Designing and Deploying 802.11n Wireless Networks

Gain a practical understanding of the underlying concepts of the 802.11n standard and the methodologies for completing a successful wireless network installation

ciscopress.com

Jim Geier

Designing and Deploying 802.11n Wireless Networks

Jim Geier

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Designing and Deploying 802.11n Wireless Networks

Jim Geier

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing June 2010

Library of Congress Cataloging-in-Publication Data

Geier, James T.
Designing and deploying 802.11n wireless networks / Jim Geier.
p. cm.
ISBN 978-1-58705-889-9 (hardcover)
1. Wireless LANs. 2. IEEE 802.11 (Standard) I. Title.

TK5105.78.G448 2010
004.6'8--dc22

2010019130

ISBN-13: 978-1-58705-889-9

ISBN-10: 1-58705-889-8

Warning and Disclaimer

This book is designed to provide information about wireless networking, which includes Cisco products. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Editorial Assistant: Vanessa Evans

Cover and Interior Designer: Louisa Adair

Composition: Mark Shirar

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Tom Carpenter and Christian Estes

Copy Editor: Keith Cline

Indexer: Bill Meyers

Proofreader: Kathy Ruiz

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Author

Jim Geier is the founder and principal consultant of Wireless-Nets, Ltd., an independent consulting firm assisting organizations with the development and deployment of wireless networks. His 25 years of experience includes the planning, analysis, design, implementation, installation, and support of numerous wireless network-based solutions for enterprises, municipalities, hospitals, universities, airports, warehouses, and product manufacturers worldwide. Jim is the author of more than a dozen books, including *Deploying Voice over Wireless LANs* (Cisco Press), *Wireless Networks: First Step* (Cisco Press), *Implementing 802.1X Security Solutions* (Wiley), and *Network Reengineering* (McGraw-Hill). He is the author of numerous tutorials and other publications and has developed and instructed dozens of training courses on wireless networking topics. Jim has been active within the Wi-Fi Alliance, responsible for certifying interoperability of 802.11 (Wi-Fi) wireless LANs. He has also been active with the IEEE 802.11 Working Group, responsible for developing international standards for wireless LANs. He served as Chairman of the IEEE Computer Society, Dayton Section, and Chairman of the IEEE International Conference on Wireless LAN Implementation. Jim's education includes a Bachelor's and Master's degree in electrical engineering, with emphasis in wireless communications.

Jim Geier's contact information:
E-mail: jimgeier@wireless-nets.com
Website: www.wireless-nets.com

About the Technical Reviewers

Tom Carpenter is the Senior Consultant for the Systems Education and Consulting Company (SYSEDCO) located in Marysville, Ohio. Tom holds several industry certifications, including CWNA, CWSP, and vendor-specific certifications in the wireless industry. He has authored several books on wireless networking and VoIP and database solutions, and he speaks regularly at training events and technical conferences. Tom lives with his wife and four wonderful children in central Ohio.

Christian J. Estes is a Senior Wireless Engineer on the Escalation / CAP Team in the Wireless Business Unit at Cisco Systems, located in Silicon Valley. During the four years he has been at Cisco, he has participated in the design, deployment, and remediation of enterprise class wireless architectures and specializes in Voice over Wireless LAN technologies, protocols, and applications. He was a member of the CCIE Certification Development Team for the Wireless track and holds the CCNP, CCVP, and CWNE certifications. In addition, he is currently in the process of acquiring the CCIE certification. He has degrees in computer engineering and organizational leadership and is currently pursuing a graduate degree from Stanford University in management science and engineering.

Dedications

I dedicate this book to my wife, Debbie.

Acknowledgments

I want to thank the Pearson production team for their time and effort with creating this book:

- Thanks to Mary Beth Ray for getting this book contracted and managing the process from beginning to end.
- Thanks to Christopher Cleveland, Mandie Frank, and Keith Cline for their fantastic editing of the book.
- Thanks to the many others at Pearson who were part of developing and producing this book.

I also want to thank Tom Carpenter for providing technical feedback on the many topics that this book covers. Also, thanks to Christian Estes for providing technical feedback about Cisco solutions.

Contents at a Glance

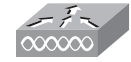
Contents

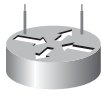
Icons Used in This Book

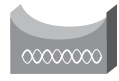

Access Point

Mesh Access Point

Lightweight Access Point


WLAN Controller

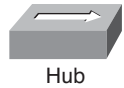

Wireless LAN Router


Wireless Bridge


Router


Multilayer Switch


Ethernet Switch


Hub


Repeater

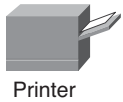

Call Manager


Voice Gateway


IP Telephony Router


PC


Laptop


Printer


Server


Web Server


Database


Cell Phone


PDA


Wireless Inventory/Manufacturing Device


Phone


Camera/PC Video


WiMax Base Station


Network Cloud

Introduction

The 802.11n amendment to the IEEE 802.11 wireless LAN (WLAN) standard was ratified in September 2009, and enables 802.11 systems to provide much higher performance and range than before. The majority of network equipment manufacturers now offer 802.11n-compliant equipment as their primary WLAN solution. WLANs based on earlier versions of the standard (802.11a, 802.11b, and 802.11g) are considered "legacy," and there is significant risk that these existing non-802.11n systems will become obsolete. As a result, organizations deploying new WLANs should definitely implement 802.11n-compliant equipment. In addition, organizations with existing non-802.11n WLANs should begin planning the migration to 802.11n-compliant networks.

This how-to book focuses on planning, designing, installing, testing, and supporting 802.11n wireless networks for a variety of applications. The methods, recommendations, and tips in this book are based on the author's many years of practical experience deploying WLANs. Organizations with no existing wireless network and those migrating from legacy wireless networks to 802.11n-compliant networks will find this book to be a valuable guide.

Goals and Methods

The overall goal of this book is to guide you through the steps of deploying an 802.l1n WLAN. To accomplish this, the book includes the following elements:

- **Step-by-step approaches:** The book breaks each phase of WLAN deployment into clearly defined steps that provide the basis for understanding and planning the details of the phase.
- **Case studies:** The book includes several case studies that provide explanations of concepts and methods as they are practiced in actual deployments.
- **Hands-on exercises:** The book includes exercises that make use of free and inexpensive tools that help you gain practical experience with concepts described in the chapter.
- **Tips:** Concise tips are distributed throughout the book and provide insightful information related to deploying WLANs.

Who Should Read This Book?

This book is intended for a variety of people, from someone with basic knowledge of networking to others who might have years of experience working with WLANs but have little if any experience implementing 802.11n networks.

How This Book Is Organized

Although this book can be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to learn just the information that you need.

This book covers the following topics:

- Part I, "Fundamental Concepts": This part of the book includes chapters that cover important underlying concepts that must be understood before deploying an 802.11n wireless network. Readers already familiar with WLANs may be able to skip one or more of the chapters in this part of the book.
  - Chapter 1, "Introduction to Wireless Networks": This chapter defines the markets and applications of WLANs and the wireless technologies that support them.
  - Chapter 2, "Radio Wave Fundamentals": This chapter explains radio wave fundamentals so that you have the basis for understanding the complexities of deploying WLANs.
  - Chapter 3, "Wireless LAN Types and Components": This chapter describes ad hoc, mesh, and infrastructure WLAN types and various components, such as access points, controllers, client radios, amplifiers, and others.
  - Chapter 4, "Wireless LAN Implications": This chapter explains the impacts of radio signal interference, security vulnerabilities, multipath propagation, roaming, and battery limitations on WLANs.
- Part II, "The 802.11 Standard": This part of the book includes chapters that contain in-depth coverage of the most current medium access and physical layers of the IEEE 802.11 standard (including 802.11n functionality). The focus here is on the elements of the standard that readers should know to be successful at deploying and supporting 802.11n wireless networks.
  - Chapter 5, "Introduction to IEEE 802.11 and Related Standards": This chapter provides a background and importance of 802.11 standards and an overview of the 802.11 standard and related standards, such as IEEE 802.2.
  - Chapter 6, "IEEE 802.11 Media Access Control (MAC) Layer": This chapter explains details of the 802.11 standard that you need to know to help you best configure and troubleshoot 802.11n WLANs.
  - Chapter 7, "IEEE 802.11 Physical (PHY) Layers": This chapter describes the modulation functions that are part of the 802.11n physical layer and legacy physical layers (802.11a, 802.11b, and 802.11g).

- Part III, "Wireless Network Design": This part of the book includes chapters that cover steps necessary to design an 802.11n wireless network for various scenarios.
  - Chapter 8, "Planning a Wireless LAN Deployment": This chapter provides an overview of the steps that you should complete when deploying a WLAN and details on defining the project scope, developing a work breakdown structure, identifying staffing, creating a schedule, developing a budget, evaluating risks, and analyzing feasibility.
  - Chapter 9, "Defining Requirements for a Wireless LAN": This chapter explains how to gather, analyze, and document requirements for an 802.11n WLAN.
  - Chapter 10, "System Architecture Considerations": This chapter explains what to consider when designing the access network and distribution system for an 802.11n WLAN.
  - Chapter 11, "Range, Performance, and Roaming Considerations": This chapter explains the various tradeoffs for enhancing the range, performance, and roaming capabilities of an 802.11n wireless LAN.
  - Chapter 12, "Radio Frequency Considerations": This chapter covers important radio frequency (RF) design considerations for 802.11n WLANs, such as frequency band selection, transmission channel settings, difficult-to-cover areas, and radio signal interference reduction techniques.
  - Chapter 13, "Security Considerations": This chapter explains important methods and techniques for securing a WLAN, including encryption, authentication, rogue access point detection, RF shielding, and security polices.
- Part IV, "Wireless Network Installation and Testing": This part of the book includes chapters that explain the steps necessary to install and test an 802.11n wireless network.
  - Chapter 14, "Test Tools": This chapter describes the tools that you need to effectively design and support an 802.11n WLAN.
  - Chapter 15, "Performing a Wireless Site Survey": This chapter explains the steps and techniques, such as inspecting the existing network, analyzing radio signal interference, and performing signal propagation testing, that you need to follow when determining the optimum installation locations for access points.
  - Chapter 16, "Installing and Configuring a Wireless LAN": This chapter explains how to plan the installation, stage the components, install the access points, and document the installation of a WLAN.
  - Chapter 17, "Testing a Wireless LAN": This chapter describes the steps and techniques necessary to test a wireless LAN, which includes signal coverage testing, performance testing, in-motion testing, security testing, acceptance testing, simulation testing, prototype testing, and pilot testing.

- Part V, "Operational Support Considerations": This part of the book includes chapters that explain what to consider when supporting an 802.11n wireless network. Readers will learn how to establish specialized support for wireless networks and perform help desk operations, network monitoring, and troubleshooting.
  - Chapter 18, "Managing a Wireless LAN": This chapter describes important operations and maintenance functions that you should consider when supporting a WLAN, including help desk, network monitoring, maintenance, engineering, configuration management, security management, trouble call coordination, operational support tools, and operational support transfer preparation.
  - Chapter 19, "Troubleshooting Wireless Networks": This chapter explains how to identify problems, such as connectivity and performance issues, and determine the underlying causes.
  - Chapter 20, "Preparing Support Staff": This chapter describes what you should consider when evaluating the experience and education of staff for supporting a wireless LAN.
- Glossary: The glossary describes terms that this book uses.

Hands-on Exercises

As mentioned in the "Goals and Methods" section, this book includes exercises that make use of free and inexpensive tools that help you gain practical experience with concepts described in the chapter. You can find these exercises on the following pages:

- Chapter 6:
  - Hands-on Exercise: Observing 802.11 Dynamic Rate Shifting—141
  - Hands-on Exercise: Observing 802.11 Active Scanning—150
  - Hands-on Exercise: Observing the 802.11 Connection Process—154
  - Hands-on Exercise: Observing 802.11 Beacons—169
  - Hands-on Exercise: Observing 802.11 Frames Resulting from Typical User Traffic—175
- Chapter 7:
  - Hands-on Exercise: Understanding Performance Impacts of Increasing 802.11n Spatial Streams—192
  - Hands-on Exercise: Understanding Performance Impacts of 802.11n Channel Bonding—193
- Chapter 11:
  - Hands-on Exercise: Analyzing Impacts on Range Using Different Data Rate Settings—305

Chapter 1

Introduction to Wireless LANs

This chapter will introduce you to:

- Wireless LAN Markets and Applications
- Benefits of Wireless Networks
- Wireless Network Technologies
- Other Wireless Network Technologies
- Wireless LANs: A Historical Perspective

Applications of wireless local-area networks (WLANs) have become commonplace in many markets throughout the world. Newer WLANs based on the 802.11n standard now offer performance needed for effectively supporting a high density of users and a broad range of high-end applications, such as voice, video, and image processing. This chapter defines the markets and applications of WLANs and the wireless technologies that support them.

Wireless LAN Markets and Applications

In general, WLANs are applicable to all markets with a need for user mobility or when the installation of physical media is not feasible. Wireless LANs prove especially useful when employees must process information on the spot via electronic-based forms and interactive menus. Wireless networking makes it possible to place portable computers in the hands of mobile users, such as doctors, nurses, warehouse clerks, inspectors, claims adjusters, real estate agents, and salespeople.

The implementation of portable devices with wireless connectivity facilitates access to a common database and applications that meets the needs of users, eliminates unnecessary paperwork, decreases errors, reduces processing costs, and improves overall efficiency. It also introduces user mobility by allowing the user to move from one WLAN to another seamlessly. The alternative to this, which many companies still employ today, is using

paperwork to update records, process inventories, and file claims. This method processes information much more slowly, produces redundant data, and is subject to input errors caused by illegible handwriting. The approach to mobile computing over a WLAN using a centralized database enhances productivity and is clearly a superior approach.

The sections that follow provide a general description of the WLAN market and applications within those markets. This will help stimulate ideas with regard to how WLANs will benefit your company or organization.

Retail

Retail organizations need to order, price, sell, and manage inventories of merchandise. A wireless network in a retail environment enables clerks and storeroom personnel to perform their functions directly from the sales floor. Salespeople are equipped with a pen-based computer or a small computing device with bar code reading and printing capabilities, while connected to the store's database via the WLAN. They can then complete transactions such as pricing, bin labeling, placing special orders, and taking inventory from anywhere within the store.

When printing price labels that will be affixed to the item or shelves, retailers often use a Symbol handheld bar code scanner (from Motorola) and Monarch printer (from Avery Dennison) to produce bar coded or human-readable labels. A database or file contains the price information located either on the handheld device, often called a *batch* device, or on a server somewhere in the store. In batch mode, the price clerk scans the bar code (typically the product code) located on the item or shelf edge, the application software uses the product code to look up the new price, and then the printer produces a new label that the clerk affixes to the item.

In some cases, the batch-based scanner/printer has enough memory to store all the price information needed to perform the pricing functions throughout a shift or an entire day. This situation makes sense if the user needs to update pricing information in the database through the day, typically during the evening. The clerks load the data onto the device at the beginning of their shifts, and then walk throughout the store pricing items. However, if the memory in the device is not large enough to store all the data, a wireless network is probably necessary. If the handheld unit is equipped with a wireless network connection, the handheld can be configured for a WLAN and data can be stored on a centralized server or mainframe and accessed each time an item's bar code is scanned. In addition, a wireless network-based solution has merit if it is too time-consuming to download information to a batch device.

In addition to traditional retail stores that use a WLAN to access server-based applications, store owners are finding it beneficial to advertise and distribute product videos to monitors located throughout the store. An 802.11n network is ideal for connecting wireless displays to a centralized video server. The nature of 802.11n, and the enhanced level of throughput, allows the store to locate displays across the WLAN. This is ideal when considering the higher level of performance that will be facilitated when deploying an 802.11n solution to support high-definition video displays.

Warehousing

Warehouse staff must manage the receiving, shelving, inventorying, picking, and shipping of goods. These responsibilities require the staff to be mobile. Warehouse operations traditionally have been paper intensive and time-consuming. An organization can eliminate paper, reduce errors, and decrease the time necessary to move items in and out by giving each warehouse employee a mobile handheld computing device with an Intermec bar code scanner, for example, connected via a wireless network to a warehouse inventory system.

Upon receiving an item for storage within the warehouse, a clerk can scan the item's barcoded item number and enter other information from a small keypad into the database via the handheld device. The system can respond with a location by printing a put-away label. A forklift operator can then move the item to a storage place and account for the procedure by scanning the item's bar code. The inventory control system keeps track of all transactions, making it very easy to produce accurate inventory reports. In addition, the online interaction with a database will identify mistakes immediately, enabling the operator to correct the mistake before it becomes a problem.

As shipping orders enter the warehouse, the inventory system produces a list of the items and their locations. A clerk can view this list from the database via a handheld device and locate the items needed to assemble a shipment. As the clerk removes the items from the storage bins, the database can be updated via the handheld device. All these functions depend heavily on wireless networks to maintain real-time access to data stored in a central database.

Warehouses involve a host of functions where the use of wireless IP phones can provide significant benefits. Clerks end up being scattered throughout the warehouse facility, which can be quite expansive, and communications with other clerks and managers is essential to perform various functions. In most cases, it is not practical for the clerks and managers to meet face to face to communicate. In fact, it is often not possible for them to even find each other, because of the numerous rows of bins and products. For example, an order may come in for the shipment of a particular item to a customer. Rather than wait for a clerk to return to the main office, it is must faster and productive for the shipping department to call a clerk directly and have the clerk pick the item.

Many warehouses already have existing WLANs; however, because these wireless networks primary support relatively low-performance bar code solutions for implementing inventory management functions, the existing WLAN will likely not have enough capacity to support a large number of wireless IP phones. In most cases, the much higher capacity of 802.11n networks is necessary to support voice applications in warehouses.

Wireless Bar Code System for Warehouses

A manufacturer in North America is a leading provider of bar code printers and supplies. As part of the company's goal to streamline processes within its manufacturing plant and warehouse, a process improvement team applied the use of mobile handheld bar code scanning and printing devices with the support of a WLAN within its central distribution center (CDC).

Before implementing the system, the CDC was experiencing inefficiencies because clerks needed to walk back and forth between stacks of finished goods and a desktop terminal used to determine a warehouse storage location for the items. The clerks would collect information from the finished goods by writing it down on a piece of paper, and then walk to the terminal to query the company's warehouse management system for a recommended storage location. The clerk would write this location information on a large label, walk back to the product, and affix the label to the product's container. Later, a forklift operator would come by and place the container in the correct location on the warehouse floor. The process of walking back and forth between the products and the terminal made inefficient use of the clerk's time, which slowed the movement of products through the plant.

The solution to this problem consists of a bar code scanner equipped with a radio card and a WLAN. 802.11 access points throughout the warehouse connect to an Ethernet network that interfaces to a server running a warehouse management system. The clerk can now scan the finished product's bar code, which is used to query the warehouse management system for a valid put-away location. The system then prints a label on a printer connected to the bar code scanner indicating the applicable location information.

Through the use of this scan, print, and apply function, the solution eliminates the need for the clerk to walk back and forth to the terminal, increasing productivity by 50 percent. In addition, the solution provides significant gains in accuracy through the elimination of human error.

Healthcare

Healthcare centers, such as hospitals and doctor offices, must maintain accurate records to ensure effective patient care. A simple mistake can cost someone's life. As a result, doctors and nurses must carefully record test results, physical data, pharmaceutical orders, and surgical procedures. This paperwork often overwhelms healthcare staff, taking 50 percent to 70 percent of their time.

Doctors and nurses are also extremely mobile, going from room to room caring for patients. The use of electronic patient records, with the capability to input, view, and update patient data from anywhere in the hospital, increases the accuracy and speed of healthcare. This improvement is made possible by providing each nurse and doctor with a wireless pen-based computer, coupled with a wireless network to databases that store critical medical information about the patients.

A doctor caring for someone in the hospital, for example, can place an order for a blood test by keying the request into a handheld computer. The laboratory will receive the order electronically and dispatch a lab technician to draw blood from the patient. The laboratory will run the tests requested by the doctor and enter the results into the patient's electronic medical record. The doctor can then check the results via the handheld appliance from anywhere in the hospital.

Wireless LANs also help patients in hospitals, too. Patient monitoring devices, such as those from Draeger, monitor the vital signs of patients and wirelessly send the information to monitors located in the patient room and nursing stations. This allows patients to

get out of bed and move around their room without the nuisance of cables attaching them to monitoring equipment.

Another application for wireless networks in hospitals is the tracking of pharmaceuticals. The use of mobile handheld bar code printing and scanning devices dramatically increases the efficiency and accuracy of all drug transactions, such as receiving, picking, dispensing, inventory taking, and tracking drug expiration dates. Most important, though, it ensures that hospital staff is able to administer the right drug to the right person at the right time. This would not be possible without the use of wireless networks to support a centralized database and mobile data collection devices.

Hospitals were one of the first users of wireless IP phones, mainly because of the significant needs for effective communications among high-valued medical staff. The ability for doctors and nurses to respond quickly with verbal instructions is crucial for saving the lives of patients. Patients receive a higher level of care, which leads to faster recovery. Wireless IP phones allow hospital staff to not waste time looking for a phone to use.

An issue with deploying voice over wireless solutions in hospitals, however, is the difficulty in providing adequate WLAN coverage. Hospitals include x-ray rooms surrounded by lead, irregular metal objects, and unpredictable traffic flows of people. This leads to significant attenuation and multipath propagation. In addition, radio frequency (RF) interference from other wireless systems operating in the 2.4-GHz band, such as frequency-hopping spread-spectrum devices, can cause degradation in performance. 802.11n, with its capability to operate well in "RF hostile" environments, is a good choice for healthcare facilities.

Wireless Robots at OSU Medical Center

The Ohio State University Medical Center (OSUMC), situated in Columbus, is Central Ohio's most honored hospital with physicians and staff serving 800,000 patient visits each year. In addition, the hospital hosts $100 million worth of research each year, and operates a top-notch medical school. I recently visited OSUMC to observe their new fleet of robots.

A Mobile Robotic Project Is Born

To improve operational efficiency, OSUMC has developed the Automated Transport System (ATS). The ATS includes robotic "transporters" that take care of moving materials around the hospital, including carrying patient meals, linen, supplies, and wastes between patient wings and a service floor, with interfaces to the kitchen, laundry, and supply and trash areas.

FMC Technologies Inc. (Chalfont, Pennsylvania) is implementing the ATS at OSUMC. With more than 300 systems and 2500 automated guided vehicle (AGV) systems deployed worldwide, FMC Technologies is a leading supplier of AGVs in many of the industries that use automated vehicles.

The Payback

The ATS at OSUMC will include 46 transporters making 3000 material movements each day. Each transporter can lift and move delivery carts weighing as much as 1000 pounds each. A variety of different carts can be used to accommodate various types of loads.

After purchasing the ATS and making associated building renovations, the OSUMC expects to see a return on investment within 5 to 7 years. Most of the savings results from reducing the amount of time staff members spend moving materials, allowing them to spend more time with patients or other important tasks.

In addition, the system should decrease wait time for materials and replace an outdated rail system that has been used to move materials. Because new elevators were built exclusively for the robots, there is also less traffic now in patient and visitor elevators.

Robots Find Their Own Way Around

Each transporter uses laser guidance for getting around the hospital. A rotating infrared light on top of the transporter hits multiple reflectors attached to the walls strategically located throughout the hospital. The transporter catches the reflections coming back from reflectors, and uses the associated information to calculate its position. Every point in the hospital returns a different signature from the reflectors, which maps to a specific location.

The transporter carries a signature map (stored in memory) to plot its exact location. Think of this as a passive form of a Global Positioning System (GPS) connected to mapping software, with satellites attached to the walls. Of course, in the case of the ATS, the satellites are just small strips of reflective material that do not require electrical power. Also, like GPS, the system is redundant. Even if a couple of strips are knocked from the walls, there will still be enough for the transporter to accurately locate itself.

Robots Get Physical

The transporters move materials through hallways to multiple floors. There are 9 dedicated elevators and 264 pickup and drop-off locations. The ATS automatically calls the elevators at the appropriate time when a transporter needs to change floors. To keep things clean, separate “clean” and “soiled” carts make it possible for the transporters to keep wastes and dirty dishes away from fresh linen and food. When a transporter arrives on a patient wing floor, lights and pagers signal the arrival of the cart.

The transporters periodically receive their duty schedules from a central computer system. Staff within the hospital input the needs for such items as patient meals, linen, and trash pick-up, and the computer system assigns the tasks to specific transporters. Without argument, the transporters go about their work in a timely manner without any intervention from humans.

Things Could Get in the Way

The transporters have a sophisticated obstacle detection that makes them stop if something gets in the way. The transporter can detect the presence of even small items several

feet away. When something such as a human or box blocks the path, the transporter politely responds. For example, it might simply say, "Vehicle is approaching," which should prompt humans to clear the path.

In case a transporter gets into a jam, a human can take manual control via an attached handset with a joystick used to control the transporter's movement. After typing in an access code, you can make the transporter go wherever you desire.

Robots Need Breaks, Too

Similar to humans, robots need to fuel up, clean themselves, and occasionally have repairs done. The ATS central computer, for example, tracks the transporters' battery charges and maintenance records. Nickel cadmium (NiCad) batteries on board each transporter provide about five hours of continuous operation.

If a battery runs low, the central computer adds a "gas stop" to the transporter's schedule. The transporter simply parks over a charging spot, and connections and charging actions occur automatically. Many charging locations are conveniently located next to elevators and service areas. Battery power for the transporter can be allowed to run low because a place to recharge is always located nearby.

As part of a preventive maintenance program, the central computer instructs transporters to take carts to an automatic cart wash for cleaning. This resembles a common automatic car wash that you find at many gas stations. The transporters drop off the cart in position for the cart to automatically go through the cart wash. The transporters themselves are sanitized by hand once each week.

If more serious maintenance is due, the central computer directs the transporter to a special maintenance area. Real people (not robots) then perform the maintenance as needed.

Chosen Development Environment

The centralized computer runs FMC Technologies' AGV Manager software that controls the ATS. The AGV Manager integrates several programs together, which send and receive commands to and from the transporters, elevators, cart washers, operator displays, and other interface equipment. The AGV Manager operates on a Windows-based platform, and the programs were written using C++ and Visual Basic. FMC preferred this platform to ease training requirements, and to maximize the comfort level of support personnel. Each transporter has software on board to control its movement. The operating system on each transporter is Phar Lap, which FMC Technologies chose for robustness and good real time control. Phar Lap is a Windows-friendly, real-time operating system.

Both the AGV Manager and transporter software have a development layer and application layer. The development layer is a standard release that is identical for all FMC Technologies installations. The application layer is written in a FMC Technologies programming language called A+, which enables developers to customize the system and transporters for a specific project.

Wireless LAN Provides Connectivity

All instructions between the AGV Manager and the transporters take place using TCP over an 802.11 (2.4-GHz) WLAN. In fact, each transporter is a node on the network, complete with its own IP address.

Generally, the AGV Manager and transporters remain in constant communications. The AGV Manager receives a current status message from each transporter once each second. This data provides information regarding the transporter's current health and position, an essential element in the operation of the transporters. Without instructions from the AGV Manager, the transporters stop operating.

Coverage Holes a Potential Problem

As with many other mobile applications, small coverage holes may exist, causing the transporters to occasionally lose touch with the WLAN.

This is primarily caused by difficulties in providing complete coverage within a hospital environment (primarily because of the somewhat RF-hostile concrete-and-steel construction). Also, the constant movement of large groups of people (such as visitors, doctors, and medical students) offers varying attenuation that results in erratic coverage.

When humans use a WLAN, they instinctively adapt to coverage holes by moving to an area having stronger signals. We are all accustomed to doing this with cellular telephones. If the telephone does not work in a particular area, you move to where the telephone works better. Similarly, a transporter is permitted to continue three moves along its current route if it loses connectivity. This distance is typically approximately 8 feet and amounts to about 15 seconds, based on the speed of the transporter.

In other words, the transporter is able to cruise on its own for a short time without communication. This could make some people nervous, but remember that the transporter has extremely good obstacle-avoidance mechanisms! If communication is lost for an extended period of time, the transporter stops, and the AGV Manager notifies the appropriate personnel of the condition.

Challenges to Think About

FMC Technologies claims that the biggest challenge in implementing the ATS was developing "mistake-proof" software. Mistake-proofing involves automating as much of the process as possible by removing operator actions. This requires the programmer to consider all the actions that could be made by the operator or transporter, and to eliminate them with additional processes and verifications. Because of the complexity of the ATS controlling 46 robots around a hospital, this is not easy. Mistake-proofing the ATS required extensive software testing, and reviews by peers and managers. The result is a system that is less susceptible to system instability, and being safe to use in a hospital environment.

The primary nontechnical challenges impacting the OSUMC are space recovery and the many operational changes that must take place. Over the years, many different OSUMC departments had to use space around the elevators on various floors. OSUMC had to

recover this space for the ATS to use for recharging and elevator-access functions. This meant working with the individual departments to evaluate their uses of the space and help them look at alternatives. Naturally, making changes like this and accepting the idea of having robots take on large labor-intensive efforts once performed by people goes against human nature. Considerable education must take place to prepare people to accept the changes.

Certainly, the development of a mobile wireless system such as the ATS is a monumental project, something that you do not want to try without some solid experience with similar solutions. The combination of logistics, robotics, and wireless connectivity in a hospital environment requires proven experience, dedication, and a bit of trust in the developers.

Hospitality

Hospitality establishments check customers in and out and keep track of needs such as room service orders and laundry requests. Restaurants need to keep track of the names and numbers of people waiting for entry, table status, and drink and food orders. Restaurant staff must perform these activities quickly and accurately to avoid making patrons unhappy. Wireless networking satisfies these needs very well.

Wireless computers are very useful in situations where there is a large crowd, such as a sports bar restaurant. For example, someone can greet a restaurant patron at the door and enter his name, the size of the party, and smoking preferences into a common database via a wireless device. The greeter can then query the database and determine the availability of an appropriate table. Those who oversee the tables use a wireless device to update the database to show whether the table is occupied, being cleaned, or available. After obtaining a table, the waiter transmits the order to the kitchen via the wireless device, eliminating the need for paper order tickets. Keep in mind, however, that the wireless network approach in finer restaurants may not be appealing to patrons. In that case, the patrons may expect waiters to memorize their orders.

Voice over WLAN

Voice over WLAN (VoWLAN) systems are an extension to wired VoIP systems and an alternative to traditional analog and digital voice communications. VoWLANs offer significant benefits of providing mobility and wirelessly converging voice with data applications. With VoWLANs, hospitals, enterprises, retail stores, warehouses, and homeowners can reduce telephony costs and enable mobile applications.

Examples of the systems that VoWLANs can replace include the following:

- Wired telephones
- Cellular telephones
- 2-way radios

With VoWLANs, individuals and teams can use VoWLAN phones to communicate by voice over the WLAN to others inside and outside a facility. The experience is similar to using a traditional wired telephone; however, the user is free to roam about the building where Wi-Fi has been deployed. Furthermore, a VoWLAN phone can operate from many of the growing Wi-Fi hotspots, allowing a person to make use of the same mobile phone while within or away from the office or home. Some cellular phones incorporate VoWLAN capability, which allows users to make calls over traditional cellular networks when no WLAN is available and then switch to a WLAN seamlessly when the user roams onto the Wi-Fi enabled network.

Figure 1-1 illustrates the basic usage models of a VoWLAN system. The optimum approach depends on user requirements and existing telephone hardware.

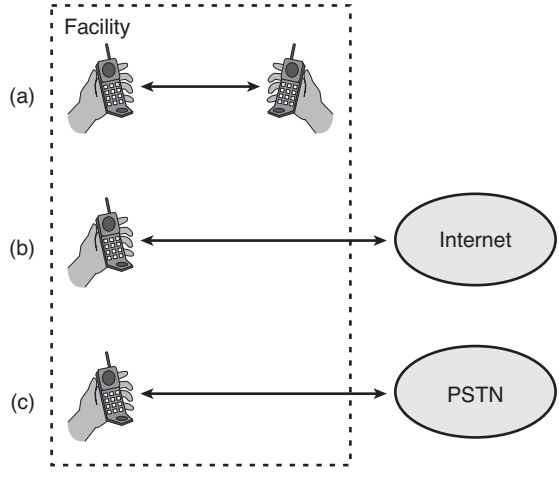


Figure 1-1 *VoWLAN Usage Models: (a) Local-Only, (b) Telephone via Internet, Telephone via PSTN*

Case Study: USC University Hospital

At the USC University Hospital, as with other hospitals, doctors and nurses must have immediate contact with each other to quickly implement solutions for patients. An issue at this hospital, however, was that the existing standard telephone system was ineffective because it did not provide mobility. To contact a doctor, for instance, someone would send a message to a pager with the phone number to call. Because doctors and nurses are constantly on the move, they generally had to leave each other voice messages. The resulting phone tag significantly slows down communication and introduced inaccuracies. It is easy to misinterpret a voice message without interacting with the person leaving the message. In addition, the delays necessary for follow-up are not acceptable for adequate patient care.

Instead of relying on cellular technology, which did not provide full coverage, the hospital decided to move forward with a VoWLAN system. This enabled hospital staff to use VoWLAN phones that connect wirelessly to the hospital's PBX system. The hospital went forward with the deployment without conducting a formal ROI study; however, the resulting VoWLAN solution is paying off in leaps and bounds for this hospital. Now, the entire mobile staff can contact each other directly without delay.

The hospital considered using a 900-MHz cellular solution, but 802.11 was chosen instead because of the future needs for wireless data applications. VoWLAN phones were given to all staff who move around a lot, such as doctors, nurses, IT personnel, and maintenance staff.

As part of the deployment, the hospital connected available phone ports on their existing Nortel PBX to Cisco VG200 voice gateways, which translate the digital signals to IP. The hospital did not plan on any additional phone traffic because they figured that the users would use their new wireless phones in place of their standard phones. In some applications, however, the introduction of mobile phones increases overall phone traffic because of enhanced communications. For example, a maintenance person repairing an air conditioning unit may use their mobile phone to call someone to look up a part number rather than walk back to their desk and look up the information themselves.

Eighty WLAN access points were installed and connected to a separate VLAN for security purposes. To determine optimum access point installation locations, the hospital conducted an RF site survey. It is important to ensure high enough signal strength and cells overlap throughout the hospital to maintain effective operation of the phones and roaming.

The entire VoWLAN system rollout took 120 days from start to finish, which is typical of other VoWLAN deployments of this size and scope. The price tag was approximately $500,000 in equipment and $300,000 in services. Without a formal return on investment (ROI) study, it is difficult to fully assess the feasibly of this solution, but the hospital officials claim that it is definitely a success.

Video Surveillance

Several companies, such as Linksys and D-Link, sell small video cameras that relay moving images to monitors and recording devices over WLANs. The installation of these cameras is much easier than traditional ones because there is no need to run wires between the cameras and the company's network. The video signals flow over a WLAN and into a video server or PC. As a result, a company can set up a Wi-Fi video surveillance system much faster and in scenarios where it is not feasible to install traditional wired cameras.

Wireless video surveillance is beneficial for many industries. For example, the San Mateo County installed Wi-Fi video cameras around the courthouse while the Scott Peterson trial was taking place. With this system, security officials could keep a continual eye on crowds and their behavior. In addition, public facilities, such as hotels and shopping malls, use Wi-Fi cameras to watch over shopping areas, inside elevators, and exit doors.

Enterprises are also taking advantage of Wi-Fi cameras to monitor lobby entrances and parking lots.

Home and Small Office

With a WLAN, employees can bring laptops home from work and continue working just as they do from their offices. For many professions, this makes it possible for people to work from home more effectively, whether it is to spend a few more hours researching on the Internet or to enable telecommuting on a daily basis.

Of course with a wireless laptop, a person can truly work from any place in the house. There is nothing tying you down to a desk in a particular room. You are free to use the Internet or access files on other computers while relaxing in a comfy chair in front of a TV, lounging on the patio breathing fresh air, or sitting at a desk in a quite bedroom.

WLANs at home are good for PCs, too. Unlike companies, Ethernet cabling in homes is nearly nonexistent. That makes wireless is the best way to connect stationary PCs to the network. You will have much more flexibility in locating a PC to any part of the house without being near the broadband modem.

Many homes now have more than one computer. After purchasing a new PC, homeowners will generally hold on to the older PC. It might not be the best for running some of the newer games, but it still offers a good station for browsing the Web and interacting with e-mail. Of course, some people will also bring a laptop home from work or purchase one instead of upgrading to a newer PC.

With multiple computers, it is extremely beneficial for home uses to connect to the same broadband connection. Because of the ease of installation, a WLAN is the best solution for sharing access to the Internet and other PCs in the home. Just be sure to install a WLAN router (not an access point) to ensure that you have Network Address Translation (NAT), Port Address Translation (PAT) and Dynamic Host Configuration Protocol (DHCP) services necessary for all the computers to share a single official IP address supplied by your Internet service provider.

Without a WLAN, most home users must cable their printer directly to a PC or the Ethernet connector on the broadband modem. This limits the number of places that the printer can reside. Generally, it must sit within a few feet of the PC or modem.

A Wi-Fi print server, however, enables the printer to be accessible from over the WLAN. This makes printer placement extremely flexible. For example, you might find it most useful to have the printer in the family room where you do most of your laptop computing. Or, it might make more sense to have the printer just inside the door that leads to your patio. You can also easily move the printer to new locations whenever you want to.

General Enterprise Systems

In the past, the implementation of a WLAN was relatively expensive, compared to the higher-performing Ethernet networks. This required a WLAN application to provide a tremendous gain in efficiency to make it cost-effective. As a result, many existing applications of WLANs are in markets such as healthcare, warehousing, and retail, where mobility provided efficiency gains capable of significantly lowering operational costs. With WLAN prices continuing to drop and performance increasing with 802.11n, though, many enterprise information system managers are beginning to seriously consider the use of WLANs rather than traditional Ethernet. The benefits are to provide mobile and portable access to general network functions such as e-mail, Internet browsing, access to databases, and so on and to eliminate the time and expense of installing and supporting physical cable. Thus, WLANs are now effectively satisfying applications in horizontal markets.

An oil exploration company operating in Columbia, South America, experienced high expenses when relocating its drilling rigs. The oil drilling setup requires two control rooms in portable sheds separated 5000 feet from the drilling platform to provide 500-kb/s computer communication between the sheds and the drilling rig. The existing communications system consisted of Ethernet networks at each of the three sites. Each shed had four PCs running on the network, and the drilling site had one PC for direct drilling-control purposes.

Every time the oil company needed to move to a different drilling site, which occurred four or five times each year, it had to spend between $50,000 and $75,000 to reinstall optical fiber through the difficult terrain between the sheds and the drilling platform. With rewiring expenses reaching as high as $375,000 per year, the onsite system engineer designed a wireless point-to-point system to accommodate the portability requirements to significantly reduce the cost of relocating the drilling operation. The solution includes a spread-spectrum radio-based wireless system that uses directional antennas to establish point-to-point communication between the sheds and the drilling platform.

The cost of purchasing the wireless network components was approximately $10,000. Wherever the oil company now moves its drilling operation, it will save the costs of laying a new cabling infrastructure between the sites.

Location-Aware Wireless Applications

More and more companies are now beginning to apply location-based services over wireless networks to enable rather interesting enhancements to applications. In general, a location-based system (LBS) keeps track of the position of users on the network as they roam throughout the facility. A centralized system collects and integrates this positioning information to drive additional functions that identify the position of users in relation to the facility and pertinent areas, such as information booths, emergency centers, stores, products, and so on.

Within healthcare facilities, doctors, nurses, and sometimes patients, are very mobile. As a result, many hospitals have WLANs to support patient monitoring, electronic patient

records, and narcotics tracking. In this situation, an LBS can also track doctors throughout the hospital, which enables a nurse to know whether a particular doctor is nearby and able to take care of a specific emergency.

In addition, an LBS enables hospital staff to track the whereabouts of patients, and if they go astray or anything adverse happens to them, an alarming system will alert the closest doctors and nurses. For example, some homes for the elderly implement LBSs over WLANs to trigger an alarm when patients try to leave the facility.

Hospitals also need to track expensive equipment that is often required to save lives. An LBS enables hospital administration to know the exact location of this equipment for accountability and usability purposes. If a nurse needs a specific portable x-ray machine in the emergency room, stat, the LBS can display where to find it. If it leaves the facility, chokepoints can be installed in major corridors or exits showing when a piece of equipment or a user leaves a given area of the hospital or passes through an exit where a chokepoint is installed.

Department stores and shopping malls can reap huge benefits from LBSs. A customer can use his or her PDA to download an interactive store map and find the exact location of any item within the store. By entering a few search criteria, the PDA can provide a description of where the item has been moved to on the WLAN. The same concept also applies to shopping malls. A WLAN can cover the entire parking lot and inside of a large shopping mall, and customers using a wireless PDA are able to more easily find stores. Once a customer is in the mall, a real-time map constantly shows the shopper where each store is in relation to his/her position. The LBS can also send promotions from specific stores as shoppers pass by them.

An LBS also provides convenience to people in large public areas. In a convention center, for example, a wireless user can take advantage of moving maps that identify meeting rooms, position of vendors on a tradeshow floor, and emergency exits in relation to the position of the user.

As a patron using a wireless PDA passes a specific display case at a museum, an LBS can download voice and possibly video information describing the contents of the display. The user can move about the museum and receive location-based information, which enhances the learning and enjoyment of the visitor.

Similar to a convention center, wireless users within an airport can also easily find their way around using an LBS solution. For example, the LBS can display routes to various locations, such as restaurants, coffee shops, and emergency exits. Tenants within the airport can also display location-aware advertisements, which offer the airport a revenue stream for advertising in addition to network access.

An LBS system can make the job of security guards immensely easier. The security control room can constantly track the position of every guard, alerting them when there is an incident occurring in their area. All of this traverses the WLAN. Of course, this means that the WLAN requires enhanced security mechanisms to ensure this information is not available to thieves.

Because of the vast amounts of data, such as maps and tracking updates, that an LBS generates, the higher performance and reliability of 802.l1n is imperative. This is especially true when supporting LBS in addition to other wireless applications, such as voice.

Case Study: Acme Healthcare is Ready to Go Wireless

Acme Healthcare is a fictitious 250-bed acute care hospital that surfaces throughout this book to emphasize the primary considerations when deploying an 802.11n wireless network.

Acme Healthcare serves the healthcare needs of a medium-sized community in the United States. The hospital has very few wireless networks, which are mainly operated independently by several of the clinics. The existing networks are a mix of 802.11b and 802.11g networks, and they primarily serve connections between laptops and the hospital's healthcare information system.

The hospital CIO, Arthur, has attended a couple of healthcare conferences and learned that many of the other hospitals are in the process of deploying WLANs to support mobile applications, such as voice communications, electronic medical records, x-ray image distribution, video surveillance, asset tracking, patient monitoring, and foreign language translator systems. Arthur envisions similar applications and substantial resulting benefits for his hospital. With the masses of baby boomers getting older, Acme Hospital's profit has been increasing steadily over the past few years, and Arthur is now ready to move forward with a hospital-wide wireless system.

Note Upgrade your existing network to 802.11n to support higher-speed mobile applications and avoid implications of the legacy WLANs (802.11a, 802.11b, and 802.11g) possibly becoming obsolete within the coming years.

Benefits of Wireless Networks

The emergence and continual growth of WLANs are being driven by the need to lower the costs associated with network infrastructures and to support mobile networking applications that offer gains in process efficiency, accuracy, and lower business costs. The following sections explain the mobility and cost-saving benefits of WLANs so that you can better justify the expense of deploying a WLAN.

Mobility

Mobility enables users to move physically while using an appliance, such as a handheld PC or data collector. Many employers require their employees to be mobile in an effort to increase efficiency. Inventory clerks, healthcare workers, policemen, and emergency care specialists, for example, are ideal candidates to benefit from wireless mobility.

Of course, wired networks require a physical tether between the user's workstation and the network's resources, which makes access to these resources impossible while roaming about their work environment.. Wireless mobility increases the users' freedom of movement and results in significant return on investment because of gains in efficiency.

Mobile applications requiring wireless networking include those that depend on real-time access to data, which is usually stored in centralized databases. If your applications require mobile users to be aware immediately of changes made to data, or if information put into the system must immediately be available to others, you have a definite need for wireless networking. For accurate and efficient price markdowns, for example, many retail stores use wireless networks to interconnect handheld bar code scanners and printers to databases having current price information. This enables the printing of the correct prices on the items, making both the customer and the business owner more satisfied.

Note As compared to legacy WLANs, 802.11n offers greater range, which improves user mobility.

Installation in Difficult-to-Wire Areas

The implementation of wireless networks offers many tangible cost savings when performing installations in difficult-to-wire areas. If rivers, freeways, or other obstacles separate buildings you want to connect, a wireless solution may be much more economical than installing physical cable or leasing communications circuits, such as T1 service. Some organizations spend thousands or even millions of dollars to install physical links with nearby facilities. 802.11n bridges, coupled with directional antennas, can easily provide wireless connectivity over thousands of feet, depending on obstacles along the path.

The asbestos found in older facilities is another problem that many organizations encounter. The inhalation of asbestos particles is extremely hazardous to your health; therefore, you must take great care when installing network cabling within these areas. When taking necessary precautions, the resulting cost of cable installations in these facilities can be prohibitive.

Some organizations, for example, remove the asbestos, making it safe to install cabling. This process is very expensive because you must protect the building's occupants from breathing the asbestos particles agitated during removal. The cost of removing asbestos covering just a few flights of stairs can be tens of thousands of dollars. Obviously, the advantage of wireless networking in asbestos-contaminated buildings is that you can avoid the asbestos removal process, resulting in tremendous cost savings.

In some cases, it might be impossible to install cabling. Some municipalities, for example, might restrict you from permanently modifying older facilities with historical value. This could limit the drilling of holes in walls during the installation of network cabling and outlets. In that situation, a wireless network might be the only solution. Right-of-way restrictions within cities and counties might also block the digging of trenches in the ground to lay optical fiber for networked sites. Again, in this situation, a wireless net-

work, especially an 802.11n system because of its superior range over legacy systems, might be the best alternative.

Increased Reliability

A problem inherent to wired networks is downtime because of cable faults. Moisture erodes metallic conductors via water intrusion during storms and accidental spillage or leakage of liquids. With wired networks, a user might accidentally break his network connector when trying to disconnect his PC from the network to move it to a different location. Imperfect cable splices can cause signal reflections that result in unexplainable errors. The accidental cutting of cables can bring down a network immediately. Wires and connectors can easily break through misuse and normal use. These problems interfere with users' ability to use network resources, causing havoc for network managers. An advantage of wireless networking, therefore, results from the use of less cable. This reduces the downtime of the network and the costs associated with replacing cables.

Reduced Installation Time

The installation of cabling is often a time-consuming activity. For LANs, installers must pull twisted-pair wires or optical fiber above the ceiling and drop cables through walls to network outlets that they must affix to the wall. These tasks can take days or weeks, depending on the size of the installation. The installation of optical fiber between buildings within the same geographical area consists of digging trenches to lay the fiber or pulling the fiber through an existing conduit. You might need weeks or possibly months to receive right-of-way approvals and dig through ground and asphalt.

The deployment of wireless networks greatly reduces the need for cable installation, making the network available for use much sooner. Thus, many countries lacking a network infrastructure have turned to wireless networking as a method of providing connectivity among computers without the expense and time associated with installing physical media. This is also necessary within the United States to set up temporary offices and rewire renovated facilities.

Long-Term Cost Savings

Companies reorganize, resulting in the movement of people, new floor plans, office partitions, and other renovations. These changes often require rewiring the network, incurring both labor and material costs. In some cases, the rewiring costs of organizational changes are quite substantial, especially within large enterprise networks. A reorganization rate of 15 percent each year can result in yearly reconfiguration expenses as high as $750,000 for networks that have 6000 interconnected devices. The advantage of wireless networking is again based on the lack of cable; you can move the network connection by just relocating an employee's PC or IP phone.

Productivity Gain Is the Answer

For compelling reasons to install WLANs, you need to show continual productivity benefits. For example, consider using 802.11-equipped laptops. This enables users to read and respond to e-mail and browse the Internet during office meetings, assuming the user can be responsive when needed at the meeting while plunking away at their laptop. Even though this seems trivial, the productivity gains can be significant.

Assume a person attends three hours worth of meetings each day. If the user spends approximately 15 minutes per hour responding to e-mail and other Internet-related tasks during each meeting, the user will have 45 minutes more time each day to work on other tasks. This seems pretty reasonable, considering the average person and office setting.

A 45-minute productivity gain equates to company cost savings that depend on the person's cost per hour. At $50 per hour, the savings will be $37.50 per person-day. A smaller company with 20 users will save $750 per day, $15,000 per month, $180,000 per year, and so on. After including WLAN installation costs, you may see a positive ROI in just a few months. Even if you factor in the cost of new laptops for everyone, you should still see a positive ROI in less than 1 year.

As a result, the use of WLANs can prove financially beneficial in common office environments, even if it only enables people to make better use of their time during meetings. Once a WLAN is in place, however, you will surely think of additional productivity-enhancing applications.

Determining Benefits of a VoWLAN System

The calculation of savings resulting from a VoWLAN solution includes the combination of quantitative and qualitative benefits. Let's take a look at each of these types of benefits and see how they can help justify VoWLAN costs.

Quantitative Benefits

The quantitative benefits comprise the actual dollar savings resulting from the deployment of a VoWLAN solution. This is generally cash that a company avoids paying for particular services, but it can also include sales of hardware that the VoWLAN system is replacing. The following are the types of quantitative benefits that you can realize with a VoWLAN solution:

- **Reduced long-distance telephone charges:** The routing of inter-company VoIP telephone calls is nearly free; therefore, a VoWLAN system can eliminate the long-distance charges (toll bypass) associated with each VoWLAN user.
- **Fewer wired telephone lines:** A company can eliminate the need for a wired telephone line for each VoWLAN user, which saves any associated fees. Because VoWLAN users are wireless, there is no need to rewire telephone lines when changes are made to the workforce.

- **Increased productivity:** This one is somewhat difficult to define in some cases, but it allows employees to complete work faster and better server customers. This results in higher revenues for the company, which is certainly a benefit.

Qualitative Benefits

Qualitative benefits enhance the operation of the company, but they do not result in definable dollar savings. These types of benefits often lean management toward funding the project when quantitative benefits are marginal or not well defined. The following are the types of qualitative benefits that you should consider when performing a ROI study for a VoWLAN solution:

- **Improved safety:** This is certainly important to any company. In some cases, the regular use of VoWLAN phones can provide vital and immediate communications in the time of emergency situations.
- **Better image to customers:** With the use of VoWLAN phones, customers will see company employees getting things done faster and more efficiently, which makes the customer more inclined to do business with the company.
- **Increased employee moral:** Employees equipped with VoWLAN handsets have less frustration by eliminating telephone tag and searching for phone when they need one.

Note For details on implications of WLANs, such as radio frequency interference and security issues refer to Chapter 4, "Wireless LAN Implications."

Wireless Network Technologies

In most cases, a standards organization defines the specific protocols and radio technology, and an industry group certifies the products based on the standard. The most relevant example of this is the IEEE 802.11 Working Group, which defines the 802.11 standard for WLANs, and the Wi-Fi Alliance, which provides interoperability testing for 802.11 products. A similar relationship exists between IEEE 802.16 Working Group and the WiMAX Forum.

802.11n-based WLANs are what you should deploy today, but there are several different types of WLANs existing in companies and organizations. As a result, it is important that you understand the different WLAN types and their capabilities. In most cases, especially if there is an existing wireless network, it will be cost-effective to deploy an 802.11n WLAN and make use of the existing legacy networks. Over time, as the needs arise and the funding is available, you should focus on migrating all users and applications to 802.11n.

The following sections provide a brief overview of the wireless network specifications and standards. The emphasis of this book is on IEEE 802.11-compliant WLANs because

802.11 is expected to continue being the preferred standard for supporting WLAN application. Other technologies, such as 802.16 (WiMAX), 802.15 (Bluetooth), Wireless USB and ZigBee, may better suit your needs in some situations, however. As a result, this chapter provides a brief overview of these non-802.11 technologies.

IEEE 802.11 (Wi-Fi)

Wireless LAN technologies offer wireless connectivity within building, campus and city-wide environments. Figure 1-2 illustrates the basic concept of a WLAN. The 802.11 standard has been evolving for more than a decade, resulting in today's 802.11n and several legacy standards (refer to Figure 1-3).

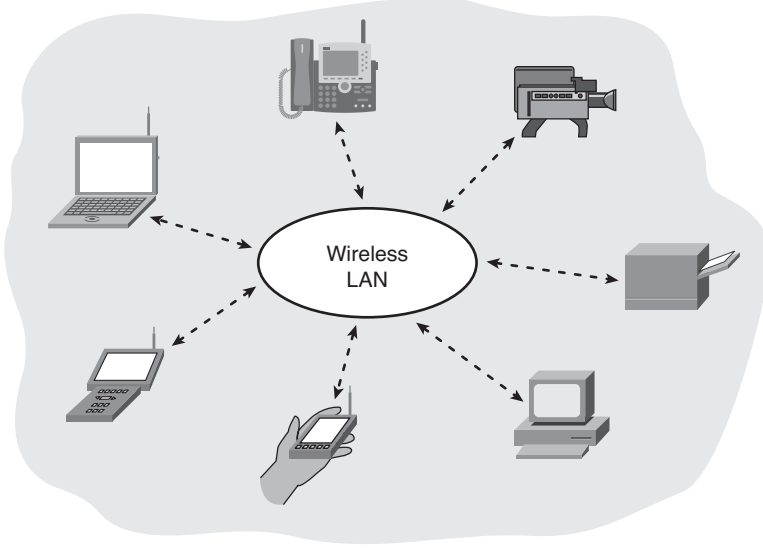


Figure 1-2 *Wireless LANs Support Wireless Communications Among a Variety of Client Devices*

Initial 802.11

The initial IEEE 802.11 WLAN standard, ratified in 1997, specifies the use of both direct-sequence spread-spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) for delivering 1-Mb/s and 2-Mb/s data rates in the 2.4-GHz band. DSSS and FHSS are different forms of transmitting data over a WLAN. The lower data rate provided by this initial standard was more than enough bandwidth at the time to support bar code applications, which were the first commercial uses of WLAN technology. In general, however, the products based on this initial standard did not proliferate because of their high costs. In addition, some of the wireless data collector vendors were reluctant to move from proprietary wireless technologies to 802.11-based devices, primarily because they wanted to continue selling their own wireless base stations and only allow their data collectors to operate on it.

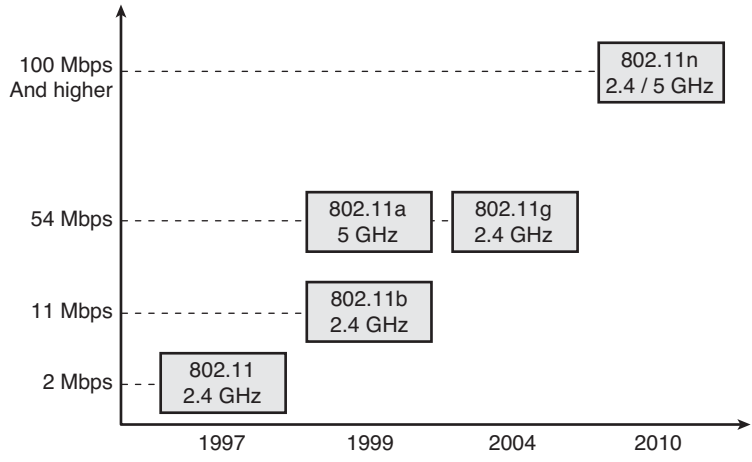


Figure 1-3 *IEEE 802.11 Standardization Has Led to Higher Performance*

802.11a

In 1999, the 802.11 group ratified the 802.11a standard, which offers data rates up to 54-Mb/s in the 5-GHz band using orthogonal frequency-division multiplexing (OFDM). Even though the 802.11a standard was available in 1999, 802.11a access points and radio cards did not become commercially available until several years later. The primary reasons for the delay to market were the difficulties in developing 5-GHz, 802.11 hardware and the weak market potential for WLAN components that do not interoperate with the existing 2.4-GHz WLANs. 802.11a products have been available now for several years, but their use is somewhat limited to specialized applications, especially where high performance was necessary (and interoperability with 2.4-GHz systems was not necessary).

A significant advantage of 802.11a is that it offers very high capacity compared to other legacy WLANs. The reason is that the 802.11a, 5-GHz spectrum defines a greater number of RF channels that do not overlap in frequency. Another advantage of 802.11a is that it operates in the 5-GHz band, which is mostly free from sources of RF interference. Microwave ovens, Bluetooth devices, most cordless phones, and the majority of neighboring WLANs operate in the 2.4-GHz band of frequencies. The lower noise floor in the 5-GHz band affords lower retransmissions rates and higher resulting throughput as compared to 802.11b and 802.11g systems.

802.11b

To provide higher data rates when operating in the 2.4-GHz band, the 802.11 group also ratified the 802.11b physical layer in 1999, enhancing the initial DSSS physical layer to include additional 5.5-Mb/s and 11-Mb/s data rates. Soon after ratification of the 802.11b standard, 802.11b access points and radio cards began shipping with those improvements. It was a fairly easy modification to existing 802.11 DSSS devices to become 802.11b-compliant. In fact, most users could upgrade their existing access points and radio cards

with simple firmware upgrades. For several years, 802.11b devices proliferated throughout the industry and became the most commonly installed WLAN hardware.

Unfortunately, a great deal of RF interference, resides in the 2.4-GHz band, which impacts 802.11b users. A microwave oven can cause significant degradation in throughput because radio waves from a microwave oven can block 802.11b (and 802.11g) radio cards from accessing the medium or create bits errors in the 802.11 frames in transit. The potential for RF interference in the 2.4-GHz band is one reason why a company would strongly consider using 5-GHz solutions.

A limiting factor of 802.11b is that it supports only up to three non-overlapping radio cells in the same area. The 2.4-GHz frequency spectrum is roughly 90-MHz wide, and an 802.11b radio card or access point uses approximately 30-MHz when transmitting. To avoid inter-access point interference (also referred to as co-channel interference), 802.11b access points must be set to specific channels. For example, access points in the United States can be set to channels 1, 6, and 11 to avoid overlap and mutual interference. This is especially important if there are many active wireless users. As a result of this frequency plan and limited data rates, 802.11b has limited capacity (and data rates).

802.11g

802.11g, ratified in 2004, further enhances 802.11b to include data rates up to 54-Mb/s in the 2.4-GHz band using OFDM. 802.11g is backward compatible with 802.11b, which is referred to as *802.11b/g mixed-mode operation*. For example, an 802.11b radio card can associate with an 802.11g access point. Because of its support for data rates up to 54-Mb/s, 802.11g offers higher performance than 802.11b systems. Capacity is still somewhat limited, however, because 802.11g operates in the 2.4-GHz band, which still limits the number of non-overlapping channels to 1,6, and 11, as with 802.11b. As a result, 802.11g systems have less capacity than 802.11a WLANs. 802.11g, for example, can have up to three non-overlapping channels with 54-Mb/s per channel.

A single 802.11b station associating with an 802.11g access point invokes the use of protection mechanisms, such as request-to-send/clear-to-send (RTS/CTS). The reason that this is necessary is that that 802.11b and 802.11g use different modulation, which means that they cannot interoperate and coordinate transmissions according to the 802.11 protocol. The access point informs all stations that an 802.11b station is present by setting an applicable bit in the body of each beacon frame. As a result, all stations begin using protection mechanisms.

The RTS/CTS protection mechanism requires each station to implement the entire RTS/CTS process for each data frame needing transmission. The problem with this requirement is that throughput suffers because of the RTS and CTS frames. Thus, a mixed environment of 802.11b and 802.11g users significantly degrades the throughput of the WLAN, often by as much as 30 percent, which reduces the number of simultaneous voice calls that the network can support.

This is why most vendors allow administrators to configure access points to allow only 802.11g station associations, referred to as 802.11g-only mode. Of course the problem

with this is that all users must have 802.11g radio cards. 802.11b-equipped devices will not be able to associate with the access point. But, at least the throughput will remain relatively high.

Some vendors also allow you to disable protection mechanisms in mixed mode, which supports both 802.11b and 802.11g connections. This is a good approach if there are a limited number of active users because the probability of 802.11b and 802.11g devices transmitting at the same time is minimal.

Many 802.11g implementations use 802.11b-only mode to avoid interoperability issues and maximize range. Sometimes 802.11b client radios have trouble connecting to 802.11g access points, and administrators often fix the problem by switching the 802.11g access points to b-only mode. 802.11b also has slightly better range because of lower minimum data rate. 802.11b can operate with data rates as low as 1-Mb/s; whereas, 802.11g can only operate as low as 6-Mb/s. The lower minimum data rate operation of 802.11b allows longer-range operation as compared to 802.11g.

In addition, most 802.11g access points set to b-only mode will send beacons as 1-Mb/s instead of 2-Mb/s (which is what 802.11g uses). This extends the reach of 802.11b access points beyond 802.11g access points. In addition, the use of b-only mode eliminates the need for the access point to use protection mechanisms since users are all 802.11b and not a mix of 802.11b and 802.11g.

802.11n

802.11n does a better job than legacy systems (802.11a, 802.11b, and 802.11g) at providing higher performance, availability and predictability of the network because of multiple-input multiple-output (MIMO) operation, channel bonding, and more efficient protocols, such as packet aggregation. With 802.11n, usage of the wireless network is comparable to wired Ethernet connections. In addition, support costs are relatively low because there isn't as much need to continually fine-tune the network as compared to legacy networks. The MIMO technology of 802.11n overcomes interference issues, which improves reliability and reduces the time needed to troubleshoot related problems.

The 802.11n standard, ratified on September 11, 2009, specifies data rates well above 100-Mb/s and at much better throughput than legacy systems. In 2008, the Wi-Fi Alliance started certifying WLAN products based on Draft 2.0 of the 802.11n standard, which offers a solid technology that requires only software upgrades to be compatible with the ratified version of the 802.11 standard. Draft 2.0 802.11n differs from earlier pre-802.11n, which was based on several earlier and differing 802.11n drafts. A problem is that most of the pre-802.11n products do not interoperate between vendors. As a result, it is not likely possible to upgrade pre-802.11n products to the Draft 2.0 or ratified versions of the standard.

802.11n supports operation in both the 2.4-GHz and 5-GHz bands, which provides flexibility for satisfying a multitude of wireless requirements. In addition, 802.11n is backward compatible with 802.11g and 802.11a legacy WLANs, and protection mechanisms are necessary to coordinate access to the network similar to 802.11b/g mixed mode opera-

tion. Of course protection mechanisms impose a great detail of overhead, which hampers throughput. The backward compatibility makes it possible to continue use of existing legacy WLAN devices; however, to achieve the full performance potential of 802.11n, you should implement 802.11n-only devices in the 5-GHz band.

Comparison of 802.11 Standards

Table 1-1 provides a comparison of the different characteristics of the 802.11a, 802.11b, 802.11g, and 802.11n standards.

Table 1-1 *802.11 Standards Comparison*

	RF Spectrum	Max Speed	Compatibility	RF Interference impacts	Date Ratified
802.11a	5-GHz	54 Mb/s	Does not work with 802.11b or 802.11g	Slight	1999
802.11b	2.4-GHz	11 Mb/s	Works with 802.11g	Moderate	1999
802.11g	2.4-GHz	54 Mb/s	Works with 802.11b	Moderate	2004
802.11n	2.4-GHz and 5-GHz	Hundreds of Mb/s depending on the configuration	Works with 802.11g	Slight	2009

Note For more details on the 802.11n amendment to the 802.11 standard, see Chapter 6, "IEEE 802.11 Medium Access Control (MAC) Layer," and Chapter 7, "IEEE 802.11 Physical Layers."

Wi-Fi Certification

The Wi-Fi Alliance (which began its work known as the Wireless Ethernet Compatibility Alliance or WECA) is an international, nonprofit organization focusing on the manufacturing, marketing, and interoperability of 802.11 WLAN products. The Alliance is the group that pushes the term (actually brand) "Wi-Fi" to cover all forms of 802.11-based wireless networking (whether 802.11a, b, g, or n); they also are the group behind Wi-Fi Protected Access (WPA), the stepping-stone between the much-criticized WEP and the 802.11i security standard.

Note For a current list of certified Wi-Fi equipment, refer to the Wi-Fi Alliance website at http://www.wi-fi.org/.