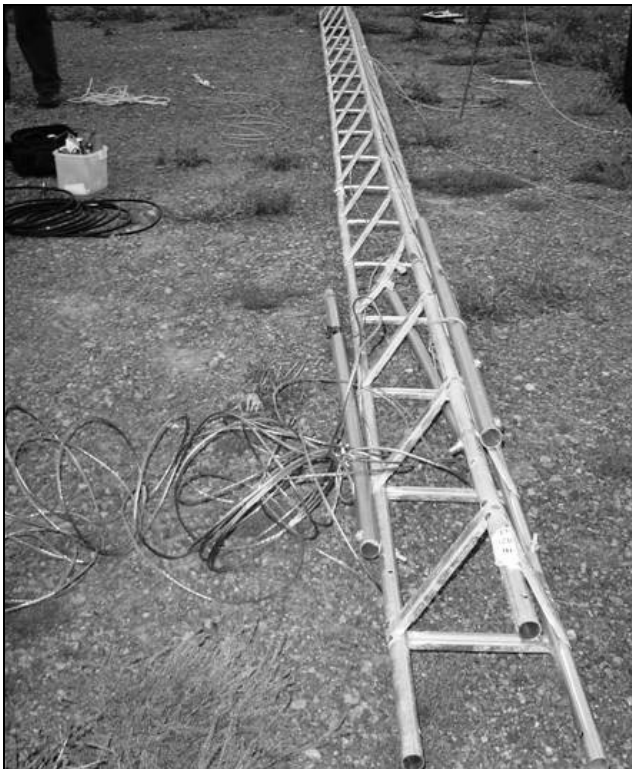


Photo 12-12: Thick Copper Grounding Cable

---



### Adding an Uninterruptible Power Supply

---

In addition to the system used to provide primary power for the AP, the use of an UPS can be of benefit to prevent brief power interruptions, surges, or short periods of under-voltage. This is particularly important when loading in new firmware into an AP, where a power glitch could result in the AP firmware memory being corrupted and unable to be reloaded.

The specifications of the UPS should match the power requirements of the node plus 100% as a rule of thumb. Thus if 10 Watts of power is required, the UPS should be rated at 20 Watts load. The typical time for off-the-shelf units is 15 minutes of power backup. For remote applications, this period should be doubled to 30 minutes.

### Improving RF Shielding

---

Most consumer Wi-Fi APs are designed to be used as standalone units. It is assumed in the design that there will be no other APs in close proximity and at most a limited number of client transceivers nearby. As a result, governments have waived commercial specifications for electromagnetic interference (EMI) emissions and susceptibility. Instead, more relaxed consumer EMI rules have been applied.

However, equipment configurations for rural/remote applications will have multiple APs, some in bridge mode, repeater, and AP. Thus, shielding solutions like those shown in Photo 12-6 and Photo 12-7 are required.

### Mounting Options

---

There are a number of options on where to place the AP hardware for your installation. Which one is best will depend greatly on whether the AP will be at an existing building or a stand-alone tower location.

#### ***Mounting Inside a Building***

Figure 12-1 shows this option.

In it, you should place the AP indoors in a ventilated area where temperatures stay below 35 C. It should be enclosed in a metal box and wall-mounted on a plywood board.

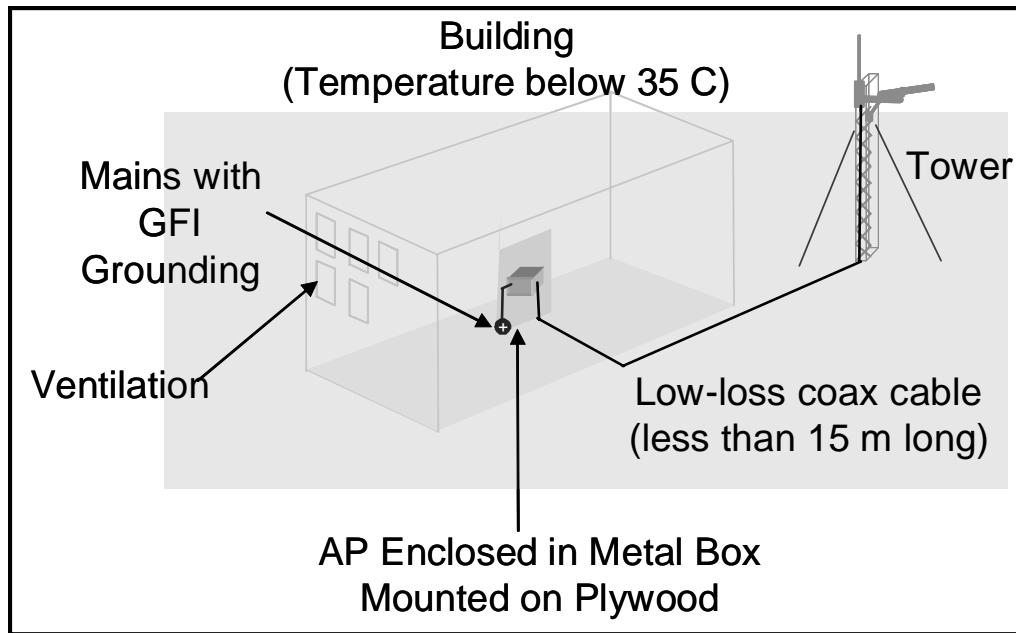
Coax cable runs to the outside antenna should be as short as possible (less than 15 meters of low-loss cable, 0.4 dB loss per metre). The coax cable to antenna connection must have a lightning arrestor, as described

## Part III: Installing Your Wi-Fi Network

earlier. Any Ethernet cable should be category 5 or 6, and runs must be less than 100 metres.

If power is provided by local mains, it must be on a ground-protected circuit (ground fault interrupter or GFI). You should ground the AP box to the building's electrical ground.

**Figure 12-1: Mounting in a Building**



### ***Mounting at the Tower Base***

Figure 12-2 shows this option.

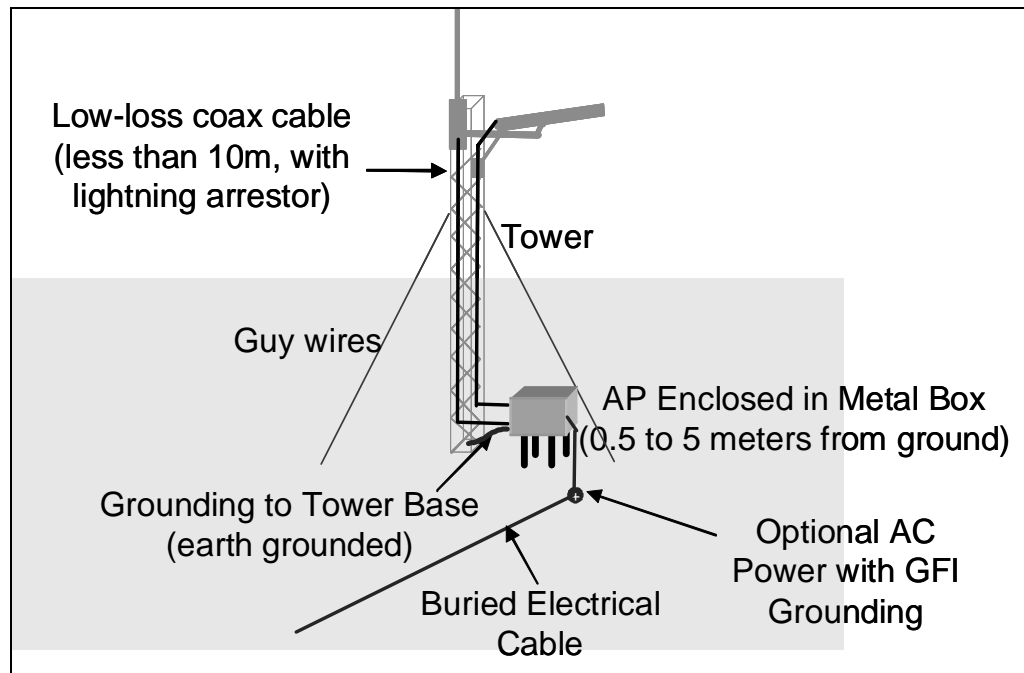
In it, the metal AP box is mounted 0.5 to 5 meters from ground for easier access. This reduces the weather exposure and is easier to get to. The box must be electrically grounded to the tower base, which is earth grounded. It can be mounted with metal strap brackets or by a similar method. It should be able to be easily removed or put back.

The coaxial cable should be of a low-loss type (AMR 400 or equivalent), and have a lightning arrestor. If the coaxial cable run from the AP will be over 10 meters, the AP should be placed higher up on the tower to keep RF losses minimized.

## Part III: Installing Your Wi-Fi Network

AC power, if available, should be on a GFI-protected circuit. The cable should be buried at least  $\frac{1}{4}$  of a metre below the surface.

Figure 12-2: Mounting Near the Tower Base



### ***Co-located with Other Packages in a Common Cabinet***

In this option, you use a common weather-resistant cabinet with ventilation slats. The cabinet should support three APs at least, with room for batteries or UPS. The cabinet should be mounted either on leg supports or on the tower, a minimum of 1.5 metres off the ground. If the cabinet is metallic, it should be also grounded to earth. A simple padlock can be used to secure the cabinet.

### ***Mounting on Top of Tower (Not Recommended)***

Many solutions for outdoor AP mounting place the package near the antenna at the top of a tower to minimize the RF power loss in the coaxial cable. Unless the tower is very short, such as a short tripod tower used on roofs, *this type of mounting should be avoided*. The reasons?

- In tall towers, the AP is difficult to mount as well as to repair. The tower either must be lowered or be climbed.

## Part III: Installing Your Wi-Fi Network

---

- It is susceptible to harsh weather conditions such as wind-driven rain.
- With multiple APs, the weight on the tower plus wind loading will require a heavier duty tower be utilized with additional guy wires.

### Antenna - Cable VSWR

---

In using standard coaxial cable (50 Ohm) rated for low loss at 2.5 GHz, you should take care in how the cable is terminated at the AP or client adapter card, as well as any intermediate connectors or connector adapters. The reason is 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 connectors have 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 lightning antenna strike. In the event that this occurs, replacement of the cable is required.

In our testing, we generally encountered minor VSWR, with the cable adapter not seating correctly. This caused a mismatch in *impedance* and thus lowering the transmit output power.

---

**However, we did encounter major impedance matching with one bridge unit, the D-link 900. It took us a very long time to discover the problem. The manufacturer subsequently fixed the problem and replaced the unit with another model, the 2100. The lesson we learned from this is not to assume that consumer units will work as advertised.**

---

# Part III: Installing Your Wi-Fi Network

## In this part...

**N**ow that you have all your equipment assembled and configured, it's time to go into the field and get things set up.

- Chapter 13 covers how to get your towers up safely.
- Chapter 14 helps you align the directional antenna on top of a local AP, so that it points back at the right angle.





# 13. Putting up Your Towers

Towers provide the essential antenna elevation to get over near field obstacles and allow the establishment of useful service areas. Three people can set up a 15-metre tower in less than an hour, complete with antennas and cabling. Standard carriage bolt hardware is required along with simple tools (wrenches, pliers, etc). See Photo 13-1.

Alternatively, you can use an existing mast or pole that is already available at the location for attaching antennas, as long as you are careful about the loading.

In this chapter, we will look at various types of towers and how to put them up safely.

**Suggested audience for this chapter:**



## Part III: Installing Your Wi-Fi Network

---



Important terms in this chapter include:

Bearing	A surveying term used to designate direction. Used in wireless networks to designate the direction an antenna is pointing.
Gauge	The width of a wire
Guy wire	A wire used to attach a tower to a guy anchor and the ground
Polarization	<p>Radio waves exhibit the property of polarization, which is the plane of their electrical fields.</p> <p>Polarization is typically referred to as being horizontal or vertical, but the actual polarization can be at any angle. Circular polarization is also possible. Receiving a horizontally polarized signal with an antenna oriented to be vertically polarized, or vice versa, will reduce the amount of signal received.</p>
Sectional tower	A tower which consists of various sections
Thimble	A device to prevent crimping of guy wire
Turnbuckle	A screw fitting for adjusting the tension of shrouds and stays

---

## Towers versus Masts or Poles

---

*Sectional towers* typically come in 3-metre sections that are simply bolted together. The top of the tower is constructed so that a steel mast pipe can be mounted along with any extra items such as an antenna rotator. Such towers have been designed for rural television antenna use. They can easily support a number of typical 2.5 GHz antennas. With guy wires, this type of tower can be used up to 26 m. At lower heights, the tower can be supported by a building using a special mounting bracket, eliminating the need for guy wires. Such towers are very durable. They are rated at winds of over 160 kph.

Masts or poles that are already available at the location 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 does not sway in moderate to heavy winds. Excessive antenna movement of over 10 degrees will affect the link performance due to misalignment of the antenna's signals.

---

## Tower Location and Placement

---

Several factors determine the general area in which to locate a tower, the most important of which are reach and coverage.

Now that you know the general area where to locate the tower, you should consider several additional factors to determine the best *specific* location.

- Tower height elevation above average terrain

The tower and its antenna must be located so they can be higher than any obstacles (buildings, trees, or mounds) that interfere with the line-of-site view along the path between the towers that are to communicate with each other (point-to-point).

- Omnidirectional coverage

In the case of a tower intended to cover most of a village using an omnidirectional antenna, you should select the location so that the tower's height can clear most of the obstacles surrounding the tower. Single trees or poles are not a concern unless they are very close, e.g., closer than 2 m.

- Tower base and structural or guy wire supports

The tower should be located at a spot so that its base can be placed on a concrete pad or on partially buried cement blocks. The spot should

## Part III: Installing Your Wi-Fi Network

---

also have sufficient room for bracing the tower. This is very important; you must find adequate anchoring. You should look for two bracing options:

- Using a building wall
- Using guy wires.

### Safety First

---



Once you have selected a suitable tower location, you should consider several safety factors before you raise the tower:

- **Very Important!** Keep away from any close-by power lines that can be in the way when raising the tower or if it falls.
- Do not place towers near trees that can:
  - Shadow the tower, interfering with the signal
  - Sway into the tower during wind storms
  - Eventually grow to shadow the tower.
- Do not climb the tower unless it is specifically rated to support a person's weight on the struts of the tower.
- Do not place the tower on the approach to nearby runways or helicopter landing areas. If it must be there, the tower must be painted with red and white stripes to warn aircraft. A beacon light may also be necessary, depending on local regulations for tower height.

### Grounding and Lightning Protection

---

→ We have already covered this subject in the section “Adding Lightning Protection” of Chapter 12. However, it is such a crucial safety subject that it cannot harm to repeat the basics here.

Antennas, especially on the top of towers in open areas, are an open invitation for lightening to strike (more than once!). It is a matter of when the strike will occur and not if.



The antenna and tower must be able to absorb a direct lightning strike without passing the discharge onto the attached radio equipment. If this discharge is not diverted or absorbed, equipment is usually destroyed.

### Cable Runs and Equipment Placement

---

The cable between the antenna and the radio transceivers must be as short as possible to ensure that cable losses between the antenna and

transceivers do not become too large. Some loss is acceptable, but care should be taken.

There are several options for placing the electronic equipment relative to the tower and antennas. It can be:

- Housed against the weather in a separate building, with the tower located immediately adjacent to the building  
Unless immediately adjacent to the tower, coax cable runs may end up being too long. You should avoid runs over 15 meters unless you use amplifiers in your Wi-Fi system.
- On the tower near the antenna  
This option requires the tower be in a location where guy wires can be used to stabilize the tower with a top-heavy portion. This provides the best RF performance. However, equipment costs can be three to four times as high to make the equipment reliable against weather.
- At the base of the tower, with a length of coax feeding the antenna(s) on the tower  
Here, you should find a location that has some access security to prevent tampering with the equipment. *This approach is inexpensive and provides a good compromise between minimal cable losses and costs.*
- Housed in a cabinet or in its own separate enclosure  
This placement option is a bit more costly. In a cabinet, the equipment can be in less expensive enclosures as long as the cabinet provides some basic environmental protection.
- On or at the base of the tower or inside a building, with a roof-mounted tripod or short tower  
This is again a reasonable compromise, by reducing coax feed lengths and tower size if the building provides some height advantage.

### Making it Sturdy

---

Most inexpensive towers require guy wires or need to be attached to the side of a building to prevent them from falling over. The tower bases must also be staked using 3 cm by 1 metre galvanized steel drive stakes, or bolted to a cement-mounted bracket on the ground.

A viable solution for both the end user's tower and the main AP tower is the use of sectional towers, such as typically in use for TV antennas in rural areas. You can purchase a complete tower mounting kit for building

## Part III: Installing Your Wi-Fi Network

mount or guy wire supported towers. These towers can be over 20 meters in height depending on the support system. As a rule, any bracketed tower will require guy wires if it is higher than 6.5 meters from where it is attached to the building.

On tall towers over 12 metres of unsupported section, the guy wires should be placed at half the total height of the tower or halfway between a supporting bracket to the top of the tower as well as at the top of the tower.

For towers of 12 metres or lower, guy wire only at the top of the tower will be required. This is just a rule of thumb. If you are in area where the tower will be exposed to high winds, a second set of guy wires at the half the tower height should be used.

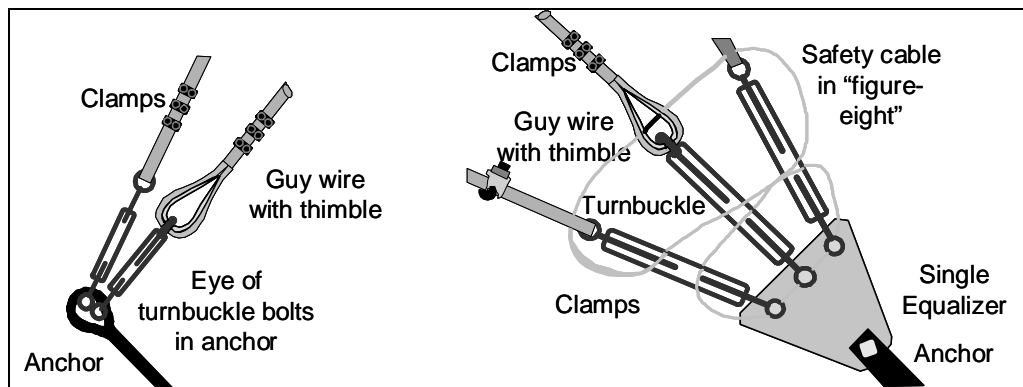
The anchor points of the guy wires from the base of the tower should be 75% of the tower's height again as a rule of thumb. Closer anchors (50% distance) require that more guy wires be placed around the tower, like 6 for example every 30 degrees. It is done this way on ships.

The wires have to be placed at 120-degree intervals (3 cables) or at 90-degree intervals (4 cables) around the tower. A guy wire ring or bracket is used on the tower to attach the wire loops to the tower.

Figure 13-1 shows different approaches for anchoring the guy wires to the ground. This diagram and the one in Figure 13-3 below are adapted from similar diagrams for amateur radio at the web URL:

<http://www.astrosurf.com/lombry/qs1-tower-assembly/5.htm>

Figure 13-1: Guy Wire Anchoring Approaches



Some of the parts used in these anchoring solutions are:

- Cable clamps for terminating the guy wires
- Thimbles to prevent crimping of guy wire and preformed terminations  
They are one size larger than the guy wire when terminated with cable clamps, or two sizes larger than the wire when terminated with guy grips.
- Turnbuckles used to tension guy wires  
They come in two formats: “eye and eye” or “eye and jaw”.

Figure 13-2 shows these parts.

Figure 13-2: Anchoring Parts

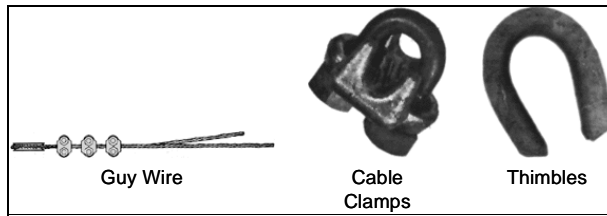


Figure constructed from photos at:

<http://www.texastowers.com/mischard.htm>

The guy wires' thickness should be at least 4.7 mm. These wires should be made of twisted stands of flexible extra high strength steel wire. They are designed to take 2 tonnes or more tensile force. See Photo 13-1.

Photo 13-1: Guy Wires and Turnbuckle



Photo 13-2 shows a very simple approach to connecting guy wires to the tower. However, there are much better ways to secure the tower, as

## Part III: Installing Your Wi-Fi Network

---

shown in Figure 13-3 below. One alternative (A) uses a building bracket. The other three alternatives show the use of guy wires only.

---

**Photo 13-2: Simple Attachment of Guy Wires to Tower**

---

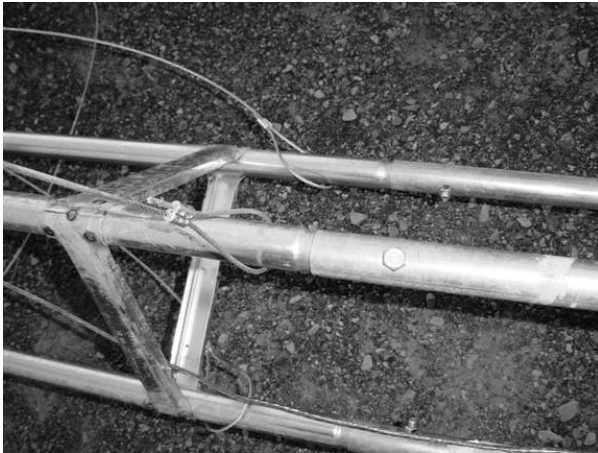
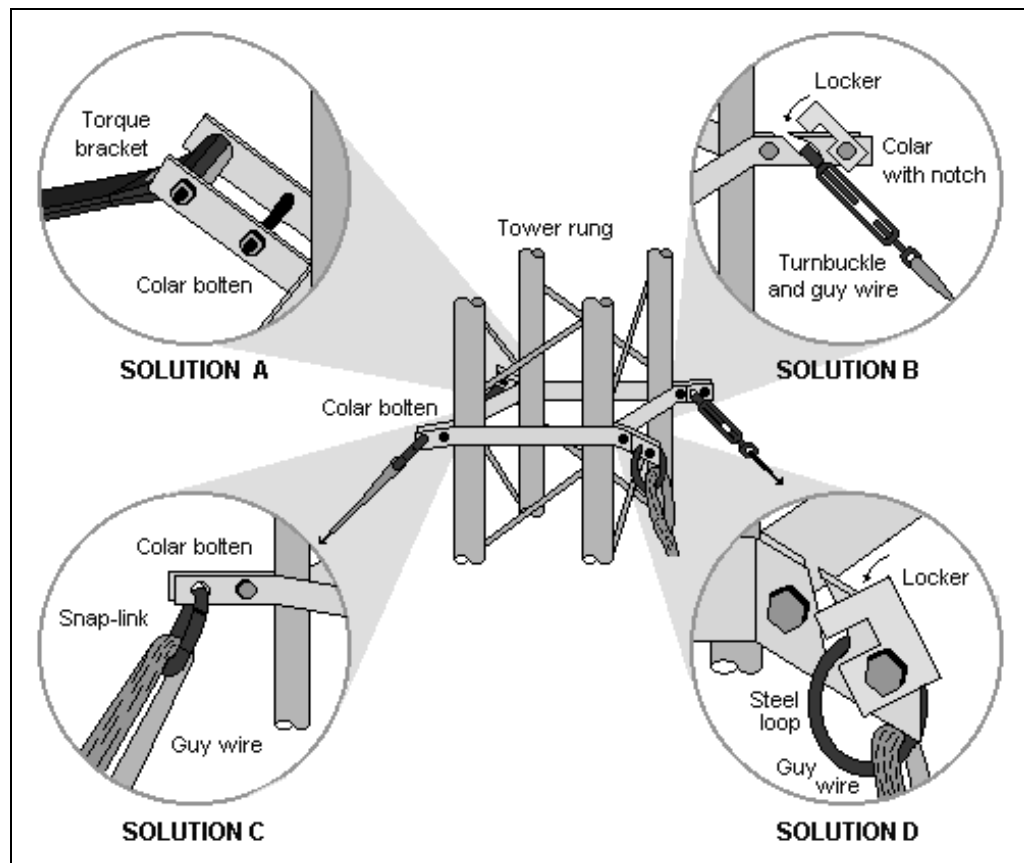




Figure 13-3: More Secure Tower Connection Approaches



## Raising the Tower

### Major Steps

The job is divided in several steps:

- Assembling the antenna on the ground
- Preparing the area to raise the antenna and accessories
- Measuring out the location of the guy wire anchors and installing them.
- Installing the guy wires and any necessary supporting hardware to the tower
- Placing the mast pipe onto the tower and adjusting its length.
- Installing the antenna on the mast pipe and making sure it is properly oriented for polarization when the antenna is in position. Some anten-

## Part III: Installing Your Wi-Fi Network

---

nas have arrows on them to guide you in setting the polarization correctly; see Photo 13-3.

- Connecting and tying down of the cables (coax) and lightning arresting cables.
- Raising the assembled tower and antenna.

The tower is positioned to give coarse alignment (*bearing*) for the antenna, and hooking and adjusting tension of the guy wires to the ground anchors.

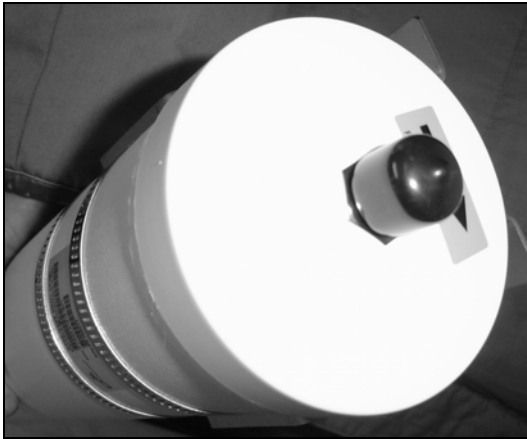
- Fine antenna bearing adjustment of the antenna using RF testing system to get peak RF levels from the distance station to be linked.

For an omnidirectional antenna, except for vertical alignment, there is no bearing adjustment needed.

---

### Photo 13-3: Arrow on Antenna to Help Set Polarization

---



Read the manufacturer's instructions carefully on how to use such arrows to help you set the polarization you want.

#### ***Details of Grounding***



- You should install an electrical ground at or near where the tower will be placed.

The ground consists of a copper rod that is approximately 1.6 cm in diameter and 3 metres long. You should drive it all the way in. The rod has a cable clamp that can allow a 6 *gauge* copper cable to connect to it.

- A heavy copper cable (6 gauge) should be used to connect the tower and the antenna lightning arrestor mounted in-line with the coaxial cable feeding the antenna.

### ***Details of Raising the Tower***

The raising of a tower is a community project. At least four people are needed for the job if the tower is over 8 meters. The order of business is:

- The area where the antenna tower is to be located must be prepared to mount the base and guy wires.



You should anchor the base of the tower so it will not slip on the ground as it is raised. You can accomplish this with ground pegs against which the tower legs push. You can also use large rocks. A person must be also at the base of the tower to ensure it does not slip during the raising.

- The guy wires that are attached to the tower should be laid out on the ground roughly in the position they will be when the tower is raised. The tension-adjusting turnbuckles on the guy wires should be extended fully to allow the guy wires to be hooked onto their anchors once the tower is raised.

- A strong rope (approximately 1 cm diameter polypropylene) should be tied to the antenna midway up the tower.

This rope will be pulled by several people to help raise the tower.

- A person will now lift the tower near the antenna and start lifting and walking toward the base, much the same way you would raise a standard ladder.

The person on the rope is also pulling the mid part section of the tower at the same time, to help raise the tower while keeping the alignment (bearing).

- To help in “walking up” (raising) the tower, a person can use a strong pole to further push on the tower as it goes out of their reach.

The push is needed sometimes if the tower is top heavy.

- Once the tower has been raised, the guy wires require adjusting to prevent the tower from toppling over or swaying in the wind.

This requires each guy wire be attached to the ground anchors and have its tension adjusted by using the turnbuckle. The guy wires must be adjusted so that the tension is the about the same on each cable to keep the tower straight. Too much tension can result in the tower being twisted or flexed by the cables pulling too much. The ideal tension will have the guy wires adjusted just enough to keep the tower straight.

## Part III: Installing Your Wi-Fi Network

---

- Once the tower is up, connect the RF coaxial cable from the radio to the RF test system to do the final antenna adjustment.

Photo 13-4 shows a tower prior to raising. The raised tower can be seen in Photo 13-5.

---

### Photo 13-4: Tower Ready for Raising

---



Enclosure containing Wi-Fi equipment is sitting to the side of the tower.

---

### Photo 13-5: View up the Raised Tower

---



## Final Tower Alignment

---

When the tower is installed, you must take care to make sure it is straight and level. This is required to properly align the directional antennas with respect to the far end station.



When placing the tower, ensure that the antenna is pointed at the correct area. Once the tower is in place, you can adjust the antenna. However, if you have not made provision for rotating the antenna from the ground, *someone will have to climb the tower to rotate it for alignment.*



# 14. Aligning Your Antennas

You have to be very methodical and patient to align antennas over point-to-point and point-to-multipoint links, so as to get the best possible signal levels and therefore throughput. Professional equipment and commercial test software are needed to do this completely successfully in all circumstances. However, if your budget is very limited, it is possible to achieve some success with the techniques we have adapted for Wi-Fi from other types of wireless systems. These techniques are described in this chapter.

**Suggested audience for this chapter:**



## Part III: Installing Your Wi-Fi Network

---



Important terms in this chapter include:

Active scanning	Any method of detecting a Wi-Fi signal in which the test equipment interrogates the APs.
Antenna tilt	The angle an antenna makes relative to the horizontal. Tilt could be positive (up) or negative (down).
Continuous Wave (CW) Transmitter	A transmitter that outputs a sustained or oscillatory wave whose successive oscillations are, under steady-state conditions, identical.
Effective Radiated Power (ERP)	The amount of power actually radiated by a transmitter and antenna combination (the applied power multiplied by the efficiency of the antenna).
Link budget	A calculation involving the gain and loss factors associated with the antennas, transmitters, transmission lines, and propagation environment.
Height Above Ground level (AGL)	Used for specifying how high a tower or other object is above its immediate surroundings.
Passive scanning	Any method of detecting a Wi-Fi signal in which the test equipment simply accepts the signal without interrogating it or responding to it.
RF	Radio Frequency
Spectrum analyzer	An instrument that displays the frequency spectrum of an input signal
VSWR	Voltage Standing Wave Ratio. A measurement of mismatch in a circuit, cable, waveguide, or antenna system.

---

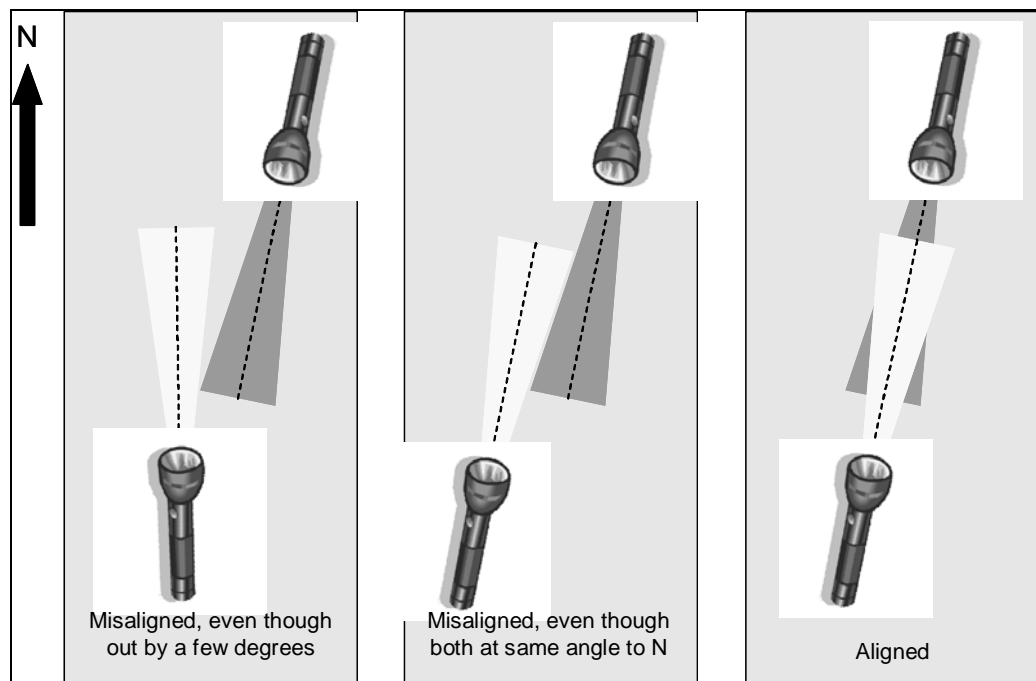


## Why Align Antennas?

There is no need to align an omnidirectional antenna on an AP, other than to ensure that it points upwards, which is easy to do. However, highly directional antennas for backhaul need to be aligned accurately. The beamwidths of such antennas are so small that if you are out by several degrees, the received signal strength will be down considerably. You might not even be able to detect any signal at all!

The reason why this occurs is shown by analogy in Figure 14-1. There, you see two flashlights pointed roughly at each other. They represent two highly directional antennas; one might be at the POP and the other an AP in the field. Even though the width of the flashlight beams is not that small, say,  $15^\circ$ , the tolerance for misalignment is much smaller. Even if they point at *exactly* the same angle relative to North, they can completely miss one another!

Figure 14-1: Explaining (Mis)alignment of Directional Antennas



### Equipment for Alignment

---

#### ***Spectrum Generators and Analyzers***

One possible solution is to use a combination of a signal generator on one end of the link and a signal analyzer on the other. Photo 14-1 shows such a signal analyzer.

---

#### **Photo 14-1: Highly Flexible Professional Signal Analyzer for Wi-Fi**

---



Manufacturer: Tektronix

Specifications:

Analyzer: WCA300 series  
Software: WCA11G Signal Analysis  
Software for IEEE 802.11a, b, and g

Such a combination has several serious drawbacks for inexpensive rural Wi-Fi networks:

- It is very expensive.  
One such piece of equipment can cost tens of thousands of dollars. However, if you already have the equipment, this is not a factor.
- It is not specifically designed for antenna alignment.
- It has such a wide range of capabilities that it can be difficult to use.

#### ***Wi-Fi Antenna Alignment Tools***

Fortunately, specific equipment for aligning Wi-Fi antennas has just appeared on the market; see Photo 14-2. This equipment costs about \$800 US.

If you have the money, such equipment is probably the best approach to use, because it is the fastest way to get the antennas aligned.

## Chapter Error! Reference source not found.: Error! Reference source not found.

### Photo 14-2: Professional Antenna Alignment Kit for Wi-Fi



Manufacturer: Tektronix

Specifications:

Center Frequency: 2445 MHz

TX Output Power: 500 mW

RX Sensitivity: -100 dB

Gain Adjustable Range: 50 dB

Battery Powered RX

Connector: N-type Female

Operating Temp: -30 to 70 deg C

#### ***Using a Home-Brew Test Setup***

This is the least expensive way. However, the antenna alignment can take longer than with tools like that shown in Photo 14-2.

### Preparing for Initial Antenna Alignment

#### ***Prerequisites***

In previous chapters, we covered the criteria for site locations, antenna selection, use of amplifiers, and tower heights. The use of these criteria resolves most of the major issues in terms of overcoming major obstacles, path losses, *link budgets*, best locations to achieve reasonable line of sight coverage to most users, and proximity to supporting systems such as power.

Given this has been done with some care, you must now optimize the antennas to ensure adequate signal levels. The main variables that you can now adjust to ensure adequate receive levels are the antenna clearance and adjustment of the antenna orientation.

However, before you do the alignment, there are some preparatory things to do.

## Part III: Installing Your Wi-Fi Network

---

### **Antenna Isolation**

On towers using multiple antennas, you should take care to ensure that the antennas do not introduce strong signals into co-mounted antennas. Isolation is achieved by orienting 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 interference 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 at least 0.5 metres.
- With back-to-back directional antennas, a wire screen should be used between the repeater's antennas back to prevent excessive interference from antenna back lobes.

### **RF Setup Procedures**

All antenna alignment should be done in fair weather conditions. Excessive rain and any other precipitation such as fog or heavy mist must not be present during the alignment procedure.

---

#### Procedure 14-1: Setting up the RF for Antenna Alignment

---

Step	Step Description	Notes	Done?
1. Set the AP unit in the correct mode.	AP <i>Infrastructure mode</i> should be used. The beacon interval should be set at 100ms.	This ensures that the signal is seen by the receiver quickly when it is in scanning mode.	<input type="checkbox"/> Yes <input type="checkbox"/> No
2. Set the AP units to use only an external antenna.	The antenna should be 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.	<input type="checkbox"/> Yes <input type="checkbox"/> No

## Chapter Error! Reference source not found.: Error! Reference source not found.

Step	Step Description	Notes	Done?
3.	Set the power settings of the APs to the maximum level available.	Typically, this is +17 dBm or 52 mW.	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.	Do a site survey for any other APs that may be operating nearby.		<input type="checkbox"/> Yes <input type="checkbox"/> No
5.	Select a channel that is as far as possible from those used by any other APs seen.	This helps avoid interference.	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.	Determine the distance between the near and far antenna sites.		<input type="checkbox"/> Yes <input type="checkbox"/> No
7.	Look up the expected path loss from the supplied tables or spreadsheet.	You will need to know the tower heights and type of terrain.	<input type="checkbox"/> Yes <input type="checkbox"/> No
8.	Do a path analysis to ensure there are no major obstructions blocking the antenna line of sight to the far end.		<input type="checkbox"/> Yes <input type="checkbox"/> No

## Part III: Installing Your Wi-Fi Network

Step	Step Description	Notes	Done?
9.	If there is, consider moving the tower or raising the antenna such that the obstacle can be adequately cleared	0.6F1 if possible.  With more distance objects (200 or more metres away), 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 than what a clear path will deliver. This can be acceptable as long as the received level is +10 dB above -87 dBm. Otherwise, the antenna must be raised to have the radio path raised until a higher level is achieved.	<input type="checkbox"/> Yes <input type="checkbox"/> No

### Doing the Initial Antenna Alignment

You should verify the path to the far-end antenna to ensure that as much as possible you can see a line of sight, i.e., a radio line of sight respecting the first Fresnel zone clearance of  $0.6F1$  for the tower heights selected. Procedure 14-2 documents how to do this.

#### Procedure 14-2: Initial Coarse Antenna Alignment

Step	Step Description	Notes	Done?	
1.	Study a map	Determine from the map the AGL of the antennas with the proposed tower heights to see that major obstacles are cleared.	You will need topographic maps (1:50,000 or better) and visual inspection from aerial photos or inspecting the radio right-of-way from the ground.	<input type="checkbox"/> Yes <input type="checkbox"/> No

## Chapter Error! Reference source not found.: Error! Reference source not found.

Step	Step Description	Notes	Done?
2: Inspect the optical path	<p>Spot the location of the far-end antenna on the horizon by using a telescope plus a:</p> <ul style="list-style-type: none"> <li>• strobe light,</li> <li>• bright flashlight, or</li> <li>• signalling mirror.</li> </ul> <p>If you cannot spot the location, the radio link is grazing obstacles or is below the optical horizon. This will result in severe signal loss. (See urban signal strengths predictions for non-line-of-sight paths in spreadsheet.)</p>	<p>You cannot always achieve line of sight. However, the path can still be viable with diffraction as long as the path distance is shortened to make up for the graze loss.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
3: Adjust the tower height	<p>If you cannot see the line of sight because of obstacles on the path such as buildings or tree ridges, an increased tower height or change in position is required for best performance.</p>	<p>If signal strengths are high enough, losses can be tolerated if the path is grazing on short paths.</p> <p>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.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
4: Do a visual bearing alignment if possible	<p>If you can see the far end antenna location, the bearing of the antenna can be set accurately.</p>		<input type="checkbox"/> Yes <input type="checkbox"/> No

## Part III: Installing Your Wi-Fi Network

Step	Step Description	Notes	Done?
5. Otherwise, do a bearing alignment based on the reciprocal bearing angle of the far-end antenna.		For example, given a far-end antenna with 260 degrees bearing, the reciprocal angle is $260 - 180 = 80$ degrees.	
6: Set the antenna tilt at 0 degrees			<input type="checkbox"/> Yes <input type="checkbox"/> No
7: Set the antenna polarization to the same orientation as the far-end antenna	Rotate the antenna about its horizontal axis.	Signal strength is often maximized if the two antennas have the same polarization. However, the polarization angle can rotate between the two antennas due to obstacles.	<input type="checkbox"/> Yes <input type="checkbox"/> No
8: Do a direct RF alignment coarse bearing	If visibility is too poor (less than 1-2 km) due to weather or pollution, have the far-end antenna send a test signal that can be searched for at the local end of the link.	<p>This method can work as long as there is a reasonable estimate of antenna height, and bearing is determined by doing the initial site analysis from map and loss charts information.</p> <p>Use the passive RF measuring technique 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 antenna's orientation will be.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No



## Chapter Error! Reference source not found.: Error! Reference source not found.

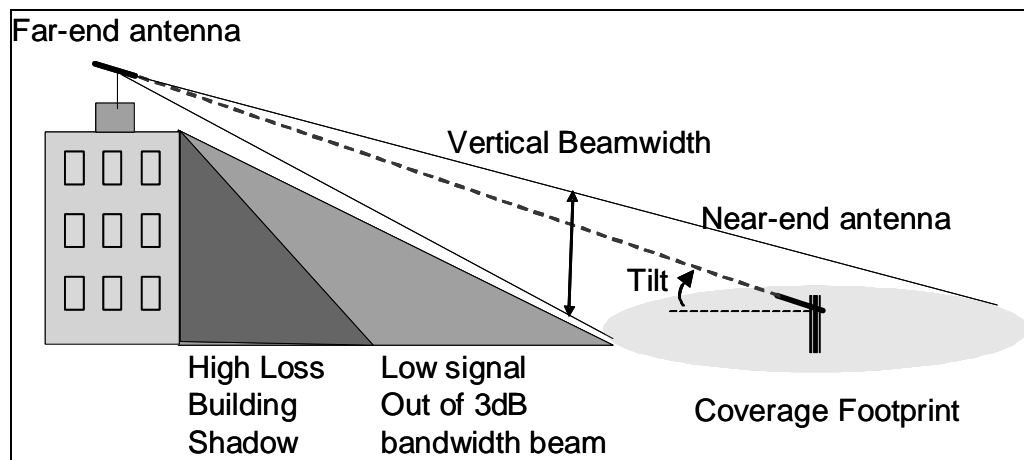
Step	Step Description	Notes	Done?
------	------------------	-------	-------

In addition, higher power should be used if possible (1 Watt limit for Effective Radiated Power, or ERP).

### Antenna Tilt

If you correctly followed Procedure 14-2, then your near-end antenna should have zero tilt, i.e., be parallel to the ground. Why do you have to change this? As you can see from Figure 14-2, the far-end antenna and the near-end antenna can be at different heights above the ground. When that happens, you should tilt both so that they meet each other along the line between them. One will be tilted down, the other up.

Figure 14-2: Antenna Tilt Versus Path Reach



### Different Approaches to Fine Antenna Adjustments

You can align antennas either by using a Continuous Wave (CW) signal with a spectrum analyzer or the 802.11 transceivers themselves. We cover both approaches below.

### ***Direct RF Measurement Approach***

The classical way to measure RF field strength is to use a CW source transmitter such as a signal generator and an RF field strength meter, or even better a sensitive spectrum analyzer. This classic method 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 used. It can allow antenna setup 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.

Direct measurement techniques 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.

### ***802.11 RF Approach***

In our own fieldwork, we tried to put ourselves in the position of someone who has a very limited budget. In particular, we assumed that you do not have access to the tools a professional would use for this type of job. Instead, we tried shareware tools running on a notebook to do the RF level monitoring for antenna alignment.

This approach generally works well, although it can be slow compared to the use of professional tools. However, there are a number of caveats for the type of software used and the specific tasks it will be applied to. We observed several behaviours that could lead to misinterpretation of the performance of links as well as difficulty in determining if signals are present or not.

If 802.11 RF software test tools are used, we recommend passive mode for adjusting the antennas accurately.

## **Fine Adjustment of the Antenna Orientation and Tilt**

---

You should expect that tilt and polarization will require minimal readjustment. By contrast, as we explained at the beginning of this chapter, the antenna bearing can be very significant, with a few degrees change mak-

## Chapter Error! Reference source not found.: Error! Reference source not found.

---

ing a profound difference in signal level. Here, you should do slight shifts above and below the coarse bearing adjustment to see if there is any improvement.

Typical ranges of adjustment are:

- Tilt: +/- 2 to 3°
- Bearing: +/- 10°
- Polarization alignment: +/- 30°.

Procedure 14-3 gives the fine-tuning procedure.

---

### Procedure 14-3: Fine-tuning the Antenna Alignment

---

Step	Step Description	Notes	Done?
1. Finely align the antenna bearing	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) off the coarse alignment bearing used. Note if the signal is increasing or decreasing and see if the level peaks. If you cannot find a peak, return to the original bearing and now go to the left. Set the antenna bearing for the best level.		<input type="checkbox"/> Yes <input type="checkbox"/> No

## Part III: Installing Your Wi-Fi Network

Step	Step Description	Notes	Done?
2.	If there is no signal and the initial bearing adjustment appears way off, consider widening the bearing swing.	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.	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.	Adjust the antenna tilt	Adjust the antenna tilt up 0.5 degrees then down 0.5 degrees. Note any peaks in signal level. Again, set the antenna for maximum level.	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.	Fine tune the polarization.	Polarization should be changed +/- a few degrees to see if there is a signal peak observed.	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.	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. You will observe the best signal strength when the antennas are exactly in centerline with each other, as shown in Figure 14-1.	<input type="checkbox"/> Yes <input type="checkbox"/> No

### Final Steps

You need to put each AP 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:

- Set both APs to wireless bridge mode.

## Chapter **Error! Reference source not found.:** **Error! Reference source not found.**

---

- Enter the MAC number of the far end AP into the configuration information of the local AP. Similarly, enter the MAC number of the local AP in the far-end AP configuration window.
- The two APs should be passing layer 2 traffic or administrative messaging.
- Once the bridge is working, connect the bridge AP to the omnidirectional AP to provide Internet coverage for remote users.



# **Part V: Appendices**

# In This Part...

You will find further reference material like acronyms, technical terms, references, etc.



# Appendix A:

## Acronyms

All acronyms used in the Cookbook are defined here. We have also included a variety of other acronyms that you are likely to encounter in general reading in this area of Wi-Fi networks.

**Table A-1: Acronyms**

Acronym	Meaning	Definition	Notes
AC	Alternating Current		See DC
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).	
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		

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Acronym	Meaning	Definition	Notes
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, power, gain, loss, or frequency in logarithmic form against a reference.	Typical references include Volts, Watts, or Hz. Decibels are calculated using the expression: $dB = 10 \cdot \log(x/y)$ .
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.	
DoS	Denial of Service	A form of network attack in which a network is flooded with traffic. The system cannot then respond normally, so service is curtailed or denied.	This is a favourite technique of network saboteurs.
DRMASS	Digital Radio Multiple Access Subscriber System		
DSL	Digital Subscriber Line	A means of accessing the Internet at very high speed using standard phone lines.	

Acronym	Meaning	Definition	Notes
EHAAT	Effective Height Above Average Terrain		One of the means used to characterize an antenna's height.
EMI	Electromagnetic interference	The interference in signal transmission or reception caused by the radiation of electrical and magnetic fields.	
ERP	Effective Radiated Power	The amount of power actually radiated by a transmitter and antenna combination (the applied power multiplied by the efficiency of the antenna).	
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 orbit and 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 measurement (one hertz = one cycle per second).	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Acronym	Meaning	Definition	Notes
IC	Industry Canada		A Canadian Government department.
IEEE	Institute of Electrical and Electronics Engineers	A standards-setting body for North America.	
IP	Internet Protocol	A set of instructions defining how information is handled as it travels between systems across the 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	Companies or organizations that provide access to the Internet.	
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		
LMDS	Local Multipoint Distribution Service	Broadband wireless point-to-multipoint communication system in the 28 GHz band.	
LOS	Line of Sight	A description of an unobstructed radio path or link between the transmitting and receiving antennas of a communications system.	The opposite is Non-Line of Sight (NLOS)
LOS	Loss of Signal		

Acronym	Meaning	Definition	Notes
MAC	Media Access Control	The unique physical address of each device's network interface card.	
MMDS	Multichannel Multipoint Distribution Service		
MPPT	Maximum Power Point Tracking		Used in solar energy to increase efficiency of power collection.
MTBF	Mean Time Between Failure		
NAT	Network Address Translation		NAT devices translate IP addresses so that 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	North American Manufacturer's Association		
NOC	Network Operations Centre	A facility or organization responsible for maintaining, monitoring, and troubleshooting a network infrastructure.	
OAM	Operations, Administration and Management		
PC	Personal Computer		
PCI	Peripheral Component Interconnect		The main bus interconnection in PCs.

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Acronym	Meaning	Definition	Notes
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	Any frequency within the electromagnetic spectrum normally associated with radio wave propagation.	
RIP	Routing Information Protocol	A standard mechanism for exchanging routes (paths) between routers.	
RSSI	Received Signal Strength Indicator	A number in the range 0 to 255 that indicates the relative strength of a Wi-Fi signal	
RTS	Request to Send	A signal from a remote receiver to a transmitter for data to be sent to that receiver.	

Acronym	Meaning	Definition	Notes
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 levels 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 cryptographically strong replacement for the UNIX utilities rlogin, telnet, ftp, and other programs.	Protects against "spoofing", man in the middle attacks, and packet sniffing.
SSID	Service set identifier	A unique identifier that Wi-Fi stations must use to be able to communicate with an access point.	The SSID can be any alphanumeric entry up to a maximum of 32 characters.
S/I	Signal to Interference ratio		
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 called WEP2.

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Acronym	Meaning	Definition	Notes
UPS	Uninterruptible Power Supply	A battery backed-up 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 (LAN)		Can be used to segregate traffic on different sub-LANs of a Wi-Fi network, which improves performance and ease of network management.
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	A means of establishing secure communication channels on the Internet using various forms of encryption.	
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 traveling waves.	VSWR can be used as a measure of impedance mismatch between the transmission line and its load.



Acronym	Meaning	Definition	Notes
WAN	Wide Area Network	A network of computers and interconnected LANs typically spread out over a large area.	
WEP	Wired Equivalent Privacy	A security protocol for wireless local area networks.	WEP was intended to provide the same level of security as that of a wired LAN. However, it has been found that WEP is not as secure as once believed. It does not offer end-to-end security.
Wi-Fi	Wireless Fidelity	Trademarked by the Wireless Ethernet Compatibility Alliance. It stands for the IEEE 802.11 standard, which provides a flexible wireless local area network (WLAN) for mobile devices.	We also use the term for WWAN services.
WLAN	Wireless Local Area Networks	Local area networks (LANs) that transmit and receive data over the air, usually in the unlicensed sector of the spectrum, using either radio or infrared technologies, providing users with both access and mobility.	
WPA	Wi-Fi Protected Access	The successor to WEP.	Considerably more secure.
WWAN	Wireless Wide Area Network	Wireless networks that cover a large geographic area.	



# Appendix B:

## Technical Terminology

All jargon used in the Cookbook are defined here. We have also included a variety of other technical terms which you are likely to encounter in general reading in this area of Wi-Fi networks.

**Table B-1: Technical Term Definitions and Notes**

Term	Definition	Notes
100BaseT	100 Mb/s baseband data transmission over twisted-pair copper wire.	There is also 10BaseT and 1000BaseT.
24/7	24 hours a day, 7 days a week.	Used to indicate a system this 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 Mb/s.
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 Mb/s.
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 Mb/s.
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.

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
Addressing	A mechanism for identifying the address of a called endpoint in terms of the network, such as an IP address.	
Amplifier	A device for converting an input signal (usually low level) into a larger version of itself.	Amplifiers increase both the desired 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 more than one antenna 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 tilt	The angle of an antenna relative to the horizontal.	Tilt could be positive (up) or negative (down).
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.	
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 its 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).	

Term	Definition	Notes
Baud rate	The speed at which data is transmitted.	
Balun	a device that adapts one cabling type to another, including physical layout, impedance and connecting balanced to unbalanced cables.	
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 (b/s) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).
Beacon	A wireless LAN packet that signals the availability and presence of the wireless device.	Beacon packets are sent by access points and base stations. However, client radio cards send beacons when operating in non-base station mode.
Beacon interval	Time between attempts to locate a Wi-Fi source when the scanner is in scan mode.	
Beacon mode	A mode of an AP in which scanning is being done.	
Beamwidth	The width (in degrees) of an antenna directivity pattern.	
Bearing	A surveying term used to designate direction.	Used in wireless networks to designate the direction an antenna is pointing.
Best-effort	Refers to treatment of a call without regard to pre-defined Quality of Service.	
Blocking	Refusal of a system to accept a request for use of a vital system resource(e.g., call attempt to use a voice circuit)	
Boot (noun)	Waterproof connector.	
Boot (verb)	Start a system up.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
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.	
Broadband	A communications network in which a frequency range is divided into multiple independent channels for simultaneous transmission of signals (as voice, data, or video).	Often informally used in the much looser sense of a high-speed network.
Broadcast traffic	Traffic above and beyond the base amount.	
Buffer	An amount of memory that temporarily stores data to help compensate for differences in the transfer rate of data from one device to another.	Data that is in a buffer is said to be “buffered”.
Cable network	Networks that use existing cable TV infrastructure that your cable company uses for TV signals, to transmit data to and from the Internet.	Since cable TV was designed as a broadcast system, the cable is shared amongst the users in your neighbourhood and is considered high speed or broadband Internet access.
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.
Charge controller	A component of a photovoltaic system that controls the flow of current to and from the battery subsystem to protect batteries from overcharge, over-discharge, or other control functions. The charge controller may also monitor system operational status.	

Term	Definition	Notes
Cisco	A manufacturer of communications equipment.	
Clearance	The amount of additional height you have to account for above obstacles in order to transmit a good wireless signal.	
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 (also known as "Coax")	A type of communication transmission cable in which a solid center conductor is surrounded by an insulating spacer that in turn is surrounded by a tubular outer conductor (usually a braid, foil or both). The entire assembly is covered with an insulating and protective outer layer.	Coaxial cables have a wide bandwidth and can carry many data, voice and video conversations simultaneously.
Continuous Wave (CW) Transmitter	A transmitter that outputs a sustained or oscillatory wave whose successive oscillations are, under steady-state conditions, identical.	
Corridor	A line of relays between two serving areas.	
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 wireless equipment.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
DC-to-DC converter	A circuit that converts DC power from one voltage to another.	It is a special class of power converter.
Dial-up	Internet access services which use a telephone line and modem attached to a PC to connect users to the Internet. This is the most basic form of service for consumers, primarily to access the Internet and World Wide Web.	
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.
Directional antenna	An antenna that focuses its energy into a limited beam width.	
Duplex	A duplex communication system is one where signal can flow in both directions between connected parties.	
Dynamic IP Address	An IP address that changes with each connection to the Internet.	
Encryption	A method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data.	Only individuals with access to a password or key can decrypt and use the data. The data can include messages, files, folders, or disks.
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 Mb/s. 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.	
Facility	A system for transporting traffic and signals, usually consisting of a pair of terminals and either a cable or a wireless link.	



Term	Definition	Notes
Filtering	The process by which particular source or destination addresses can be prevented from crossing a bridge or router onto another portion of the network.	Bridges and switches can reduce the level of congestion on a LAN through the process of filtering. A filtering bridge or switch forwards a packet from one LAN segment to another only as required. Packets that are not forwarded by a bridge or switch are said to be "filtered".
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 that is embedded in a hardware device that allows reading and executing the software, but does not allow modification, e.g., writing or deleting data by an end user.	
Float charged	The charging of a battery, taking into account a minimum "float" or reserve charge.	
Foliage	The leaves of a tree or other plant.	
Free space	Remoteness from material objects that could influence the propagation of electromagnetic waves.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
Frequency	The number of back-and-forth cycles per second, in a wave or wave-like process.	Expressed this way, the frequency is given in units of Hertz (Hz), named after the scientist who first produced and observed radio waves in the lab.  Other units are: <ul style="list-style-type: none"> <li>• Kilohertz (thousands of Hz, abbreviated KHz)</li> <li>• Megahertz (millions of Hz, abbreviated MHz)</li> <li>• Gigahertz (billions of Hz, abbreviated GHz)</li> </ul>
Fresnel Zone	The area around the visual line-of-sight between transmitter and receiver.	Radio waves disperse as they leave the antenna. Obstructions in this zone of dispersion (Fresnel Zone) attenuate the signal. In the 2.4GHz Wi-Fi band, this is particularly true of objects with large moisture content such as trees.
Gain	The amount of increase in signal power or voltage or current expressed as the ratio of output to input.	
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 provide a means of interconnection. See Bridge
Gauge	The width of a wire.	
Ground Fault Interrupter (GFI)	An electrical safety device that is able to detect a short circuit and shut off power automatically.	Used as a protection against electrical shock.
Ground station	A satellite terminal with associated equipment for electrical power, control, etc.	
Guy wire	A wire used to attach a tower to a Guy Anchor and the ground.	

Term	Definition	Notes
Guyed	Steadied or reinforced with a guy.	
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.	
Head	The pressure exerted by a fluid; "a head of steam"	
High-gain antenna	An antenna whose maximum power is very large.	
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.
Hybrid solution	A mix of different network technologies (e.g., Wi-Fi and fibre) to achieve a stated objective	
Infrastructure mode	A mode of an AP in which it is serving as an AP.	
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.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
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 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 VLAN	A VLAN that is segmented based on Layer 1 (physical) information, such as a physical port.	
Layer 2 VLAN	A VLAN that is segmented based on Layer 2 (bridging) information.	
Layer 3 VLAN	A VLAN that is segmented based on Layer 2 (routing) information.	
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.	
Loss	The portion of energy applied to a system that is dissipated and performs no useful work.	In wireless, loss is usually measured in Decibels (dB).
Mains	The AC power distribution lines provided by a power utility.	

Term	Definition	Notes
Median	The middle number in a defined statistical distribution.	When looking at estimates, median refers to the estimate above and below which lie an equal number of estimates for the period indicated.
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.	
Microcell	A small wireless coverage area.	
Microwave	The subset of the Electromagnetic Spectrum encompassing wavelengths between 0.3 and 30 centimetres, corresponding to frequencies of 1-100 Gigahertz.	
Mobility	Movement of a wireless client.	
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.
Network partitioning	Dividing a network into parts that can be separately identified and managed.	Also known as segmenting. A network switch is used to interconnect network segments.
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).	
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.
Omnidirectional antenna	An antenna, which provides roughly equal power at all angles around it.	Often called an "Omni".

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
Optical network	A network that carries digitized voice or data at very high rates on multiple channels of light.	
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.
Pelton wheel	A turbine with many small fans arranged in a wheel.	
Penstock	A large pipe or conduit to carry the water from the reservoir or dam to a turbine or water wheel	
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.
Pull-back Testing	A backhaul testing technique in which you set up a portable antenna in a nearby location, and then successively move this antenna out to farther and farther locations along the same bore sight.	
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.

Term	Definition	Notes
Port	An interface through which data is sent and received.	<p>A hardware port is an outlet on a piece of equipment into which a plug or cable connects.</p> <p>A network port is an interface for communicating with a computer program over a network. Network ports are usually numbered and a network implementation like TCP or UDP will attach a port number to data it sends.</p>
Port grouping	Treating a set of ports as if they were equivalent in some sense.	
Port Number	A number identifying a certain Internet application.	For example, the default port number for the WWW service is 80.
Port switching	Switching on the basis of a port, so that each is its own collision domain.	
Power budget	The allocation, within a system, of available electrical power, among the various functions that need to be performed.	
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.
Preamble	A sequence of encoded bits that is transmitted before each frame to allow synchronization of clocks and other circuitry at other sites on the channel.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
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: <ul style="list-style-type: none"><li>• The type of error checking to be used</li><li>• Data compression method, if any</li><li>• How the sending device will indicate that it has finished sending a message</li><li>• How the receiving device will indicate that it has received a message.</li></ul>
Proxy	A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.	A software agent that acts on behalf of a user, typical proxies accept a connection from a user, makes a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
RADIUS server	Remote Authentication Dial-In User Server / Service. A server for authentication, authorization, and accounting of endpoints and endpoint aliases.	
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 fibreglass.
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 system.	
Rated	Assigned a normal capacity or power.	
Reach	The distance an antenna of a certain type and height above average ground level can transmit with adequate power over a certain type of terrain, given a receive antenna of a certain type and height.	
Receiver	The part of a communication system that picks up or accepts a signal or message from a channel and converts it to perceptible forms.	
Relay	A wireless terminal that passes on traffic to another one.	See repeater.
Reliability	The per cent of time that a system such as a network is functioning properly during the time it is supposed to be available.	
Repeater	A network device used to regenerate or replicate a signal.	In a data network, a repeater can relay messages between sub-networks 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.	
Route (n.)	The path between two end-points.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
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.	
Sectional tower	A tower that consists of various sections.	
Sectored antenna	An antenna that covers only part of a 360 degrees angle.	
Sensitivity	In an electronic device, e.g., a communications system or receiver, the minimum input signal required to produce a specified output signal having a specified signal-to-noise ratio.	May be expressed as power in dBm.
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	
SMC Connector	A type of connector, used in Wi-Fi client cards, amongst other uses.	The SMC name derives from SubMiniature C (the third sub-miniature design). The SMC design was developed in the 1960's. SMC has threaded coupling, with 10-32 threads. It is available in 50 and 75 Ohm impedances.
Solar panel	An electrical device consisting of a large array of connected solar cells.	
Span	Any link on a route.	

Term	Definition	Notes
Spanning Tree	A method used by bridges to create a logical topology that connects all network segments, and ensures that only one path exists between any two stations.	
Spectrum analyzer	An instrument that displays the frequency spectrum of an input signal.	
Standby generator	An electrical generator that is used only in the case of power loss.	
Static IP Address	A permanently assigned address on the internet.	Usually used for servers, printers, VPNs (Virtual Private Networks), etc.
Stepped pseudo-sine wave	An electrical waveform that looks like a square wave with some steps in it.	
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 router before being sent out on the outgoing link.	
Stub antenna	The stubby antenna on most Wi-Fi cards	
Sub-network	A network segment.	Subnetting allows you to break down a large network into smaller ones that result in reduced network traffic, simplified administration, and smoother performance.
Subnet field	A 32-bit bitmask used to inform routers as to how much of an IP address identifies the subnetwork the host is on and how much identifies the host.	Also known as subnet mask.
Survivability	The ability of a system such as a network to continue to function and provide service even during a failure of part of the system.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
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.
Telnet	A program that enables you to open an interactive login session over TCP/IP networks like the Internet.	
Terminus	Either end of a communications route.	
Thimble	A device to prevent crimping of guy wire.	
Throughput	The amount of data that can be sent from one location to another in a specific amount of time. Usually measured in Kb/s, Mb/s, or Gb/s.	It refers to 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.
Topographic map	A map containing contours indicating lines of equal surface elevation.	
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.	

Term	Definition	Notes
Transmitter	A device used for the generation of signals of any type and from which are to be transmitted.	In wireless, it is that portion of the equipment that includes electronic circuits designed to generate, amplify, and shape the radiofrequency energy that is delivered to the antenna where it is radiated out into space.
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.	
Turbine	A device for converting the flow of a fluid (air, steam, water, or hot gases) into mechanical motion that in turn produces electricity.	
Turnbuckle	A screw fitting for adjusting the tension of shrouds and stays.	
Virtual subnet	A Layer 3 VLAN.	
Virus	A parasitic program written intentionally to enter a computer without the user's permission or knowledge.	
Watch dog	A device or system that continually 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.	
Wireless Bridge	A bridge that operates wirelessly.	

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

Term	Definition	Notes
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.

# Appendix C:

## References

### Specific

---

The following documents form the technical basis for much of the book:

- D. Reid, Ian Easson, W. Almuhtadi, “Rural/Remote Wireless Research Project, Final technical Report” submitted in August 2004 to CIDA, Industry Canada, and NCIT.
- The Jhai PC and Communication System Project  
[http://www.jhai.org/jhai\\_remoteIT.htm](http://www.jhai.org/jhai_remoteIT.htm)
- Clif Cox, Bhutan Migration to New Technology (Wireless VoIP) Mission Report, prepared by ITU, 2002, <http://www.bhutan-notes.com/clif/>
- Dr. Onno W. Purbo, Wi-Fi and VoIP projects  
<http://sandbox.bellanet.org/~onno/>  
<http://www.apjii.or.id/onno/>  
<http://onno.vlsm.org>  
<http://www.bogor.net/idkf/>
- Field measurements using: [www.PCPitstop.com](http://www.PCPitstop.com)
- Field measurements using: Downloads | [NetStumbler.com](http://www.NetStumbler.com)
- Linksys manuals and websites for Wi-Fi equipment  
<http://www.linksys.com/products/>
- D-Link manuals and websites for Wi-Fi equipment  
<http://www.dlink.com/products/category.asp>
- [www.sveasoft.com](http://www.sveasoft.com) provides a basis for looking into other features that could be incorporated in subsequent architectures for rural use.

### General

---

The following is a good list of general reading on wireless and Wi-Fi.

- Brian Carter and Russell Shumway, *Wireless Security End to End*. John Wiley & Sons; 1st edition (August 15, 2002).
- Cisco, *Security for Next Generation Wireless LANs*

## Building Rural Wi-Fi Networks: A Do-it-Yourself Cookbook

- *IEEE 802.11g™ standard*, Standards Board of the Institute of Electrical and Electronics Engineers, 2003.
- Frank Ohrtman and Konrad Roeder, *Wi-Fi Handbook: Building 802.11b Wireless Networks*. McGraw-Hill Professional; 1st edition (April 10, 2003), ISBN: 0071412514.
- Jack Unger, *Deploying License-Free Wireless Wide-Area Networks*. Cisco Press, 1st edition (February 26, 2003) , ISBN: 1587050692
- Janice Reynolds, *Going Wi-Fi: A Practical Guide to Planning and Building an 802.11 Network*. CMP Books, 2003.
- James LaRocca, *802.11 Demystified: Wi-Fi Made Easy (Telecommunications)*. McGraw-Hill, 2002.
- Lee Barken, *How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN*. Prentice Hall, 2003.
- Microsoft, *Planning Guide for Securing Wireless LANs*. A Windows Server 2003 Certificate Services Solution.
- Preston Gralla, *How Wireless Work*. Que Publishers.
- Rob Fleckinger, *Building Wireless Community Networks*, 2nd Ed, O'Reilly Media.
- Shelly Brisbin, *Build Your Own Wi-Fi Network*. McGraw-Hill, 2002.
- Simon R. Saunders, *Antennas and Propagation for Wireless Communication Systems*. John Wiley & Sons, 1999.
- Thomas Maufer, *Field Guide to Wireless LANs for Administrators and Power Users*, A. Prentice Hall, 2003. *Planning Guide for Securing Wireless LANs*. A Windows Server 2003 Certificate Services Solution. Microsoft.



Prepared by:

Algonquin College  
1385 Woodoroffe Ave  
Ottawa, Ontario Canada  
[www.algonquincollege.com](http://www.algonquincollege.com)

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION  
SECRETARIAT

35 Heng Mui Keng Terrace Singapore 119616

Tel: (65) 6775-6012 Fax: (65) 6775-6013

Email: [info@apec.org](mailto:info@apec.org)

Website: [www.apec.org](http://www.apec.org)

© [2005] APEC Secretariat