A Guidebook for Mitigating Disruptive WiFi Interference at Airports

DETAILS

98 pages | 8.5 x 11 | PAPERBACK
ISBN 978-0-309-30842-7 | DOI 10.17226/22187

AUTHORS

Michael Carroll, Hollis Stambaugh, Joseph Kolesar, Stephen Berger, Heidi Benaman, and Zachary Varwig; Airport Cooperative Research Program; Transportation Research Board; National Academies of Sciences, Engineering, and Medicine

AIRPORT COOPERATIVE RESEARCH PROGRAM

ACRP REPORT 127

A Guidebook for Mitigating Disruptive WiFi Interference at Airports

Michael Carroll
Hollis Stambaugh
SYSTEM PLANNING CORPORATION
Arlington, VA

Joseph Kolesar
SAGE-SOLUTIONS GROUP, INC.
Arlington, VA

Stephen Berger
TEM CONSULTING, LP
Georgetown, TX

Heidi Benaman
Zachary Varwig
FAITH GROUP, LLC
St. Louis, MO

Subscriber Categories
Aviation • Data and Information Technology

Research sponsored by the Federal Aviation Administration

TRANSPORTATION RESEARCH BOARD
WASHINGTON, D.C.
2015
www.TRB.org

AIRPORT COOPERATIVE RESEARCH PROGRAM

Airports are vital national resources. They serve a key role in transportation of people and goods and in regional, national, and international commerce. They are where the nation's aviation system connects with other modes of transportation and where federal responsibility for managing and regulating air traffic operations intersects with the role of state and local governments that own and operate most airports. Research is necessary to solve common operating problems, to adapt appropriate new technologies from other industries, and to introduce innovations into the airport industry. The Airport Cooperative Research Program (ACRP) serves as one of the principal means by which the airport industry can develop innovative near-term solutions to meet demands placed on it.

The need for ACRP was identified in *TRB Special Report 272: Airport Research Needs: Cooperative Solutions* in 2003, based on a study sponsored by the Federal Aviation Administration (FAA). The ACRP carries out applied research on problems that are shared by airport operating agencies and are not being adequately addressed by existing federal research programs. It is modeled after the successful National Cooperative Highway Research Program and Transit Cooperative Research Program. The ACRP undertakes research and other technical activities in a variety of airport subject areas, including design, construction, maintenance, operations, safety, security, policy, planning, human resources, and administration. The ACRP provides a forum where airport operators can cooperatively address common operational problems.

The ACRP was authorized in December 2003 as part of the Vision 100-Century of Aviation Reauthorization Act. The primary participants in the ACRP are (1) an independent governing board, the ACRP Oversight Committee (AOC), appointed by the Secretary of the U.S. Department of Transportation with representation from airport operating agencies, other stakeholders, and relevant industry organizations such as the Airports Council International-North America (ACI-NA), the American Association of Airport Executives (AAAE), the National Association of State Aviation Officials (NASAO), Airlines for America (A4A), and the Airport Consultants Council (ACC) as vital links to the airport community; (2) the TRB as program manager and secretariat for the governing board; and (3) the FAA as program sponsor. In October 2005, the FAA executed a contract with the National Academies formally initiating the program.

The ACRP benefits from the cooperation and participation of airport professionals, air carriers, shippers, state and local government officials, equipment and service suppliers, other airport users, and research organizations. Each of these participants has different interests and responsibilities, and each is an integral part of this cooperative research effort.

Research problem statements for the ACRP are solicited periodically but may be submitted to the TRB by anyone at any time. It is the responsibility of the AOC to formulate the research program by identifying the highest priority projects and defining funding levels and expected products.

Once selected, each ACRP project is assigned to an expert panel, appointed by the TRB. Panels include experienced practitioners and research specialists; heavy emphasis is placed on including airport professionals, the intended users of the research products. The panels prepare project statements (requests for proposals), select contractors, and provide technical guidance and counsel throughout the life of the project. The process for developing research problem statements and selecting research agencies has been used by TRB in managing cooperative research programs since 1962. As in other TRB activities, ACRP project panels serve voluntarily without compensation.

Primary emphasis is placed on disseminating ACRP results to the intended end-users of the research: airport operating agencies, service providers, and suppliers. The ACRP produces a series of research reports for use by airport operators, local agencies, the FAA, and other interested parties, and industry associations may arrange for workshops, training aids, field visits, and other activities to ensure that results are implemented by airport-industry practitioners.

ACRP REPORT 127

Project 01-23
ISSN 1935-9802
ISBN 978-0-309-30842-7
Library of Congress Control Number 2015932785

COPYRIGHT INFORMATION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

Cooperative Research Programs (CRP) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply TRB or FAA endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from CRP.

NOTICE

The project that is the subject of this report was a part of the Airport Cooperative Research Program, conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by the Transportation Research Board and approved by the Governing Board of the National Research Council.

The opinions and conclusions expressed or implied in this report are those of the researchers who performed the research and are not necessarily those of the Transportation Research Board, the National Research Council, or the program sponsors.

The Transportation Research Board of the National Academies, the National Research Council, and the sponsors of the Airport Cooperative Research Program do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of the report.

Published reports of the

AIRPORT COOPERATIVE RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

COOPERATIVE RESEARCH PROGRAMS

CRP STAFF FOR ACRP REPORT 127

Christopher W. Jenks, *Director, Cooperative Research Programs*
Michael R. Salamone, *ACRP Manager*
Theresia H. Schatz, *Senior Program Officer*
Terri Baker, *Senior Program Assistant*
Eileen P. Delaney, *Director of Publications*
Scott E. Hitchcock, *Editor*

ACRP PROJECT 01-23 PANEL
Field of Administration

John Newsome, *Greater Orlando Aviation Authority, Orlando, FL* (Chair)
Pamela E. Bell, *Ross & Baruzzini, Inc., Bellevue, WA*
John A. Buckner, Jr., *Salt Lake City Department of Airports, Salt Lake City, UT*
Timothy M. Mitchell, *Boeing, Seattle, WA*
Jeffrey Rae, *United Airlines, Chicago, IL*
Dawoud Stevenson, *Savannah Airport Commission, Savannah, GA*
Kiem Hoang, *FAA Liaison*
Alvin Logan, *FAA Liaison*
Aneil Patel, *Airports Council International–North America Liaison*

FOREWORD

By Theresia H. Schatz
Staff Officer
Transportation Research Board

ACRP Report 127: A Guidebook for Mitigating Disruptive WiFi Interference at Airports is a guidebook written for airport leadership and other stakeholders that describes the WiFi interference problems at airports and offers solutions to mitigate disruptions. Interference is addressed in the context of the business and regulatory structure within which airports operate. The guidebook is designed to provide practical assistance for improving WiFi performance by enhancing the ability of airport authorities to identify when radio frequency interference is occurring and then how to eliminate, reduce or at least minimize its impact. The guidebook addresses issues at a variety of types and sizes of U.S. airports with the following considerations:

- Quantification of the extent and magnitude of the interference problems;
- Best technical and business practices to provide accessible, secure service with adaptable band width to meet the needs of all stakeholders;
- Communication and collaboration efforts among parties to maximize the benefits of a cooperative approach;
- Reference designs, adaptable to different airport environments (small, medium, large, dominant carrier, no dominant carrier, and other tenant mix), including security requirements for all stakeholders;
- Techniques for identifying and resolving interference issues outside reference designs;
- Strategic vision that addresses potential impacts due to increasing demand, rapidly evolving technologies, and new uses (e.g., 802.11 ac, HD video, 4G backhaul); and
- Total cost of ownership and return on investment, including intangibles.

Wireless networks have become critical for various operational applications on the airport including baggage reconciliation, aircraft-to-gate data communications, facilities maintenance, and security, among others. In addition to the operational applications, wireless networks have become an expectation of the public which is using an increasing variety of smartphones, tablets, and personal mobile hotspots. These uses compete for the same spectrum and have the potential to create major radio frequency interference that is disruptive to all users.

The FCC ruled that airports could not regulate the use of the WiFi spectrum or prohibit tenants with exclusive leases from installing WiFi in their leasehold areas. FCC staff recommended airports and tenants explore cooperative arrangements and innovative solutions to mitigate disruptive interference.

Airport and airport tenants' dependence on wireless networks is increasing and will compound any interference problems that currently exist. Research was needed to quantify the impacts of interference to the end user and define mitigation solutions.

Under ACRP Project 01-23, research was conducted by System Planning Corporation in association with Sage-Solutions, TEM Consulting, and Faith Group LLC. A survey was sent to 45 airports to obtain information about wireless system interference and disruptions and the extent to which these problems affect operations. More in-depth research was conducted during site visits to 9 airports that represented all sizes of airports. In addition, measurements were taken of the RF spectrum and WiFi utilization for 93 gates and other passenger areas at 23 airports.

CONTENTS

Note: Photographs, figures, and tables in this report may have been converted from color to grayscale for printing. The electronic version of the report (posted on the web at www.trb.org) retains the color versions.

SUMMARY

A Guidebook for Mitigating Disruptive WiFi Interference at Airports

Over time, wireless services at airports have expanded from a voice communication tool for radio communications between air traffic control and pilots or between airport public safety agencies such as police, fire, and airport operations, to a ubiquitous and complex system of voice, data, and video services usually supported through a shared network infrastructure. Today the dominant wireless services utilize the wireless fidelity (WiFi) and cellular networks.

Wireless services, particularly WiFi, are in transition from being high-end amenities, used by relatively few travelers, to technologies commonly used by a majority of travelers and, significantly, also by the airport to support core operational functions. However, these networks often are not viewed or funded as an essential component of an airport's core infrastructure. They are funded and managed in a variety of creative ways, which are understandable given their history, but are proving insufficient for their emerging role at airports. The complexity of the highly technical task of managing these networks requires funding and management structures that are equal to the task. The management structures used at airports must also be appropriate for the larger ecosystem of the WiFi and cellular communities.

The business structures and ecosystem of WiFi and cellular networks, and the companies that create and support them, are a study in contrast. The service quality gives evidence of the differences that result from these contrasting business ecosystems. Complaints about performance and radio frequency interference are increasingly rare from cellular users. However, complaints are common and increasing among users of the WiFi network for data communications. Both WiFi and cellular are wireless service networks that are susceptible to radio frequency (RF) interference; however, business and other non-technical differences are resulting in very different technical outcomes related to RF interference.

A key finding of the research performed to create this Guidebook was that solving RF interference problems often requires dealing with several different issues. An example is the RF interference created by travelers' choices. The market is giving consumers a variety of choices for accessing the Internet. They can use the airport's WiFi service, they might prefer to use the free WiFi provided by an airport coffee shop or airline VIP lounge, or they can access the Internet through their cellular network. Some of these choices have the potential for creating interference to the airport's WiFi network.

The need for a good WiFi plan is critical for an airport to provide wireless capabilities that meet the current and future growth of its use by travelers and employees. Airports must first understand the basic business models of service providers. For example, the cellular network operates in dedicated frequency bands which the cellular operators purchase rights to through a competitive bidding process. These cellular companies have paid billions of dollars for the right to utilize licensed spectrums. In addition, the companies have funded the cost of establishing and operating their own networks. Funding comes from subscribers who each month contribute to a portion of the initial cost of setting up the network and for the ongoing network operating cost. Network operators decide what devices they will allow onto their networks and subscribers must choose a device from among those approved for use on the network. To ensure the quality of their network, the cellular operators have created a device certification through their trade association, CTIA, and rigorously test devices before allowing them onto their network.

In contrast, the WiFi network providers operate in unlicensed spectrums and networks which are built ad hoc, and in some cases with no single entity responsible for the entire network. Travelers have come to expect free WiFi service at an airport, just as they expect lights, air conditioning, and well-maintained bathrooms. Travelers bring their own equipment such as smartphones, laptops, and tablets, and commonly expect to pay no fees to use the airport's network.

In contrast to the cellular network, the revenue stream generated by the WiFi network is much more complex, indirect, and difficult to quantify. Further, there are often discontinuities between the cost of network maintenance and the revenues generated by the network. Users may pay for content, but services like video and voice are only effective if the network provides enough bandwidth. The traveler may be willing to pay for Netflix but then expects the airport to provide the bandwidth to watch that video stream. The result is that a patchwork of revenue sources may be used to fund WiFi networks, including relatively unpopular user fees, advertising, and a variety of commercial support services. Although the WiFi Alliance has a WiFi certification program, no entity has the power to approve devices before they are allowed onto the network. The result is that funding is problematic and the power to manage the network is limited. It is important to understand how airports install and operate their WiFi networks, because any interference problem must be resolved within the structure used to manage the network and within the limits of available resources. Simply put, time and money are limited and solutions to network problems are only viable to the degree that they conform to these realities.

One of the emerging realities is conflicting expectations between some airport managers and travelers. Service expectations of WiFi networks vary widely among both airport network managers and travelers. Some airport managers and travelers have come to view WiFi as part of the necessary infrastructure. Others view WiFi as a free service and fringe benefit. With the rapidly changing environment surrounding WiFi, expectations on all sides extend across a significant range.

Research conducted at airports for this Guidebook uncovered a number of important findings. One is that nobody really understands the range and variation of indoor RF environments. The spectrum measurements made during this study represent one of the few and current broad surveys of the RF environments that exist at airports. A direct consequence of this effort is the initiation of a separate effort led by researchers at the National Institute of Standards and Technology (NIST) to gather spectrum data on an even wider basis so that product developers and network managers can have a better understanding of RF environments they must plan for. This additional effort is being coordinated through the ANSI ASC C63.27 standards committee.

Another finding is that the dominant source of WiFi interference is from other WiFi devices. WiFi operates in shared use bands and a large variety of other types of equipment operate in these bands, particularly in the 2.4 GHz band. Historically there have been many documented cases of interference from other kinds of equipment. For example, microwave ovens, Bluetooth, and cordless phones have all created interference problems. However, in the current research the most common source of interference to WiFi at airports was from other WiFi devices.

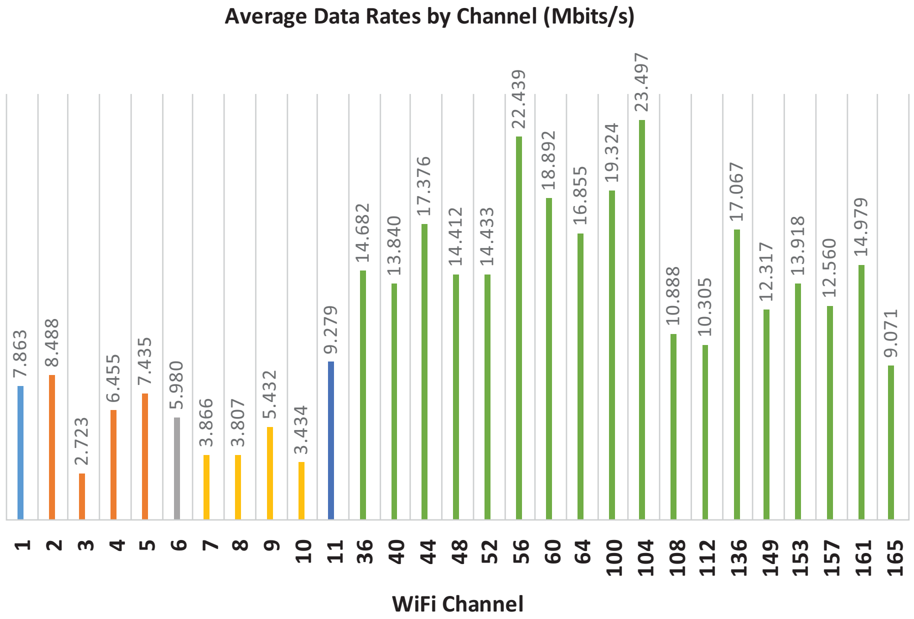


Figure 1. WiFi data rates by channel observed at 28 airports.

The study also showed that there is a strong correlation between band crowding and interference. Repeatedly it was documented that the most significant interference problems occur in the most spectrally congested locations and on the most heavily used channels. It could be said that interference problems largely can be attributed to crowding in the 2.4 GHz band, where data rates averaged under 6 MBs, compared to channels in the less crowded 5 GHz band, where data rates were significantly higher, nearly reaching 24 MBs (Figure 1).

When channels become congested and suffer interference, their data rates slow down and the error rates go up and result in data retransmissions. Although packet retransmissions occur routinely in WiFi communications, the common metric is that retransmissions greater than 1% are a symptom of interference in the channel. Overcrowding in the 2.4 GHz band results in lower data rates and a higher level of transmission errors, which require a large number of packet retransmissions, in contrast to the 5 GHz band (Figure 2).

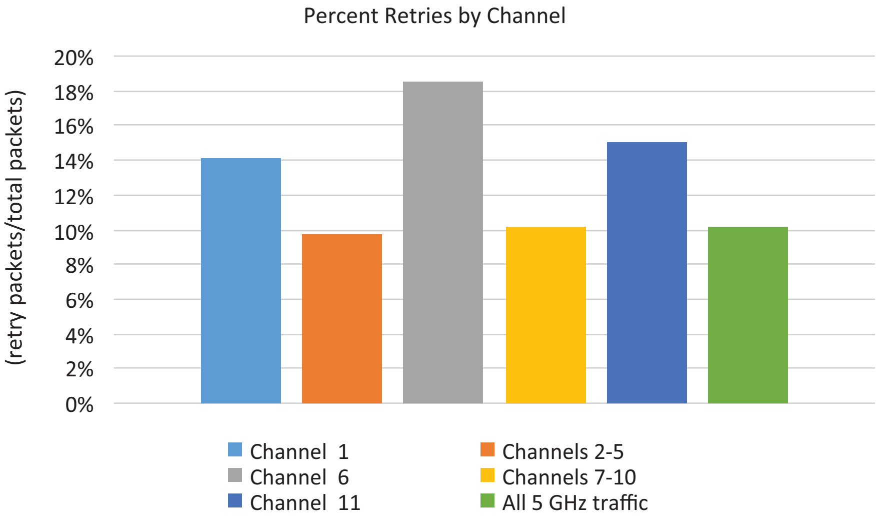


Figure 2. Packet retransmission rates observed at 28 airports.

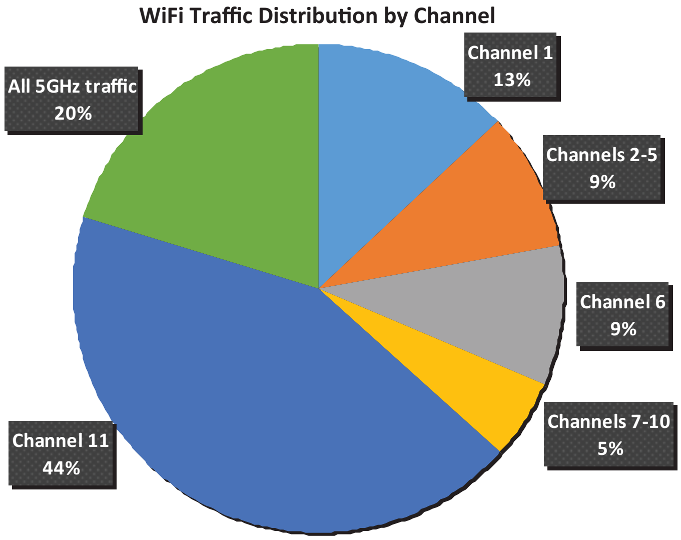


Figure 3. Traffic distribution among WiFi channels.

The crowding is compounded by WiFi traffic that is crowded into two channels of the 2.4 GHz band that together account for 57% of distribution (Figure 3). To make the situation even worse, the 2.4 GHz band is used not only by WiFi but also by Bluetooth, ZigBee, and a wide range of other devices. The 2.4 GHz industrial, scientific, and medical (ISM) band is clearly a victim of its own success. For reasons perhaps not unlike those that require workers to drive downtown in the morning and to the suburbs in the evening, the 2.4 GHz band is host to high levels of congestion and interference, but it nevertheless continues to be where the bulk of the WiFi traffic resides. Radio frequency interference should be addressed strategically, taking into consideration how much wireless networks are used by travelers and by airport operations. A cost-effective RF interference solution is critical for viable service implementation.

An emerging source of interference is largely being created by the need to support two networks in an increasing number of frequency bands. The result is that antennas for the WiFi and cellular networks are often placed close to each other, and at times they share the same antenna in a shared distributed antenna system. Strong RF signals can create intermodulation products and a variety of related problems. These issues are well-known to the military, where many RF sources are often crowded close together on aircraft and ships. The same problems are starting to emerge in airport systems.

Another class of interference problem is created by technology changes. In some cases, innovations made to reduce interference actually end up causing more interference. An example of technology changes causing interference is Institute of Electrical and Electronics Engineers (IEEE) 802.11b. Newer versions of the IEEE 802.11 standard have moved away from direct sequence spread spectrum modulation to orthogonal frequency-division multiplexing (OFDM) modulation. However, support for the older IEEE 802.11b was necessary for backward compatibility. In the research for this Guidebook, it was not uncommon to still find IEEE 802.11b devices operating. However, they often become sources of interference because they are mismatched with how most WiFi devices currently operate.

This Guidebook describes the issues surrounding interference and congestion, and options for solving these problems, including solutions that build on cooperation among all stakeholders and reduce RF interference in ways that provide a good return on investment.

CHAPTER 1

Radio Frequency Primer

This Guidebook includes a primer, or tutorial, on radio frequency (RF) interference that focuses on the complex airport terminal WiFi environment. The primer is provided in its entirety in Appendix A. It explains RF interference associated with WiFi and commercial wireless communications devices in the unlicensed spectrum and the resulting issues for airports and tenants. Written primarily for network engineers, it is a technical guide for that audience.

The following is a brief introduction for non-technical personnel.

Interference is a basic phenomenon described in physics in which two waves superimpose to form a resultant wave of greater or lower amplitude. For example, when two raindrops fall near each other in still water, the rings produced by each travel until they intersect with each other, disrupting the circular ring patterns (Figure 4). This visible analogy is a simplistic view of how RF interference occurs when a radio transmission or radiation from some other device interacts with another radio. However, in the RF domain the environment can be more complex, with one or multiple interferers at overlapping operating frequencies and at the same or different signal strengths from different access points interacting with the "victim" receiver (indicated by the blue arrow in Figure 5). The result can be a disruption, degradation, or limitation of the performance to the victim radio receiver circuitry.

From the airport terminal operations perspective, there are several interacting mechanisms associated with WiFi that can contribute to interference or what appears to be interference. The user and the airport WiFi network have little control over these. They include:

a. Overlapping frequencies in the 2.4 GHz band (assignment of these was done by the FCC).
b. WiFi equipment not containing quality interference-resistant designs and components, as typically found in low-cost commercially available equipment.
c. Multiple versions of WiFi equipment in use.
d. Spontaneous and simultaneous use of WiFi that can cause interference within some localized area(s).
e. Use of rogue WiFi "hotspots" or other such radio transmissions in the airport terminal environment exceeding FCC spectrum regulations.
f. User congestion exceeding network capacity in areas of the airport.

The above independent mechanisms are not always intuitively obvious as to their root cause and can lead to other causes often mistaken as interference. For example, the overlapping frequencies mask the spectrum interference under network behavior such as lowering the throughput. In addition, there is no clear agreement on what is a level of tolerable interference. WiFi equipment responds to the asynchronous demands of the user, which can be simultaneous and lead to congestion through parts of the network. User WiFi equipment in the airport terminal environment can be designed according to different IEEE standards design and manufactured

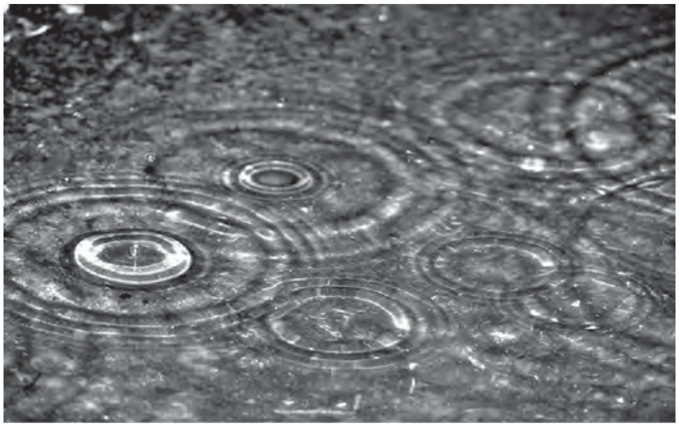
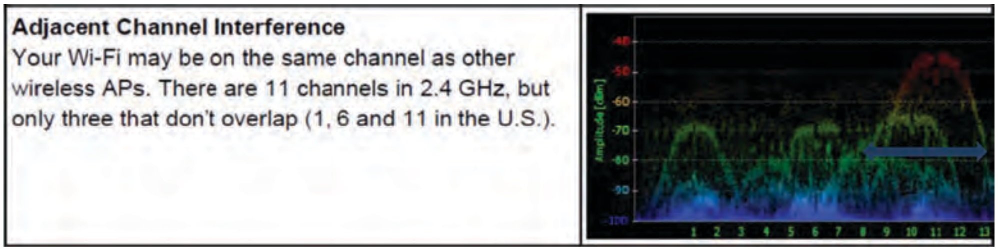


Figure 4. Raindrops illustrating concept of interference.



Adjacent Channel Interference
Your Wi-Fi may be on the same channel as other wireless APs. There are 11 channels in 2.4 GHz, but only three that don't overlap (1, 6 and 11 in the U.S.).

Figure 5. Example of multiple channel WiFi interference.

by different vendors. Such equipment can operate in the same spectrum, but have varying and different susceptibility to interference. It is important for the reader to understand that these mechanisms impact interference through the network differently, and manifest themselves in different ways.

The details of the Radio Frequency Primer are contained in Appendix A, which covers:

- The historical perspective on spectrum regulatory governance, interference mitigation techniques, and tolerable interference acceptance evolution.
- How the Federal Communications Commission (FCC) manages the non-government spectrum and is the regulatory agency that provides rules and regulations on the use of the spectrum.
- A more in-depth overview of interference and perceived misconceptions.
- A process to work through interference incident reports at airports.
- The practical side of how to resolve RF interference issues for airport authorities and tenants.
- Conclusions and a way forward.

CHAPTER 2

WiFi Service at Airports and the Problem of Interference

Wireless communication, most commonly encountered through the use of either wireless fidelity (WiFi) or the cell phone, has become a routine tool for daily life. However, wireless communication is subject to radio frequency (RF) interference. The increasing use and importance of wireless, not only as a passenger amenity but as an integral part of airport operations, makes its reliability and performance critical for modern airport operations. Security is critical too because wireless has become a potential attack vector, a way to disrupt an airport's operation. Thus, a robust secure network that is well-managed and upgraded in accordance with increased demands and applications is a major concern for airport managers.

As part of the research for this Guidebook, team members collected information from airports regarding their experience with WiFi, in particular problems with interference, capacity, and performance. The team was also interested in what solutions had been tried and whether they were successful. Through a distributed survey completed by 18 airports as well as site visits to 9 airports, the researchers gathered background information that helped inform this chapter.

This chapter describes the technical aspects of RF interference, the associated issues, and the potential solutions. While the primer (Appendix A) is written with airport management in mind, it is the information technology network engineer (or contractor carrying out this responsibility) who is the targeted audience for this chapter. Included are processes, techniques, procedures, and applicable tools that can be used to isolate the cause of interference and define solutions to mitigate the problem. Readers will be encouraged to ascertain when interference may be due to causes other than RF emanations—causes such as network congestion, equipment interoperability problems, or simply poor coverage. This chapter also provides recommendations on alternate methods and resources that can be accessed when the problem exceeds the engineer's usual efforts. For smaller airports, which typically do not employ full-time systems engineers, there is a separate chapter, Chapter 6 *WiFi at Small and General Aviation Airports*.

The most appropriate solutions for any given airport will depend upon the airport's goals for WiFi service and the amount of funding available to correct problems and expand capacity.

WiFi at Airports

WiFi service level requirements have rapidly gone from best-effort service being broadly accepted to the current expectation by many travelers that wireless networks have reliability and performance close to that of a wired network. In the early days of WiFi, passengers were pleased to have any wireless service at all and they expected to pay for it. Today, passengers expect connectivity everywhere, with service levels similar to a wired connection or at least equal to the wireless service they enjoy in their homes. As airports and their tenants integrate wireless connectivity into their operations, even higher service levels are necessary and justified.

Service expectations of WiFi networks vary widely among both airport network managers and travelers. Some airport managers and travelers have come to view WiFi as part of the necessary infrastructure. They expect WiFi to work well, just like they expect the lighting to be good and restrooms to be clean and functioning. On the other hand, some airport managers place a lower importance on their airport's wireless network capacity than they do other management issues demanding attention.

Travelers with high expectations for WiFi service will view poorly an airport that does not meet their expectations for seamless communications service. Further, as there are limited opportunities for airport managers and travelers to negotiate and align their expectations, airports that do not provide high quality WiFi may find that a percentage of travelers may choose other airports for departing or connecting flights. Business travelers in particular need reliable Internet connectivity to do work while waiting for flights, especially when flights are delayed or canceled, disrupting business schedules.

At some studied airports, the WiFi network is still viewed primarily as a passenger amenity and service expectations are low. In contrast, others view their network as part of their core infrastructure. These airports tend to take the traveler's experience very seriously and recognize that the quality of a passenger's experience with the network is part of their total airport experience.

Network Management Arrangements

Not surprisingly, there are a variety of network management arrangements. Some airports manage their own WiFi and work directly with cellular network providers for cellular coverage in the terminal. Others contract out both the WiFi and cellular network management, delegating the relationship with cellular providers to their chosen wireless network management company. Once the company is selected, some airports view their responsibility for network management as over, until the next contract negotiation. Other airports have found they must increasingly become more involved in network management and have a close working relationship with their chosen vendor. At several of the largest airports visited, however, airport managers noted they did not have the level of expertise necessary to adequately oversee the work of their network management vendor. These airports have contracted with a second vendor that has in-depth RF and network management expertise to provide measurements and independent input on network operation and the service level provided.

Many airports run parallel services. The free service offers limited data speeds and often requires users to listen to commercials before being allowed to access the Internet. In parallel, paid service is available for a fee, paid either per instance or by subscription. This essentially is attempting to model WiFi after the cellular network. Travelers have a choice. They can access the Internet through their cellular devices and share that connection with their other devices easily.

Table 1 summarizes key aspects of WiFi at nine airports that participated in the case study analysis.

Causes of WiFi Interference and Disruption

Operational Definition

What is considered RF interference? This is not as straightforward as might be imagined. For this study, degradation in performance or disruption of communication was considered interference. A disruption of communication is easy to understand. Users cannot connect to the network, but they should be able to. Something is blocking or disrupting the communication. A degradation of performance is more involved. If packets are lost due to another transmitter,

Table 1. At-a-glance WiFi summary of case study airports.

Topic	ABIA	ACT	BOS	BWI	DFW	GRK	JAN	LAX	SEATAC
Responsible authority	City of Austin Information Technology Department	City of Waco, TX	Massachusetts Port Authority	Maryland Aviation Admin.	Dallas/Fort Worth Airport's Department of Information Technology	City of Killeen, TX	City of Jackson, MS	Los Angeles World Airports	Port of Seattle (a public corporation under King County)
WiFi network management vendor	Boingo (and subsidiary Concourse Comm.)	In-house	AWG (now part of Boingo)	Boingo	AT&T	In-house	Wandering WiFi	AWG (now part of Boingo)	In-house (Boingo provides advertising only)
Flights/day	483	96	882	734	1854	31	137	1674	868
Passengers/year	10,017,158	61,401	30,236,088	22,501,353	60,436,266	174,000	1,200,000	66,667,619	34,824,281
Access point vendor and type	CISCO CleanAir	CISCO 1 access point	CISCO	Aruba	CISCO 1,000 access points	Various	8 CISCO Aironet; 1100 access points	CISCO	CISCO
Bandwidth to Internet	200 Mbps	Not provided	Not provided	Not provided	Approaching 1,000 Mbps	Not provided	Not provided	Not provided	Not provided
Operating metric	95% coverage 95% of the time	No metrics developed	Customer complaints that reach MassPort and complaints to help desk not tracked by MassPort	No routine reporting or testing of network performance or capacity. Customer complaints are monitored via social media and addressed.	User experience is the central metric used. They translate this to mean 8-10 Mbps for every user of the free WiFi.	Customer complaints, however service is judged against a low quality of service expectation because the service is free.	Customer complaints judged against a low expectation for quality of service because the service is free.	Customer complaints	Coverage/Bandwidth/Protocol: Minimum 2 access points at gates (only 6 in whole concourse). Putting in 24 access points in baggage claim area and expanding concessions significantly. 5 Mbps up and down

Note: Mbps= megabits per second.

that is interference. If the communication is slower than it should be when another device is transmitting, that also is considered interference.

There is a difference between interference and interference that causes problems. Some airports run more of their operational functions over the network and they need those functions to operate reliably. Others compete with other airports for passengers and the quality of the traveler's experience is extremely important to them. There are many factors that affect an airport authority's expectations for connectivity and whether they view the degree of interference as problematic or not.

Intentional Interference

The intentional creation of interference has already become reasonably common. It is a growing security risk that must be considered. In the research for this project, one airport reported that occasionally people come to the airport and set up a rogue hotspot using the airport's service set identifier (SSID) in an attempt to get people's login and password information. Rogue hotspots can operate at higher output power than is permitted in the 2.4 GHz unlicensed spectrum and, when doing so, cause interference. Airport managers reported that their network operator had techniques that allowed them to use the network to suppress these fraud hotspots when detected. Presumably, since networks regularly turn their power down to avoid interference, they can also turn their power up to create interference for a fraudulent hotspot. That this airport's network manager had good motives still leaves the fact that people with bad motives can create interference.

As wireless becomes increasingly integrated into an airport's operation, it must also become part of the security planning at the airport. This is particularly true if security cameras and access control devices are connected wirelessly, because a cyber-attack could suppress the wireless connection and therefore circumvent the security system.

When thinking about a security issue of this type, it is typical to think about detection, prevention, and mitigation. If intentional interference is created, how will it be detected and who will be notified? What can be done to prevent intentional interference? If efforts to prevent interference fail, what can be done to mitigate its impact? Finding and implementing answers to these questions becomes increasingly important as the use of wireless grows and evolves, becoming more deeply integrated into the infrastructure.

2.4 GHz Band Congestion

One of the most striking findings from this study was the congestion in the 2.4 GHz band. Although there are many more channels and much more spectrum in the 5 GHz band, by far the majority of the traffic is packed into the 2.4 GHz band. To make matters even worse, traffic was repeatedly congested into a signal channel in the band.

For both the WiFi and cellular networks, the ability to use new frequencies in the 5 GHz bands opens up the opportunity to spread users out, separating them in frequency so that they can receive better service and avoid interfering with each other. However, that opportunity is appearing to wither in the presence of market forces that congregate devices into the 2.4 GHz band. It appears as if market dynamics are equipping the majority of devices to only operate in the 2.4 GHz band. A natural consequence of this is that the 2.4 GHz band is becoming increasingly crowded in many locations where multiple users congregate. Further, dual-band devices generally default to this crowded band, even though they are capable of operating in the much less crowded 5.8 GHz band.

The use of WiFi and Bluetooth, quickly being joined by ZigBee, on the 2.4 GHz ISM band, has become the dominant choice for product designers who want to include a wireless interface

Table 2. Single vs. dual-band WiFi devices—all certified devices.

Year	Dual-Band Devices	Single-Band Devices	% Dual-Band
2013	1405	2826	50%
2012	1425	3445	41%
2011	1016	2885	35%
2010	582	1975	29%
2009	388	1197	32%
2008	249	818	30%
2007	218	724	30%
2006	115	501	23%

in their product. In a recent technology trends article published in *Electronic Design*, "Bluetooth and Wi-Fi Rule the Airwaves," Louis E. Frenzel stated:

> With dozens of short-range wireless standards to choose from, engineers still defer to Bluetooth and Wi-Fi. After more than 15 years, they continue to grow, improve, and provide new features and benefits. These amazingly useful technologies both use the 2.4-GHz industrial-scientific-medical (ISM) unlicensed spectrum.[1]

Although the 5.8 GHz band is available and offers more bandwidth and higher data rates, most product designers only equip their products to operate in the 2.4 GHz band. As a result, interference is a growing problem in the band and devices equipped to operate in the 2.4 GHz band do not have the option of moving to a less congested band when they encounter congested conditions.

The data in Table 2 were gathered from the WiFi Alliance database of WiFi certified devices. Devices qualified for IEEE 802.11b are assumed to support only the 2.4 GHz band, while devices that are qualified for both IEEE 802.11a and 802.11b support both the 2.4 GHz and 5.8 GHz bands.

All Certified WiFi Devices

Total certified WiFi devices:	15,748
Total devices with 802.11a capability:	5,471
Percent of all devices with 802.11a capability:	35%

As Figure 6 and Figure 7 demonstrate, 77% of network access points are operating in the 2.4 GHz band and 80% of the traffic is using this band. However, the 2.4 GHz band only has 3 non-overlapping WiFi channels versus 25 channels in the 5 GHz band. That means that 80% of the traffic and 77% of the network access points are crowded into 10.7% of the available channels, leaving the remaining 89.3% of the channels to carry only 23% of the traffic.

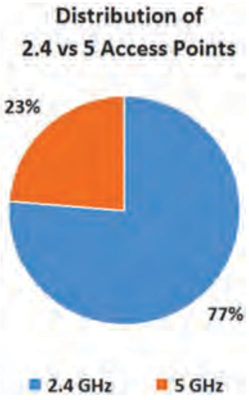


Figure 6. Access point distribution by band.

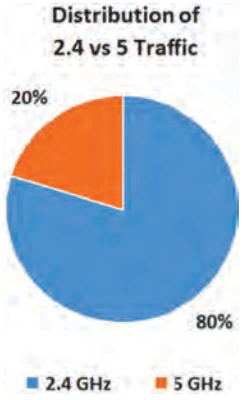


Figure 7. Traffic distribution by band.

The crowding is compounded by WiFi traffic being crowded into only 3 bands, most dominantly WiFi channel 11, which carried 44% of the traffic in this sample (Figure 8).

When channels become congested and suffer interference, their data rates slow down and the error rates go up, resulting in data retransmissions. Although packet retransmissions occur routinely in WiFi communications, the common metric is that retransmissions greater than 1% are a symptom of interference in the channel. Overcrowding in the 2.4 GHz band results in lower data rates and a higher level of transmission errors, which require a large number of packet retransmissions. However, as Figure 9 makes clear, high rates of packet retransmission are common at airports and represent data packet captures of over 1500 channels at 162 locations at

[1] Louis E. Frenzel, "Bluetooth and Wi-Fi Rule the Airwaves," *Electronic Design,* July 11, 2013.

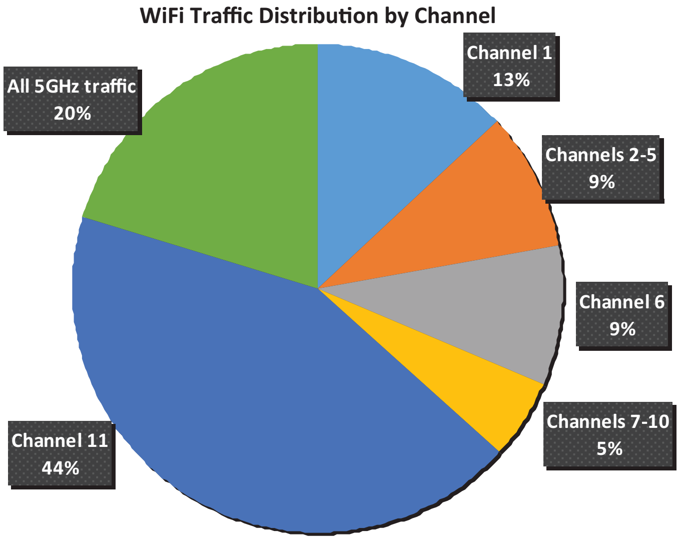


Figure 8. Traffic distribution among WiFi channels.

28 airports; retransmission rates of over 10% and as high as 70% are relatively common on airport WiFi networks.

The situation becomes even clearer when the retransmission rates for channels in the crowded 2.4 GHz band, which were only able to achieve data rates under 6 MBs (Figure 10), are compared to those channels in the less crowded 5 GHz band that were able to achieve data rates of ≥ 24 MBs. When channels become congested and suffer interference, their data rates slow down and the error rates go up. Figure 10 suggests that slow channels in the 2.4 GHz band are commonly suffering interference. In contrast, channels in the less crowded 5 GHz band achieve much higher data rates with a far lower error rate (Figure 11).

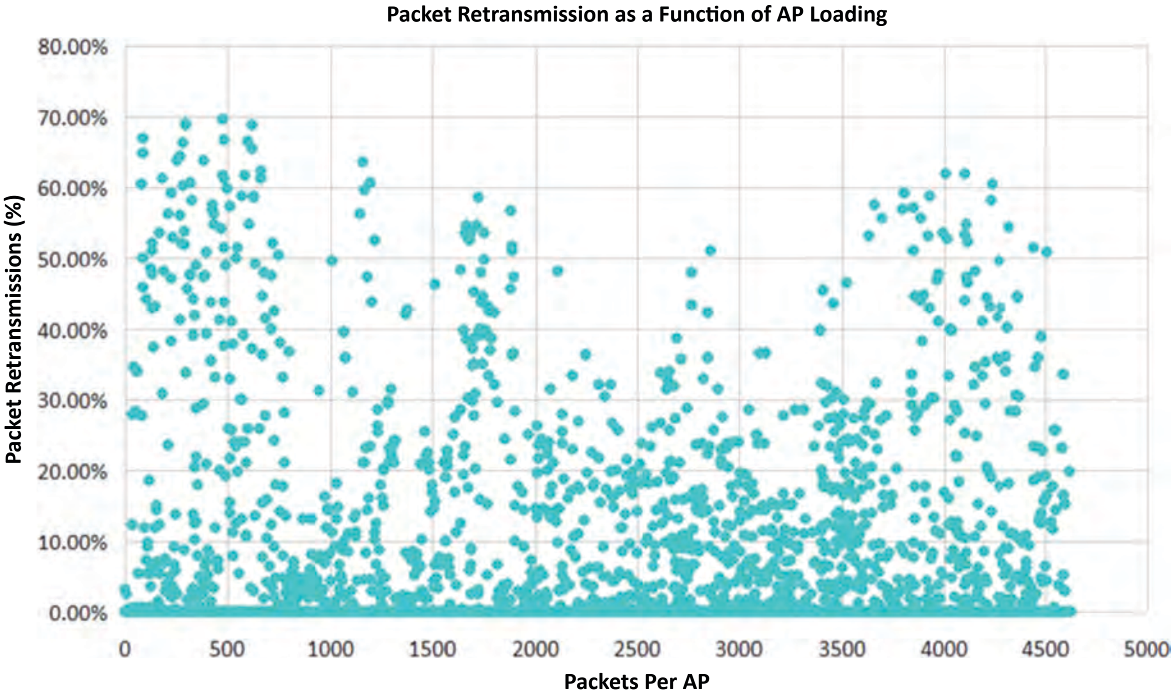


Figure 9. Percent of packet retransmission as a function of access point (AP) load at 28 airports.

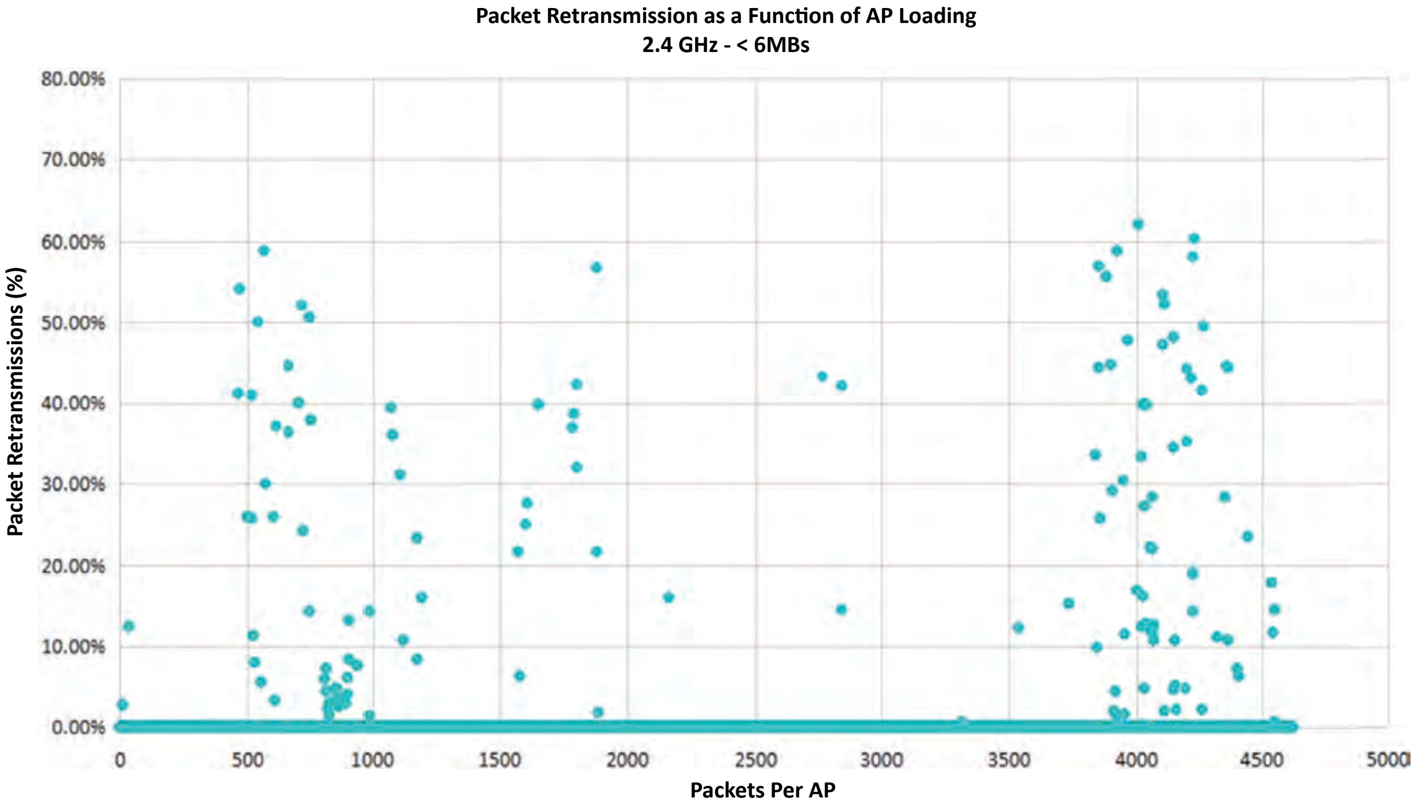


Figure 10. Percent of packet retransmission as a function of access point (AP) load at 28 airports for channels in the 2.4 GHz band with < 6 MBs data rates.

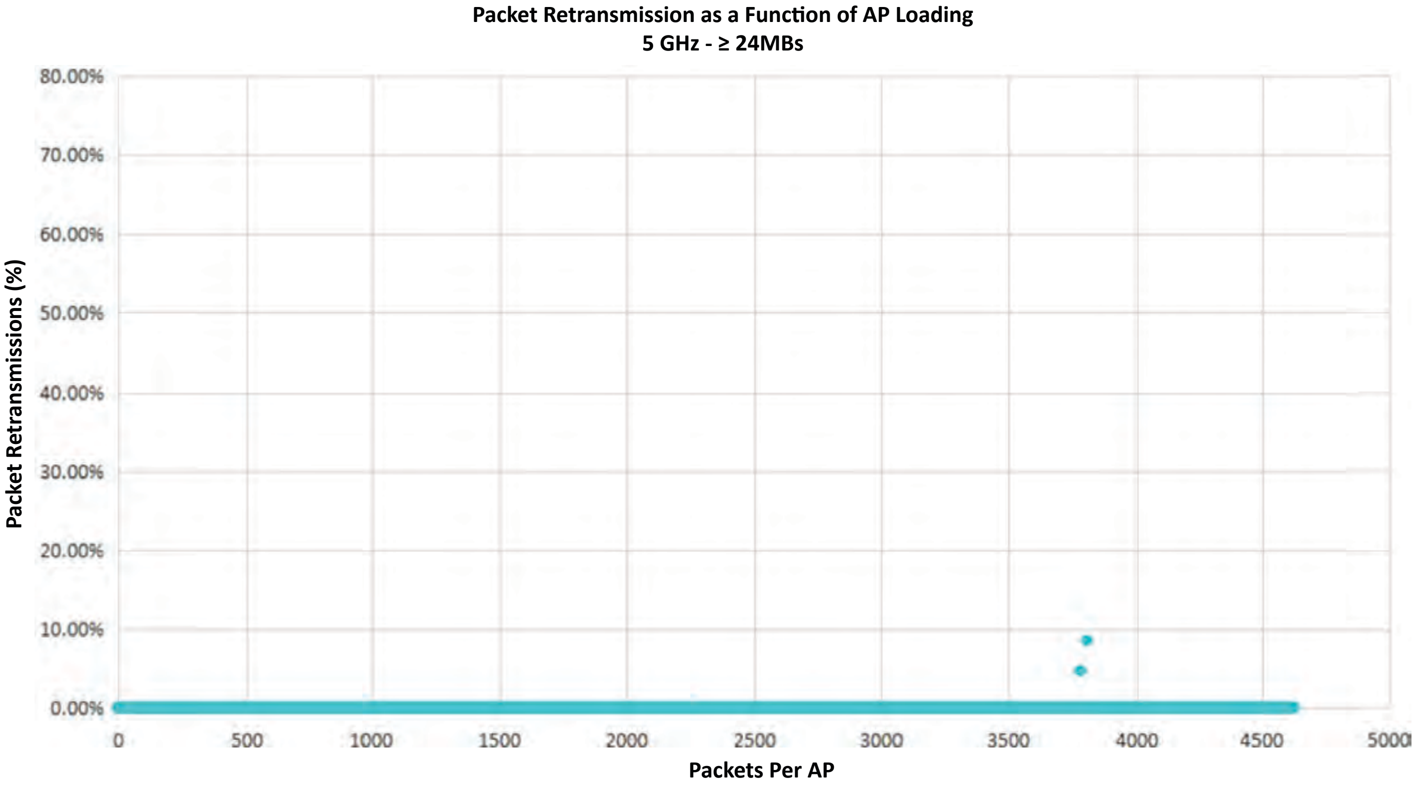


Figure 11. Percent of packet retransmission as a function of access point (AP) load at 28 airports for channels in the 5 GHz band with ≥ 24 MBs data rates.

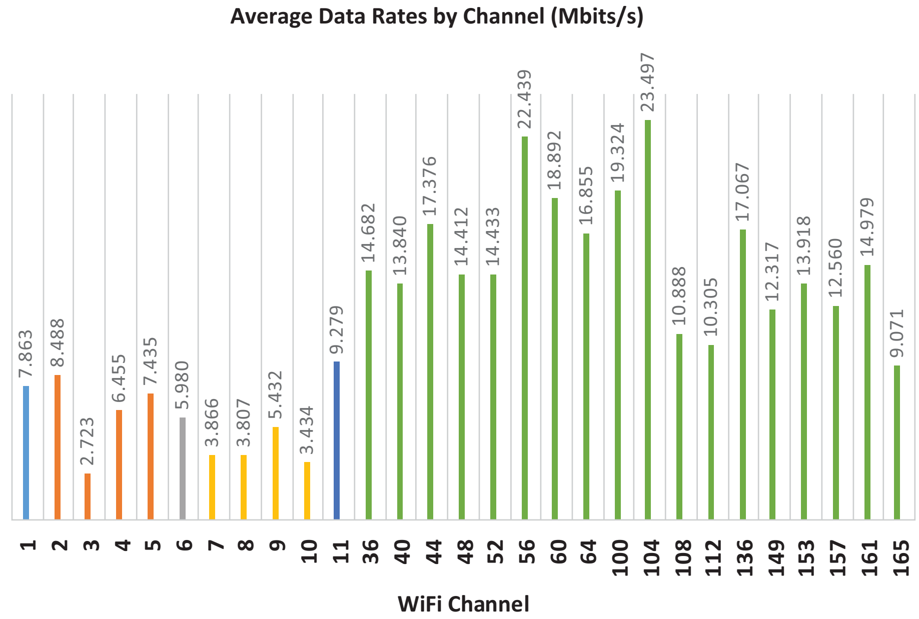


Figure 12. WiFi data rates by channel observed at 28 airports.

A result of the 2.4 GHz band crowding is low data rates, reported in Figure 12, and a high level of transmission errors requiring packet retransmission, reported in Figure 13. The realized data rates are very slow compared to the specified maximum rates for WiFi, and those in the 2.4 GHz band are approximately half of those experienced in the 5 GHz band. Transmission errors are also much more common in the 2.4 GHz band, as seen in Figure 13.

It is noteworthy that WiFi channel 6 has an unusually high percentage of error when compared to WiFi channels 1 and 11, which carry a higher percentage of the traffic. It is believed this is because WiFi channel 6 has overlapping WiFi channels to either side, while channels 1 and 11 only have that situation to one side. This doubles the potential for adjacent channel interference, which appears to be a real problem for channel 6.

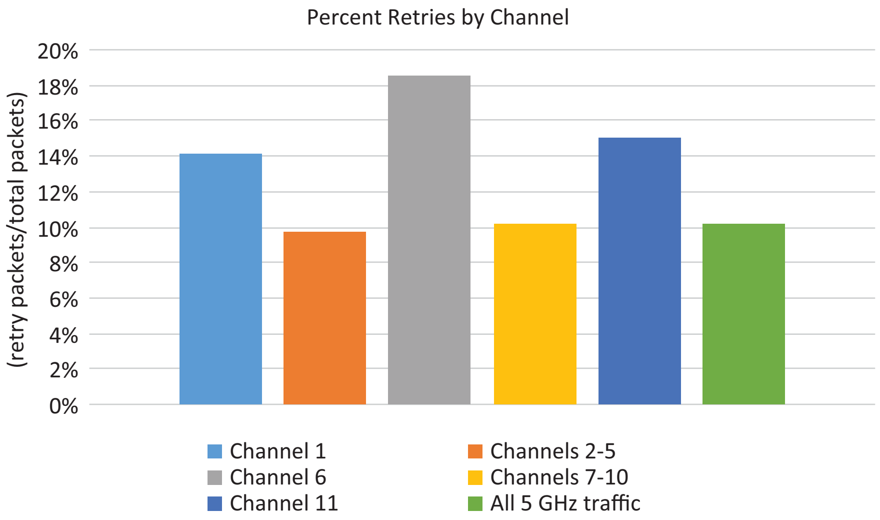


Figure 13. Packet retransmission rates observed at 28 airports.

Table 3. Sample of use of the 2.4 GHz band at access points at 28 airports.

Airport	2.4 GHz Channels 1-14
Amsterdam Airport Schiphol (AMS)	100.00%
Austin-Bergstrom International Airport (AUS)	54.30%
Baltimore Washington International Airport (BWI)	71.29%
Birmingham Shuttlesworth International Airport (BHM)	73.68%
Charlotte Douglas International Airport (CLT)	88.00%
Chicago Midway International Airport (MDW)	61.62%
Chicago O'Hare International Airport (ORD)	63.75%
Copenhagen Airport (CPH)	100.00%
Dallas/Fort Worth International Airport (DFW)	57.61%
Dallas Love Field (DAL)	66.90%
Denver International Airport (DEN)	76.20%
Hartsfield-Jackson Atlanta International Airport (ATL)	96.72%
John Wayne Airport, Orange County (SNA)	71.86%
Killeen-Fort Hood Regional Airport (GRK)	100.00%
Logan International Airport (BOS)	75.75%
Long Beach Airport (LGB)	68.70%
Los Angeles International Airport (LAX)	58.41%
McCarran International Airport (LAS)	66.37%
Minneapolis-St. Paul International Airport (MSP)	100.00%
Nashville International Airport (BNA)	81.96%
Newark Liberty International Airport (EWR)	87.50%
Oakland International Airport (OAK)	64.09%
Philadelphia International Airport (PHL)	96.64%
Reagan National Airport (DCA)	81.34%
Seattle-Tacoma International Airport (SEA)	75.39%
Tampa International Airport (TPA)	64.56%
Waco Regional Airport (ACT)	100.00%
William P. Hobby Airport (HOU)	90.57%

An examination of WiFi use at airports shows that the trend toward band congestion is pronounced. Table 3 gives a sampling of the band usage at 28 airports. Data were gathered at 173 airport locations, mostly at the gates. These data represent the distribution of access points, and show how the airport network makes itself available on a band basis. A quick scan shows congestion lies in the 2.4 GHz band. A significant variation between airports is also seen.

Figure 14 shows the distribution of band usage as measured at 26 U.S. airports and 2 European airports, including 162 gates and 11 additional locations, such as baggage claim. Although this is just a snapshot in time, the results illustrate that 73% of usage is crowded into the 2.4 GHz band. This is indicative of the results experienced throughout the study.

Airport networks have distributed their access points in ways that generally follow the distribution of consumer devices. However, this has created a vicious cycle that contributes to overcrowding into the 2.4 GHz band. If the congestion in the 2.4 GHz band is to be reduced, then

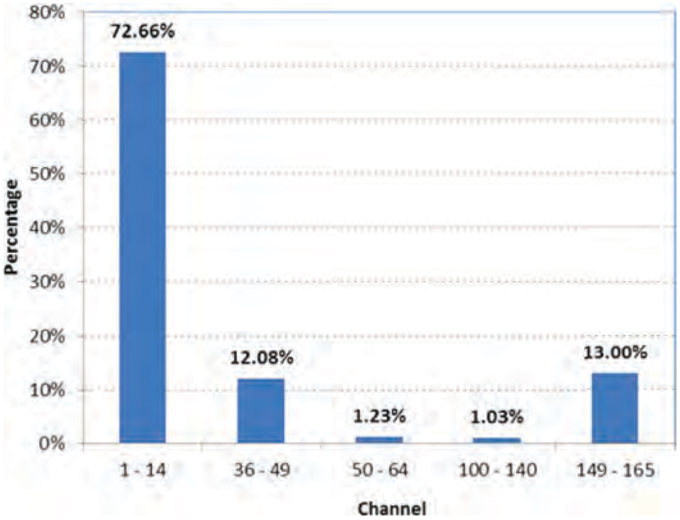


Figure 14. Distribution of band usage at 162 airport gates.

both more opportunities to connect in other bands must become available and an increasing number of network users must be incentivized to use those opportunities.

Adjacent Channel Interference

Radio frequency devices do not have perfect frequency boundaries. While they are designed to put as much of their energy as possible into the channel they are using, there is an influence on or from devices operating on nearby channels. For a WiFi transmitter, some of its energy will spill over into nearby channels, which will add noise to those channels and reduce their ability to communicate with the device they are intending to connect to. When receiving the signal, filtering and front-end RF circuitry allow some energy from an adjacent channel transmission to come in and influence the WiFi receiver. Figure 15 shows the way energy from an adjacent channel transmission may affect a WiFi receiver and is often the dominant effect on a WiFi device's performance.

When two WiFi devices are close and have good signal strength between them, there is an operating margin and the impact of adjacent channel transmissions will be much less, perhaps negligible. The worst problem occurs when a WiFi device is trying to communicate over distance, resulting in a weak intended signal, but the adjacent channel transmission is close, resulting in the energy spill-over being much higher, at times high enough to totally prevent communications.

As can be seen in Figure 15, there are two contributors to adjacent channel interference. Both must be improved for WiFi devices to operate more reliably. WiFi transmitters must reduce the amount of energy they spill over into other channels. However, that alone will not be enough. It is also necessary that WiFi receivers have better filters which give them improved resistance to adjacent channel transmissions.

Other Sources of Interference

An emerging source of interference is largely being created by the need to support two networks in an increasing number of frequency bands. As a result, antennas for the WiFi and cellular networks are often placed close to each other, and at times they share the same antenna

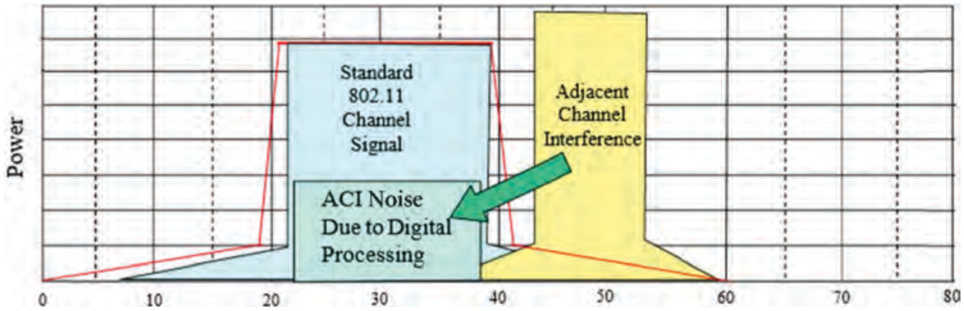


Figure 15. The effect of adjacent channel interference (ACI).[2]

in a shared distributed antenna system. Strong RF signals can create intermodulation products and a variety of related problems. These issues are well-known to the military, where many RF sources are often crowded close together on aircraft and ships. The same problems are starting to emerge in airport systems.

Another class of interference problem is created by technology changes. In some cases, innovations made to reduce interference actually end up causing more interference. An example of technology changes causing interference is IEEE 802.11b. Newer versions of the IEEE 802.11 standard have moved away from direct sequence spread spectrum modulation to orthogonal frequency-division multiplexing (OFDM) modulation. However, support for the older IEEE 802.11b was necessary for backward compatibility. In this research, it was not uncommon to still find IEEE 802.11b devices operating, but when they do they often become sources of interference because they are mismatched with how most WiFi devices currently operate.

Interference Mitigation Techniques

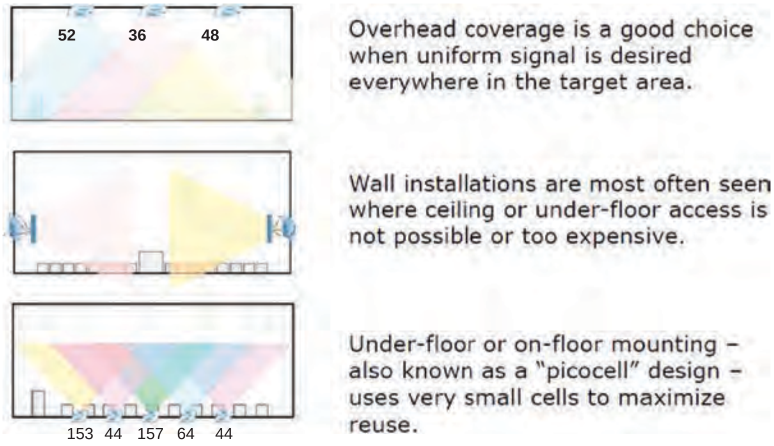
Mitigation measures need to be selected based on what is affordable and at the same time most likely to resolve the interference to the particular type(s) of WiFi problems at that airport. Some airports will find these techniques completely reasonable and readily adopt them, while other airports may view them as challenging or unaffordable.

Multiple-input, Multiple-output

Multiple-input, multiple-output (MIMO) is a promising technology that can contribute to the airport environment. Multiple-input, multiple-output is a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time, taking advantage of multipath propagation, in which transmitted signals bounce off walls, ceilings, and other objects and reach the receiving antennas at different angles and times. Multiple antennas work together to enable them to combine data streams arriving from different paths and at different times to increase receiver signal-capturing power, which increases data throughput and mitigates potential interference from reflected signals.

Multiple-input, multiple-output uses multiple antennas at both the transmitter and receiver to transfer more data at the same time to improve communication performance. It offers significant increases in data throughput and link range without additional bandwidth or increased transmit

[2] Texas Instruments White Paper, "The Effects of Adjacent Channel Rejection and Adjacent Channel Interference on 802.11 WLAN Performance," SPLY005—November 2003.



Overhead coverage is a good choice when uniform signal is desired everywhere in the target area.

Wall installations are most often seen where ceiling or under-floor access is not possible or too expensive.

Under-floor or on-floor mounting – also known as a "picocell" design – uses very small cells to maximize reuse.

Figure 16. Optimal coverage can be achieved through the use of a variety of antenna placements with appropriate antenna beamwidths.[3]

power by spreading the same total transmit power over the antennas to achieve an array gain that improves the spectral efficiency (more bits per second per hertz of bandwidth) and the link reliability. MIMO is part of modern wireless communication standards such as IEEE 802.11n (WiFi).

In IEEE 802.11n, MIMO is used to achieve maximum speeds by allowing devices to connect using multiple data streams spread in frequency. However, MIMO is also an interference mitigation technique. If a device can connect on multiple frequencies and one of those frequency channels is being interfered with, even though the device may lose some connection speed, it can still communicate with the network on the frequencies that are not receiving interference.

Multiple-input, multiple-output is now heavily integrated into the WiFi standards. For close distances with good signal conditions, multiple streams of data can be sent simultaneously to multiply the data rate. At far distances or under poor signal conditions, MIMO can be used as a type of antenna diversity, allowing a unit to pick the best signal quality from several options. Alternatively, advanced signal analysis techniques can be used to improve the total signal quality using multiple signal sources.

A variety of antenna placements, using antennas with different beam width, as shown in Figure 16, provide the tools for optimal area coverage and capacity provision. Antennas with directionality can be used overhead to provide uniform signal illumination over the widest possible area. When overhead installation is not feasible, side-mounted antenna, usually with a slight downward tilt, can provide the needed coverage.

Even-floor or under-floor placement is the right solution for some situations. In some situations, it is even feasible to place an antenna under concrete and have it beam up through the concrete, as shown in Figure 17 and Figure 18.

For any implemented WiFi solution, the airport authority should consider having the installed system tested to verify it meets performance and design specifications. In addition, periodic or on-going network performance testing is also recommended to monitor system performance under actual user conditions, which allows continual tuning of network performance and early warning of developing problems.

[3] Lukaszewski, Chuck, "Ultra-High Density WLAN Design & Deployment," Wireless LAN Professionals Summit 2014, presentation slide 9.

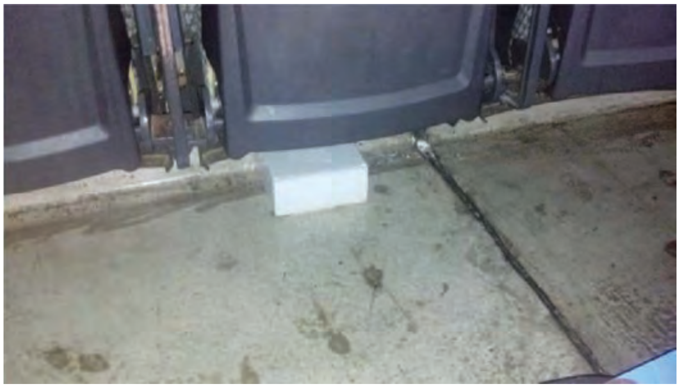


Figure 17. **Floor mounting, under seating, is a good solution in some circumstances.**[4]

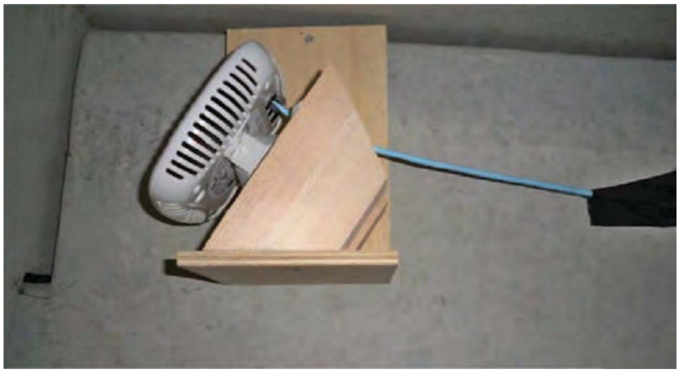


Figure 18. **Through-concrete placement can even work in some situations.**[5]

Other WiFi and Network Problems

Interoperability Issues

Interoperability issues have also been sources of problems. Vendors implement the same requirements in different ways. Some systems have been reported to work well with one model of access points but prove to be problematic with another. At times, a vendor's equipment has been known to cause false triggers, causing the network automation to malfunction.

Another problem is when equipment manufacturers design equipment to use within a particular network architecture. If the network designer uses that equipment in a different design architecture, then there may be interoperability issues. Equipment and functions that may work very well in one context may become more of a problem than a solution when operating in a network design that its manufacturer did not anticipate.

Uncoordinated WiFi Use

A serious problem for airport networks is the independent and uncoordinated use of WiFi. There are several categories of uncoordinated WiFi use at airports. From a management

[4] Ibid., slide 10.

[5] Ibid., slide 11.

viewpoint, there are those WiFi users that, with agreement between the airport and the users, potentially could be coordinated but currently are not coordinated. A second category of uncoordinated use is those situations where getting an agreement between the airport and the user is unlikely to be feasible because the user is transient. This category contains travelers and contractors who bring their own equipment to the airport but are only there for a short time.

With WiFi users who are permanently at the airport or who regularly come to the airport—tenants, airlines, and some contractors—it is possible to come to a shared plan for coordinated use of WiFi. At some airports the majority of the WiFi users in this category participate in a single network managed by a neutral provider. To be effective, this approach must meet the cost and performance goals of all participants. If the neutrally hosted network costs substantially more than other options or fails to meet the performance objectives of some participants, then the airport is likely to pursue any of an increasingly wide range of alternatives.

Frequent travelers are also a group that can potentially be attracted to a neutrally hosted network. The objective of HotSpot 2.0 is to lower the burden of accessing a network by providing an automatic login and a plan that works at multiple locations. Users can pay a subscription fee and their devices will automatically authenticate and log onto a participating hotspot when they are in range. If the vision for HotSpot 2.0 becomes a reality, frequent travelers will be able to pay a monthly subscription and their devices will automatically connect to networks at a wide number of airports and other locations.

It should be observed that the coordination mechanism is very different in these cases. With a permanent vendor, there will almost certainly be discussions between representatives of the airport and the tenant or airline and some signed agreement. With frequent travelers, the HotSpot 2.0 provider will market the service to them and success will depend on how attractive the offering is.

The last category of uncoordinated WiFi use involves those users who come to the airport infrequently and bring their own WiFi direct applications. This presents two different situations. With infrequent visitors, there isn't the opportunity to interest them in a subscription service unless it becomes very widely used by the general population. These users come with their WiFi devices and will use them. Many of these have mobile hotspots of various kinds and are using the cellular network for Internet access. Locally their device, which is often a smartphone but may be a dedicated hotspot device, will provide a local WiFi signal and relay the traffic to the Internet through the cellular network. This kind of service is a competitor to HotSpot 2.0 and users are likely to compare cost, performance, and convenience when deciding which service to use.

Then there are an increasing number of device-to-device services that use WiFi for connectivity. In these applications, one device is sending data to another device and really is only using WiFi because it is inexpensive and easily integrated into the products. Many of these devices will have an option to connect to a smartphone app to provide further convenience when performing its function. The first problem with these uses of WiFi is that when the devices operate on the same channel that the airport network is using for an access point in the area, it degrades the signal-to-noise ratio and slows the network down. When such a device is close enough to either an access point or to a client device on the airport's network to trigger the clear channel assessment (CCA) threshold, these other devices will back off, to allow it to use the channel. Of course under the CCA protocol, it should also be backing off for the airport network and its client devices. However, while the CCA protocol prevents direct interference, it impacts both the airport network and the independent users by reducing the time available to transmit.

A second problem is created when these independent WiFi users are on an adjacent channel. WiFi devices vary greatly in how frequency-selective they are and some are sensitive to transmissions that are many channels away from the one they are operating on. In this situation, the adjacent channel transmission will usually not be recognized as a WiFi signal and so will not trigger the CCA protocol. With adjacent channel operation, the result is similar to what happens when non-WiFi transmitters are in the area. The transmissions create noise, slow the transmission rates, and cause packet loss requiring retransmissions. When the CCA protocol is triggered, there is an impact to network performance, but the loss is controlled and planned to minimize the impact. When energy enters into a WiFi device from an adjacent channel, the interference is much worse because there is no mechanism to coordinate use.

Network Design Solutions to Reduce Interference

Radio frequency environments at airports are constantly changing and reflect the wide swings in network use by travelers who bring their own devices, as well as the new ways that airport operations take advantage of this technology. The challenge is to design a network that is equal to the challenges it will face and then integrate the tools and practices that will optimize the network in a timeframe that is meaningful, given the ongoing nature of the network's environment.

Active Network Testing

Many network administrators assume that all they can do is just respond to complaints. An alternative to resolving problems ad hoc is to actively test the network and monitor its performance. Active testing can identify a problem and potentially correct it before users even notice that a problem is occurring, whereas in passive testing performance is observed and reported, but nothing is done to change the network. There are as many as 600 different parameters that can be measured. Each one provides different information and insight to the network's performance. The kind of testing or monitoring that will best serve an airport network depends on its size, complexity, and applications running on the network.

With passive testing, monitoring can be external to the network or it can be integrated into the network. There are advantages and disadvantages to each approach. If monitoring is done outside the network, the number of tools available is much larger. A number of devices are available to do packet captures and each has particular strengths. If RF is the primary concern, then spectrum analyzers can be used to see what is happening in the RF environment. Increasingly, low-cost spectrum analyzers are coming to the market and they provide an excellent value for the performance they deliver. However, for some measurements only more capable instruments will make the needed measurement.

All the major network equipment vendors are integrating tools for monitoring the network into their equipment and software. Integrated monitoring has the advantage of being built-in, portraying interference the way the network experiences it. Of course, that can also be a disadvantage. Some kinds of interference happen because the network is not able to monitor the sources but is impacted by them. To get a handle on those problems takes an external tool. Integrated network monitoring is the right tool for many purposes and situations, but other situations require tools that give an independent view of interference with data transmission.

Active testing of a network involves using the network in some way and recording its performance. A very popular active test is to check the upload and download speed from a particular connection. Active testing gives better insight into network speed, latency, and capacity. Passive monitors can only observe what is happening with the data others are transmitting or receiving through the network. With active testing, the data load and way it is sent is under the control of the test.

Like monitoring, active testing can be integrated into the network or it can use external tools. An example is a specialized access point used to simulate a client device and test the speed and capacity of the access points near it. These kinds of specialized access points can be integrated into the regular network and create an independent testing sub-network.

The goal of both monitoring and testing is to spot problems early or sometimes before they actually occur, with the objective to resolve problems very quickly or prevent them altogether. The right tools and methods will depend on the characteristics of a specific network, the training and skill of the network management staff, and the service levels the network must support. With the increasing reliability expectations of modern networks, testing and monitoring are as essential as warning lights and periodic checkups of cars, planes, and other systems we rely on.

Clear Channel Assessment

Clear channel assessment (CCA) is an attempt by the WiFi system to determine if the transmit channel is busy or available before it attempts to transmit any data. If busy, it will estimate the duration for how the long the medium will be used before attempting to transmit. If a WiFi device is too sensitive to signals in an adjacent channel, that energy is included in its CCA. However, because the signal is not operating on its channel the CCA will often not identify the device as a WiFi device and will transmit at much higher levels, potentially causing interference to that device and also receiving interference from that channel.

The problem is that CCA assumes WiFi devices are capable of isolating transmissions on their channel from transmissions on other channels. However, for cost savings many WiFi devices do not have the frequency selectivity they need and are very sensitive to transmission on other channels. The lack of frequency selectivity is not important when there are no transmissions on other channels. However, in a crowded environment like an airport, good frequency selectivity is critical for devices to be able to operate simultaneously on different channels and for CCA to operate as intended for those operating on the same channel.

A key is to install the appropriate number of access points, but to place them so that they are as isolated from each other's signals as possible.

There is a big difference between installing an access point with its antenna pointed up through concrete arbitrarily and doing a seemingly identical installation with good data and understanding of the entire network design. It is undesirable to arbitrarily place an antenna out of sight because its appearance has been deemed architecturally unacceptable, without an understanding of how the placement affects coverage. It is better to choose such a placement after testing has assessed the loss introduced by the concrete and efforts have been made to accommodate that loss in the design.

A particularly interesting network diagnostic application of directionality is to have one access point with multiple directional antennas, or an antenna array that allows beam formation, and then actively test the surrounding access points and monitor network performance. Using directionality, one access point can look in multiple directions. It can be used as a spectrum analyzer to look for sources of interfering RF. It can act as a client, actively connect to a neighboring access point, and test the data rate of that network node. Active, integrated network testing will be discussed in greater depth later in this Guidebook, but antenna directionality is an enabling technique.

Placement of Access Points: Path Management

The installation of WiFi access points must take into account the airport's interior architecture and design. The path between the access points and users is critical to connection quality and network performance. The RF characteristics of walls, ceiling tiles, and other objects between an access point and its users have a profound impact on how well the signal gets to its intended recipient.

Most access points come with installation instructions and grounding planes, and are designed to operate from ceilings or elevated mounts. However, a common problem is for architectural or aesthetic considerations to conflict with optimal placement of access points. The person with architectural control may decree that the access point be placed out of sight, perhaps behind the ceiling tiles. If the impact of that decision on the RF signal quality is explored, there may be workable solutions.

In a typical installation, an access point needs power and an Ethernet connection to the wired network. These are not always available in the best location for the access point. Availability of power and an Ethernet connection are legitimate concerns, as are architectural aesthetics. However, network performance is also a legitimate concern. Measurements should be made during and after installation to support the placement decisions with good data on the impact to system performance. Complying with equipment installation instructions and working with the airport manager will help mitigate these potential problems.

Distributing WiFi Traffic

Crowded communication channels are harder to manage. Hence, one of the clear opportunities for reducing WiFi interference is to distribute the WiFi traffic more evenly and then to optimize that distribution for the specific electromagnetic environment for problematic locations.

To successfully distribute WiFi traffic requires action on both the network and the user sides. There are also several challenges to address, which are discussed in the remainder of this section.

In the measurements made at airports, an unbalanced distribution of WiFi traffic was observed. Approximately 80% of WiFi traffic is crowded into the 2.4 GHz band, even though there are many more channels and much less interference in the 5 GHz bands. When looked at on a per channel basis, in many cases a majority of the traffic is concentrated in a single channel. This was observed in both the 2.4 GHz and 5 GHz bands, where the traffic in the bands was concentrated into one or sometimes into two or three of the available channels.

When the band utilization was compared to the number of transmission errors, there was a clear correlation. As a channel gets more congested, the number of transmission errors goes up.

Optimizing for the Electromagnetic Environment

At some locations, there are particular challenges. For example, a leaky microwave might be emitting strongly at 2.45 GHz. This would cause interference to the channels in the center of the 2.4 GHz band but not those away from the center. If the microwave cannot be removed, perhaps because it is owned and necessary for a tenant's operation, then using channels that operate away from its emissions might be a solution.

There are a variety of location-specific issues that can arise. Where the interfering source is fixed or frequently present at a location, one option is to plan the network around that reality. While it is preferable to remove sources of interference, that is not always possible. Therefore, an alternative is to plan the network so that the potential for interference is avoided.

Optimizing for the electromagnetic environment is challenging but much more achievable than planning for a dynamic environment. However, with a bring-your-own-device environment the electromagnetic environments are very dynamic. To address this, some network equipment manufacturers are building in the capability for the network to monitor and automatically configure itself to avoid interference. This concept is still very early in the implementation stage and will take some time to mature.

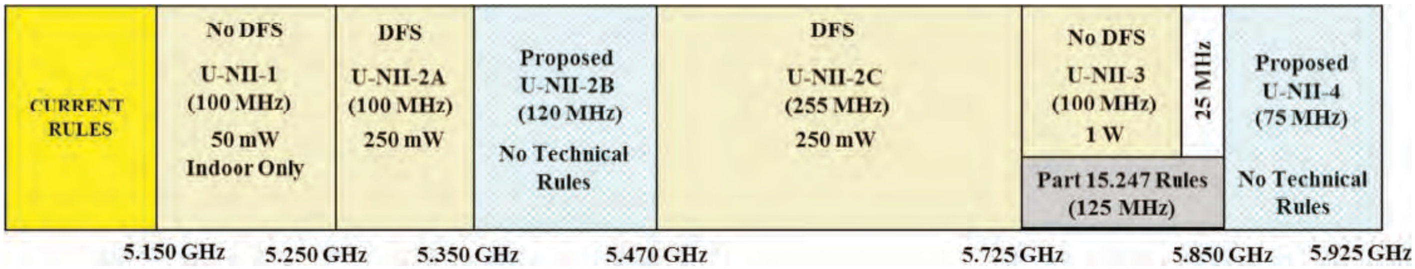


Figure 19. U.S. band plan for the unlicensed national information infrastructure bands with dynamic frequency selection requirements shown.[6]

Dynamic Frequency Selection and Transmit Power Control Requirements

Dynamic frequency selection (DFS) is the process of detecting signals (i.e., radar) that must be protected against WiFi interference, and upon detection switching the WiFi operating frequency to one that is not interfering with protected systems. Transmit power control is used to adapt the transmission power based on regulatory requirements and range information. Dynamic frequency selection and transmit power control are used in WiFi systems to change frequencies in order to avoid interfering with other users, as well as to keep the power as low as possible consistent with their ability to communicate and support their intended function. Transmit power control ensures the WiFi noise in the environment is no higher than needed for it to do its job.

Although DFS channels have been made available by the FCC, there are challenges to be addressed. A random sampling of equipment found that it is relatively common for manufacturers to bring their equipment to the market without qualifying it for operation on the DFS channels. It was also found that most of the equipment surveyed came with the DFS channels turned off as the default setting. The user had to go into the configuration and manually turn on the channels. This was true of both access point and user equipment. To use the DFS channels, both the network operator for the airport and the traveler connecting to the network must turn on the DFS channels.

The FCC requires a number of channels to implement DFS and transmit power control measures to avoid the potential for interference with other radar systems that share their frequencies. The belief that the DFS channels should be avoided to protect radar is a misunderstanding of the FCC's intentions. The FCC wants to see the spectrum utilized effectively. The DFS and transmit power control mechanisms are designed to give adequate protection to radar systems. Network designers do not need to avoid these channels. There have been problems with some manufacturers or network designers disabling these features, with resulting interference to radars in areas where WiFi and radar were in close proximity. However, a function that is turned off cannot be judged to be ineffective.

The ability to successfully use the DFS channels at airports is demonstrated at Dallas/Fort Worth International Airport (DFW), Logan International Airport (BOS), and Baltimore–Washington International Airport (BWI), which have Terminal Doppler Weather Radar systems using DFS channels in their terminal WiFi networks.

Figure 19 shows the current U.S. band plan for the unlicensed national information infrastructure bands and the band extensions being considered by the FCC. These DFS channels represent important opportunities to distribute WiFi traffic more evenly and reduce congestion and interference by simply moving to channels where there is no interference. In addition to

[6] FCC 14-30, paragraph 4.

what is shown here, there are other bands used by WiFi: the new TV White Space band, and the 3.6 GHz, 4.9 GHz, and 60 GHz bands.

Spectrum Reuse and Load Distribution

Spectrum reuse and load distribution are important aspects of network planning. Spectrum reuse looks at the selection of RF channels so that access points do not interfere with each other. Load distribution seeks to even out the data load being processed to avoid bottlenecks or imbalances in the network.

There are relatively few WiFi channels available. The network should be planned so that each access point has full use of its channel with a minimal potential for interference from neighboring access points on the same or an overlapping channel. Spreading out the RF channels is a simple concept but can become complex to implement well.

Similarly, load distribution is a simple concept. Ideally the various communication streams would be spread out among the various communications paths so that the processing power of the network is being utilized optimally. It can be challenging to avoid imbalances when some access points or specific channels in an access point are overloaded and experiencing problems, while others are underutilized.

In an optimized network, the communication sessions will be spread among the available RF channels and data paths in ways that make best use of network resources. However, this ideal is seldom observed in operating networks. Measurements at airports show a high percentage of the traffic being crowded into the 2.4 GHz band and, within that band, into one of the available channels. This leads to congestion, WiFi-to-WiFi interference, high error rates, and a variety of network problems.

Access Point Channel Distribution

Poor channel assignments can create a number of problems in networks. Increasingly WiFi network control software will automatically change the channel assignment of access points in an effort to separate them in frequency. However, under some circumstances the software can do just the opposite of what it is designed to do and put neighboring access points on the same channel, which results in interference between them and their client devices. The same kind of problem can be created when the channels are assigned manually without taking into account the importance of separating neighboring access points in frequency. Figure 20 shows a poor distribution of WiFi channels, with channel 1 being used in a number of adjacent access points. Such a design is likely to result in interference problems.

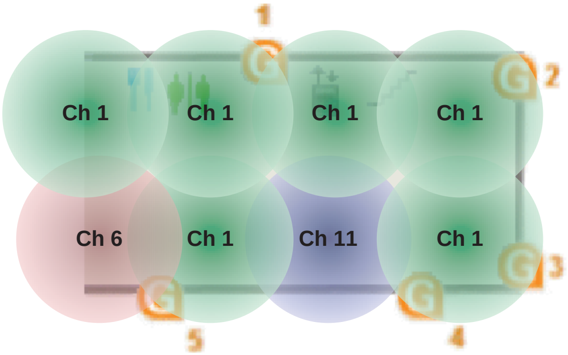


Figure 20. An example of poor spectral reuse.

Table 4. An example of an airport gate with significant potential for adjacent channel interference.

WiFi Channel	Airport Network Access Points	Non-Network Access Points
1	2	4
2		1
3		
4		
5	1	
6		6
7		
8		
9	1	
10		
11		4

Table 4 shows the frequency assignments at a gate in one of the largest U.S. airports. Notice that the network designer tried to distribute the access points among the non-overlapping channels in the 2.4 GHz band. There are two access points using channel 1, which might be problematic.

However, in the layout shown in Table 4 the real problem is from the non-network access points, which are using the same or an overlapping adjacent channel. There is a strong potential for these access points and the clients that connect to them to have significant adjacent channel interference, with the resulting degradation in network performance. In a good network design, access points that use the same channel will be distributed to have channels with the same frequency spaced as far apart as possible.

Automated Network Management

In the past, radio systems were relatively rare by today's standards, seldom used, and often in a fixed location. Managing radio systems of the past could be done with paper and pencil and plans developed in meetings among the users and managers of the systems. However, today's wireless systems are everywhere and in constant operation. Networks and devices are in regular communication, with no user intervention involved. Many services like automatic e-mail alerts are activated when devices have data to deliver; no person is involved in the communication session. Given the very dynamic environment in which airport WiFi networks operate, manual methods cannot keep up. WiFi networks at airports are faced with a constantly changing environment in which the load placed on them and the competition for spectrum from other WiFi devices and non-WiFi devices are in a constant state of flux. Only by embedding into the network the ability to sense its environment and adjust in near real-time can there be a possibility of keeping interference at a minimum and network performance at target levels. That is what automated network management accomplishes.

There are a variety of software and hardware options available for automating network management tasks that previously had to be done manually. Newer versions of the WiFi standards support multiple modulation and coding states that allow a wide range of data transmission rates. When signaling conditions are good and competing traffic is light, a user can experience superb transmission speeds. However, as the signal degrades, perhaps because the user is farther away or because of interference from other transmitters, the system backs off, dropping to a slower speed but more reliable modulation methods. Some systems will track the availability of other access points and switch access points when the signal from one becomes better than the current connection. However, network automation is in its infancy, and due diligence and performance monitoring are essential to successfully using it. For the airport manager concerned with network performance, the relationship with the network manager may need to be more hands-on than in the past.

Key tools used by network automation are changing channels and adjusting power levels. The objective is to get access points assigned to channels and operating at power levels that provide maximum performance with minimum interference. However, the automation algorithms have shown a tendency to misallocate both channels and power levels. The result can be an unstable system.

There is no option to return to the past, slow, manual methods of network management. New automatic network management tools are under active development, but they are far from achieving all that is needed from them. Manufacturers must sell today's products to raise the revenues to improve them. Network managers must practice due diligence and equip themselves with the tools and expertise to manage their networks just as they would any other complex system.

A repeated problem area is when equipment manufacturers design equipment for use with a particular network architecture, and then the network designer uses different design architecture. Equipment and functions that work well in one context may become more of a problem than a solution when operating in a network design that its manufacturer did not anticipate. For example, a method used in automated network management is to automatically adjust power levels downward to keep access points from interfering with each other. Often the decision is made by measuring the signal level of neighboring access points and adjusting the power so that the signal level is below a predefined limit. However, unless client connectivity and area coverage are appropriately considered, the result can be performance issues and a poor client experience. The network design may need access points to have a certain signal strength to adequately reach into remote parts of the facility. Turning the power down may minimize interference between two access points at the expense of providing coverage to the entire facility. Sometimes compromises are needed and the automated algorithms are not always equipped to understand conflicting needs.

Network automation has a growing role in managing the ever-increasing complexity and demand placed on networks. However, those responsible for network performance need to be vigilant in its use, particularly when it is new.[7]

Channel Assignments

One technique that has proven useful is to look at the channel plan on the network's management console. The channel numbers need to be superimposed on an area map. The purpose is to analyze the distribution of channels. Are all of the allowed channels being used? Are the channels evenly allocated within the area? Are neighboring access points using different channels?

The check of channel assignments should initially be repeated several times a day to look for unnecessary churn. Proper channel allocation is a key element of achieving good network performance with minimal interference.

[7] For further discussion of the topic, see: Veli-Pekka Ketonen, "WLAN Access Point Automation Issues: What You Can Do," 2014. Available at: http://7signal.com/blog/wi-fi-access-point-automation-issues-what-you-can-do/

Next, the power levels and field strength need to be checked over the coverage area. Power levels at the low end of the power range are likely to result in poor coverage and decreased performance. Cases have been reported where access points are configured by automated systems to operate close to 0 dBm. Such low power levels are unlikely to be consistent with good performance.

HotSpot 2.0

Another capability to automate the management of WiFi networks is the use of HotSpot 2.0. HotSpot 2.0 originated in the standard IEEE 802.11u and is designed to allow automatic connecting for all of its users. It is viewed as the secure and easy option for roaming with cellular data.[8] The idea is for mobile users to be able to automatically join WiFi subscribers whenever the user enters an area of coverage. The key elements are network discovery and selection, streamlined network access, security, immediate account provisioning, and provisioning of operator policy for network selection. Another improvement is integration with WiFi Passpoint, a program certifying that access points and devices comply with technical specifications.[9] HotSpot 2.0 would alleviate a great deal of the congestion currently occurring, as well as provide faster speeds for mobile users.

Distributed Antenna Systems

A distributed antenna system (DAS) is a network of spatially separated antenna nodes connected to a common source via a transport medium that provides wireless service within a geographic area or structure. Distributed antenna system elevations are generally at or below the clutter level, and node installations are compact. Use of DAS allows the network manager to split the level of power transmitted over an area by spreading the transmission over multiple antennas versus one antenna. The net effect is to reduce the possibility of interference to local users as well as increase reliability.

[8] Ruckus Wireless, "HotSpot 2.0: Making the Wi-Fi Roaming Experience as Secure and Easy to Use as With Cellular Data." Available at: http://www.ruckuswireless.com/technology/hotspot2

[9] vonNagy, Andrew, "WiFi Alliance Rebrands Hotspot 2.0 as WiFi Certified Passpoint" 2012. Available at: http://www.revolutionwifi.net/2012/05/wi-fi-alliance-rebrands-hotspot-20-as.html

CHAPTER 3

Airports and Network Operators: Issues and Solutions

An underlying assumption commonly held is that the interests of the airport management, the network operator, and airport stakeholders are the same, but there is little validity to this assumption. For example, perhaps both the airport authority and network operator might benefit from a network technology upgrade, but doing the upgrade might create a cash flow problem for the operator or significantly impact their profits for the quarter.

Airport managers need to have tools and processes in place to monitor the network and ensure it is operating in ways that they find satisfactory. The network operator has the challenge of finding the right balance between hiring skilled personnel and paying them adequately. Airport stakeholders may be more interested in how the system immediately benefits their business or operation. On the other hand, the airport authority is more interested in how well the network performs, especially during peak demand and irregular operation events.

Implementing a service level agreement is one way to address this issue for both airport managers and network operators, as well as all airport stakeholders. Service level agreements provide a method of identifying expected performance levels, operational performance metrics, and even shared revenues. More importantly, they ensure the buy-in and cooperation of all airport stakeholders prior to the implementation, upgrade, or expansion of any WiFi system. Service level agreements can also result in the reduction of costs by potentially distributing those costs across multiple entities if desired or applicable.

Service Level Agreements

Service level agreements (SLAs) are a core tool for network management. An SLA identifies expectations and should have enough specificity to be both verifiable and enforceable. These agreements should also clarify expectations for all parties. For the network operator, there should be enough detail so that the implications for equipment selection and network architecture are clear.

It is important that SLAs find a realistic balance between high-quality, high-reliability operation and the current limits of technology and realities of network management. Achieving this is not easy. Given the rapid pace of change in WiFi technology and wireless technology in general, that realistic balance is ever-changing, and SLAs should be regularly reviewed and updated to keep them current.

At many airports, there is a single SLA between the airport authority and the network operator. However, with the changing role of wireless networks, there is a need to provide multiple levels of service. The process of establishing each level, particularly for those services that are more critical to airport operations, needs to carefully consider the metrics that will be used to verify compliance with the agreement. This is particularly true for irregular operations performance. The last thing an airport wants to learn is that their network operator failed to implement the network with the capability to support their needs during an irregular operations event.

Airports and network operators should consider the following as they develop their master SLA:

1. A master SLA is a core component of the contract between the airport authority and their network operator.
2. An SLA should address passenger service. There may be multiple levels of service for passengers. Better service could be offered on a paid network and a lower level of service offered on the free network.
3. Uses of the network to support airport operational functions need their own SLA, and there may be several of these addressing the needs of different functions and applications.
4. An SLA should be negotiated between the network operator and the department responsible for a new application to make sure that the network is capable of providing the required level of service.
5. Tenants will often have their own SLAs. A tenant may want to provide a different level of service for their customers, which should then be defined in their SLA. If the tenant is using the network to support their own business processes, they are likely to require higher levels of service.

When performance metrics are used, they tend to focus on availability, usually meaning coverage, but not on more detailed metrics supporting a targeted quality of traveler experience. Here is a list of areas that an SLA may include, followed by a discussion of these elements:

1. Coverage
2. Capacity
3. Currency (keeping up with technology)
4. Equipment quality
5. Security
6. Irregular operations support (flex with changing needs)
7. Active and/or periodic performance testing
8. Reporting to airport management
9. Cooperative interference mitigation
10. Emergency management
11. Revenue sharing

Coverage and Capacity

Coverage should be defined technically. Signal strengths of –64 dBm for the 2.4 GHz band and –61 dBm for the 5 GHz band are generally recognized as valid metrics to support the full capabilities of current WiFi equipment. The coverage specification in an SLA should specify the areas to be covered; the percentage of those areas to be covered, e.g., 95%, 99%, etc.; and what signal strength is deemed to be adequate coverage. Particularly for the 5 GHz band, the channels to be covered should be specified. This is because the 5 GHz band covers a wide spectrum range and values will vary across the band. Hence, the coverage requirement might be acceptable for some channels but not for others. For simplicity, it may be enough to specify the coverage will meet the stated level at the low, middle, and high channel in the band.

Currency

Some airports require that their network manager keep the WiFi network at the current published level of IEEE 802.11, or no more than one generation behind. This is not unreasonable but is very general and misses a number of issues. In the IEEE 802.11 standards, there are a number of options that manufacturers have flexibility to include or leave out of their equipment. Some of these are important to a crowded, bring-your-own-device environment like an airport.

A survey of the WiFi Alliance Passpoint certification program revealed how many variations there are in WiFi equipment. Not all IEEE 802.11n or IEEE 802.11ac equipment is the same, and some of those differences affect the airport's ability to operate a quality network. Someone knowledgeable about the equipment options and their impact on network management should assist the airport in drafting its requirements. The importance of some options depends on the specific network architecture and management methods used at an airport. Airports may vary in what is important to them based on the way they manage their network. This should be known and specified in the SLA.

Equipment Quality

Equipment quality is a very important area to be specified in an SLA. WiFi equipment covers a wide range of capability and quality. Expectations need to be clarified if the airport is to get the level of service it needs.

A particularly important area is the equipment's resistance to interference. Historically, WiFi equipment was designed to be very cost-sensitive, sometimes omitting filters and other features regularly used in other kinds of radios to improve their frequency selectivity and tolerance of other signals operating in close proximity. Broadly speaking, there are two classes of interference problems, weak signal and strong signal problems.

The weak signal category occurs when an access point and client device may be too distant from each other or for some other reason have a low signal level. Under this condition, the equipment's ability to receive the intended signal in the presence of other signals in an adjacent channel, or even an adjacent band, is critical. Testing in highly regarded studies has found WiFi equipment currently on the market can vary by factors of 100 or even nearly 1,000 in terms of its ability to successfully receive a signal in the presence of another signal in an adjacent channel. While an airport cannot dictate the client equipment, it can know the capability of its own equipment and require that it be representative of better quality equipment currently on the market.

The strong signal category occurs when a WiFi device finds itself in an environment with a very strong RF transmission. This can happen if a cell phone is operating very close to the WiFi device. It can also happen if a DAS antenna for cellular is placed very close to a WiFi access point. It is guaranteed to occur if the same DAS is used to support both the WiFi and cellular networks. In this case, strong WiFi and cellular signals will be sent through the same components and a variety of strong signal interactions become possible.

Specific and specialized testing is required to determine if strong signal problems are occurring. Dealing with them is always difficult but even more so after a network is installed and operating. It is very important to evaluate these issues as part of the equipment selection process and then confirm that the installation did not introduce new problems.

Security

The ACRP released a separate study to address WiFi security issues, so security is not detailed in this Guidebook. It is mentioned here because security is a basic tenet that the airport manager must take adequate steps to ensure. It is recommended that security be included in the SLA. This is particularly critical for those irregular operations services required by the airport in times of emergency operations.

Irregular Operations Support

Service level agreements can and should address the particular service level and performance requirements needed to sustain irregular operations or, specifically, emergency operations. The networks can be designed to provide priority message service or dedicated channels for critical airport operations such as security. Irregular operations services should be implemented taking into account all stakeholder services provided to the airport.

Active and/or Periodic Performance Testing

If active or periodic testing is required, then it should be specified. How the data will be collected, analyzed, reported, and to whom should also be specified.

Network testing, particularly active testing, produces an enormous amount of data. The level of performance can just as easily be hidden in a mountain of unfathomable data as it can in no data at all. A process is needed for gathering the data and analyzing it. Criteria will be needed so that there is common ground between the network manager and the airport manager. For example, if only one location fails to meet a requirement, is that considered a failure? What percentage is acceptable? Similarly, what if there are occasional failures, but most of the time the criteria are met?

The best metrics and criteria arise out of experience. To require that all locations meet the maximum coverage and capacity requirements all the time is unrealistic and likely to result in unnecessary costs. However, working from averages may neglect important issues such as peak usage times. What is needed is a middle ground—requirements that find the right balance, such as 90% of locations shall be able to meet the service requirements 90% of the time. Another question is what criterion to use for evaluating network performance when designing improvements to the network. When developing criteria like these, it is important to know exactly how they will be measured. Criteria that are difficult to measure are of little value in an SLA agreement.

Most airports want to provide a positive traveling experience to passengers using their facilities and this includes their experience with the airport WiFi. Since most travelers will only be in an airport for an hour or two, their experience will be determined during that time. It would seem appropriate to set the evaluation analytics based on what the airport hopes the travelers' experience will be. Therefore, the right metric would be a one- or two-hour sample taken periodically during a high traffic time, with a target that certain service level standards are met 90% or 99% of the time for each channel being used. It is important to evaluate each channel separately because if channels are averaged together, the retransmission rates become extremely small. That average, of course, is of no concern to the traveler having trouble connecting to the network, who probably is unaware of what channel the device is trying to connect on or how it compares to other available channels.

What is being suggested is that some level in the probability distribution of traffic and transmission errors is the appropriate metric for this purpose. The right threshold might be 90%, 95%, or 99%; a cost/benefit analysis would be reasonable to help choose the appropriate threshold.

Whatever the final determination, careful thought and research into the performance evaluation criteria is worth the effort invested. By translating the desired performance quality into technical specifications that can be measured and used in managing and improving the network, the right set of metrics will directly correlate to traveler satisfaction with the WiFi network.

Reporting to Airport Management

Data on performance metrics and results of their analysis should be shared with all interested parties. How often the data are provided, what data are shared, and the format for presenting the data should also be identified in an SLA. The criticality of the operations supported can help determine the frequency for reporting. Not all results need to be reported at the same time. Some may require weekly reports or even monthly. Others may require immediate action. This reporting then becomes the basis for the airport manager and collective stakeholders to make decisions regarding substandard performance, mitigating interference, and upgrading or expanding the WiFi network.

Cooperative Interference Mitigation

The cooperative approach is mainly driven by the FCC ruling that an airport authority cannot control installation and usage of WiFi at airports. However, the enforceable component is that the devices comply with FCC regulations. A cooperative approach is needed to mitigate interference within the terminal, and the methodology to do so can be specified in the SLA.

It is in the best interest within the airport terminal that RF interference mitigation involves all entities concerned. Best interest is defined as a reporting, analysis, and action process to mitigate RF interference that considers the responsibilities of the airport, the business case of the tenants, as well as the responsibilities of the passengers. Passengers are included and have the responsibility of operating equipment that complies with the FCC part 15 rules and regulations, i.e., mainly to not exceed power limitations. Hotspot devices purchased by airport passengers sometimes can exceed the power limits, depending on manufacturers. These devices, if brought in number into the airport environment, can contribute to mutual interference among themselves and other WiFi devices such as laptops.

Emergency Management

An "emergency environment" caused by a fire, mishap on the runway, terrorist act, etc., will impact all communications in the terminal, including WiFi. Emergency management is focused on resolving such a situation, and the responders must be assured of communications. Emergency responders may use the established WiFi network and require priority in its use to ensure interference-free message completion in execution of their duties. The prioritization of emergency communications should be included in the SLA and can be a cessation or reduction of WiFi use for all but emergency instructions to passengers. The scope of the WiFi disruption can also be identified in the SLA.

The basis to enable such an action is contained in Section 15.3(m) of the FCC Part 15 regulation. The definition of harmful interference is stated as ". . . any emission, radiation or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communications service operating in accordance with this chapter." This is an operational definition using terms that do not have strict "technical" thresholds associated with the "victim" receiver except for the radio navigation functions and safety services. Radio navigation applies to safety of flight. One commonly associates this with interference affecting radio navigation systems supporting flight operations, including equipment located near the airport. Minimum or no interruption or induced errors to radio navigation is tolerable. WiFi communications systems can fall into this interpretation, particularly in emergency situations as related to safety and security. Note that, at the present time, the frequency bands of communications systems are largely different from WiFi bands, and interference is highly unlikely to be experienced. The exception is if WiFi is used by airport security or safety functions within or near the airport facility. The interference aspect may also be addressed in the SLA to include levels of emergency and the associated WiFi use for these levels.

Revenue Sharing

If revenue sharing is applicable, then it can also be addressed in the SLA or part of a larger contract. Revenue sharing is still in its infancy and there is not a clear path forward. If a commercial provider of the WiFi network can visualize a way to earn additional revenue via customers using the system, then it holds that the airport authority or stakeholders may benefit by acquiring equipment at a discount, as one example. If a subscription is used to allow business representatives additional data throughput or higher priority service, then those fees can be shared or a portion set aside to reduce the cost of maintaining or upgrading the WiFi network. These are just two examples that demonstrate the need or benefit to document the revenue-sharing agreement in an SLA or contract.

Network Analytics

Management processes are only as good as the feedback and control systems that enforce them. Active or even routine monitoring of network performance is rarely done by airports. However, even if a more nuanced set of network analytics were used, it is unclear that improvements could be required under the current SLAs.

Results from the survey of airports and the case study visits to airports revealed that the most common metric used to evaluate network performance is traveler complaints. A commonly reported method was that the airport public relations and/or operations department monitors traveler comments about the airport. When travelers express dissatisfaction with the airport's WiFi, the airport examines the potential for improving performance. This approach essentially defines high-quality WiFi performance according to traveler input and assumes that the WiFi network is primarily there for the traveler. Some airports, however, have taken into consideration the airport's own use of WiFi and built solutions around their particular needs as well.

The ability to use customer complaints as a metric depends on the value the airport manager or stakeholder believes the WiFi network provides. There is no defined number of complaints or threshold identified. The airport manager must determine what is acceptable and over what duration of time, i.e., 5% of all users registering complaints over a 30-day period. Using customer complaints may be a better indicator of a decrease in the level of acceptable performance over time, indicating that some action is required.

Assessing Traveler Satisfaction with Airport Wireless Capabilities

Does having quality wireless actually affect customers' decision-making on how to travel? What methods of providing wireless are best received (small fee but high quality, free with time limit, completely free, free with a survey, etc.) and are most effective? What actually is perceived as being an upgrade in public-access WiFi? These are questions that airports may pose to travelers for a more complete picture of how the network is working, rather than solely using complaints as the basis for problem-solving.

There are numerous ways of assessing how satisfied travelers are with the WiFi service at airports. In this study, social media was mentioned by several airports as one source of insight. Airports can search for traveler reviews by combining such key words as *wireless*, *airports*, *traveler*, and so forth. While not scientific, social media postings provide some clues as to the public's experience, though it should be recognized that far more people take the time to write reviews if they are dissatisfied than if they are pleased. Nevertheless, a quick check into one social media site's posts regarding WiFi quality at four airports shows the results indicated in Table 5.

Table 5. Traveler reviews of WiFi quality at four airports per a social media site.

Airport	Sample of Comments
Airport #1	• WiFi offering is slow and unreliable. • I love this airport. Free WiFi. • Love the free WiFi. • Free WiFi + outlets everywhere. • I'm dropping you a star based on your WiFi. Service is spotty at best and only one hour of free WiFi and then you want money.
Airport #2	• Lots of power outlets. • Free WiFi. • Advertisement at a competing airport: "Fly through us. We aren't [other named airport]!" • Free WiFi is always a huge plus.
Airport #3	• Lots of power outlets, free WiFi but spotty at best. Kind of slow and requires a re-login about every 45 minutes. Deducted one star for lack of free WiFi. • Paid WiFi? Booo! • No free WiFi, they still rely on Boingo service.
Airport #4	• Few power outlets. • No free WiFi here. • 10 mb/s!

System Performance Oversight

Evaluating system performance in essence involves ascertaining whether the right level and amount of resources are in place to support wireless services, and then evaluating whether those resources are being used effectively to deliver an appropriate level of service. (As stated earlier, airport managers can define appropriate level of service by implementing an SLA with the network provider and stakeholders.) This is particularly challenging for airport managers that do not have a technical background. Even if upper management has some technical background, the technology is changing so fast that only those who work with it on a daily basis can stay current, and even network operators may be challenged by the rate of change in wireless networking.

For airports that manage their own networks, the problems remain the same, but the way they are managed changes. One major airline assumes management responsibility for the whole WiFi network at several airports, with little stakeholder involvement. The advantage is complete control, but the disadvantage is that the airline absorbs all costs. Often airport managers have less hands-on control and delegate to the main WiFi provider or in some cases multiple providers. In these cases, there may or may not be coordination of the airport manager with all providers. The cost absorbed by the airport may be less, but the potential for interference is greater. There continues to be a requirement for the right level and type of resources in place. A critical resource is the technical expertise of the staff managing the network and those monitoring its performance. If those personnel work directly for the airport manager, then there is more control but also more responsibility for the airport manager to ensure staff are staying technically current.

Two-Vendor Model

Among the case study airports, several observed that their relationship with their network manager was changing and they were being required to be more hands-on than was previously true. In several cases, a two-vendor model was being implemented. At those airports there is a primary network manager, but also a second vendor contracted to monitor network performance and help the airport identify and deal with specific problems. This arrangement takes into account that the airport authority's interests and those of the network manager may not be the same.

An excellent example of when they diverge occurs with technology upgrades. The airport would be best served for its network to be technologically current and have sufficient excess capacity to deal with peak user periods and irregular operations events. The network manager is also benefited by a network that performs well, but must achieve that goal in terms that are consistent with the contract and profit objectives. Seldom will these interests align perfectly. There is no perfect answer, but finding the optimal balance requires that both sides have good technical network and RF expertise to help them understand how their interests translate into specific technological solutions. The two-vendor model achieves this balance of technical knowledge, increasing the chance that the airport will receive the best outcome for the incurred cost of the network.

Airport Plus Contracted Network Manager Model

At other airports studied, an internal information technology (IT) department is maintained to manage some parts of the wireless infrastructure. A common division is for the internal IT department to manage all office and operational areas, while the contracted network manager is assigned responsibility for the passenger areas in the terminal. This arrangement can also work, but IT and wireless are not synonymous. An IT department has many responsibilities and the capacity to monitor a wireless network is not guaranteed. There is a long history of managing a wireless network just like a wired network, but without the wires. However, wireless networks are fundamentally different. If an airport uses its IT department as an internal expertise resource in overseeing its network manager, it is essential that it have skilled wireless managers on its staff or at least access to wireless expertise when needed.

Inter-Airport Information Sharing

Keeping sufficient technical expertise to ensure that an airport is getting the performance it needs is perhaps an area where airports can work cooperatively. Gathering data from multiple airports and comparing network performance creates a benchmark against which airports can evaluate the performance of their own network. It will be easier for airports to stay technically current if they pool some of their resources and apply them to the ongoing effort of staying equipped with the tools and improvements they need to manage their networks.

As wireless networks grow in importance and become ever more vital to airport operations, airports will be required to become much more involved with the active management of their wireless networks. Whether they achieve this by using a second vendor to help them monitor their networks or use internal staff for that purpose, the trend toward increasing the wireless expertise of the airport authority appears to be a necessity.

Influence Management in a "Bring Your Own Device" Environment

While the airport cannot dictate what equipment travelers use, it can influence those choices. Few travelers know what types or brands of equipment are more immune to interference and will give them a better experience. However, airports can certainly share information with travelers about what equipment they find gives satisfactory results on their network.

In a closed network, network managers have direct control over all devices on their network. However, in a "bring your own device" network such as exists at an airport, those controls are minimized or absent altogether. Instead of being able to mandate practices, network managers must use influence and softer management approaches, like information sharing. This fundamental shift leaves many network managers feeling like they have lost all control over their network. In reality, they have tools available, but they may be unfamiliar and unpracticed in how to use such methods as advertising and information sharing to influence behavior.

One option available to airports is to let travelers know the impact their equipment choices will have on their network experience at the airport. Few users understand that having a dual-band WiFi device might improve their ability to connect to the network. It is important users know that most dual-band equipment comes with the default set to "off" for DFS channels. That locks out other available channels. All one must do is switch the option to "on" to access lesser used channels that can enable a better user experience, particularly in a crowded environment.

Airports might consider including tips about device features that facilitate using the airport's network. For example, flyers, blogs, and streaming text could showcase which devices will work best at the airport. That information could be added to the airport's website. There even could be an airport-ready program that would allow manufacturers to qualify their equipment if it meets requirements such as being dual-band and having all the channels activated, tested, and shown to have good RF coexistence capabilities. While it certainly is not an airport's responsibility to specify which devices produce the best results, they nevertheless could be a good partner to travelers and share that information.

Structure of Network Management

How network management is structured at airports has been, to a significant degree, a successful exercise in influence management. At most airports there is one dominant provider of WiFi and either the same or a second provider of cellular connectivity, through a DAS system that is shared by several of the cellular network operators. Only at a few airports do all cellular network operators use the DAS operated by the airport.

Similarly, at some airports there have been multiple providers of WiFi, each with their own competing network. Some vestiges of this arrangement were found at the sample airports. In some of the airports, access points were found to be operating under the name of former WiFi network companies, even some that are no longer in business. However, most airports have successfully gone to a model of a single neutral provider of both WiFi and cellular connectivity, which provides service to anyone who needs those services.

Emerging Trends

Traditionally, at both ends of a wireless connection there was a person, usually talking to the person at the other end. Increasingly the ends of a connection will now be machines sending data, many smartphones sending data to a single access point. Because there are many more people of all ages with mobile smartphones or wireless devices, the amount of data being sent wirelessly has exploded and its growth does not have an end in sight. Increased use and new functions bring consequences, both intentional and unintentional.

Internet of Things

A future technology arriving on the horizon is the Internet of Things (IoT) or the Internet of Everything. This is the rapidly growing trend for sensors, actuators, and many other types of devices and objects to be continuously connected to the Internet.[10] The purposes behind these connections vary, but often the reason is to better extract and analyze data in real time.

There were several pre-requisites for IoT that needed to be developed in order for it to become a reality. One of these necessary technologies was RF identification becoming commonly used.[11] This allowed for devices and people to become quickly identifiable. Identifying cars for tollways was one of the first ways that identification was possible from relatively great distances. Other improvements, such as barcodes, QR codes, and watermarking, allowed for near field communication to similarly pave the way for IoT.[12]

Some airports want to be able to individually meter utility uses so they can separately bill tenants for their utilities. Hardwiring the capability is very expensive. However, if the meters are connected wirelessly through the Internet, then the task becomes much easier and less expensive to accomplish. This is just one example of how the Internet gets integrated into airport operations and the value of IoT to that integration. However, it comes with a growing number of devices wirelessly connecting to the Internet.

The Internet of Things was created to be an identifier and eventually a monitor of various objects, devices, and people through the Internet. It allows for detection of basic information from each mini-communicator, with the ability to send and receive information. This allows for greater ability to make quick and effective changes, better grasp the current environment, and better protect creator rights such as patents.[13]

The benefits to these developing technologies are numerous. The U.S. government in particular has discussed the unique abilities that this progress allows for improved public safety and security. Other opportunities include improved weather monitoring, business transactions, delivery of services, productivity, business consulting, and economic growth analysis—just to name a few. Both the private and public sectors have grabbed hold of the IoT's potential, so much so that it is estimated that the IoT will generate $19 trillion in the next decade.[14]

A growing area is to equip mobile personnel with Internet access, but also to have that access become a management tool. Integrated with global positioning systems, airport managers can know where their crews are at any time. Integrated with RF identification or other object identifying technology, the manager can know not only where the personnel are but what equipment they have on the truck with them. These systems are on the market and in use today, and their use seems very likely to grow quickly.

What this means for airports is that the IoT is going to be increasing in importance to the point where it is essentially everywhere. This will create new interference issues in wireless communication, but also provide ways for airports to better handle traffic flows and customer needs seamlessly. Airports would be well-advised to proactively harness this technology for the good of the customer and for the profit of the industry as a whole. However, all changes have consequences, risks, and unintended impacts. The IoT will certainly bring benefits, but will also have its problems and unintended consequences that must be managed.

[10] Bradley, Joseph, et al., "Internet of Everything (IoE): Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector," 2013. Available at: http://www.cisco.com/web/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf

[11] Analyst Anish Gaddam interviewed by Sue Bushell in *Computerworld*, "M-Commerce Key to Ubiquitous Internet," July 2000.

[12] Techvibes, "From M2M to The Internet of Things: Viewpoints from Europe," July 2011. Available at: http://www.techvibes.com/blog/from-m2m-to-the-internet-of-things-viewpoints-from-europe-2011-07-07

[13] Wikipedia, "Internet of Things." Available at: http://en.wikipedia.org/wiki/Internet_of_Things

[14] Bradley, Joseph, et al., "Internet of Everything (IoE): Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector," 2013. Available at: http://www.cisco.com/web/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf

CHAPTER 4

Strategic Planning for Wireless Networks

Strategic planning as it relates to technology as a whole, and in this case specifically WiFi, requires a few key components to effectively phase and ultimately execute. Proper technology planning can help organizations visualize some of the roadblocks they may encounter, and ultimately better serve their customers. Implementable technology planning begins with an assessment and development of a robust communications infrastructure.

1. **Existing Systems—**The first key component of strategic planning is a firm understanding of all the systems and technology that the airport already owns. While this may sound like a simple issue, many airports do not have a centralized database, or centralized knowledge base, of all their IT systems, much less their interdependencies. A good discussion concerning airport management of systems can be found in *ACRP Report 59: Information Technology Systems at Airports—A Primer.*
2. **Future Plans—**Without unified technology planning, there rarely exists an enterprise-wide view on which system upgrades and long-term initiatives will affect other parts of the airport's IT infrastructure. Airport IT departments often play catch-up to the various pieces of technology and construction implemented in an airport. IT departments need processes in place to stay involved with all of the IT long-term initiatives.
3. **Inter-Departmental Communications—**Beyond the IT department, there are many different system users who have a firm grasp of the tools their department needs to succeed, but experience difficulty getting their functional requirements supported and in the procurement pipeline. This lack of departmental communication can result in problems with the change management process, or poor documentation of system upgrades and new installations.
4. **Focus Groups—**New initiatives ranging from utilities metering, to airfield management devices, all the way to shared tenant services, can all be initiated by separate departments, and simultaneously rely on a WiFi system that has not been provisioned for multiple services such as these. The first step often begins with focus group meetings for each separate department, working to identify and document departmental WiFi needs and objectives. Then a second group can convene to address all the objectives and priorities in line with the airport's business case and strategic plan.
5. **Technology Governance—**Following these independent meetings, technology governance is needed to make all of these interdependent parts work together. Governance, at an enterprise level, can help the many different departments of an organization develop a common goal and a common, robust infrastructure that many of the separate airport departments can utilize.

All of the preceding elements are important aspects of the airport's ability to achieve its objective. With the growing use of wireless by a wide variety of systems, it is increasingly common for the wireless and particularly the WiFi network to have a role in these processes. This key piece of supporting infrastructure is often taken for granted and not evaluated from the many perspectives of the airport's departments, travelers, customers, and partners. Strategic planning can help organizations realize the many different operational functions at their airport, and specifically how they affect their WiFi, both now and into the future.

As an example, rather than the airfield operations department developing WiFi to support their inspection of vehicles, while the airport's security department installs a wireless perimeter intrusion detection system, the organization can create a common plan that ensures coexistence, or even potentially shares a common WiFi system that everyone can utilize. This common system will help reduce interference between the separate sources of RF, while at the same time better meeting the needs of all those utilizing the WiFi connectivity and decreasing the overall cost of system ownership. This simple example applies equally to all airport interior WiFi systems, as well as those systems operating in the airplane parking aprons, baggage areas, and service areas. Coordination among all stakeholders will reduce interference and better meet the needs of all involved.

However, developing this common view, and an enterprise governance attitude, is difficult if proper planning and procedures are not put into place, hence the requirement for an airport strategic wireless plan. At least yearly needs assessments should take place among the many stakeholder groups, with priorities weighed and supporting infrastructure evaluated. Furthermore, quarterly technology governance meetings could be held with key departmental leaders to share thoughts and voice upcoming initiatives that may affect one another.

In the case of WiFi, these yearly assessments and quarterly meetings can help departments ensure systems that rely on the infrastructure are supported, and new initiatives will not threaten the integrity of the existing network. Furthermore, enterprise-wide technology planning and governance can help departments realize synergies that reduce overall system costs.

The Strategic Plan

Airports share significant similarities with healthcare in relation to WiFi networks. Airports and hospitals both have large numbers of people who transit through their facilities and commonly connect with their own devices. Airports and hospitals also share a mix of WiFi applications, supporting their visitors but also supporting core functions for the organization. In May 2014 the Association for the Advancement of Medical Instrumentation (AAMI) Wireless Strategy Task Force published "FAQ for the Wireless Challenge in Healthcare." That document states the following:

> **What are the biggest mistakes that healthcare delivery organizations make in managing wireless issues?**
>
> . . . . At a high level, these mistakes can be summarized as, "The biggest mistake a healthcare delivery organization can make with wireless is failing to create a strategic plan on how to use and implement wireless technologies. Each wireless technology, whether it be WMTS [wireless medical telemetry service] telemetry, cellular telephones, WiFi networks, or proprietary technologies for RFID [RF identification], requires a significant investment in infrastructure, and presents multiple risks, including security breaches, patient safety issues, and adverse impacts to other wireless applications. Failure to create a foundational strategy increases the probability that the risks become adverse events.[15]

Wireless services are part of total airport operations and may therefore be considered a component of the airport's strategic vision and plan. Figure 21 depicts how planning for wireless services for all customers, stakeholders, and airport operations fits into the airport's overall strategic plan. This is just one example of how different airport entities are related and conceptually depicted from a strategic planning perspective. There are other ways to depict this relationship if the airport chooses a different approach, i.e., segregate the users or take complete ownership and control of the network. However, the key is to establish a strategic plan that shows the relationship between all airport parties, minimizes future problems, and effectively plans for wireless network growth.

[15] AAMI Wireless Strategy Task Force, "FAQ for the Wireless Challenge in Healthcare," May 2014, question 4.

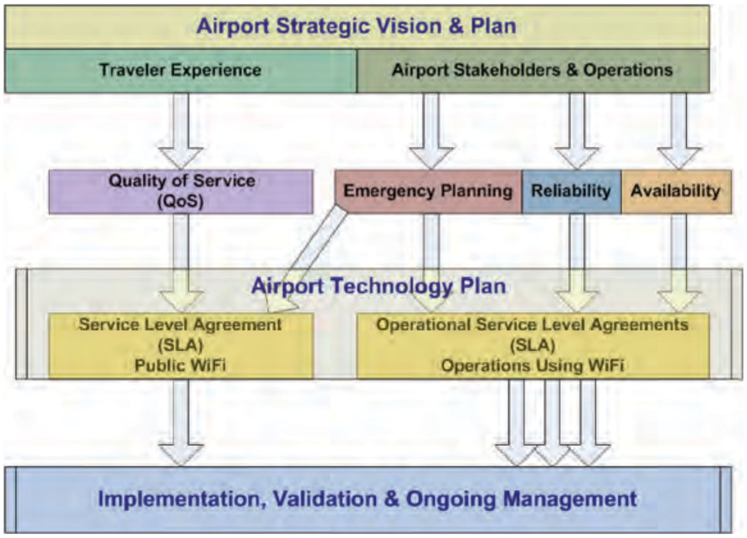

Airport Strategic Vision & Plan
Traveler Experience
Airport Stakeholders & Operations
Quality of Service (QoS)
Emergency Planning
Reliability
Availability
Airport Technology Plan
Service Level Agreement (SLA) Public WiFi
Operational Service Level Agreements (SLA) Operations Using WiFi
Implementation, Validation & Ongoing Management

Figure 21. Objectives for wireless services are a component of an airport's strategic vision and plan.

Generally the strategic plan divides into planning for the public network, stakeholders, and the airport's own operational uses for the WiFi network. The level of service desired can be very different between the three and may impact overall network design. If the airport operates only one network, then maintenance is easier and there are potential cost savings, as well as the possibility of sharing those costs across multiple stakeholders. Different services can be separated into logical networks and assigned appropriate priorities. However, they still share the same underlying network and therefore have shared vulnerabilities. The alternative is to have multiple, independent networks. This can cost more, complicate maintenance, and increase the potential for interference. However, each network can be designed for the services it is intended to provide, either for public access, stakeholders, or to support a network airport operation.

A wireless service plan is a part of the airport's overall technology plan. It must support the larger plan and fulfill its role within it. The resources required to implement the wireless services must fit within the total technology plan, which must fit within the airport's budget, fiscal objectives, and overall business case.

Rough Order of Magnitude Estimates

When planning a new airport network installation or a network upgrade, it is helpful to first do a rough order of magnitude estimate of the current airport interior WiFi needs and the future needs, within the planning horizon of the estimate. The rough order of magnitude estimate provides a ballpark assessment of the cost and complexity of the project and serves as a planning tool for more detailed project planning.

Passenger traffic flow through the airport is one of the starting places. It is important to know how many will pass through the airport and also what the traffic peaks look like. Network planners need to beware of being misled by the averages. Average traffic is very different from peak traffic. Airports want their networks to give all passengers a good experience, including those who pass through during holidays or are at the airport during an irregular operations period, such as when network traffic is high due to weather-related flight cancellations and delays. It is also important not to rely on current traffic numbers but to look at forecast traffic estimates through the master planning process.

From analyzing the airport traffic, the next step is to estimate the number of associated devices and the number of active devices expected to be used. A rule of thumb used to be that 25% of travelers have a device that can connect to the network. It is probably better to use a 50% estimate today. Associated devices are not active devices. However, every device that connects to the network has an impact on network capacity.

Network planners have a variety of ways to estimate the capacity that a network must have. In a highly dynamic network with fluid use, peaks and valleys in demand, but also the interference that occurs in open environments, excess capacity is needed. Interference impacts network capacity in a variety of ways, such as increasing the amount of data sent when retransmission rates rise and data is sent twice and sometimes multiple times. To improve tolerance for interference, extra network capacity is needed to support the mitigation measures, such as retransmission or slowing of transmission speeds, used to reduce the impact of interference.

Reference Design

Reference design or reference architecture is a loose term that applies to many things. For example, in a building like a skyscraper it refers to the architectural layout and services like elevators, central lobby, plumbing, wiring, and heating and air-conditioning. Reference design connotes a given convention for the physical layout and for services. It is not cast in concrete and has variations.

Airport building reference architecture refers to common layout modules like ticketing, baggage, transportation, food courts, passenger waiting areas, restrooms, and gates—positioned with respect to the site and to the space and operational functions inside the building.

A WiFi reference architecture can be based on similar items centered on network users. In a WiFi network the architecture would be based on the number of airport users and operational functions, the number of airport stakeholders and business concerns, the total number of transiting passengers both at off- and peak-times, the area of coverage, WiFi equipment design limitations or capabilities, as well as the airport architectural layout and its potential impact on network design. In addition, acceptable levels of performance (i.e., metrics), user priorities, stakeholder participation, and a management and reporting structure will also have to be identified as they will affect the WiFi network design. There can be other factors included in the architecture as deemed necessary by the individual airport, but these form a baseline to create a strategic plan that can be used by an airport initially installing a WiFi network or leveraged by airports wishing to mitigate interference problems, upgrade, or expand the network. Cost along with perceived value then becomes the driver for how much or how soon some of these services can be implemented.

For example, WiFi reference architecture can show how the hotspot networks are distributed throughout airport areas, the different networks they serve, and how they are controlled. Since airport designs are often common across "same size airports," the hotspots can be in similar relative positions but varied to adapt to the specific RF environment.

In essence, there are some common layouts both in space, network, and RF environments that work better than others. They are used as a starting point and adjusted if need be for optimal performance. This is not an exact science but provides a framework that can be customized based on past experience and identified RF interference issues. IEEE may have some additional definitions for certain vintages of WiFi.

Network Performance Management

An aspect of network planning is how the performance of the network will be managed. To manage network performance, one must first know the current performance, or the designed performance of a newly installed network and what its potential might be. Network performance is defined by the user, the identified metrics, as well as the equipment capabilities. It can be defined as the individual link data throughput, the aggregate throughput on a link under load, or the average or peak load on a network. Then metrics must be identified and the network monitored to ensure the network performs as designed.

It is very useful if performance monitoring is built into the network plan from the beginning and can be added as a requirement in the overall WiFi network contract. However, it is possible, but both more complicated and expensive, to add it later. An important contractual element in any agreement with a contractor hired to manage the network is that the airport authority have unfiltered access to network performance data. One of the most effective methods for monitoring network performance is to build it into the core network. This means the data are gathered by equipment installed and owned by the network operator.

Why should a contractor give data to an airport manager that may not reflect well on the company and may result in the airport manager requiring them to spend time and money improving performance? They probably will not unless there is a specific requirement in the contract that the company provide unfiltered data. If the relationship between the network operator and airport authority is a healthy one, then any differences in interests on network performance will be more situational rather than structural.

In the long run, both the network operator and airport manager want the network to operate near its peak performance and meet all operational design performance criteria. However, at a moment in time it might be quite inconvenient or completely impossible for a network operator to have the entire network at peak performance. This can be seen when there is a need to upgrade to a new version of the IEEE 802.11 standard, such as moving to IEEE 802.11ac. Many network operators are already installing equipment that supports IEEE 802.11ac and most airport authorities are giving them a reasonable period of time for this technology transition. The speed with which the network operator upgrades to IEEE 802.11ac could be a point of contention between the two. In general, airport authorities and network operators seem to be finding mutually acceptable timeframes for the upgrade.

Automated Network Management

Companies as well as individual users have become increasingly aware of the many factors that are involved in providing quality wireless control. Technological advances with wireless in general and WiFi in particular are a routine fact-of-life. Each development in turn is heralded as the cure for all ills. The reality typically is far more mundane.

Change occurs so quickly in telecommunications that static plans or manual adjustments to a WiFi network often cannot keep up. The network must be able to manage itself, making near real-time changes in response to the changing situation and demands that it confronts. WiFi equipment vendors are actively developing a variety of automated network management tools to allow WiFi networks to sense and adjust to their environments and the traffic loads placed on them. Using automated network management is necessary now and will be increasingly important with the growing and changing variety of uses of the WiFi network and the proliferation of wireless devices.

However, some of the network automation introduced to the market has fallen short of its promise and at times even caused more problems than it solved. It is not unusual to find a new approach to automation developed with only one type of network environment in mind. In a different type of environment, the automation may be problematic or simply not adaptable to the challenge.

A particular shortcoming in some automated network management tools brought to the market so far is to assume that everyone will use the same architecture and network design that the programmers are accustomed to. There are many different ways to architect a WiFi network.

Some organizations will run one physical network but several logical networks, separated by different SSIDs or virtual private networks (VPNs). The balance between coverage and capacity can be very different. When the network automation is developed assuming one type of network architecture, but the network planners implemented a different architecture, there can be real problems. Some automation has shown a tendency to misallocate channels and/or power levels, leading to system instability and a variety of performance problems.

Some automated network management software will have WiFi access points automatically lower their power levels to avoid interference with other access points. The decision is typically based on access points measuring the signal level of their neighboring access points and then keeping that signal level below a predefined limit. However, this doesn't take into account the area an access point was installed to cover. A poor client experience can result if the lower power for the area covered provides the user with an inadequate signal. An example is a long hallway with access points installed along its length. Each access point is intended to provide signal into the rooms to either side of the hall, but there will be losses through the walls, furniture, and objects in the rooms. However, the access points have direct line-of-sight to each other. If the access points lower their power to avoid interfering with each other, the result could be insufficient signal strength into the rooms the access point is intended to cover.

Automated channel selection, intended to ensure that access points use channels that are separated in frequency, have in some cases been found to assign several access points in the same area to the same channel. In other cases, feedback loops have been created in which some access points change to avoid interfering with others. However, when access points change channels, their new frequencies can cause other access points to change channels and the chain reaction continues—with access points continually changing channels trying to get out of each other's way. The result can be constant change and an incredible loading on the network for no purpose. This is a serious issue; in some installations the problems became so bad that the network manager had the automated network removed, because the access points were continuously switching channels in an attempt to find a channel without noise. The challenge is that there is always noise in dense networks, so automated channel-selection algorithms need to configure the network for the lower interference over time, while also allowing a level of interference that will always exist.

A useful technique is to look at the channel plan on an access point management console. Superimposing the channel numbers used over the building floor plan makes it relatively easy to evaluate the result of the automated channel assignments. Are all of the allowed channels being used? Are the channels evenly allocated within the area? Are neighboring access points using different channels? Because the channel assignment software will change assignments, it is useful to recheck the plan periodically. Improperly allocated channel assignments can result in a significant lack of capacity and other performance degradation.

The assigned power levels should also be checked. In some cases, it has been found that the automated control has all the access points operating at very low power levels, sometimes as low as 0 dBm—only 1 milliwatt. These checks should also be repeated periodically and particularly during times when the network is more heavily loaded.

With the growing complexity and dynamic nature of WiFi networks, control automation is becoming an integral component. However, it needs to be checked and monitored as a routine part of managing the network until confidence is established. Changes to the control automation should initiate additional monitoring to ensure continued confidence in the tools. Returning to manual control of WiFi networks might be feasible for smaller airports, but it will be increasingly unworkable for major airports in the future.

CHAPTER 5

Stakeholder Relationships and Business Model Options

An airport authority has multiple stakeholders it must work with regarding its wireless services. The solutions to interference must be solved within the business models and stakeholder relationships that either currently exist or that can be adopted. If an RF interference solution is not affordable, it will not be implemented. If one stakeholder is suffering interference, but another must pay for the solution, there is unlikely to be a change. Costs and consequences must be aligned. Those that suffer the consequences of RF interference must find ways to incentivize and compensate those who have the ability to mitigate the interference and improve performance.

While passengers using WiFi may be the first stakeholders to come to mind, airport tenants and an airport's own operations personnel are equally vested in having a reliable network and, in fact, may be considered more important users of the network. Another stakeholder group is the airport's own emergency services (such as aircraft rescue and firefighting), as well as off-airport mutual aid responders. Their equipment follows the general trend and increasingly integrates WiFi and wireless functionality. While they may not operate at the airport on a daily basis, they do not want an internal airport terminal interference problem with their WiFi equipment during an actual emergency.

Television stations and media should also be considered. Media are always interested in aviation stories such as stranded travelers, security events, or other irregular operations. Many airports have specific media staging areas for them to broadcast from near the terminal or sometimes inside the terminal. What is not planned is how remote broadcast television trucks may cause interference with internal airport WiFi networks since some stations have an assigned auxiliary broadcast frequency overlapping the 2.4 GHz band.

Another operational capability for airports is related to security and uses wireless technology for perimeter intrusion detection along the fence line or in vulnerable areas inside the airport. This technology may also be deployed to help alert and avoid movement area incursions—incidents where vehicles, pedestrians, and/or aircraft have entered into a controlled area of the airfield without proper authorization. Wireless capabilities that alert the airport or air traffic control to such occurrences are becoming increasingly popular technology installations.

All of these relationships come together in the master service level agreement (SLA) between the airport and the network operator it selects. There may be other SLAs established for specific tenants or services. An SLA is recommended anytime a new use for the WiFi network is planned. These individual SLAs give the organization introducing the new service and the network operator a formal method for translating service expectations to technical requirements. Particularly for high-reliability services such as those supporting emergency or security operations, an SLA is important for ensuring that the network operator has agreed it can provide the level of reliability desired.

Master Service Level Agreements

Many airports throughout the U.S. utilize a third-party operator to run their WiFi. This third-party operator often has complete control over the WiFi system, with a simple set of functional guidelines to adhere to throughout the long length of the contract.

These functional guidelines are often based on metrics that enforce system operability and coverage, ensuring that all airport stakeholders are able to use the WiFi network in the many different areas of the airport. Bandwidth and system revenue are often large drivers of these SLAs, as third-party operators are required to provide a certain amount of bandwidth per user, along with positive cash flow from advertising or other WiFi-generated opportunities. Furthermore, these SLAs often enforce non-emergency and emergency maintenance services onto the WiFi operator. Some call for 99% up-time for the system or other measures of network availability. There can be component-level requirements for coverage, defined by minimum signal strength for an access point over the entire area to be serviced. There can also be requirements for controller availability.

Service Level Agreement Enforcement

Contracts and SLAs with varying complexity exist throughout the U.S. SLAs consistently include penalties for service deficiencies, often in the form of daily liquidated damages from the inoperability of the system. The ultimate penalty, of course, is lease termination.

However, despite existing SLAs, there are still interference and coverage problems, even in third-party operated locations. There are several reasons for this. In some cases, the terms of the SLA are insufficient to ensure the required level of performance. Writing specific, enforceable SLA requirements requires in-depth knowledge of WiFi and network operation. If the SLA is overly general or fails to address a key area, the result can be inadequate service.

Another common problem comes not from the SLA's inability to hold third-party operators to their contracts, but from airport authorities that do not monitor the system and the performance metrics adequately. It takes special tools and expertise to evaluate network performance. A major reason airports contract with a network operator is that they do not have the time or tools to do the job themselves.

Airports across the U.S. do not regularly measure the performance of their WiFi system, especially as it pertains to interference. Reports are regularly filed by third-party operators of the WiFi, with little airport oversight or testing of the system in the field.

As such, airport managers should employ their own RF testing schedule within their facility, and ensure that the airport's WiFi operators are living up to the conditions of the SLA. Wireless site surveys should be conducted on a monthly or at most quarterly basis, in order to gain an understanding of RF interference sources. The results of these surveys should be reviewed with third-party operators, and areas with less than satisfactory coverage addressed.

Shared Tenant Services

WiFi, and in general device connectivity to the network, is more and more commonly viewed as an expected utility instead of an added service. This utility is used not only by those traveling through the airport but by those employed by, and working in and around, the airport facility. Often, some of the heaviest and most consistent users of the WiFi at an airport are not its travelers, but those who earn their livelihood working at the airport as employees.

These daily users require data connectivity along with wireless service but, for a variety of reasons, may not wish to rely on an airport's WiFi service. The alternatives to airport-managed WiFi could include the installation of tenant-owned access points within their lease area, or activation of hotspots or cell phones to satisfy the coverage need. Tenants have a variety of conveniently available options for Internet access, but the airport's WiFi network is benefited when it is used as a shared resource.

Alternative Revenue Sources

Some airports have alternate non-airline revenue sources such as gambling in McCarran International Airport (LAS) and gas wells at Dallas/Fort Worth International Airport (DFW), which offer increased budget options to support their WiFi networks. In general, the pattern is that a network operator installs and manages the network and balances capital and ongoing operating cost with revenues. The airport authority negotiates the contract with the vendor and once the airport is satisfied with the balance between cost/revenue and customer satisfaction, they are happy to leave the technical planning and operation of the network to the selected network operator.

Alternative Connections and Their Impact

Not dissimilar to the traveling public, airport and stakeholder employees will find alternative ways to acquire wireless connectivity if an airport's connectivity is not adequate. Operational areas, tenant lease spaces, and third-party offices provide their own wireless if it is not available for them.

The addition of alternative access points or other wireless devices within an airport environment only compounds the problem of wireless interference. Connections and networks operating independently, and often without coordination with the main WiFi network, can push a strained system to its functional limits. This has been evidenced by airlines and tenants installing their own support infrastructure systems without the airport's knowledge. If the airport does not provide these services as part of a lease contract, or does not have any policies in place to deter such practices, there is little control over the growth of multiple systems.

However, providing connectivity for these tenants and operational areas from the airport's existing wireless infrastructure is not as simple as installing additional access points. Service set identifiers and possibly fully separate virtual local area networks (LANs), with dedicated bandwidth and administrative support, will be required to make the wireless usable for whichever tenant requires it. This additional infrastructure and configuration comes with expenses, and in the case of free WiFi, additional upkeep and maintenance, along with higher bandwidth needs from the airport's Internet service provider. All this must be offered to the tenant for a cost that is attractive when compared with other options available to them.

This combination of wireless needs in tenant spaces, compounded by additional expenditures in providing additional infrastructure, results in the need for the airport manager to take a new look at shared tenant services for WiFi connectivity.

Benefits of Shared Tenant Services

Shared tenant services (STS) are a multi-tenant environment business model in which a property owner provides a common set of sophisticated technical services. Telephone service, cabling infrastructure, and wireless data networks are some examples of resources that can be airport owned, managed, and shared among various tenants. In a traditional model, rather than each tenant purchasing, installing, and maintaining an individual system, airport tenants and the airport share a common system. For voice applications (the traditional and most common type of STS in airports), this may include a private branch exchange (PBX) telephone system or a voice over Internet protocol (VoIP) system. Shared tenant services provide the potential to effectively and efficiently address all the telecommunications, data network, and tenant services requirements at an airport, including accountability, communications, processes, and response. Tenants benefit from the convenience of having one stop for all their communications requirements, including on-site support.

Shared Tenant Services Pricing Model

Shared tenant services can be implemented either as a new revenue stream, or as a method to recover costs and improve customer service. Pricing models for airports should first examine their fundamental approach to servicing tenants and customers at the airport, and whether pure customer service, or profitability, forms the core of an STS wireless model.

The fundamental assumption of the wireless STS pricing model is that each new service provided for a tenant is incremental to the existing infrastructure. As such, the pricing for the additional wireless services reflects at least the recovery of the additional costs, along with any margin that the airport wishes to implement. These additional cost components associated with wireless service for tenants include the following:

- **Administration:** The administrative costs include a possible help desk, cable management system, coordination, and costs associated with developing and marketing the overall program.
- **Connectivity:** The connectivity costs include network costs (specifically Internet access) associated with a particular access point.
- **Hardware:** The hardware costs include the amortized cost of new hardware (i.e., network switches) necessary to provision a particular service.
- **Cable Installation:** The cable installation costs include the amortized cost of installing new cable, along with possible installation of fiber infrastructure. Conduit, tubes, and termination blocks should be excluded from these calculations.
- **Provisioning:** The provisioning costs are the initial costs associated with creating a new circuit. These include infrastructure assignments, cross connections, escort time, and circuit testing.
- **Maintenance:** The maintenance costs include personnel costs associated with maintaining and troubleshooting the connection over the course of the agreement.

Many costs associated with implementing a wireless STS model are fixed, and therefore represent a higher percentage of overall STS charges. It should be noted that costs, and the subsequent rates charged to tenants, need to remain competitive with other wireless connectivity options. If costs are not competitive, then tenants may seek to use other connectivity options, increasing the chance of interference and decreasing financial support for the airport's WiFi infrastructure.

Business Model

Any solution to an RF interference or network performance problem must be implemented in the context of the airport's business case—how the airport creates, delivers, and captures value in economic, social, cultural, or operational requirements for wireless services generally and for the WiFi network specifically. This process of implementing an interference mitigation plan is part of the overall business strategy. If the cost of the solution is not perceived as affordable, it will not be implemented or may be only partially implemented. The solution must also be temporally feasible. For example, it is unlikely an airport manager will solve a complaint about interference reported at Gate 9 by planning a total and costly network upgrade that would take months to be approved, let alone implemented.

However, the perceived business case and the real business case can be different. This is particularly true with the changing role of the WiFi network. Many still perceive WiFi as a high-end amenity that has little impact when it is not available. However, with the network's increasing integration into airport operations, the cost of disruption can be substantial.

The temporal aspect can also be falsely perceived. Choice of metrics is critical. If an airport's metric is customer complaints, then the timeframe for resolution is very short. The complaining customer wants the problem resolved during the time they are in the airport. However, if a different, more forward-looking metric were chosen, then timeframes of months or years might be available to solve a growing problem. The options available multiply.

There is a rule of thumb based on experience among engineers who specialize in interference resolution that the cost of the solution goes up not by an increment, but by an order of magnitude for every stage of implementation. The time when a change is most expensive and when options are the fewest is after a network is deployed and products are installed. Few solutions are then available and their cost is extremely high. Installing an interference solution during a network upgrade will often be a tenth of the cost, and many more solutions become possible.

It is not uncommon to find that all that is needed for major improvement is, first, determining the sensitivity to interference—known in the field as the devices' coexistence capability—and then selecting more interference-resistant equipment. If manufacturers receive negative feedback focused on their equipment from many sources such as airports, they perceive potential loss of sales. Market forces can often make the difference in cost between interference-resistant equipment and interference-sensitive equipment small or even non-existent.

One missing component between WiFi consumers and the manufacturers is information on interference-related complaints about products, accompanied by a drop in sales. For example, if filters to reduce interference from adjacent WiFi channels were installed, some, but not all, of the adjacent channel interference could be removed.

Similarly, linear amplifiers could preclude some transmission interference on the WiFi waveform. Manufacturers will likely fix these and other sources of equipment-generated interference if they perceive a profitable business case via airports or other similar applications where interference mitigation is needed. But manufacturers need to know how much and what type of interference resistance airports want before they start development of a new generation of products. They can often build those specifications into the design for a small fraction of what it would cost to provide a similar solution as a retrofit to an already designed product. Similarly, if chip and component manufacturers know what interference resistance is needed in products that use their components and how that end performance relates to specifications, they can often provide interference-resistant components at a small fraction of the cost of adding that same solution to existing product design.

Beyond influencing WiFi manufacturers, the airports can work with standards development bodies, such as the IEEE 802.11 committee, and trade associations, like the WiFi Alliance, to make RF immunity and coexistence part of the standards and product certification process. Such efforts may take place years before the impact will be seen in products installed in networks, but they have the lowest total cost and open up the largest possible set of solutions. Not every airport can do this, but if airports as a whole had representation, then they could influence future standards as well as mitigate potential future interference issues. There may even be a cost savings by ensuring higher quality equipment as well as avoiding the cost of resolving future network problems.

A list of best technical practices to ensure accessible WiFi service is provided in Appendix B.

CHAPTER 6

WiFi at Small and General Aviation Airports

Small and general aviation airport terminals are smaller and typically simpler architectural structures. They generally are not as busy as major airports in terms of number of flights and passengers. These airports are likely to have less dense requirements for WiFi usage, certainly not to the level needed at major airports. Designing a reliable network and resolving interference problems are still necessary tasks, but the solutions are even more sensitive to costs.

Small and general aviation airports will likely scale their WiFi and other wireless services to the affordable necessities. For example, only low-cost network computers, servers, and WiFi hotspots may be acceptable in this environment. These supportable reference architectures can vary from airport to airport depending on affordability. It is still practical to design a reference architecture for small and general aviation airports using the previously identified stakeholders. An airport strategic plan is just as important for a small airport as for a larger airport.

There are models in the Cisco publication “Smart Airports: Transforming Passenger Experience to Thrive in the New Economy”[16] that larger airports mostly follow, and which also can be used in part for smaller airports.

The first model is for “agile airports” that adapt well to a changing technical and business environment and operate at a fast-paced operational tempo. Services provided include managed communications, VoIP telephony, broadband, WiFi, and video surveillance at competitive market prices, without the need to deploy and maintain their own technology solutions. Such a system “offers advanced operational efficiencies.”

The second model comprises “smart airports” that fully exploit the power of emerging and maturing technologies for communications and services. “Systems are built around a ‘digital grid’: a single, converged, often carrier-class IP network that enables high-speed broadband traffic throughout the entire ecosystem, including the airport, airport city, airlines, seaport, logistics, authorities, and other parties.”

WiFi is imbedded in both system reference architectures. Both technical approaches are predominantly focused on larger airports where the size of the conglomerate scope of business can economically support the installation and maintenance of either system.

The cost of these two systems is likely to be unaffordable to small and general aviation airports, especially since the WiFi and Internet connections for integration interconnects do not need to be as sophisticated as those implemented at larger airports. However, the systems can be examined for an abbreviated WiFi extraction analysis. Most of the steps that follow are but a small percentage of the full scope of network planning, but are practical for smaller airports. The steps are not complicated and can be accomplished by a person who is familiar with the WiFi basic technology

[16] Cisco, “Smart Airports: Transforming Passenger Experience to Thrive in the New Economy,” July 2009.

or by small, reputable WiFi service companies in the area. The key is to establish what level of WiFi service is needed and plan for growth. These points would need to be further verified and quantified from recent history and then through future projections of growth and usage.

The following sections summarize a simplified design methodology that captures the WiFi design considerations and specifications for small and general aviation airports.

Step 1: Identify WiFi Requirements Per Physical Areas

1. From "The End-to-End Passenger Journey" described in the Cisco publication, address 10 elements (of the 33) that are most likely to impact the WiFi network design. These include:
    - Check-In
    - Baggage
    - Passports
    - Customs
    - Security
    - Food
    - Retail
    - Gate
    - Boarding
    - Entertainment

    The relative physical area layout containing these points of interest should be determined within the airport terminal, along with the expected quality and maximum expected WiFi throughput requirements documented.
2. Document any additional passenger WiFi elements needed in the specific airport that are not on the above list. Correspondingly, eliminate items not needed.
3. Document any additional airport WiFi element requirements that need to be included in the system for critical operation of the terminal and airport. Note special consideration and analysis may be necessary for elements that are critical to the airport, such as security, inside terminal emergency response, and alert notifications. These should be provided with priority for message completion reliability. Some analyses may be needed to assure acceptable levels of service. Note in small or general aviation airports, dedicated non-WiFi communications systems may already be in place and work well. Keeping what works cost-effectively and reliably is the simple rule to follow.
4. Document whether WiFi is to transit through cables internally or externally from the airport.

Step 2: Quantify Desired Service Levels and Begin Design

The next step is to provide quantitative numbers for the above requirements and start the design specifications. Some considerations are as follows:

1. The physical area layout should start with a construction blueprint or equivalent that is to scale. Locations and areas of WiFi service, along with minimum acceptable signal levels, can be marked or referenced to a list. This layout will eventually indicate the WiFi performance specifications in figure format, i.e., areas of coverage and minimum signal levels. Multiple copies of the layout diagrams may be generated to specify the WiFi service level requirements, particularly in different areas of the airport or for different services provided.
2. If an existing WiFi system is in place and is to be upgraded, consider the following:
    - Note any past problems with WiFi and include appropriate mitigation actions in the new specifications. These can include location, assigned frequency, signal strength of hotspots, or other items.

- Note any unresolved problems; check if the new design can be expected to resolve the issues. This may be placed in a specification for installation if contracted out.
- Determine signal strengths and performance throughput of the existing installed system throughout the airport. Note if measurements were performed periodically; estimate the growth slope for least, medium, and high WiFi usage areas. Upgrade the specification, including new areas, using this information to establish desired growth margins.
- Establish priorities of service for the airport if not already in existence; expect security, inside terminal emergency response, and alert notifications to have top preference. Ticketing, baggage, RF identification, and other support functions inside the terminal may be second in priority preference. Entertainment can have high priority or the lowest priority depending on the business model within the airport. Note that a well-designed WiFi network layout under reasonable load may not need a priority schema except in emergency circumstances.

3. Make a final set of measurements documenting the existing WiFi network performance. Stress system load as much as practical to achieve good or acceptable performance results. Use this set of measurements for acceptance tests to assure upgrade starts at this same level of load and performance and has margin for growth.
4. Check on the airport supplier of WiFi over the air (or cable) to assure the derived requirements can be met with the WiFi input to the terminal building. If the WiFi supplier has a weak input signal to the terminal and it is determined to be unacceptable, postpone installation or upgrade until the WiFi input is optimized.
5. Document all of the above in specification format.
6. Choose an installer by bid or existing contractor.
7. Check the installation proposed, particularly the location and frequency assignment of adjacent hotspots, to avoid potential interference from adjacent channel overlap.
8. Finally, perform acceptance runs to verify system performance as specified above. Periodically perform some subset of these acceptance runs to check on the health and status of the installed system.

In some cases where the airport is very small and the usage is limited to a few services like Internet access only, self-installation using off-the-shelf components may be the most economical solution, provided the airport has someone who is WiFi knowledgeable. Local small business WiFi expertise may be a possibility for a starter system.

Step 3: Establish and Maintain Data

Finally, it is recommended that a database of problem reports and solutions be kept in a simple format and that periodic measurements be taken to assure performance. These best practices and other recommendations are listed in Appendix B of this Guidebook.

CHAPTER 7

References and Resources

This chapter is a compilation of recommended reading and resources on the topic. These resources each have significant value in gaining a better understanding of WiFi and the best methods for maximizing network efficiency. Standards related to the management of WiFi are also cited.

Standards

[1] IEEE 1900.2:2008: IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence between Radio Systems

[2] ISO TR 20000-1:2011: Information Technology—Service Management

[3] ISO TR 80001-1:2010 Application of Risk Management for IT-Networks Incorporating Medical Devices—Part 1: Roles, Responsibilities and Activities

[4] ANSI/AAMI/IEC TR 80001-2-3:2012: Application of Risk Management for IT-Networks Incorporating Medical Devices—Part 2–3: Guidance for Wireless Networks

[5] AAMI TIR 18:2008: Guidance on Electromagnetic Compatibility of Medical Devices in Healthcare Facilities

Best Practices for WAN Interference Management

[1] BAA's Response to Ofcom's Consultation, Higher Power Limits for License Exempt Devices, 2006.

[2] Cisco Systems, Cisco Intelligent Airport Wireless (WI-FI) Network Solution, 2004.

This white paper is now rather dated but shows how quickly this area is changing. For example, statements that laptops now are including WiFi and that there are over 10,000 WiFi hotspots in the U.S. now seem like ancient history. However, many of the basic management techniques presented continue to be used effectively.

[3] Cisco Systems, Enterprise Mobility 4.1 Design Guide.

Available at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

This book describes the design and implementation of the Cisco Unified Wireless Network solution for the enterprise, using the features incorporated in the Wireless LAN Controller software Release 4.1.

[4] Hoglund, David, Are Mobile Medical Devices "Hospital Grade"? Meeting the Challenge of Today's Healthcare WLANs, April 29, 2013.

Available at: http://info.ixiacom.com/rs/ixiacom/images/Ixia-David-Hoglund-Medical-Device-Testing.pdf

Integra Systems and Ixia provide this healthcare white paper focused on the growing need to validate and verify the performance of wireless medical devices and healthcare networks. They propose the need for proper validation as a critical paradigm change in the medical device and healthcare provider marketplace. The new model of testing and validating the performance described in this paper can decrease costs, mitigate serious risk to providers' brand reputation, and vastly improve the overall quality of the wireless experience.

[5] Raymond, Phil, The Wireless Challenge: Achieving a Robust and Reliable Network, *Biomedical Instrumentation & Technology*, May/June 2013.

This article is a very useful overview, written by someone who deals with the issues on a daily basis.

[6] Silver Peak Systems, Inc., Best Practices for Deploying WAN Optimization with Data Replication.

Available at: http://www.silver-peak.com/sites/default/files/infoctr/silver-peak_wp_best_practices_withdatareplication.pdf

[7] Silver Peak Systems, Inc., Five Ways to Optimize Offsite Data Storage and Business Continuity

Available at: http://www.silver-peak.com/sites/default/files/infoctr/silver-peak_wp_optimize_offsite_dr.pdf

[8] WiFi Alliance, WiFi in Healthcare: The Solution for Growing Hospital Communication Needs, 2011.

Available at: http://www.wi-fi.org/downloads-registered/wp_Wi-Fi_in_Healthcare_20110217.pdf/Wi-Fi%25C2%25AE%2Bin%2BHealthcare%253A%2BThe%2Bsolution%2Bfor%2Bgrowing%2Bhospital%2Bcommunication%2Bneeds%2B%25282011%2529

[9] WiFi Alliance, WiFi in Healthcare: Security Solutions for Hospital WiFi Networks, 2012.

Available at: http://www.wi-fi.org/downloads-registered/wp_201202_Wi-Fi_Security_for_Hospital_Networks-Final.pdf/Wi-Fi%25C2%25AE%2Bin%2BHealthcare%253A%2BSecurity%2BSolutions%2Bfor%2BHospital%2BWi-Fi%2BNetworks%2B%25282012%2529

[10] WiFi Alliance, WiFi in Healthcare: Improving the User Experience for Connected Hospital Applications and Devices, 2013.

Available at: http://www.wi-fi.org/downloads-registered/wp_201305_Healthcare-Improving_User_Experience.pdf/Wi-Fi%25C2%25AE%2Bin%2BHealthcare%253A%2BImproving%2Bthe%2Buser%2Bexperience%2Bfor%2Bconnected%2Bhospital%2Bapplications%2Band%2Bdevices%2B%25282013%2529

[11] Smith, Graham, Dense Apartment Complex Capacity Improvements with Channel Selection and Dynamic Sensitivity Control, presentation to IEEE 802.11, IEEE 802.11 document IEEE 802.11-13/1487r2.

This presentation claims dynamic sensitivity control produces improvements of:

– 296% for Single Apartment Complex
– 412% for Double Apartment Complex

[12] Smith, Graham, Airport Capacity Analysis, IEEE 802.11-13/1489r2.

This presentation extends the author's apartment analysis to airports.

IEEE 802.11ac & 802.11ad

[1] Perahia, Eldad, and Gong, Michelle X., Gigabit Wireless LANs: An Overview of IEEE 802.11ac and 802.11ad, *ACM SIGMOBILE Mobile Computing and Communications Review*, Volume 15, Issue 3, July 2011, pgs. 23-33.

Available at: http://www.informatik.uni-trier.de/~ley/pers/hy/p/Perahia:Eldad.html

An excellent introduction to the history of the IEEE 802.11ac and 802.11ad standards, their development history, and use cases. Eldad Perahia, one of the authors, was chair of the IEEE 802.11ad committee and hence, an authoritative source for this information.

[2] Myles, A., and de Vegt, R., WiFi Alliance (WFA) VHT Study Group Usage Models, IEEE 802.11-07/2988r4, March 19, 2008.

Available at: https://mentor.ieee.org/802.11/dcn/07/11-07-2988-04-0000-liaison-from-wi-fi-alliance-to-802-11-regarding-wfa-vht-study-group-consolidation-of-usage-models.ppt

A presentation of the WiFi Alliance usage models used as a basis for the IEEE 802.11ac and 802.11ad standards.

[3] WildPackets, 802.11ac and 802.11ad: What They Are and How They Will Impact Your Network, April 5, 2012.

Technology Trends

[1] Department of Defense, Electromagnetic Spectrum Strategy (EMS), September 11, 2013.

The DoD sets forth its spectrum strategy and in doing so highlights how it will address a variety of issues in spectral management. This document is significant for the insight it gives to future DoD activities related to spectrum management.

[2] Frenzel, Louis E., Freescale's Ritu Favre Discusses Today's RF Technologies, *Electronic Design*, October 3, 2013.

Component manufacturers work closely with their leading customers to support their needs and have the components available for the next generation of technology. This article is a good example of how that methodology can give insight to emerging trends. Freescale is a leading provider of RF components, particularly power amplifiers, and a good example of how new components show the next steps their customers will be taking with their products.

[3] Frenzel, Louis E., WiFi and Bluetooth Rule the Airwaves, *Electronic Design*, July 11, 2013.

A very interesting article discussing the growing dominance of Bluetooth and WiFi operating in the 2.4 GHz ISM band.

[4] The joint ACI, Airline Business, and SITA report, The 2012 Airport IT Trends Survey.

This is a very useful survey of airport technology trends and priorities.

[5] Radisys, LTE-A and Small Cell Deployment Strategies, May 2013.

Presented in an eBook format, this document presents Radisys's views on the development of heterogeneous networks and the introduction of Long Term Evolution—Advanced (LTE-A) features. It discusses the advantages it sees these developments bringing to network providers and their users.

Small Cell Interference

[1] The Small Cell Forum, Release 3: Urban Foundations, WiFi/Cellular Radio Co-existence in Enterprise Products, Document #064.03.01, December 2013.

Most recent release available at: http://www.scf.io

This very brief report provides important conclusions on the potential for interference from small cell deployments, but unfortunately keeps the underlying research confidential.

[2] Worsham, J., WiFi Femtocell Interference Testing Final, 2010.

[3] 3GPP. TR 36.816: Evolved Universal Terrestrial Radio Access (E-UTRA); Study on Signaling and Procedure for Interference Avoidance for In-Device Co-existence, 2011.

Radio Frequency Measurement

[1] Agilent Technologies, Digital Modulation in Communications Systems—An Introduction, Application Note AN1298.

[2] Feher, Gabor, Bit-Error Analysis in WiFi Networks Based on Real Measurements, 5th International ICST Conference on Access Networks, Nov. 4, 2010.

This is a very useful paper for several purposes. It provides a good rationale for understanding network performance at multiple layers and how cyclic redundancy check (CRC) and other error-correcting mechanisms can hide what is happening at lower layers. The measurements made give significant insight to network performance and how to adapt by decreasing data rates.

[3] Frenzel, Louis, Understanding Error Vector Magnitude, *Electronic Design*, October 10, 2013.

Available at: http://electronicdesign.com/engineering-essentials/understanding-error-vector-magnitude

An excellent and well-illustrated tutorial on modern RF modulations and error vector magnitude.

[4] IxChariot Roaming Test Plan

Available at: http://www.ixiacom.com/sites/default/files/resources/test-plan/wlan_roaming_0.pdf

Ixia's recommended test plan for evaluating WLAN roaming using their IxChariot.

[5] VoIP Testing with IxChariot

Available at: http://www.ixiacom.com/sites/default/files/resources/test-plan/voip_0.pdf

Ixia's recommended test plan for evaluating VoIP performance over WLANs using their IxChariot.

[6] Scott, A.W., and Frobenius, R., RF Measurements for Cellular Phones and Wireless Data Systems, Wiley/IEEE, 2008.

[7] Shafik, R.A., et al., On the Error Vector Magnitude as a Performance Metric and Comparative Analysis, IEEE 2nd International Conference on Emerging Technologies, November 2006.

Multiple-in, Multiple-out

[1] Bhagavatulay, R., Heath, R.W., Jr., and Linehan, K., Performance Evaluation of MIMO Base Station Antenna Designs, *Antenna Systems & Technology*, Vol. 11, No. 6, Nov./Dec. 2008.

Other Articles & White Papers

[1] ISCO International, Airport Communications at Risk, 2012.

[2] Cisco Systems, Wireless RF Interference Customer Survey Results, 2010.

Available at: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/white_paper_c11-609300.pdf

The survey results are very interesting but more useful as a representation of generally held opinion than a research result. Based on this survey, RF interference is clearly an issue in the minds of a majority of IT managers. However, to verify if that belief is accurate requires objective evidence to differentiate true RF interference from other sources of performance degradation.

[3] Cisco Systems, 20 Myths of WiFi Interference: Dispel Myths to Gain High-Performing and Reliable Wireless.

[4] Cisco Systems, The Future of Hotspots: Making WiFi as Secure and Easy to Use as Cellular.

[5] Cisco Systems, Guidelines and Tools for Migrating to the Cisco Unified Wireless Network.

[6] Kerner, S.M., Cisco Aims for Clean Air on WiFi, 2010.

[7] Frenzel, L., WiFi and Bluetooth Rule the Airwaves, *Electronic Design*, July 11, 2013.

This article gives an excellent overview of WiFi and Bluetooth protocols. Its main purpose is to discuss their market dominance, which it accomplishes with considerable insight.

[8] Visiwave, Visualize Your Wireless Network.

Available at: www.visiwave.com

[9] Bandspeed, Understanding the Effects of Radio Frequency (RF) Interference on WLAN Performance and Security, 2010.

[10] Howard Preston Cinema Systems, The Wireless Jungle, 2009.

[11] IEEE 802 Working Group Project Timelines

Available at: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

[12] Metageek, Interference Identification Guide.

[13] Novarum Inc., High Density WLAN Comparison Testing: Aruba, Cisco and Juniper, September 2013.

A useful study showing the capacity performance differences using equipment from different vendors.

[14] Paul, U., Kashyap, A., Maheshwari, R., and Das, S.R., Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection, 2013.

[15] Intel, USB 3.0* Radio Frequency Interference Impact on 2.4 GHz Wireless Devices, April 2012.

This paper from Intel explains the reason why USB 3.0 data connections can cause WiFi interference and offers suggestions about how it can be mitigated. The paper is well-researched and presented and illustrates an important example of a class of WiFi interference from unintentional emitters.

[16] Coleman, D., and Diener, N., Protecting WiFi Networks from Hidden Layer 1 Security Threats, 2007.

[17] Schneider Electric Industries SAS, WiFi in the 5 GHz Band, April 2011.

Available at: www.schneider-electric.co.uk

This white paper gives a good overview and history of the use of WiFi in the 5 GHz band and the role DFS and transmit power control had in its proliferation. The paper also provides a good summary of the state of international harmonization for the channels in this band.

[18] Matsumoto, Y., Takeuchi, M., Fujii, K., Sugiura, A., and Yamanaka, Y., A Time-Domain Microwave Oven Noise Model for the 2.4 GHz Band, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 45, No. 3, August 2003.

[19] Wireless World Research Form, Working Group C, Communication Architectures and Technologies, Multi-RAT Network Architecture, June 30, 2013.

[20] Zeto, J., Bringing WiFi to Healthcare, *Wireless Design Magazine*, July-Aug 2013.

[21] Thonet, G., et al., Schneider Electric Innovation Department, ZigBee—WiFi Coexistence.

[22] Zubow, A., Sombrutzki, R., and Chausse, R., Reinvestigating Channel Orthogonality—Adjacent Channel Interference in IEEE 802.11n Networks, SAR-PR-2011-14, Humboldt University, 2011.

Available at: http://sar.informatik.hu-berlin.de/research/publications

[23] Villegas, E., López-Aguilera, E., Vidal, R., and Paradells, J., Effect of Adjacent-Channel Interference in IEEE 802.11 WLANs

Available at: http://upcommons.upc.edu/e-prints/bitstream/2117/1234/1/CrownCom07_CReady.pdf

[24] Lakshmanan, S., Lee, J., Etkin, R., Lee, S.-J., and Sivakumar, R., Realizing High Performance Multi-Radio 802.11n Wireless Networks.

Available at: http://www.ece.gatech.edu/research/GNAN/archive/tr-mrd.pdf

CHAPTER 8

Acronyms and Definitions

Acronyms

AAMI	Advancement of Medical Instrumentation
ACI	adjacent channel interference
AP	access point
CCA	clear channel assessment
CRC	cyclic redundancy check
DAS	distributed antenna system
dBm	decibel-milliwatt
DFS	dynamic frequency selection
E-UTRA	evolved universal terrestrial radio access
FCC	Federal Communications Commission
GHz	gigahertz
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet protocol
ISM	industrial, scientific, and medical
IT	information technology
LANs	local area networks
LTE-A	long term evolution—advanced
Mbps	megabits per second
MCS	modulation and coding scheme
MIMO	multiple-in, multiple-out
NIST	National Institute of Standards and Technology
OFDM	orthogonal frequency-division multiplexing
PBX	private branch exchange
QoS	quality of service
RF	radio frequency
RFID	radio frequency identification
SDM	spatial division multiplexing
SGI	short guard interval
SLA	service level agreement
SSID	service set identifier
STS	shared tenant services
TDD	time-division duplexing
UE	user equipment
VoIP	voice over Internet protocol
VPN	virtual private network

WAN	wide area network
WFA	WiFi Alliance
WiFi	wireless fidelity
WLAN	wireless local area network
WMTS	wireless medical telemetry service

Definitions

Access Point: A bridge between a wireless medium and a wired medium.

Advanced Encryption Standard: A symmetric-key encryption standard.

Distributed Antenna System (DAS): An antenna system that collects wireless signals and routes them to centralized locations.

Dynamic Frequency Selection (DFS): A mechanism for dynamically selecting frequencies to avoid interference sources—usually used in conjunction with the mechanism 802.11a-based systems used to avoid frequencies used by radar systems.

Media Access Control: Part of the link layer in the open system interconnection reference model.

Multiple-in, Multiple-out (MIMO): The use of multiple antennas at both the transmitter and receiver to improve communication performance.

Personal Area Network: A computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.

Physical Interface: The Open System Interconnection Reference Model layer of a communication controller that interfaces to the physical world.

Quality of Service: The capability or means of providing differentiated levels of networking performance in terms of traffic engineering (packet delay, loss, jitter, bit rate) to different data flows.

Service Set Identifier (SSID): The 802.11 term that describes a logical grouping of multiple basic service set identifiers.

Unlicensed National Information Infrastructure: Unlicensed spectrum in the 5 GHz range used by IEEE 802.11an devices and wireless Internet service providers.

Voice over Internet Protocol (VoIP): A technology that allows telephone calls to be made over computer networks.

Wide Area Network (WAN): A communication network that spans a large geographical area, providing data transmission across metropolitan, regional, or national boundaries.

Wired Equivalent Privacy: The original security mechanism of 802.11 which has been superseded by TKIP (aka WPA) for legacy devices and AES (aka WPA2) for all 802.11-certified devices since 2006.

APPENDIX A

Radio Frequency Primer

One may do Internet searches on “electromagnetic interference” and find many references to the subject. However, they tend to span the range from a Wikipedia explanation of the fundamentals to complex circuitry and radio frequency (RF) interference effects. What is missing is a special case tutorial relative to the airport terminal wireless fidelity (WiFi) environment. The airport WiFi environment is increasingly complex and the intent of this primer is to (1) provide some basics on interference phenomena, (2) relate interference to the governing regulatory processes, and (3) provide information on possible ways to manage the WiFi network in the airport environment. The purpose is to explain RF interference associated with WiFi and commercial wireless communications devices in the unlicensed spectrum and the resulting issues for airports and tenants.

Introduction

Interference is a basic phenomenon described in physics in which two waves superimpose to form a resultant wave of greater or lower amplitude. For example, when two raindrops fall near each other in still water, the rings produced by each travel until they intersect with each other, disrupting the circular ring patterns (Figure A-1). This visible analogy is a simplistic view of how RF interference occurs when a radio transmission or radiation from some other device interacts with another radio. However, in the RF domain the environment can be more complex, with one or multiple interferers at overlapping operating frequencies and at the same or different signal strengths from different access points interacting with the “victim” receiver (indicated by the blue arrow in Figure A-2). The result can be a disruption, degradation, or limitation of the performance to the victim radio receiver circuitry. This is a simplistic explanation of RF interference, and additional information can be found online.

The Federal Communications Commission (FCC) manages the non-government spectrum and is the spectrum regulatory agency that provides rules and regulations on the use of the spectrum. An abbreviated historical perspective of the spectrum regulatory governance evolution and the meaning of “harmful interference” will be provided first, followed by an overview of interference and perceived misconceptions, a process to work through interference incident reports at airports, and the practical side of how to resolve RF interference issues for airport authorities and tenants.

Historical Perspective: Spectrum Governance, Interference Mitigation, and Tolerable Interference Evolution

This section is intended to provide a brief history of the U.S. regulatory process and the basics of interference and mitigation for readers that may not be familiar with these topics. Then it introduces a potential way forward based on Harm Claim Thresholds.

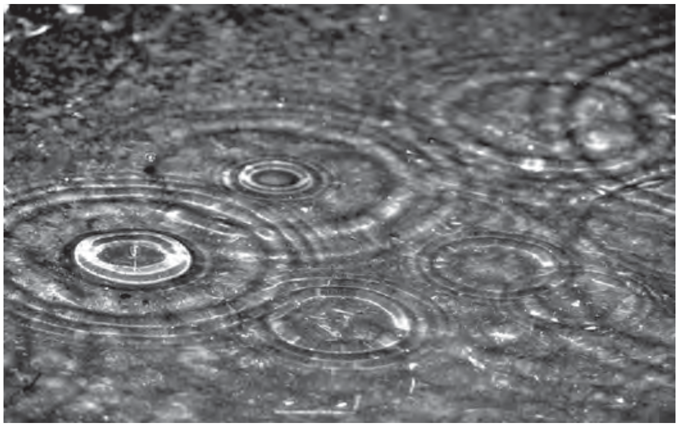


Figure A-1. Raindrops illustrating concept of interference.

The Communications Act of 1934 established the Federal Communications Commission. The stated purposes of the Communications Act are:

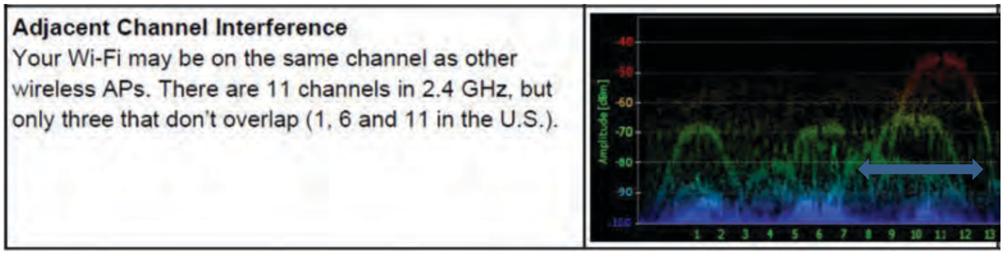
> "regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, nationwide, and worldwide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, and for the purpose of securing a more effective execution of this policy by centralizing authority theretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is hereby created a commission to be known as the Federal Communications Commission, which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this Act." (*1*)

The FCC designed the Communications Act of 1996:

> "to provide for a pro-competitive, de-regulatory national policy framework designed to accelerate rapidly private sector deployment of advanced information technologies and services to all Americans by opening all telecommunications markets to competition . . ." (*2*)

The Telecommunication Act of 1996 also added and changed some rules to account for the emerging Internet.

There are recently proposed amendments (*3*) to the Communications Act of 1934 to require the FCC to publish on its website and submit to Congress a biennial report on the state of the communications marketplace (*4*). That report would include an analysis of "the state of competition in the markets for voice, video, and data services, as well as the availability of high-speed and high-quality telecommunications services" in the United States and also "require the FCC to determine whether laws and regulations pose a barrier to entry into communications markets and to include that information in the biennial report" and cancel a number of preexisting requirements for various other reports from the FCC (*5*).



Adjacent Channel Interference
Your Wi-Fi may be on the same channel as other wireless APs. There are 11 channels in 2.4 GHz, but only three that don't overlap (1, 6 and 11 in the U.S.).

Figure A-2. Example of multiple channel WiFi interference.

A brief summarization of the spectrum interference management governed by the Communications Act of 1934 and technology that influenced the proliferation of small personal communications up to the present time is provided in Attachment 1: Spectrum Management in Its Early Days. The regulatory process to place these devices in the spectrum and difficulties they pose to management in an airport environment are discussed in the following sub-sections.

Key Points of the FCC Part 15 Unlicensed Spectrum That Apply to WiFi

The industrial, scientific, and medical (ISM) radio bands are reserved internationally for the use of RF energy for ISM purposes other than telecommunications such as WiFi. An abbreviated walk-through of the complex background and issues in the WiFi use of unlicensed spectrum bands in the airport will be provided. The FCC explains in "Part 15—Radio Frequency Devices Rules and Regulations" the regulations under which an intentional, unintentional, or incidental radiator may be operated in unlicensed bands. It also contains the technical specifications, administrative requirements, and other conditions relating to the marketing these Part 15 devices.

The reader is referred to the complete Part 15 text for all details; only the specifics and difficulties that apply to operation of Part 15 devices such as WiFi and other similar technologies in an airport environment will be discussed.

Definition of Harmful Interference

In FCC Part 15 Section 15.3(m), the definition of *harmful interference* is stated as:

> "Any emission, radiation or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communications service operating in accordance with this chapter."

This is an operational definition and uses terms that do not have strict "technical" thresholds associated with the "victim" except for the radio navigation functions and safety services. Radio navigation applies to safety of flight. One commonly associates this with interference affecting radio navigation systems supporting flight, including equipment located near the airport. Minimum or no interruption or induced errors to radio navigation is tolerable. Communications radios may fall into this interpretation, particularly if related to safety or security. The frequency bands of communications systems are different from WiFi bands for the most part at the present time, and interference is highly unlikely to be experienced. The exception is if WiFi is used by airport security or safety functions within or near the airport facility. In this case, it can lead to a dilemma to invoke Part 15 mitigation if security is using the same airport WiFi network as vendors or passengers. Another interesting contentious case would be if some WiFi is used for managing vehicle traffic on the tarmac. Radio frequency WiFi leakage from inside the airport could potentially interfere depending on the airport's specific layout and building structure. Both systems could be Part 15 but have different levels of criticality of airport service and hence different thresholds for interference. Extensive knowledge of such WiFi implementations at all airports would be needed to provide guidance on whether to strictly use Part 15 or possibly place cases like this at the top priority of "tolerable interference," discussed next.

For the remainder of the systems in the band governed by the FCC Part 15, one could interpret the words to infer different thresholds for different victim receivers; i.e., some are very susceptible to interference while others are more interference-tolerant by design, with better components. Priority levels of "tolerable interference" based on criticality of supported airport functions served and passenger priority could be established. At the top level, WiFi uses for security, tarmac vehicle control, baggage check-in, and wireless credit card transactions require higher priorities, while conducting business or watching videos in the airport gate area is a lesser priority. These priority levels may be used for airport WiFi distribution or RF isolation of the more critical WiFi uses and the criticality of resolving interference complaints.

There are a multitude of examples in each of the above categories that could be given; however, the point to take away is that each interference interaction can have interpretive meaning to the FCC Part 15 operational definition of harmful interference. The equitable mitigation of interference of Part 15 device emissions in an airport depends on understanding interference and what can be done about it.

Difficulties Posed by Part 15 to Strictly Enforce in Airport Terminal Environment

The important excerpts of the Part 15 regulations pertaining to the use of WiFi and other wireless systems operating in the 915 MHz, 2.450 GHz, and 5.800 GHz ISM radio bands are as follows:

> "Persons operating intentional or unintentional radiators shall not be deemed to have any vested or recognizable right to continued use of any given frequency by virtue of prior registration or certification of equipment, or, for power line carrier systems, on the basis of prior notification of use pursuant to § 90.35(g) of this chapter."
>
> "Operation of an intentional, unintentional, or incidental radiator is subject to the conditions that no harmful interference is caused and that interference must be accepted that may be caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator."
>
> "The operator of a radio frequency device shall be required to cease operating the device upon notification by a Commission representative that the device is causing harmful interference. Operation shall not resume until the condition causing the harmful interference has been corrected."

The quoted words express clear intent. One very important impactful usage of these words is to enforce the cessation of "rogue" hotspot (*6*) devices that could be brought into the airport environment.

Part 15 and Interference Mitigation User Responsibilities

In actuality, resolving the responsibility of interference has complexities. In the ideal cases described above and in the Part 15 wording, it is assumed the "blame" is due to an identified RF interference caused by one system. This can be accomplished if the interference is identifiable, emanating from a system with known spectrum characteristics different from WiFi such as a microwave oven in the food court. It is not always easy or straightforward to identify unknown spectrum interference sources. The interference could be from different WiFi networks or multiple systems. Spectrum analyzer traces or equivalent measurement data are needed, accompanied by diagnostic search and identify procedures to uniquely resolve the originating RF interference source.

There can also be a "perception" of interference not related to RF. For example, many system users trying to use the same spectrum at the same time can cause a throughput reduction. Dropped packets and reduced message throughput occur and can portray the illusion that interference is present. The real cause may be a network design issue, the network nearing a user-created demand situation, or, if frequently occurring, the networked system may be approaching the replacement time. There are many similar scenarios, but the point is that reductions in throughput alone do not uniquely indicate interference. As WiFi increases in presence at airports, resolution of "perceived interference" vs. RF interference can become an increasing part of the interference mitigation.

Harmful Electromagnetic Interference as Applied to WiFi at Airports

Legacy spectrum allocation is built on a hierarchy of licensed users in the spectrum bands, e.g., "primary and secondary." This hierarchy organizes the interference mitigation process by spectrum allocation priority. On the other hand, all users in the ISM band are equal in priority under the Part 15 governance. There is in general good and not so good equipment in the ISM band depending on the manufacturer's business model, resulting in high-quality vs. low-cost equipment. Furthermore, there is ambiguity in what is meant technically by *harmful interference* as applied to the various Part 15 ISM band users. It is unclear what measurements need to be made and compared with established thresholds for declaring whether harmful interference is present or not. This situation is not readily amendable to be enforced by turning off the interferers, as indicated in the FCC rules.

Note airport security, medical, or other critical functionality may require some RF interference protection within the airport if using the same WiFi bands as vendors and other users. However, if using Part 15 equipment, these higher priority systems are not provided any protection in the ISM bands by the strict interpretation of the FCC regulations.

What Part 15 Means to WiFi Governance in the Airport Terminal Environment

The airport terminal environment will be difficult to manage by simple enforcement of the Part 15 regulations per se. Two alternative solutions/methodology approaches are presented for consideration.

Cooperative Approach to Mitigate Interference Within the Terminal

The cooperative approach is mainly driven by the FCC ruling that the airport authority cannot control installation and usage of WiFi at airports (*7*).

It is in the best interest within the airport terminal that RF interference mitigation be accomplished between all concerned. Best interest is defined as a reporting, analysis, and constructive action process to mitigate RF interference that considers the responsibilities of the airport, the business case of the tenants, as well as the responsibilities of the passengers.

Passengers are included and have the responsibility of operating equipment that complies with the FCC Part 15 rules and regulations, i.e., do not exceed power limitations. Hotspot devices that are purchased by airport passengers sometimes can exceed the power limits depending on manufacturers. They may be locally beneficial in a home, office, or other spaces where the RF energy emitted by one or a few such devices provides WiFi coverage in dedicated areas. However, these devices brought in number into the airport environment can cause mutual interference to themselves and other WiFi devices such as laptops. If some exceed their specifications, they can make the interference more disruptive to WiFi users. It should be noted that the hotspots may not be the sole source to blame; the network in that locality of the airport may be partially to blame, i.e., the network WiFi adjacent nodes may be operating on the same channel or adjacent channels in the 2.4 GHz band or their settings could be non-optimal. Note WiFi in the 2.4 MHz band does not have guard bands; rather, the bands can overlap unless deliberate network efforts are made to separate local areas by assuring one or two unused frequencies are kept open between adjacent areas. RF hotspots interference is similar in nature, and effects revert to the early days of spectrum management as described in Attachment 1, with the consequence that guard bands were needed between user frequencies to avoid out of band (OOB) emissions on neighboring channels to spill over on simultaneous transmissions. Simultaneous WiFi transmissions on the same or adjacent frequencies in a network have the potential to interfere with each other. A more promising candidate solution could be to use the 5 GHz band, where there are many more available channels and the channels do not overlap. The topic of passenger hotspots presents potentially severe issues in the WiFi environment that deserve more in-depth analysis.

In the following section, a straw man methodology to address interference issues is provided. However, the details need to be further integrated into the spectrum regulatory area before being adopted in the airport environment.

Potential Way Forward Based on Harm Claim Thresholds

Harm claim thresholds are a method to quantitatively define *harmful interference* with measurable, agreed-upon thresholds that apply to equipment in bands of the unlicensed spectrum. The FCC issued a White Paper for comments in January of 2013 regarding interference limits policy (*8*).

The basics of this paper are: "Receivers can be brought into the policy picture with minimal regulatory intervention by introducing an 'interference limits' policy; that is, the establishment of ceilings, *called harm claim thresholds*, on in-band and out of band interfering signals that must be exceeded before a radio system can claim that it is experiencing harmful interference. Manufacturers and operators are left to determine whether and how to build receivers that can tolerate such interference, or even determine that they will choose to ignore these limits. Harm claim thresholds thus allow the FCC to provide guidance on the optimization of receiver performance without unduly restricting technical and commercial choice." Figure A-3 provides a graphical depiction of the approach.

Note these harm claim thresholds simply map to levels that the in-band or out of band signal must adhere to preclude harmful interference; however, the manufacturer has the option to implement them or not. The concept has merit in the airport environment and could be implemented to control the presence of rogue devices if they exceed the harm claim thresholds, and allow users to select the WiFi equipment that can minimally satisfy the harm claim threshold within the airport environment. Essentially the airport has no say in what equipment is used within its confines. This is in keeping with the spirit of the FCC, which sided with Continental

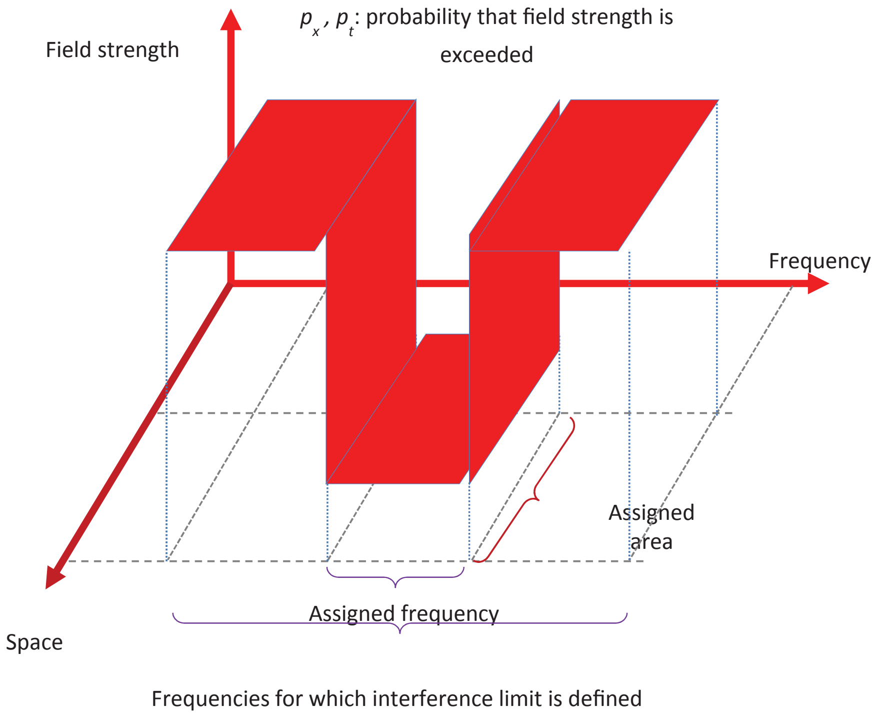

Field strength
p_x, p_t: probability that field strength is exceeded
Frequency
Assigned area
Assigned frequency
Space
Frequencies for which interference limit is defined

Figure A-3. Interference limits policy approach.

Airlines in a ruling that the Massachusetts Port Authority cannot restrict WiFi use at Boston's Logan International Airport, but leaves the Port Authority the power to have interference corrected to comply with the interference claim thresholds.

The bottom line is, in an ideal world, if such an approach were taken with thresholds established and manufacturers accepted for particular environments such as airports, the mitigation of harmful interference becomes simplified and enforceable in the airport environment.

Stricter Governance of Interference to Licensed Systems Near Vicinity of Terminal

It is to be noted that there may be a possibility that licensed users are assigned in the ISM bands within or near the airport terminal. This presents a special case where the WiFi system has to mitigate any RF interference to these systems.

Perceived Misconceptions, Root Cause Determination, and Interference Incident Reports

The intent of this section is to provide an overview of interference, its root cause determination and mitigation techniques, and a method to quantify the magnitude of the RF interference.

Interference reporting from airport WiFi users is expected to be mostly from the observable perspective, with occasional exceptions of persons who have experienced interference and learned some observable indicators, such as someone in the near vicinity of WiFi equipment using electronic equipment or transmitting on a radio. The issue is that these observable reports do not always correlate with RF interference but may be "perceived" interference related to performance of the WiFi equipment in the environment.

Perceived Misconceptions

Perceived misconceptions are basically a first guess result of observed phenomena relating to the performance degradation of the "victim" WiFi wireless receiver or other commercial communications radio emissions in the ISM bands. Specific examples of performance degradation causes include: hardware or software failures of equipment within network, e.g., routers and radios; disruptions in a particular link or network to the communications receiver; erroneous settings in radio or network; overloading of network during peak usage hours; temporary area RF blockage within the building or caused by local construction; low-cost equipment that has operational limitations in a dense usage environment; and other causes. These few examples are meant to illustrate causes that are not related to RF interference but can mask as interference to the WiFi users.

Relate Interference Reports to Root Cause

The expected growth of WiFi and other commercial communications at airports will inevitably produce many interference-related reports. Airport authorities can't expect to have dedicated personnel to resolve each and every report of interference issues. Ideally what is needed is a process that enables airport authorities to resolve the issues within their own personnel resources and capabilities. The process must use a formalism that is simple and adaptable to the complexities of airports, leverages the history of reported interference and past experience of resolving interference mitigation, and adapts to future growth of expected wireless usage at the airport terminal. One plausible way forward would be the development of an "interference incident report" that includes a description of what was observed and a standardized questionnaire.

These incidence reports can be generated by anyone using or working with the WiFi system and saved in a database format (discussed later in this appendix). Note it would be ideal to leverage the reported and resolved interference experience across all airports. This inter-airport database can enable access to resolutions of past interference issues, saving the expense of individual airports rediscovering the mitigation of known solutions, and sharing the technology and interference mitigation experience not available at all airports.

Perceived Interference Unrelated to Electromagnetic Interference

The process must also be adaptable to maximize the resolution of perceived interference. One plausible way forward would be the development of procedures or quick check tests that the airport authority and/or impacted user could perform. The results would isolate perceived interference using guidance to be developed, and be reported within the "interference incident report." If not resolved by the procedures, then the interference is likely to be RF-related.

RF-Related Interference

The process must also be adaptable to address RF interference at an airport. The airport authority could have access to spectrum test equipment, e.g., a spectrum analyzer; however, affordability may be a hindrance at small airports and a rental or low-cost instrument may be an option. Measured observations of the interference can be recorded and used to confirm if the interference is RF-related. If the source is determined to be RF-related, the steps appearing later in this tutorial could be followed.

The Practical Side to Resolving RF Interference

The intent is not to itemize RF interference mitigation solutions here but to provide a top-level methodology for airport authorities to address the interference issues when they are found.

The FCC ruling that the airport authority cannot control usage of WiFi at airports, combined with the ambiguity of the definition of harmful interference in the regulations, makes it difficult for airport authorities to manage and mitigate WiFi interference. WiFi is important to the functioning of an airport if related to a navigation, airport security, or other related safety issue within the airport. Passengers are important since they are the financial input to airports. Tenants and passengers are becoming more dependent on WiFi and other wireless devices. The airport is a business place for its vendors and an extension of its passengers' office or entertainment space.

One reviewer provided a noteworthy comment that characterizes the complexity of the WiFi environment and its enforcement:

> "There is no question that the FCC reserves control in the context of regulation for itself. However, the over-the-air reception devices (OTARD) rule cited grew from a condominium owner dispute with a landlord (association) over the placement of an RF receiver on their exclusive use/owned space. This was later extended to include RF transmitters in addition to receivers. So control must be considered in the context of the agreement a tenant has. If the agreement is an exclusive lease and use one, the tenant can install and operate RF transmitters in the ISM bands; in those cases, resolution is limited in most cases to reasoning around avoiding 'mutual destruction' and achieving mutual benefits, and around cost incentives or dis-incentives that the airport can create. If the agreement is not an exclusive lease and use one, the airport can prohibit the tenant from installing and operating receivers and transmitters. To use an analogy, a condo owner can install a transmitter in their condo but not in the pool or lobby area even though technically they may own a 'share' in those areas."

The legal enforcement issues are tangential to interference and they are well-taken. They introduce other methods to preclude interference by the placement of devices that focus on building codes, overall safety of employees and passengers, and installation standards for wiring and security. They also introduce questions relating to interference that need to be considered. For example, are there communications or operations uses of WiFi in the same or a nearby spectrum that could be impacted by interference for safety, emergency response, or security? Any one of these listed considerations could limit or preclude antenna location installation at the airport. If the installation proceeds forward, the FCC Part 15 compliance as applied to the use of WiFi equipment must be addressed. The only way to stop use of any system transmitting is to show that the user is not transmitting an acceptable quality signal by using the FCC Part 15 regulations, i.e., the device is over the power limit or violating some other restriction.

Note compliance with FCC Part 15 can be invoked with the hotspot equipment and hotspots brought into the airport by passengers. If the hotspot complies with the Part 15 rules, it is essentially authorized for use. However, to enforce this in a crowded airport, with the potential of many hotspots in a localized area, could be impractical or nearly impossible. The security issue raised by passengers' hotspot devices may need further investigation to determine if it is something airports can leverage (*6*). One suggestion to alleviate concentration of hotspots in an area would be to post notices or other enticements to please turn off personal hotspots.

This primer is not the appropriate vehicle to completely address the complex issues airports face. However, the following recommendations provide guidance to mitigate and manage WiFi interference before it becomes a serious issue.

Keep in Place What Works

Many airports have lounges, smoking rooms, or dedicated lounge areas for business and regular travelers. They may have Internet using cable connection or WiFi. If the usage is acceptable with cable, keep it in place. The lowest cost to the airport is to keep these areas in operation and explore other such areas for use. If WiFi is to be installed, use one or two separated channels for the room, particularly in the 2.4 GHz band.

Structure a Cooperative Governance Approach to Establish Interference Root Cause and Quantify Interference

The first steps to defining the interference mitigation structure are meant to organize the effort. The structure needs to adapt to individual airports or groups of small, medium, and large airports since WiFi interference can depend on size and density of users. This tutorial will outline this approach, but the details need to be worked out in the future before implementation.

It is suggested if not already in place that each airport establish a governance board composed of the airport authority, vendors, and other users of WiFi equipment within or near the terminal. The structure should be simple but provide a forum where WiFi and wireless interference reports are submitted and mitigated. It should be emphasized that this way forward begins with a cooperative approach whereby resolution of WiFi and other Part 15 wireless communications interference is accomplished in a beneficial way for all.

Establish the Governance and Enforcement Framework That WiFi Users and Airport Authorities Will Follow

A general document should be prepared for governance and adapted for different sizes of airports.

The bounds within which the airport authority and WiFi users can manage and operate must be made clear. Note the airport authority cannot tell a user to shut down a device unless the device is interfering with a flight navigation or support role, e.g., a repeater, or it is operating outside the Part 15 specifications.

The future Airport Network and Location Equipment (ANLE) system (real-time aircraft position reporting on the airport surface) is performing a preliminary investigation on the applicability of wireless local area network and cellular network technologies, for use by the airport wireless system in C-band. The technology considered IEEE 802.11a, IEEE 802.11b, CDMA2000, and Wideband Code Division Multiple Access (WCDMA) (*9*). It is mentioned here as an indication of future considerations that could impact the use of WiFi systems inside the airport depending on individual airport design and frequency bands. However, this system may require protection from other WiFi interference sources within the airport. (Note that the propagation of higher frequencies can penetrate through some building walls with seemingly small openings. This potential futuristic case is one reason for including the FCC Part 15 methodology, since the ANLE system could follow its process or rules similar to protecting radio navigation devices.)

Interference Incidence Reports

An interference incident reporting system needs to be established to gather the users' observations of the interference. The basic input elements will consist of a description of the interference observed and answers to a set of questions filled out by the observer. It should also contain the originator information; the date, time, and location observed; a description of the environment in which the issue occurred; accompanying information on any actions taken to identify the source; and other pertinent information. The report information should be made available to the airport authority, all users, and others for independent inputs observing the same problem or working with interference mitigation issues. This questionnaire can be generic or tailored to specific airports.

Analysis of Interference Incidence Reports

An analysis of the interference incidence report and actions taken to determine the root cause of the reported interference should be cooperatively executed to determine if the report is in the perceived category or in the electromagnetic category. Access to all previous incident reports either by questionnaire or online database (described in the next section) will prove useful for determining root cause and potential mitigation techniques. The intent is to identify other reports of the same type and possible work-arounds or existing resolutions.

The details of the analysis may consist of reviewing previous incidence reports and resolutions, or determining if the problem is in a perceived category involving the hardware or network, or is in the RF domain. Once the RF domain is determined, spectrum measurements should be done to identify the source of interference and quantify the severity of the interference. All analyses, actions, and findings should be recorded and placed in the interference incidence reporting system. If the report is within the perceived interference category, it can transition to the closed status once the root cause is fixed and verified.

Once the source is quantified, the final resolution may be easy for interference to licensed users because the resolution actions are the responsibility of the interferer. However, resolution is probably the most difficult part in a Part 15 environment.

Database for Interference Incidence Reports and Resolutions for Future Use

It is recommended that a database be used to keep track of the reports, share resolutions, and assist airports in quantifying the magnitude of the interference issue. It will contain the originator, report identification with accompanying information on date opened, status of report (opened/closed), severity of report, actions taken, and other pertinent information. The database information should be available to the airport authority, all users, and others working with the interference mitigation issue. There are many off-the-shelf database products, some of which may be already implemented in the airport environment for leveraging.

Implementation Approach to Interference Resolution

This section focuses on the resolution of RF interference, which will likely be the most difficult issue for the airport and users. The suggestions offered in this section are not all-inclusive but are representative concepts for considerations. In addition, there may be a more optimum solution for specific airports and environments. Future work may be needed to develop a candidate list of such solutions.

First-Order Simple Solutions

Some interference can be mitigated if it is caused by a single device having simple remedies, like changing the interferer transmit antenna location, moving a non-WiFi device (e.g., microwave oven), lowering the transmit power of the interferer if the equipment has power control options, or other such changes. These solutions should be explored first for cost and expediency. If a piece of equipment is found faulty, it is advisable to seek repair or replacement.

Resolution Impacting Changes to Equipment

The mitigation of RF interference usually belongs within the interferer responsibility; however, sometimes it may be more cost-effective or expedient if one or a small number of "victims" are involved. Upgrades to software should be more palatable to users over hardware changes including replacement of their installed system. Interference may be resolved by upgrading the WiFi equipment. Some or all may not choose to make the change depending on the cost.

The first attempt towards resolution could be to have a discussion with owners of the WiFi equipment as to whether the changes would benefit all or a majority of users. If the cost were offset and linked to increased business, the changes could be agreed to over a time period.

However, an issue may occur where the root cause interference affects a large number of the WiFi users within the airport, and the hardware or software fix would alleviate a widespread RF interference problem within the terminal. It may be good business practice as a last resort for the airport to resolve the issue by offering incentives to these users to make the changes. This should not be interpreted as a direction for the airport to follow but a suggestion to consider. Each equipment upgrade has its own operating budget and business model.

The FCC regulations may be invoked if the change brings the systems into compliance with the regulations. However, enforcement is not always accomplished by this mechanism.

Resolution Involving Equipment Moving

Resolution involving WiFi equipment repositioning may be done at little or no cost to anyone if the movement is within the business area of the interferer. Moving the interferer source further away from the victim takes advantage of the increased distance dependency of path loss to weaken the interferer signal below a level that produces "tolerable" interference. The new location needs to be tested so that the interference issue isn't passed on to others. However, if the movement is outside of one or both user spaces, it may become impractical. A potential solution is adding a link (optical) from the interferer user's area to a new location of the

WiFi equipment, which could be an option at some expense. Once a satisfactory location is determined for the above cases, a first attempt towards resolution could be to have a discussion as to whether the changes would benefit the owner(s) from the cost perspective. If the RF interference is sufficiently severe to affect business, the cost of the changes may be offset by the return to the previous or greater business level and the implementation may be amortized over a time period.

Incentives for All Concerned

The interference incidents resolution will likely incur some costs to implement. It is also anticipated that vendors will be hesitant to bear the associated costs, despite the wording of the FCC regulations to turn off the interference under the stated conditions. The airport does not have authority to enforce RF interference mitigation for Part 15 devices except where there is interference to navigation systems.

In such an environment, the airport authority can offer cost-sharing or other types of incentives in cases where the parties do agree to an interference incident resolution but stall in implementing the resolution. However, this is at the prerogative of each airport authority, and further research and brainstorming are needed to accomplish the intent of interference incident resolution in an equitable way without unreasonable and unnecessary cost burden to the airport.

Some Possible New Technologies That Offer Promise

The spectrum is becoming crowded with the new technologies brought into the marketplace to meet growing communications needs, including personal, civil authorities, emergency responders, law enforcement, military, air and space. The crowding of spectrum is a natural consequence of these needs, and interference can be experienced between users in the bands. Interference topics often portray a bleak picture, but there are technology solutions that can potentially aid in avoiding interference. Research on making RF communications spectrally efficient and interference tolerant and resistant has introduced interference mitigation techniques to be implemented into radios. As time progresses, the cost of implementing these techniques diminishes to where they are plausible for low-cost radios such as WiFi. Some of these are cited below for consideration.

"Carrier sense multiple access (CSMA)," "Collision Avoidance," and "Request to Send/Clear to Send (RTS/CTS)" are becoming commonplace and readily implemented functions in software radios for precluding interference between radios and within networks for voice and data. The simple concept of each of these techniques is to listen for a clear channel before transmission. Such techniques aid to avoid interference; however, they may not always be an adequate answer in heavily used and spatially dense WiFi networked environments such as a crowded airport terminal waiting area.

Multiple-input and multiple-output (MIMO) is a promising technology that can beneficially contribute to the airport environment. MIMO uses multiple antennas at both the transmitter and receiver to transfer more data at the same time to improve communication performance. It offers significant increases in data throughput and link range without additional bandwidth or increased transmit power by spreading the same total transmit power over the antennas to improve spectral efficiency (more bits per second per hertz of bandwidth) and link reliability. MIMO is part of modern wireless communication standards such as WiFi.

Some non-WiFi systems have built-in interference avoidance capabilities to choose a frequency not in use by such techniques as "Dynamic Spectrum Access." This is emerging from the research stage and is quite promising.

Conclusions and Way Forward

Interference is a complex issue. The determination of the root cause of the interference has to separate the "perceived" from the RF in order to apply the appropriate mitigation.

The airport WiFi and wireless environment poses a challenge to mitigate the interference from Part 15 devices at airports. There is a responsibility to mitigate any WiFi RF interference to radio navigation, safety on the tarmac, or security on airport ground systems if they occupy the same or adjacent spectrum bands. Note these cases could be caused by RF leakage from inside or external to the airport terminal. There could be other systems that are unlicensed at airports that deal with ground traffic, and these will also likely require protection from interference. The enforcement can become complex if all the systems use unlicensed WiFi. However, the solution should be relatively simple, with systems focusing on safety having the priority.

The mitigation of interference between WiFi and other Part 15 devices within the airport terminal presents issues and challenges due to the absence of a regulatory process for resolution. A cooperative interference resolution is suggested; however, additional details need to be developed. The harm claim threshold approach would ideally work in an airport environment, but this approach needs further adaptation to the airport environment.

An interference incident report database methodology is suggested to assist the mitigation process, preserve records, and make available the resolutions to others. It provides a way to measure the magnitude of the interference with time, and the data collected can be leveraged by all airports, used for lessons learned and long-range planning for WiFi installation upgrades.

This primer focused on RF interference in an unlicensed spectrum and highlighted some resulting issues for airports and tenants. It should not be considered all-inclusive but provides an overview of the issues.

Attachment 1: Spectrum Management in Its Early Days

Spectrum interference management in its infancy state, governed by the Communications Act of 1934, provided "empty frequency space" known as guard bands (Figure A1-1) for adjacent channel protection on one or both sides of the assigned frequencies. This was done to "preclude out of band (OOB)" radio emission interference due to the vacuum tube radios not being able to suppress these RF signals to acceptable levels in the immediate adjacent bands. Safety of flight was the primary concern of spectrum usage outside airport facilities, and any potential radio frequency (RF) interference emanating from inside was kept out of frequency bands for flight systems. Interference management was relatively simple.

This simple technique was adequate for decades with rather large and bulky vacuum tube technology, as compared with modern hand-held devices, to preclude interference since the guard bands avoided RF spill-over into the two neighboring frequency assigned channels. Spectrum use was relatively sparse compared with the present. The broadcasters and other users were fewer in number than today. Spectrum assignments done this way precluded interference for the most part, with exceptions caused by anomalous propagation and equipment shortfalls that did not adequately preclude OOB emissions in the adjacent channels.

Early materials research since the invention of transistors provided solid state technology to gradually allow movement past the vacuum tube era. The radios gradually evolved to smaller sizes, where today the electronics are on a chip and the bulk is in the earphone or speaker. New applications of RF systems permitted automation and an explosion in numbers of devices to enable control and communicate to other devices. Laptops, tablets, computer devices, and hands-free interfaces to these devices enable tasks to be performed with greater business efficiency away from the office. The micro-electro-mechanical systems (MEMs) and nano-electro-mechanical systems (NEMs) improvements to the solid state technology permit RF radios and devices to be designed as implants. This technological revolution had profound impacts on the RF spectrum. The following is a synopsis of the evolution that caused spectrum reallocation specifically pertaining to WiFi in airports:

- The number of low-cost RF devices in the environment quickly saturated spectrum availability in the past few decades, leading to the reallocation and sale of spectrum. Note there are dedicated bands that serve critical functions (e.g., radio navigation, radio astronomy) that are mostly immune to this spectrum issue.
- Unlicensed bands such as the 2.4 GHz industrial, scientific, and medical (ISM) band were created to permit usage of the devices without spectrum regulatory frequency assignments for individual use. Some key impacts are:
  - Adjacent channel guard bands would no longer be assigned as a rule for OOB interference protection.

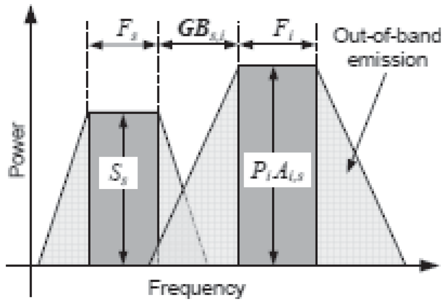


Figure A1-1. Guard band example.

  - Spectrum use specifications made resolution of interference part of non-regulatory governance (i.e., users work out the interference issues), with some exceptions in the unlicensed bands. Simply put, the vague definition of "harmful interference" was passively replaced with loose bounds of "tolerable interference" (tolerable is interpretive/subjective to individual cases) and left to the users to resolve disputes.
  - It was left to the device manufacturers to clean up their OOB emissions or operate in the environment. Low-cost components to preclude or filter OOB emissions are available on the market, but not all manufacturers implement them in their devices to make their devices competitive in the commercial marketplace.
  - Unlicensed bands change the frequency management procedures in bands like 2.4 GHz, with the users bearing the burden of handling interference.
- Low-cost RF devices proliferate in the marketplace, including WiFi. Heavy competition usually means the devices are manufactured with less robustness against interference and radio propagation effects. Examples include dropped cell phone calls; intermittent disruption of WiFi and cell phone coverage at various locations or while in motion; and over the air disruptions in urban, dense foliage, or hilly locations. The public has become somewhat tolerant to dropped calls and less than optimum performance of networks. To the user, the cause of the disruptions is not directly perceivable, but some of these short time disruptions could be due to interference.

As a direct consequence, intermittent WiFi interference disruptions or less than peak performance in crowded places such as airports may not always be objectionable but dependent on the specific circumstances. This is a key point on how to prudently manage both throughput and interference of the WiFi network with the increasing passenger demand for WiFi services in the airport environment.

However, the airport WiFi installations will expose a unique intersection between "licensed" and "unlicensed" environments. Radio frequency systems from both environments may interact and simultaneously cause "tolerable" and what is known as "harmful" interference depending on the viewpoint of the owners of the systems.

References

1. Public Law Number 416, Act of June 19, 1934, ch. 652, 48 Stat. 1064, by the 73rd Congress, signed by President Franklin D. Roosevelt, codified as Chapter 5 of Title 47 of the United States Code, 47 U.S.C. § 151 et seq.
2. Conference Report, Telecommunications Act of 1996, House of Representatives, 104th Congress, 2d Session, H.Rept. 104-458, at p. 1.
3. Federal Communications Commission Consolidated Reporting Act of 2013 (H.R. 2844; 113th Congress).
4. "H.R. 2844—Summary," United States Congress.
5. "CBO—H.R. 2844," Congressional Budget Office.
6. "Security Experts Warn of Dangers of Rogue WiFi Hotspots," Hilary Whiteman, CNN (2009).
7. On November 1, 2006, the Federal Communications Commission (FCC) sided with Continental Airlines in a ruling that Massachusetts Port Authority cannot restrict WiFi use at Boston's Logan International Airport.
8. "Interference Limits Policy: The Use of Harm Claim Thresholds to Improve the Interference Tolerance of Wireless Systems," White Paper, Receivers and Spectrum Working Group, FCC Technological Advisory Council Version 1.0 (2013).
9. Airport Wireless Local Area Network: Technology Survey and Simulation Tool Development MITRE TECHNICAL REPORT MTR 03W0000051 August 2003. Izabela Gheorghisor, Dr. Yan-Shek Hoh, Minh Nguyen (2013).

APPENDIX B

Best Technical Practices to Ensure Accessible WiFi Service

Within an airport terminal environment, all wireless airport and passenger communications systems must operate harmoniously with "tolerable" interference, albeit some functions serviced by wireless fidelity (WiFi) may need better protection against interference (for example, baggage check-in and aircraft routing ticketing, security checks, and other defined airport critical operations). The expected growth of the WiFi environment and other commercial communications at airport terminals is likely to produce an increase in interference-related reports, but not all may be sufficiently severe to be noticed or to warrant a complaint. For those interference complaints made, interference mitigation should be accomplished in the best interest of all concerned to restore interference-free operations needed for airport terminal and passenger communications. Best practices to ensure accessible WiFi service focus on establishing a reporting system, a cooperative analysis process between all concerned to determine the root cause of the interference source, and a cooperative process to mitigate interference that considers the responsibilities and perspectives of the airport authority as well as the users.

Airport WiFi Environment

The researchers focused on best practices to prevent, detect, and resolve WiFi interference issues within the terminal; however, there may be some interference from or to external sources. The largest impact is related to the operation and security of the airport, but passenger WiFi usage is also a concern. The following is a list of areas where WiFi is used inside the airport, as well as a few areas exterior to the airport. The list is not exhaustive.

- WiFi in the 2.4 GHz band provides operationally critical services to airports both inside the terminal (e.g., security check and other terminal functions) and possibly on the tarmac.
- Baggage tag scanning can be accomplished both within the terminal at the passenger check-in line and often in outdoor apron areas of airports.
- Kiosks or check of boarding passes at gates.
- Vendor wireless credit card payments.
- Future demands may include WiFi access for commercial vendors and passengers (i.e., to access food menus and place orders via the WiFi system), to order supplies, conduct inventory, and maintain sales records.
- Passenger use in departure lounges and other areas of airports to conduct business or connect to the Internet for pleasure.

Airport Organizational Approach to Managing the WiFi Environment

Research to date indicates there is a large diversity in the ways the WiFi environment is managed. WiFi was not included in the initial design of the airport environment as part of the airport infrastructure or guidelines to connect and distribute communications. The WiFi unlicensed technology opened the possibility to economically do business without expensive cable installations. As a consequence, many airports and businesses took advantage of this opportunity and took individual steps to install their own WiFi systems without any overarching airport guidance. Airports have their own unique WiFi networks using unique equipment and network designs, with the main implications for network management as follows:

- Airports in the planning stage or airports being modernized may present the only possibility of establishing an optimized WiFi network architecture based on managing interference. Optimizing existing airport WiFi networks may be addressed when the system requires updating or when resources permit.
- WiFi networks will change over time with advances in technology along with the introduction of new devices using the same spectrum.
- Benefits and potential interference issues will change created by growth or congestion within the unlicensed 2.4 GHz band and eventually this may occur in the 5 GHz band as well.

Approach Taken to Identifying Best Practices

Airport architectural structures and sizes differ widely. Spectrum measurements conducted by traveling study team members within the U.S. present unique environments for each airport from a radio propagation point of view. The best practices to prevent, identify, and resolve WiFi interference issues were formulated using:

1. Research on the Internet for airport WiFi interference-related information for the U.S. and abroad.
2. Network design systems and tools to map the WiFi radio frequency (RF) in the airport environment.
3. Network management systems that attempted to identify symptoms of interference and resolutions.
4. Commercial tools that could assist in identifying and confirming interference sources.
5. Past national and international experience of professionals who worked in identifying and resolving interference for the Department of Defense and other government entities at the federal, state, and local levels.
6. Synergistic analyses that leveraged past experience for interference mitigation to formulate the best practices.

The framework used to organize the best practices includes a generalized grouping methodology and formulation approach based on separating the functional areas. The notional breakdown included:

- Passengers using WiFi for business and entertainment will mostly be in gate areas, food courts, and business lounges. Anticipate heaviest passenger-related use of WiFi use here.
- Check-in and baggage handling will be near the entrance.
- Commercial businesses (newsstands, vending machines, miscellaneous sales and services) will likely be in wings of most airports somewhat separated from flight waiting areas. Wireless credit card services will be common to most of these areas.

- Security, maintenance personnel, and handicap transport will be present throughout the airport, with expected light to moderate WiFi use.

Best Technical Practices

Best technical practices to ensure accessible WiFi service are summarized below, reflecting the accompanying spreadsheet and list of references.

1. Identify airport user groups based on airport areas or primary user functions to support baselining WiFi installations and prioritizing response. Schedule periodic spectrum/performance measurements to compare with baseline and assist with interference investigation using spectrum analyzer tools.
   a. Develop candidate grouping of WiFi services.
   b. Individual airports can prioritize the WiFi electromagnetic interference impact thresholds for each group (decibel measures that can be compared with planning/periodic "tool" output map or spectrum analyzer tools).
   c. Execute measurements applicable to the airport areas based on prioritization.
2. On smaller airports, grouping may not be an option because all WiFi uses may be on various systems in the same floor space. In this case, a priority response based on type of service, security, baggage, etc., may be a better choice.
3. Analyze collected data to identify when a particular WiFi hotspot is frequently nearing its "usage" saturation point during its prime operational period. This can be an indication that it is time to upgrade the device or all devices in a grouping before interference becomes a problem.
4. Identify the IEEE 802.xx specification of the equipment in place and plan for an upgrade to the 802.11 or other newer specification device for better throughput/spectral efficiency. This step can be executed at signs of WiFi equipment operating frequently near the saturation point.
5. Perform periodic upgrades to existing WiFi equipment as they become available and affordable. This replaces aged equipment and supports increased growth requirements.
6. Acquire one or two inexpensive commercial spectrum analyzer tools and use to identify, isolate, and confirm interference. For groupings that could possibly be affected by interference external to the airport (e.g., curbside baggage check-in), repeat the measurement near the check-in point.
7. Establish a database and map showing current WiFi installations within the airport, associated equipment information, and primary users. Airports may want to consider granting access to all individual airport databases through the creation of a centralized database possibly sponsored by the ACRP in order to leverage previous airport interference experiences and resolutions.
   a. Include all WiFi hotspots and information on all WiFi equipment.
   b. List all reported incidences of interference and resolution.
   c. Include in the database the WiFi baseline and periodic spectrum/performance measurements. Include reported WiFi interference reports (especially interference spectrum analyzer traces), status, and resolution.
   d. Include interference analyses results of each investigation documented with date, time, problem description, investigation measurements made, etc. Even if a repetition occurs from the suspected same source, document results for historical comparison. Analyze results periodically for patterns, anomalies, or unusual behavior.
   e. Look for and confirm interference with the latest affordable spectrum analyzer tools and vice networking tools. Interference can be accurately identified at the physical layer (transmitter/receiver) vice using networking tools; e.g., networking can provide a reduction in throughput which is not uniquely associated with interference.

8. Treat high-power interference sources as the highest priority and isolate them using spectrum analyzer tools. The source could be an already installed WiFi system that is malfunctioning or possibly a rogue WiFi hotspot being used by a transiting customer or waiting passenger. This could be a potential security threat as well as an interference threat.
9. Use an airport employee for the WiFi oversight administrator that has access to all real-time information and status of the WiFi network, leaving the responsibility to operate the WiFi to a hired company. The rationale is twofold: first, the airport has real-time knowledge of the health, status, and evaluation of a severe interference occurrence within the airport. Secondly, any potential security threat with connection to WiFi can be directed to airport security efficiently. If the airport manages its own WiFi networks, tie the airport employee administrator role to security.
10. When purchasing new WiFi equipment, invest in upper end/high quality WiFi hardware. Usually the higher end equipment is made with better components and designed to take precautions to control spectrum emissions (i.e., receiver noise floor). The result is better spectrum efficiency and less likelihood of causing interference.
11. Support is needed for the National Telecommunications and Information Administration and FCC "Out of Band (OOB)" Interference Limits Policy effort that is intended to identify where the interference mitigation falls; i.e., if the transmitter OOB exceeds the established limit, then the transmitter is to be responsible for the fix. If it is within the limit, then the fix is in the receiver. Note while this is in the early stages of consideration, it is a relatively simple and efficient method for resolving who fixes the interference issue.
12. ACRP research can potentially influence airport construction designs as appropriate based on the WiFi study and implementation findings. The present WiFi study, practices, and analyses of interference efforts may support surface airport layouts and construction that minimize interference and enhance WiFi (or future replacement) and security, as well as operations and businesses within the airport. Potential contributions are as follows:
    a. Groupings into business areas, such as baggage handling, ticketing, and food court, may influence the layouts of the occupied areas to reduce opportunities for interference.
    b. Groupings of WiFi areas can be further influenced by the use of RF-absorbing materials to confine the RF signal and preclude occasions of potential interference to other areas. RF-absorbing materials can be paint, transparent coatings, or built into materials that serve as area dividers. The goal is to minimize RF interference leakage in the WiFi bands into adjacent areas.
    c. RF-absorbing materials may also be used in entrance and access entry points for baggage or other similar functionality to minimize RF leakage in the WiFi bands in and out of the airport building. Interference internally created by WiFi commercial usage can be blocked by proper layout and absorbing material at access points to the tarmac.
13. Establish local airport policies to govern installation and use of WiFi systems.
    a. Local policies can address equipment transmit power limits, procedures/processes to request and install WiFi systems, interference problem reporting, and user participation.
    b. This provides a set of rules/guidance that all users are required to follow if they wish to install WiFi systems to support their operations or business.
14. Establish a formal airport stakeholders' council to address WiFi problems and future requirements. This makes everyone part of the process, which will help minimize future problems as well as resolve any interference issues that may arise.

The following is a spreadsheet that presents an abstracted summary of the above discussion. The spreadsheet provides numerical references to the basis of each best practice, followed by a list of the references.

Best Practices for WiFi Interference Mitigation

Best Practice	Airport Responsibility (Larger or Smaller)	References	Category		
			Prevent or Accept Tolerable Interference	Identify Interference Source	Resolve Interference to Tolerable Level
Identify Airport WiFi user groups based on airport areas or primary user functions to support baselining WiFi installations and prioritizing response, and schedule periodic spectrum/performance measurements to compare with baseline and assist with interference investigation using spectrum analyzer based tools. Potential grouping categories: Baggage, Ticketing, Security, Food Courts, Business Lounges, Passenger Waiting Areas, Gates, etc. **Subtasks/Practices:** i. Develop candidate grouping of WiFi services. ii. Individual airports can prioritize the WiFi interference impact thresholds for each group (decibel measures that can be compared with planning/periodic "tool" output map or spectrum analyzer tools). iii. Execute measurements applicable to the airport areas based on prioritization.	Larger and Smaller	2, 3, 4, 5, 6, 8, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24	X	X	
Establish a database and airport map identifying all WiFi installations within the airport, associated equipment information, and primary users. **Subtasks/Practices:** i. Include baseline, results of periodic measurements, and any WiFi interference reports, status, and resolution. ii. Include analyses results of each investigation documented with date, time, problem description, investigation measurements made, and resolution. Even if a repetition occurs from the suspected same source, document for historical comparison. Analyze results for anomalies or unusual behavior.	Larger and Smaller	Study Recommendation	X	X	X
Acquire one or two inexpensive commercial spectrum analyzer tools to identify, isolate, and confirm interference vice networking tools. **Subtasks/Practices:** Interference can be more accurately identified at the physical layer (WiFi transmitter/receiver) vice using networking tools. Networking problems can provide a reduction in throughput which is not uniquely associated with interference.	Larger and Smaller	4, 6, 8, 11, 12, 14, 16, 17, 18		X	
Analyze collected data to identify when a particular WiFi hotspot is frequently nearing its "usage" saturation point during its prime operational period. **Comments/Rationale:** This can be an indication that it is time to upgrade the device or all devices in a grouping before interference becomes a problem.	Larger and Smaller	3, 4, 5, 6, 7, 8, 9,10, 11, 12, 13, 14, 17, 18 19, 23, 24	X		
Identify the 802.xx specification of the equipment in place and plan for an upgrade for better throughput/spectral efficiency. **Comments/Rationale:** This step can be executed at signs of WiFi equipment frequently near the saturation point. These data should be included in the overall WiFi database.	Larger and Smaller	9, 10, 13, 20	X		

Best Practice	Airport Responsibility (Larger or Smaller)	References	Category		
			Prevent or Accept Tolerable Interference	Identify Interference Source	Resolve Interference to Tolerable Level
Treat high-power interference sources as the highest priority and isolate with available spectrum analyzer tools. The source could be an already installed WiFi system that is malfunctioning or possibly a rogue WiFi hotspot being used by a transiting customer or waiting passenger. **Comments/Rationale:** This could be a potential security threat as well as an interference threat.	Larger and Smaller	1, 4, 5, 6, 12, 14, 16, 18		X	X
Use an airport employee for the WiFi oversight administrator that has access to all real-time information and status of the WiFi network vice, leaving all responsibility to a hired company to operate the WiFi. **Comments/Rationale:** First, the airport has real-time knowledge of the health, status, and evaluation of a severe interference occurrence within the airport WiFi system. Second, any potential security threat with connection to WiFi can be directed to airport security efficiently. If airport manages its own WiFi networks, tie the airport employee administrator role to security.	Larger and Smaller	1, 21, 22, 25	X	X	X
When purchasing new WiFi equipment, invest in upper end/high quality WiFi hardware. **Comments/Rationale:** Usually the higher end equipment is made with better components and designed to take precautions to control the spectrum emissions (i.e., receiver noise floor). The result is better spectrum efficiency and less likelihood to cause interference.	Larger and Smaller	9, 10	X		
ACRP research can support spectrum issues that benefit the WiFi implementations and usage at airports. **Comments/Rationale:** Present support is needed for the NTIA and FCC Interference Limits Policy effort that influences and enables higher quality hardware.		1	X		
ACRP research can potentially influence airport construction designs as appropriate based on WiFi study and implementation findings. **Subtasks/Practices:** i. Groupings into business areas such as baggage handling, ticketing, and foodcourt, etc., may influence the layouts of the occupied areas to reduce opportunities for interference. ii. Groupings of WiFi areas can be further influenced by the usage of RF-absorbing materials to confine the RF signal and preclude occasions of potential interference to other areas. RF-absorbing materials can be paint, transparent coatings, or built into materials that serve as area dividers. The goal is to minimize RF interference leakage in the WiFi bands into adjacent areas **Comments/Rationale:** The present WiFi study, practices, and analyses of interference efforts may support surface airport layouts and construction that minimize interference and enhance WiFi (or future replacement) and security, as well as operations and businesses within the airport.		2	X		

(continued on next page)

Best Practice	Airport Responsibility (Larger or Smaller)	References	Category		
			Prevent or Accept Tolerable Interference	Identify Interference Source	Resolve Interference to Tolerable Level
Perform updates on existing WiFi equipment. **Comments/Rationale:** Replaces aged equipment and supports increased growth requirements.	Larger and Smaller	15	X		
Establish local airport policies to govern installation and use of WiFi system. **Subtasks/Practices:** Local policies can address equipment transmit power, procedures/processes to request and install WiFi systems, interference problem reporting, and user participation. **Comments/Rationale:** Provides a set of rules/guidance that all users are required to follow if they wish to install WiFi systems to support their operations or businesses.	Larger and Smaller	Study Recommendation	X		
Establish a formal airport stakeholders' council to address WiFi problems and future requirements. **Comments/Rationale:** Makes everyone part of the process, which will help minimize future problems as well as resolve any issues that may arise	Larger and Smaller	Study Recommendation	X		

References

1. BAA's Response to Ofcom's Consultation, Higher Power Limits for License Exempt Devices, 2006.
2. Bit-Error Analysis in WiFi Networks Based on Real Measurements, Gabor Feher, Budapest University of Technology and Economics, Department of Telecommunications and Informatics, 2011.
3. The Wireless Jungle, Howard Preston, Preston Cinema Systems, 2009.
4. 20 Myths of Wi-Fi Interference: Dispel Myths to Gain High-Performing and Reliable Wireless, Cisco, 2007.
5. The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular, Cisco, 2012.
6. Interference Limits Policy: The Use of Harm Claim Thresholds to Improve the Interference Tolerance of Wireless Systems, White Paper, Receivers and Spectrum Working Group, FCC Technological Advisory Council Version 1.0, 2013.
7. Cool-Tether: Energy Efficient On-the-Fly WiFi Hot-Spots Using Mobile Phones, Ashish Sharma, Vishnu Navda, Ramachandran Ramjee, Venkata N. Padmanabhan, and Elizabeth M. Belding, University of California, Santa Barbara, Microsoft Research India, 2009.
8. Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection, Utpal Paul, Anand Kashyap, Ritesh Maheshwari, and Samir R. Das.
9. IEEE 802.16 Broadband Wireless Access Working Group, Title 802.16b PHY: Spectral Mask Related Issues and Carrier Allocations; Date Submitted 2001-03-10, Source(s) Dr. Ir. Nico van Waes.
10. The IEEE 802.11 Standardization, Its history, Specifications, Implementations and Future, Justin Berg, Technical Report GMU-TCOM-TR-8, 2011.
11. Promising Interference and Radio Management Techniques for Indoor Standalone Femtocells, INFSO-ICT-248523 BeFEMTO D3.2
12. A WiFi Measurement in 802.11g Networks, Jian Lin, Feilu Liu, Thanasis Korakis, Zhifeng Taoy, Elza Erkip, and Shivendra Panwar, Department of Electrical and Computer Engineering, Polytechnic Institute of NYU, Mitsubishi Electric Research Laboratories (MERL).
13. AirMagnet WiFi Analyzer PRO: Anytime, Anywhere, WLAN Monitoring and Troubleshooting.
14. AirMagnet Planner for Cisco Small Business and Air Magnet Spectrum XT, Fluke Networks.
15. Attack tool published for WiFi setup flaw; Cisco issues warning; Cisco.
16. Cisco Aims for Clean Air on Wi-Fi, Sean Michael Kerner, 2010.

17. Cisco Spectrum Expert Wi-Fi.
18. Interference Identification Guide, Metageek.
19. The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular, Cisco, 2012.
20. Test MIMO Wi-Fi and LTE Radios over the Air, octoScope, 2012.
21. Airport Communications at Risk, ISCO International.
22. Guidelines and Tools for Migrating to the Cisco Unified Wireless Network, Cisco.
23. Visualize Your Wireless Network, TM.
24. Wireless Solution, Made in Sweden.
25. Protecting Wi-Fi Networks from Hidden Layer 1 Security Threats, David Coleman and Neil Diener, 2007.

APPENDIX C

IEEE 802 Standards

IEEE Family of Standards

The Institute of Electrical and Electronics Engineers (IEEE) 802 committee has developed a family of wireless standards that have become dominant in the unlicensed industrial, scientific, and medical (ISM) bands. Equipment designed to one or another of the standards in the IEEE 802 family is the de facto standard for wireless data networks, mobile phone headsets, and a variety of other functions. Although equipment following the IEEE 802 standards does not have exclusive use of any frequency band, it is the most commonly used class of wireless in many of the bands. As Figure C-1 illustrates, IEEE 802 standards have been developed for a wide variety of purposes and operate in a variety of frequency bands. When discussing equipment that follows IEEE 802 standards, there are a range of types. Some equipment strictly follows an IEEE 802 standard and has been tested by an independent authority, such as the WiFi Alliance, and certified for its compliance with the standard and interoperability with other certified WiFi equipment. Other devices are designed to the standard but have not been certified, leaving some question about how faithfully the standard was implemented. In other cases, devices are designed to use the IEEE 802 standards but with proprietary differences. An example in this class is a set of devices offered by Ubiquiti, a private vendor, that operate in the 900 MHz ISM band based on 802.11b/g. Similar offerings are available from other vendors. So while the IEEE 802 standards do not support the 900 MHz ISM bands, these companies have adapted them to the band. Perhaps in response, the IEEE 802 committee is now working on 802 standards to operate in this band through the IEEE 802.11ah project.

IEEE 802.11 (WiFi)

In an article in *Electronic Design*, "Wi-Fi and Bluetooth Rule the Airwaves" (July 11, 2013, pgs. 28–35), Louis Frenzel provides a very concise technical overview of the different versions of IEEE 802.11:

The first generation 11b showed up in 1997 and uses direct sequence spread spectrum (DSSS) to achieve data rates to 11 Mbits/s in a 20-MHz channel in the 2.4 GHz ISM radio band. With the growth of the Internet, that low speed soon became a disadvantage.

The second-generation 802.11a appeared in 1999. It was the first to use the 5 GHz ISM band and orthogonal frequency division multiplexing (OFDM) with 64 subcarriers spaced 312.5 kHz apart. Channel bandwidth was 20 MHz, and binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), 16-phase quadrature amplitude modulation (16QAM), and 64-state quadrature amplitude modulation (64QAM) types were defined, permitting the data rate to increase to a maximum of 54 Mbits/s.

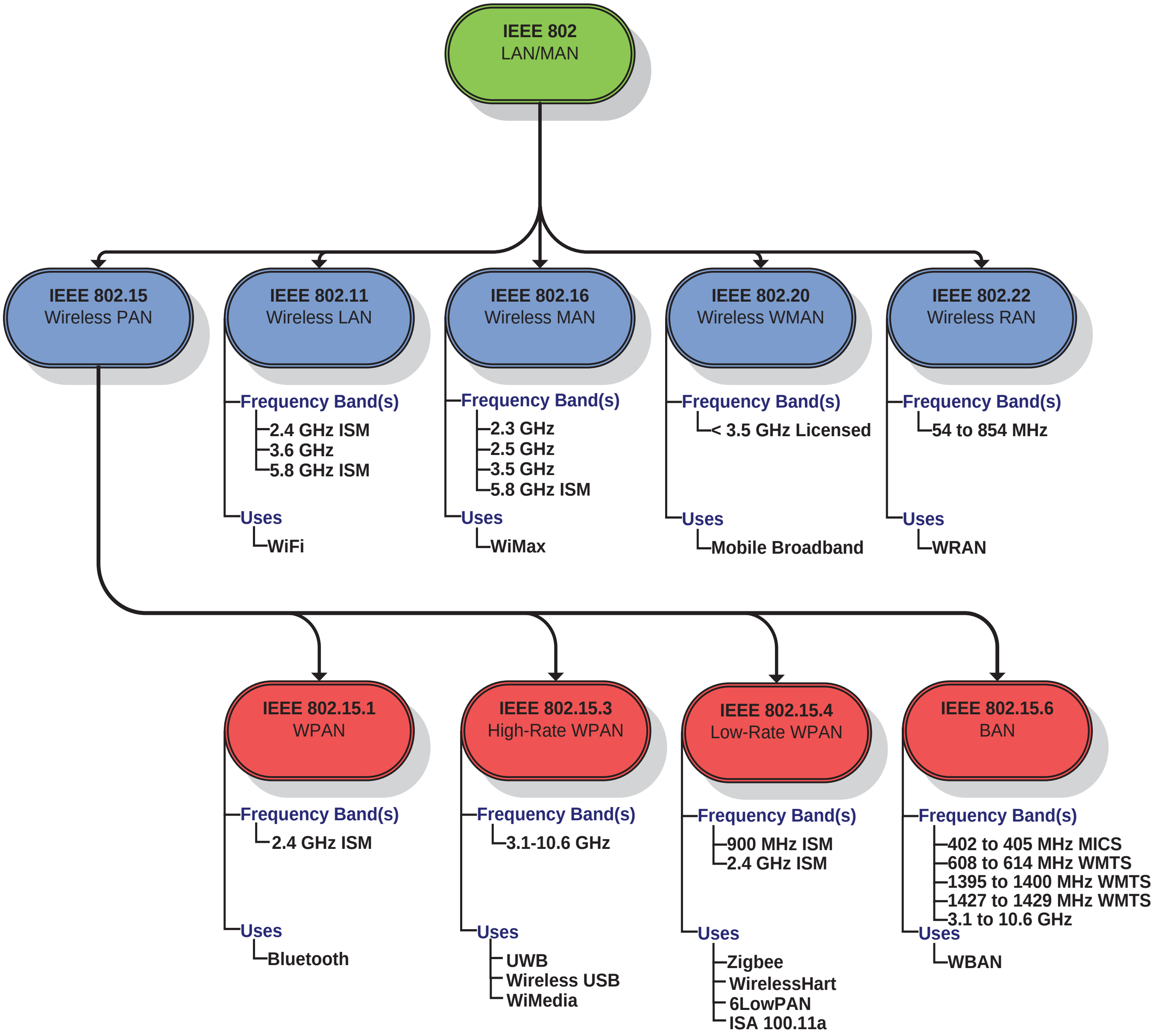


Figure C-1. IEEE 802 standards organized by field of use and frequency band.

While the 802.11a version was more robust because of the OFDM characteristics that mitigated multipath reflections and the 5 GHz assignment meant less interference, the higher frequency still limited the range. This version was never too popular despite its advantages.

The big breakthrough came when the 802.11g standard was approved in 2003. It is essentially the same as 11a but operates in the 2.4 GHz band. Using the same OFDM and modulation options, it too can deliver up to 54 Mbits/s. It was immediately popular because the many IC companies competing for the business brought chip prices very low.

The current 11n standard is a further improvement over 11a/g. It adds 40-MHz channels and multiple-input, multiple-output (MIMO) features to the OFDM, allowing data rates to increase to as much as 600 Mbits/s.

MIMO uses multiple receivers, transmitters, and antennas to achieve spatial division multiplexing (SDM). SDM transmits fast multiple data streams concurrently within the same 20- or 40-MHz channel bandwidth. Pre-coding and post-decoding as well as unique path characteristics distinguish the data streams. The data rate then can be multiplied by a factor roughly equal to the number of data streams.

The 11n MIMO standard permits up to four transmit and four receive channels (4 × 4), although 1 × 2, 2 × 2, and 3 × 3 versions are more widely used. The 600-Mbit/s data rate is achieved using 4 × 4 MIMO with 64QAM in a 40-MHz channel.

IEEE 802.15.1 (Bluetooth)

Bluetooth's market dominance and frequent use scenarios that have Bluetooth devices operating close to WiFi devices make it of particular concern when looking at WiFi interference. The Bluetooth community recently introduced a low-power version, named Bluetooth Low Energy (BLE), and Bluetooth is now being called Bluetooth Classic to differentiate it from Bluetooth Low Energy. Louis Frenzel does an excellent job of presenting the technical description of Bluetooth and Bluetooth Low Energy:

BLE still operates in the same ISM license-free 2.4 to 2.483 GHz frequency band as standard Bluetooth, but it uses a different frequency-hopping spread-spectrum (FHSS) scheme. Standard Bluetooth hops at a rate of 1600 hops per second over 79 channels that are 1 MHz wide. BLE FHSS uses 40 channels that are 2 MHz wide to ensure greater reliability over longer distances. Standard Bluetooth offers gross data rates of 1, 2, or 3 Mbits/s. BLE's maximum rate is 1 Mbit/s with a net throughput of 260 kbits/s.

Also, BLE uses Gaussian frequency shift keying (GFSK) modulation. It offers a power output of 0 dBm (1 mW) and a typical maximum range of 50 meters. Security is via the 128-bit Advanced Encryption Standard. An adaptive frequency-hopping technique that avoids interference, a 24-bit cyclic redundancy code (CRC), and a 32-bit message integrity check all improve link reliability. The most common network configurations are point-to-point (P2P) and star. Latency is only 6 ms.[17]

IEEE 802.15.4 (ZigBee)

IEEE standard 802.15.4 was developed for wireless personal area networks. Wireless personal area networks are focused on low-cost, low-speed communication between devices, in contrast to WiFi which is focused on end-users. Sensors and automation systems are the focus for this class of device. Wireless personal area networks intend to provide very low-cost communication between devices with little to no underlying infrastructure. Low power consumption is critical so that battery power is a viable alternative.

The target communications range is up to 10-meter. Data transfer rates of up to 250 kbits/s meet the needs of this class of device.

IEEE 802.15.4 only addresses the physical and media access layers. It is the basis for:

- ZigBee
- ISA100.11a

[17] Louis Frenzel, "WiFi and Bluetooth Rule the Airwaves," *Electronic Design*, July 11, 2013.

- WirelessHART
- MiWi

Each of these protocols differentiate themselves in how they develop the upper layers but have in common the lower layers, as defined in IEEE 802.15.4.

IEEE 802.15.4 was first released in 2003 with a new version released in 2006 and work continuing on future revisions. It supports operation in the following bands:

- 868.0–868.6 MHz: Europe
- 902–928 MHz: North America
- 2400–2483.5 MHz: worldwide use

Given its target application and shared frequency bands with WiFi, these devices are likely to be used in airports and add to the RF noise for WiFi. While these devices are mostly low power and intermittent in their communication, the intention to have many of them installed to provide sensing coverage creates an additive effect from their combined operation.

History of IEEE 802 Standards

This section provides a brief history of the IEEE 802 standards, from an interference viewpoint. It does not attempt to provide a definitive history of these standards and the equipment that is designed to comply with them. Instead it focuses on the milestones that are relevant to the study of WiFi interference.

In 2003, the Federal Communications Commission allocated additional spectrum for unlicensed use in the 5 GHz band and established the Unlicensed National Information Infrastructure (UNII) service to facilitate the deployment of competitive wireless broadband services.[18] Unlicensed National Information Infrastructure equipment is authorized to operate radio transmitters in the 5.15–5.35 GHz, 5.47–5.725 GHz, and 5.725–5.825 GHz bands on an unlicensed basis, but must comply with technical rules specific to UNII devices to prevent interference. In order to avoid interference to the FAA's terminal Doppler weather radar (TDWR) installations, the FCC requires that UNII devices operating in the 5.25–5.35 GHz and 5.47–5.725 GHz bands have dynamic frequency selection (DFS) radar detection functionality, which allows them to detect the presence of radar systems and avoid co-channel operations with radar systems.[19]

However, despite the requirement in the rules that UNII equipment employ DFS capability, the FCC Enforcement Bureau Field Offices continue to encounter instances of interference to TDWR systems caused by UNII devices located in close proximity to TDWR installations.[20] The FCC states that such interference ". . . poses a clear hazard to air traffic safety and requires aggressive enforcement."[21]

[18] See Unlicensed National Information Infrastructure (UNII) Devices in the 5 GHz Band, Report and Order, 18 FCC Rcd 24484 (2003).

[19] See 47 C.F.R. § 15.407(h)(2). See also 47 C.F.R. § 15.403(s) (defining U-NII devices as "[i]ntentional radiators operating in the frequency bands 5.15-5.35 GHz and 5.470-5.825 GHz that use wideband digital modulation techniques and provide a wide array of high data rate mobile and fixed communications for individuals, businesses, and institutions.").

[20] See Memorandum from Julius Knapp, Chief, Office of Engineering and Technology, FCC, and P. Michele Ellison, Chief, Enforcement Bureau, FCC, to Manufacturers and Operators of Unlicensed 5 GHz Outdoor Network Equipment Re: Elimination of Interference to Terminal Doppler Weather Radar (TDWR) (dated July 27, 2010), available at http://transition.fcc.gov/eb/uniitdwr.pdf (last visited April 27, 2013) (OET/EB Memo).

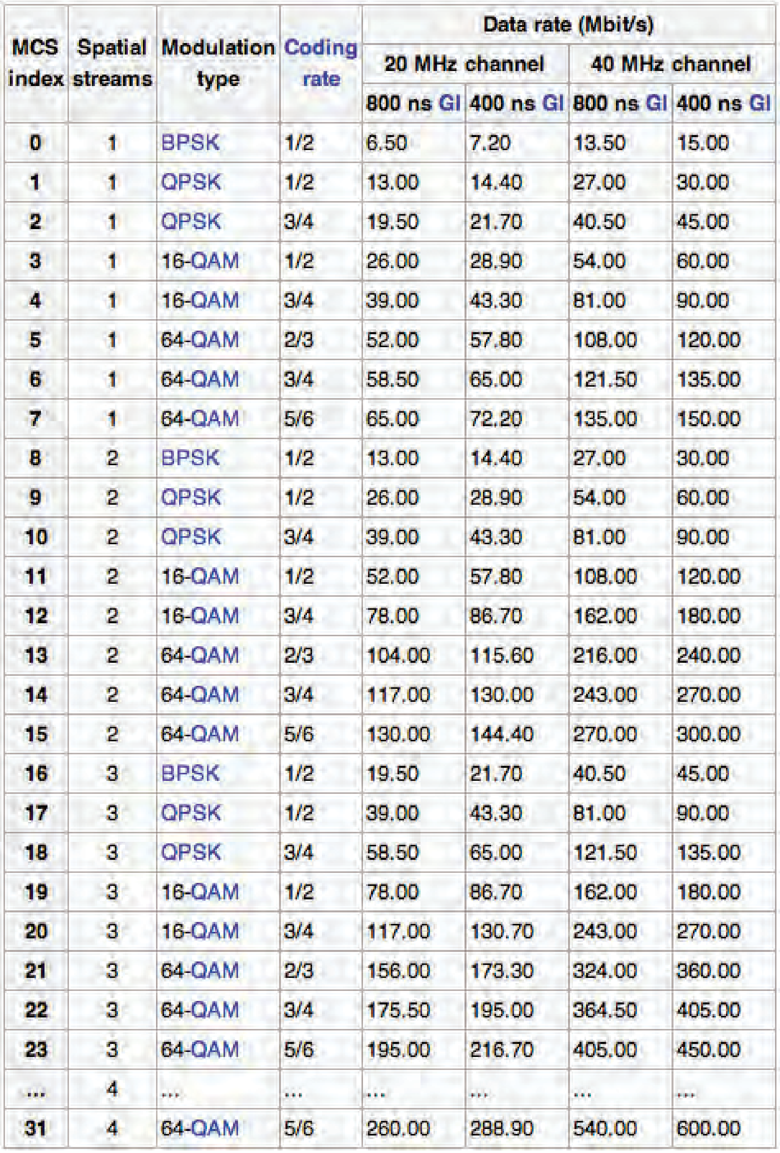
[21] Towerstream Corporation, Notice of Apparent Liability for Forfeiture and Order, FCC 13-109 released August 6, 2013.

Table C-1. Version and amendments of IEEE 802.11, WiFi.[22]

Year	Version	Band	Data Rate	Purpose
1997	802.11	2.4	2 Mbps	The original wireless local area network (WLAN) standard. Supports 1 Mbps to 2 Mbps. Based on a DSSS physical interface.
1999	802.11a	5.8	54 Mbps	High-speed WLAN standard for 5 GHz band. Supports 54 Mbps. Based on an OFDM physical interface.
1999	802.11b	2.4	11 Mbps	WLAN standard for 2.4 GHz band. Supports 11 Mbps. Based on a DSSS physical interface.
	802.11d			International roaming — automatically configures devices to meet local RF regulations.
	802.11e			Addresses quality of service requirements for all IEEE WLAN radio interfaces.
	802.11f			Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
2003	802.11g	2.4/5.8	54 Mbps	Establishes an additional modulation technique for 2.4 GHz band. Supports speeds up to 54 Mbps. Implements the physical interface based on OFDM.
2007	802.11			Consolidation of the 802.11 amendments with the base standard.
	802.11h			Defines the spectrum management of the 5 GHz band.
	802.11k			Defines and exposes radio and network information to facilitate radio resource management of a mobile WLAN.
2009	802.11n	2.4/5.8	600 Mbps	Provides higher throughput improvements. Intended to provide speeds up to 500 Mbps through the use of multiple-input, multiple-output and higher density modulations.
2012	802.11			Consolidation of the 802.11 amendments with the base standard.
	802.11s			Defines how wireless devices can interconnect to create an ad-hoc (mesh) network.
	802.11r			Provides fast (<50 millisecond), secure and quality of service-enabled inter-access point roaming protocol for clients.
	802.11u			Adds features to improve interworking with external (non-802) networks where the user is not pre-authorized for access.
	802.11v			Enhances client manageability, infrastructure-assisted roaming management, and filtering services.
2008	802.11y	3.7		Extended 802.11a to the licensed 3.7 GHz band.
	802.11z			Creates tunnel direct link setup between clients to improve peer-peer video throughput.
	802.11aa			Robust video transport streaming.
2013	802.11ac	5.8	693 Mb/s	Extends the IEEE 802.11n in the 5.8 GHz band to achieve higher data rates through wider channel bandwidths, higher density modulations, and additional multiple-input, multiple-output streams.
2012	802.11ad	60	7,000 Mbps	Uses the 60 GHz band to create very high data rate capability.
2014	802.11af	TVWS	26.7 Mbps	Operation in TV White Space frequency band (54790MHz).
TBD	802.11ah	0.9	TBD	Adds the 900 MHz band to those supported in the WiFi standards. The physical interface is OFDM based.

[22] Table from: http://www.intel.com/standards/case/case_802_11.htm

Table C-2. MCS index values (GI = guard interval).[23]



MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
16	3	BPSK	1/2	19.50	21.70	40.50	45.00
17	3	QPSK	1/2	39.00	43.30	81.00	90.00
18	3	QPSK	3/4	58.50	65.00	121.50	135.00
19	3	16-QAM	1/2	78.00	86.70	162.00	180.00
20	3	16-QAM	3/4	117.00	130.70	243.00	270.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
...	4	...	...	...	...	...	...
31	4	64-QAM	5/6	260.00	288.90	540.00	600.00

Modulation and Coding Schemes

To achieve their higher data rates, the newer versions of the IEEE 802.11 standards support a number of modulation schemes and coding rates. These are defined by the standard and are represented by a modulation and coding scheme (MCS) index value. A unit will vary the MCS used based on the channel conditions.[24]

WiFi Shipments

Shipments in 2013 of WiFi chipsets are projected to be 2.14 billion units, up 20% from 1.78 billion in 2012. Double-digit growth started at least five years ago and is expected to persist at least until 2016. By 2017, WiFi chipset shipments will amount to 3.71 billion units.

[23] Wikipedia, "IEEE 802.11n-2009," Available at: http://en.wikipedia.org/wiki/IEEE_802.11n-2009

[24] Wikipedia, "IEEE 802.11n-2009," Available at: http://en.wikipedia.org/wiki/IEEE_802.11n-2009

A total of approximately 18.7 billion WiFi chipset units will be shipped from 2011 to 2017—nearly all of which will belong to the high-performance 802.11n version.

By 2015, nearly 1.2 billion handsets out of a total of 1.9 billion cellphones produced that year will include WiFi functionality. Approximately 70% of handsets sold worldwide by then—and well over that figure in North America and Western Europe—are expected to be smartphones with embedded WiFi.[25]

ABI Research forecasts carrier WiFi access point shipments in 2018 to reach 9.7 million, with the Asia-Pacific region accounting for 70% of that number.[26]

New IEEE 802.11 Versions

The success of the IEEE 802.11 series of standards and WiFi data networks has required and supported an aggressive course of development. In recent years, the IEEE 802.11 committee has averaged a new addition to the standards every year. New frequency bands are being opened for use by WiFi. The data rates are ever increasing. An expanding variety of use cases are being supported. Field problems, not uncommonly the result of the success of WiFi, are a staple on the menu of items receiving attention from the committee.

IEEE 802.11ac

IEEE 802.11ac was approved and published in January 2014 after three years of development. Products supporting the new version of the standard were already on the market before the standard was published and some projections anticipate 1 billion IEEE 802.11ac devices by 2015.

IEEE 802.11ac was developed to support a single link throughput of at least 500 megabits per second (500 Mbits/s) and a total throughput of at least 1 gigabit per second. Concepts introduced in IEEE 802.11n are extended to accomplish these data rates, including:

- Wider RF bandwidth (up to 160 MHz)
- More multiple-input, multiple-output (MIMO) spatial streams (up to eight)
- Downlink multi-user MIMO (up to four clients)
- High-density modulation (up to 256-QAM)

New features provided by IEEE 802.11ac include:

- Extended channel binding with 80 MHz channel bandwidth mandatory for stations (vs. 40 MHz maximum in 802.11n), 160 MHz available optionally
- Support for up to eight MIMO spatial streams (vs. four in 802.11n)
- Downlink multi-user MIMO (allows up to four simultaneous downlink multi-user MIMO clients)
- Multiple STAs, each with one or more antennas, transmit or receive independent data streams simultaneously
- Space Division Multiple Access: streams not separated by frequency, but instead resolved spatially
- Downlink multi-user MIMO (one transmitting device, multiple receiving devices) included as an optional mode

[25] HIS iSuppli, "Small Cells with WiFi Set to Reshape Wireless Communications Market," *Microwave Journal*, May 15, 2013. Available at: http://www.microwavejournal.com/articles/19858-small-cells-with-wi-fi-set-to-reshape-wireless-communications-market

[26] ABI Research, "9.7 Million Carrier WiFi Access Point Shipments in 2018 as Mobile Carriers Jump on the Bandwagon," Sept. 30, 2013. Available at: https://www.abiresearch.com/press/97-million-carrier-wi-fi-access-point-shipments-in

- 256-QAM, rate 3/4 and 5/6 modulation added as optional modes (vs. 64-QAM, rate 5/6 maximum in 802.11n)
- Beamforming with standardized sounding and feedback for compatibility between vendors (non-standard in 802.11n made it hard for beamforming to work effectively between different vendor products)
- Media access control modifications (mostly to support above changes)
- Coexistence mechanisms for 20/40/80/160 MHz channels, 11ac and 11a/n devices[27]

IEEE 802.11ad

In May 2007, the IEEE 802 committee started a new study group to investigate "very high throughput" technologies. The study group initially focused on International Mobile Telecommunications-Advanced (IMT-Advanced) operation in the bands < 6 GHz. However, the focus of the study group changed to enhancing 802.11n in the 5 GHz band. In November 2007, the group took up the study of the 60 GHz band. The motivation was that the millimeter wave band could provide for much wider band channels than in the microwave band, enabling single link throughputs greater than 1 Gbps.[28]

The WiFi Alliance asked to provide usage models to help develop requirements. The general categories of the usage models included wireless display, distribution of high definition TV, rapid upload/download, backhaul, outdoor campus, auditorium, and manufacturing floor. The specific uses that are expected to be most prevalent include compressed video streaming around a house, rapid sync-and-go, and wireless I/O. It is envisioned that TVs and DVRs around the home will have wireless capability and 100+ Mbps aggregate of videos from a DVR can be displayed wirelessly on TVs in different rooms. With rapid sync-and-go, users can quickly sync movies or pictures between mobile devices such as a phone, a laptop, or a tablet. With a 1 Gbps radio link, a 1 GB video file will take much less than a minute to transfer between devices. Data rates exceeding 1 Gbps will provide the capability for a wireless desktop, with wireless connections between a computer and peripherals such as monitors, printers, and storage devices.[29]

Network World offered some interesting comments on the new use cases made possible by 802.11ad and the comparison of IEEE 802.11ac and IEEE 802.11ad:

- "802.11ac is an extension for pure mainstream WiFi," said Sean Coffey, Realtek's director of standards and business development. "It's evolutionary. . . . You're not going to see dramatically new use cases."
- 802.11ac is a development of the current 802.11n standard, producing improved performance on the same 5 GHz frequency bands. Some routers using the 802.11ac have already been deployed, and the experts on the panel agreed that it will become commonplace by early 2013.
- By contrast, 802.11ad adds 60 GHz connectivity to the previously used 2.4 GHz and 5 GHz frequencies, potentially providing multi-gigabit connection speeds and dramatically broadening the number of applications for which wireless can be used.
- "There are some unique characteristics about the 60 GHz band that really help in bringing a whole bunch of new use cases," said Mark Grodzinsky, vice president of marketing for 60 GHz pioneer Wilocity. Some of those uses include wireless docking and uncompressed HD video streaming.

[27] Matthew Gast, *802.11ac: A Survival Guide*, O'Reilly Media, Inc., 2013. Available at: http://chimera.labs.oreilly.com/books/1234000001739

[28] Eldad Perahia and Michelle X. Gong, "Gigabit Wireless LANs: An Overview of IEEE 802.11ac and 802.11ad," ACM SIGMOBILE *Mobile Computing and Communications Review*, Vol. 15, Iss. 3, July 2011.

[29] A. Myles and R. de Vegt, "WiFi Alliance (WFA) VHT Study Group Usage Models," IEEE 802.11-07/2988r4, March 19, 2008. Available at: https://mentor.ieee.org/802.11/dcn/07/11-07-2988-04-0000-liaison-from-wi-fi-alliance-to-802-11-regarding-wfa-vht-study-group-consolidation-of-usage-models.ppt.

- "60 GHz is also highly directional," he added. "So whereas in 2.4 and 5 [GHz] it's pretty much an omnidirectional transmission, meaning the antennas just blow energy in all directions, with 60 GHz, it's very focused."
- However, 802.11ad will still not represent a wholesale shift in the nature of WiFi, according to Coffey.
- "When you add in [802.11ad], I would see this as an island of super-high data rate present in a sea of gigabit WiFi. What it does is allow you to do a massive amount of WiFi offloading." The idea is that the localized but high-bandwidth 60 GHz network can be used for specific, highly demanding tasks, keeping the standard 5 GHz frequency free for normal use, he explained.
- Devices using the 60 GHz standard could begin to appear in 2014 and become more prominent in 2015. This means that the next major transition is still well over a year away—in part because 802.11ac will not be a particularly testing upgrade for most end users.[30]

In a *Microwave Journal* article, ABI Research predicts very different deployment patterns for IEEE 802.11ac and IEEE 802.11ad. The researchers at ABI expect fast, widespread adoption of IEEE 802.11ac, while IEEE 802.11ad will see a slower but still impressive adoption rate:

- The growth of 802.11ac and 802.11ad will occur in very different ways. 802.11ac will explode into devices, including smartphones, from the start while 802.11ad will see a more modest and staggered growth. 802.11ac is being pushed into smartphones by key carriers' device requirements that are in sync with 802.11ac hotspot plans for more robust WiFi offloading. "The push towards 11ac adoption overpowers the minor additional cost of dual-band 802.11n/802.11ac chipsets that will be used in smartphones," states research director Philip Solis. "Perhaps surprising even to industry insiders, we will likely see 2X2 802.11ac implementations in smartphones in a few years."
- The proportion of various 802.11ac-enabled products will remain relatively consistent from 2013 to 2018, with smartphones making up 40% of those in 2013 and 46% in 2018, where over 3.5 billion WiFi chipsets with 802.11ac will ship. The WiFi Alliance is just about to start certification of products using the protocol, yet its shipments have started and are already on track to distribute hundreds of millions this year. 802.11ac finally pushes WiFi more towards the 5 GHz spectrum, which is cleaner and permits for the much larger channel sizes that allow for greater speeds and capacity.
- 802.11ad will phase from larger to smaller products, starting from peripherals and larger non-handset mobile devices and shifting to smaller and thinner devices over time. 802.11ad will make its way into smartphones in 2015, changing the proportion of 802.11ad-enabled products compared to prior to 2015. Smartphones will account for nearly half of all 802.11ad-enabled products in 2018, though with less than half the volume in smartphones compared to 802.11ac. Even so, over 1.5 billion chipsets with 802.11ad will ship in 2018. 802.11ad pushes WiFi into higher-speed, lower-power personal area networking that will be used simultaneously with other WiFi protocols.
- "As the complexity of WiFi increases, heading towards tri-band 802.11n/802.11ac/802.11ad chipsets, interesting design tradeoffs can be made to optimize for cost, size, and functionality," notes Solis. "Choices can be made around the support of 80 MHz or 160 MHz channel and MIMO configurations based on whether or not 802.11ad is included. Smaller antennae arrays can also be used to save space."[31]

[30] Jon Gold, "Interop: Don't Sweat 802.11ac WiFi—Because 802.11ad Will Knock Your Socks Off," *Network World*, October 3, 2012. Available at: http://www.networkworld.com/news/2012/100312-interop-80211ad-263036.html

[31] ABI Research, "Smartphones Will Account for Nearly Half of Both 802.11ac and 802.11ad Chipset Shipments in 2018," *Microwave Journal*, June 11, 2013. Available at: http://www.microwavejournal.com/articles/20086-smartphones-will-account-for-nearly-half-of-both-80211ac-and-80211ad-chipset-shipments-in-2018

IEEE 802.11af

IEEE 802.11af, approved in February 2014, allows wireless local area network operation in TV white space spectrum in the VHF and UHF bands between 54 and 790 MHz. Because of its operation in the TV white space, meaning on locally unused TV channels, the standard is often referred to as White-Fi and Super WiFi.

The FCC requires special measures to be implemented to limit interference to primary users of these bands, such as analog or digital TV and wireless microphones.

The low frequencies used have excellent propagation characteristics, making these devices particularly appealing for covering larger distances or penetrating buildings and walls.

The standard supports 9 MCS standards and speeds up to 35.6 Mbps.

IEEE 802.11ah

IEEE 802.11ah is being developed to support operation in the sub-gigahertz spectrum, particularly the 900 MHz ISM band (902–928 MHz) in the U.S. and the 868.0–868.6 MHz band in Europe.

The standard is anticipated to be released in May 2016.

New Frequency Bands

With two new frequency bands, the 60 GHz and TVWS bands, being added in the past 3 years and the IEEE 802.11ah, sub-gigahertz version anticipated in the next two, WiFi is dramatically expanding the bands and operating frequencies used. In addition, the FCC is working on adding 195 MHz of new spectrum to the UNII band, where WiFi already operates.

WiFi initially just operated in the 2.4 GHz ISM band, which still holds a majority of the WiFi traffic. For general use, operation in the UNII and ISM bands between 5–6 GHz was added. Specialized applications are supported in the 3.6 and 4.9 GHz bands.

It is unclear how these expanding operating frequencies will impact airport operations or devices travelers bring into airports. However, each development is undertaken for good reasons. Some are targeted at specific uses such as the limitation of the 4.9 GHz band to public safety applications. Others, like the traditional 2.4 and 5 GHz bands, are for general use.

The new frequency bands create the opportunity to separate services in frequency, with the resulting decrease in interference and congestion. However, the increasingly complex landscape of operating frequencies brings new problems such as increased risk of intermodulation interference and system interoperability challenges. With skillful implementation, the new frequency bands will greatly reduce interference and congestion. However, it would be naive to assume that intermodulation and other problems will be entirely avoided.

Band Fragmentation

For both the WiFi and cellular networks, band fragmentation is a strong trend. More frequency bands are being opened for use by both WiFi and cellular systems. This is being driven by the tremendous popularity and benefits of these wireless networks. The picture is complicated further by the continuing technological development of both WiFi and cellular. These forces create a complex set of RF protocols and frequency bands in which they operate. The picture is made more complex by different countries, usually for very good local reasons, making different bands available or applying different operating rules to the same bands.

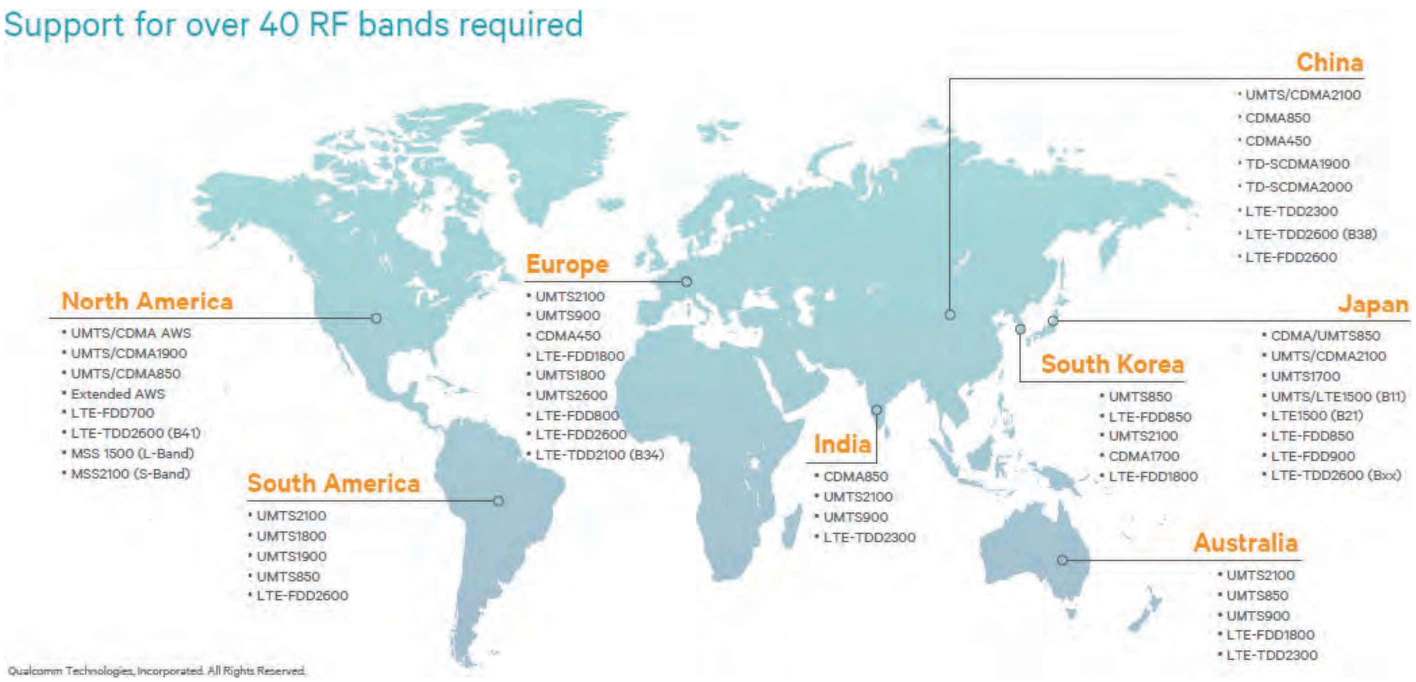


Figure C-2. A mobile device must support over 40 RF bands to be fully international.[32]

Positively, the trend toward band fragmentation makes available more spectrum in which to operate. However, it also creates a complex matrix of possible interference problems.

For equipment designers and network operators, the need to support multiple operating modes is a growing problem. According to a February 2013 Qualcomm press release:

"Band fragmentation is the biggest obstacle to designing today's global LTE devices, with 40 cellular radio bands worldwide . . . multiband, multimode mobile devices supporting all seven cellular modes, including LTE-FDD, LTE-TDD, WCDMA, EV-DO, CDMA 1x, TD-SCDMA and GSM/EDGE."[33]

As Figure C-2 illustrates, to fully enable international operation, user equipment (UE) is required to support as many as 40 bands and 7 operating modes. Even operation in a single country and on a single carrier requires that multiple frequency bands and operating modes be supported.

WiFi has its own challenges with a growing number of bands and modes in use and more being planned. While operation in the 2.4 GHz band is dominant, followed by the 5.8 GHz band, other bands are available or potentially becoming available, e.g., 900 MHz, 3.6 GHz, and 60 GHz.

The newer versions of IEEE 802.11 introduce spatial division multiplexing (SDM). SDM transmits multiple data streams concurrently within the same channel. The data rate is then multiplied by roughly the number of data streams being used. A further refinement is the use of a variety of modulation and coding schemes (MCS). Different MCS levels can be used, based on the channel characteristics, capabilities of the transmitter and receiver, and signal quality. Then there is the ability to vary the guard interval. A guard interval is a period of time between symbol transmissions that allows reflections from multipath to settle before the next symbol is sent. The rate at which data can be sent becomes a combination of the Fast Fourier Transform (FFT) time

[32] Sunil Patil, "LTE Band Fragmentation," CTIA 2013, Las Vegas, NV, May 22, 2013.

[33] Qualcomm, "Qualcomm RF360 Front End Solution Enables Single, Global LTE Design for Next-Generation Mobile Devices," February 21, 2013. Available at: http://www.qualcomm.com/media/releases/2013/02/21/qualcomm-rf360-front-end-solution-enables-single-global-lte-design-next

and the guard interval. In IEEE 802.11 a/g OFDM, the data or symbol rate is 250 kHz, or 4 µS. The 4 µS time is a combination of a 3.2 µS FFT time and 0.8 µS guard interval. However, IEEE 802.11n defines both the 0.8 µS and a short guard interval (SGI) of 0.4 µS. When channel conditions allow use of the SGI, the data rates can increase by 11%.

IEEE 802.11n defines 31 MCS states, two channel bandwidths, and two guard intervals. That makes for 124 possible combinations and a very wide range of potential data rates. IEEE 802.11ac defines 39 MCS states, four channel bandwidths, and two guard intervals. This increases the number of possible combinations from 124 to 242, and an even greater spread in the achievable data rates, as shown in Figure C-3.

RF interference can have any of several different impacts on a WiFi network. In most cases, RF noise will degrade the signal quality, lowering the achievable data rate. RF noise is not the only factor that impacts the data rate. The amount of signal reflections, multipath, in the environment will also have a very significant impact on the data rate. RF interference can also cause packet errors, decreasing the data rate because more packets must be retransmitted. An example of this is when an interferer's transmission only overlaps with a WiFi transmission some of the time. The WiFi signal might be experiencing excellent signal conditions, but periodically the interferer's transmission coincides with it, causing a packet error and the resulting need to retransmit the packet. In these cases, the impact of the interference is not a loss of connection but a slower data rate. If the user is doing something that doesn't need a high data rate, this might not even be noticeable. However, if a high data rate is needed because a lot of data is being sent or if the wireless local area network is already congested with a lot of concurrent users, then the impact can be very significant.

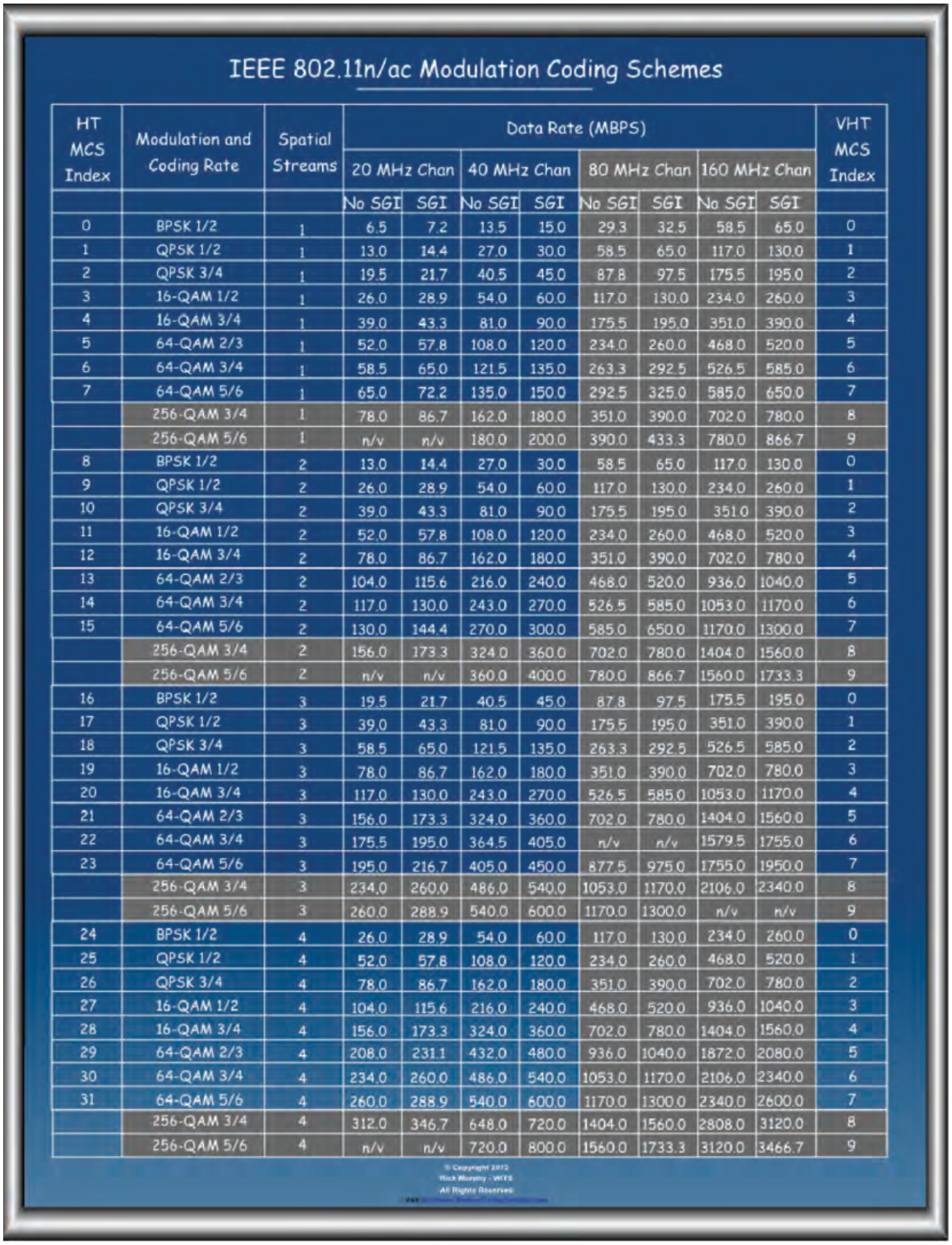
In extreme cases, RF interference can totally block a WiFi signal, at least on some channels or even in an entire band. Here again, if the interference only blocks some channels, the WiFi clear channel assessment (CCA) may simply identify that and move to a different channel, perhaps in a different band. The user may not even notice. However, under crowded conditions the loss of a channel or band could be catastrophic.

In addition, IEEE 802.11 has six different operating modes that a device can operate in:

- Master (acting as an access point)
- Managed (client, also known as station)
- Ad-hoc
- Mesh
- Repeater
- Monitor

Depending on the mode, the device will respond to network traffic differently and will pass different information to the operating system and higher-level applications. Depending on the operating mode, it may be difficult or even impossible for a user to know that they are experiencing interference. This also creates the very real possibility that network managers will not get the information they need or misunderstand the data they are getting. They may think that they are being given an accurate picture of the activity on their network, but the sources of their information may be screening off critical information and only giving them part of the picture. It is vital that network managers understand how their network data is coming to them and what information their tools may be filtering out. Filtering of data works both ways. When data is filtered in the right way for the problem being worked on, it helps the network manager to quickly spot where the problem is. But when the filter is incorrectly matched to the current need, it can blind the network manager to the true problem.

Network fragmentation creates a vast array of possible situations. When the fragmentation of the WiFi and cellular networks is brought together, an incredible number of possible combinations are created. The potential is that in any specific situation a number of combinations of



IEEE 802.11n/ac Modulation Coding Schemes

HT MCS Index	Modulation and Coding Rate	Spatial Streams	Data Rate (MBPS)								VHT MCS Index
			20 MHz Chan		40 MHz Chan		80 MHz Chan		160 MHz Chan		
			No SGI	SGI	No SGI	SGI	No SGI	SGI	No SGI	SGI	
0	BPSK 1/2	1	6.5	7.2	13.5	15.0	29.3	32.5	58.5	65.0	0
1	QPSK 1/2	1	13.0	14.4	27.0	30.0	58.5	65.0	117.0	130.0	1
2	QPSK 3/4	1	19.5	21.7	40.5	45.0	87.8	97.5	175.5	195.0	2
3	16-QAM 1/2	1	26.0	28.9	54.0	60.0	117.0	130.0	234.0	260.0	3
4	16-QAM 3/4	1	39.0	43.3	81.0	90.0	175.5	195.0	351.0	390.0	4
5	64-QAM 2/3	1	52.0	57.8	108.0	120.0	234.0	260.0	468.0	520.0	5
6	64-QAM 3/4	1	58.5	65.0	121.5	135.0	263.3	292.5	526.5	585.0	6
7	64-QAM 5/6	1	65.0	72.2	135.0	150.0	292.5	325.0	585.0	650.0	7
	256-QAM 3/4	1	78.0	86.7	162.0	180.0	351.0	390.0	702.0	780.0	8
	256-QAM 5/6	1	n/v	n/v	180.0	200.0	390.0	433.3	780.0	866.7	9
8	BPSK 1/2	2	13.0	14.4	27.0	30.0	58.5	65.0	117.0	130.0	0
9	QPSK 1/2	2	26.0	28.9	54.0	60.0	117.0	130.0	234.0	260.0	1
10	QPSK 3/4	2	39.0	43.3	81.0	90.0	175.5	195.0	351.0	390.0	2
11	16-QAM 1/2	2	52.0	57.8	108.0	120.0	234.0	260.0	468.0	520.0	3
12	16-QAM 3/4	2	78.0	86.7	162.0	180.0	351.0	390.0	702.0	780.0	4
13	64-QAM 2/3	2	104.0	115.6	216.0	240.0	468.0	520.0	936.0	1040.0	5
14	64-QAM 3/4	2	117.0	130.0	243.0	270.0	526.5	585.0	1053.0	1170.0	6
15	64-QAM 5/6	2	130.0	144.4	270.0	300.0	585.0	650.0	1170.0	1300.0	7
	256-QAM 3/4	2	156.0	173.3	324.0	360.0	702.0	780.0	1404.0	1560.0	8
	256-QAM 5/6	2	n/v	n/v	360.0	400.0	780.0	866.7	1560.0	1733.3	9
16	BPSK 1/2	3	19.5	21.7	40.5	45.0	87.8	97.5	175.5	195.0	0
17	QPSK 1/2	3	39.0	43.3	81.0	90.0	175.5	195.0	351.0	390.0	1
18	QPSK 3/4	3	58.5	65.0	121.5	135.0	263.3	292.5	526.5	585.0	2
19	16-QAM 1/2	3	78.0	86.7	162.0	180.0	351.0	390.0	702.0	780.0	3
20	16-QAM 3/4	3	117.0	130.0	243.0	270.0	526.5	585.0	1053.0	1170.0	4
21	64-QAM 2/3	3	156.0	173.3	324.0	360.0	702.0	780.0	1404.0	1560.0	5
22	64-QAM 3/4	3	175.5	195.0	364.5	405.0	n/v	n/v	1579.5	1755.0	6
23	64-QAM 5/6	3	195.0	216.7	405.0	450.0	877.5	975.0	1755.0	1950.0	7
	256-QAM 3/4	3	234.0	260.0	486.0	540.0	1053.0	1170.0	2106.0	2340.0	8
	256-QAM 5/6	3	260.0	288.9	540.0	600.0	1170.0	1300.0	n/v	n/v	9
24	BPSK 1/2	4	26.0	28.9	54.0	60.0	117.0	130.0	234.0	260.0	0
25	QPSK 1/2	4	52.0	57.8	108.0	120.0	234.0	260.0	468.0	520.0	1
26	QPSK 3/4	4	78.0	86.7	162.0	180.0	351.0	390.0	702.0	780.0	2
27	16-QAM 1/2	4	104.0	115.6	216.0	240.0	468.0	520.0	936.0	1040.0	3
28	16-QAM 3/4	4	156.0	173.3	324.0	360.0	702.0	780.0	1404.0	1560.0	4
29	64-QAM 2/3	4	208.0	231.1	432.0	480.0	936.0	1040.0	1872.0	2080.0	5
30	64-QAM 3/4	4	234.0	260.0	486.0	540.0	1053.0	1170.0	2106.0	2340.0	6
31	64-QAM 5/6	4	260.0	288.9	540.0	600.0	1170.0	1300.0	2340.0	2600.0	7
	256-QAM 3/4	4	312.0	346.7	648.0	720.0	1404.0	1560.0	2808.0	3120.0	8
	256-QAM 5/6	4	n/v	n/v	720.0	800.0	1560.0	1733.3	3120.0	3466.7	9

Visit [illegible]

Figure C-3. Modulation and coding schemes used by IEEE 802.11 n/ac.[34]

WiFi and cellular signaling combinations may operate in close proximity without any problem. However, other combinations may be very problematic. If CCA and other interference management methods work well, then the conflicting combinations may be automatically identified and avoided, without the user ever being aware of it or needing to take any action. However, in other situations these mechanisms either may not be capable of dealing with the situation they face or not have options available to avoid the interference.

[34] Figure C-3 is from the front panel of an HTML5 reference tool developed by Wireless Training & Solutions (WiTS), http://www.wirelesstrainingsolutions.com/. It is available at: http://www.aerohive.com/pdfs/Blog/MCS_Chart_802.11ac_v.06.html

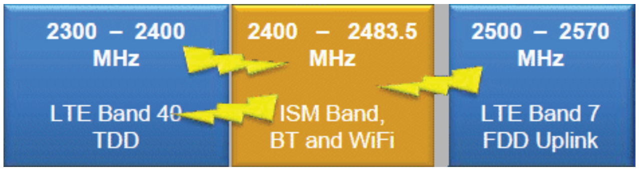


Figure C-4. Developing LTE-WiFi interference.[35]

Figure C-5. The newest Freescale Airfast LDMOS transistor.

A potential for interference that appears particularly concerning is created by the approaching use by LTE of the bands adjacent to the 2.4 GHz ISM band, which WiFi uses so heavily. Mobile phones and other LTE UE devices operating either below or above the 2.4 GHz ISM band have the potential for interfering with WiFi (Figure C-4). LTE Band 40 operates below the 2.4 GHz ISM band, using TDD between 2.3–2.4 GHz. LTE Band 41, 2496–2690 MHz, also operates in TDD mode but just above the 2.4 GHz ISM band. With these channels there is the potential for LTE to WiFi or WiFi to LTE interference. LTE Band 7 operates on an FDD basis with the UE transmitting (uplink) between 2500–2570 MHz, and the base (downlink) between 2620–2690 MHz. With LTE Band 7, the risk is only for LTE to WiFi interference.

In North America, LTE Band 7 is used by Bell and Rogers in Canada. Sprint used LTE band 41 in the U.S. nTelos is in trials using LTE band 41 in the U.S. Aeronet is planning on using the band in Puerto Rico. This suggests that interference between LTE and WiFi devices may become a problem in the areas where LTE uses bands 7, 40, or 41.

Component manufacturers work closely with their leading customers to support their needs and have the components available for the next generation of technology. Freescale is a leading provider of RF components, particularly power amplifiers, and a good example of how new components show the next steps their customers will be taking with their products.

The newest Freescale Airfast LDMOS transistors are designed specifically for TD-LTE base-stations at the 2.3/2.6 GHz frequency bands (Figure C-5). These transistors span a broad range of power points, from 50 W to 200 W. The AFT26HW050S/GS targets metrocell basestation applications in the 2496- to 2690-MHz band. In an asymmetrical Doherty configuration, it delivers 47.4 dBm of peak power.[36]

[35] Thomas Lindner, "LTE Band Fragmentation—Challenges for Cellular Platform Designs," LTE World Summit, Barcelona, May 2012, Day 2, T11.

[36] Louis Frenzel, "Freescale's Ritu Favre Discusses Today's RF Technologies," *Electronic Design*, October 3, 2013.

Freescale would not be making the significant investment that developing a new product requires if their customers didn't need it. Clearly Freescale is hearing that customers are planning on building mobile network basestations for the 2496–2690 MHz band, just above the 2.4 GHz ISM band where so much WiFi operates.

The issue of band fragmentation is complex enough if equipment can be relied on to correctly comply with local regulatory requirements. However, in today's highly mobile world, it is common for equipment designed to operate under one country's frequency allocations and service rules to be used in another. A wide array of wireless devices can be bought in one country but used in another, where they may be operating in violation of local regulations.

Abbreviations and acronyms used without definitions in TRB publications:

A4A	Airlines for America
AAAE	American Association of Airport Executives
AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
ACI–NA	Airports Council International–North America
ACRP	Airport Cooperative Research Program
ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
DOE	Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HMCRP	Hazardous Materials Cooperative Research Program
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act of 1991
ITE	Institute of Transportation Engineers
MAP-21	Moving Ahead for Progress in the 21st Century Act (2012)
NASA	National Aeronautics and Space Administration
NASAO	National Association of State Aviation Officials
NCFRP	National Cooperative Freight Research Program
NCHRP	National Cooperative Highway Research Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
PHMSA	Pipeline and Hazardous Materials Safety Administration
RITA	Research and Innovative Technology Administration
SAE	Society of Automotive Engineers
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (2005)
TCRP	Transit Cooperative Research Program
TEA-21	Transportation Equity Act for the 21st Century (1998)
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation