SCTE · ISBE

STANDARDS

Network Operations Subcommittee

SCTE OPERATIONAL PRACTICE

SCTE 255 2019

Operational Practice for Home Wi-Fi Deployment

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at http://www.scte.org.

140 Philips Road
Exton, PA 19341

Table of Contents

List of Figures

Title **Page Number**

List of Tables

1. Introduction

1.1. Executive Summary

The world of consumer devices is now a wireless world, with many devices using Wi-Fi® technology for communications.[1] Many cable subscribers no longer differentiate wireless operation from wired cable service – whether the wireless equipment is personally owned or is part of the equipment provided by the cable company – and often simply consider wireless and wired service to be the same thing. This document seeks to provide useful recommendations to enable cable operators to provide outstanding wireless services for their customers.

1.2. Scope

While many of the general principles and concepts discussed in this operational practice apply to the broader subject of wireless data service deployments, the primary focus is on residential Wi-Fi installations.

1.3. Benefits

The guidelines in this operational practice will help cable operators provide better residential wireless service and understand some of the more common problems and issues that can affect the quality of wireless service in the subscriber premises.

1.4. Intended Audience

The intended audience for this operational practice includes installers, technicians, engineers, and others who work with or are interested in the deployment of residential Wi-Fi services.

1.5. Areas for Further Investigation or to be Added in Future Versions

Topics that might be of interest for addition to future versions of this document, or part of new, standalone operational practices and similar documents include managed wireless services, commercial wireless service deployments, and outdoor wireless services.

2. Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1. SCTE References

- No normative references are applicable.

[1] Wi-Fi® is a registered trademark of the Wi-Fi Alliance (www.wi-fi.org)

2.2. Standards from Other Organizations

- No normative references are applicable.

2.3. Published Materials

- No normative references are applicable.

3. Informative References

The following documents might provide valuable information to the reader but, are not required when complying with this document.

3.1. SCTE References

- No informative references are applicable.

3.2. Standards from Other Organizations

- IEEE 802.11-2016 - https://ieeexplore.ieee.org/document/7786995/

3.3. Published Materials

- Wi-Fi Certified Home Design Public Info: https://www.wi-fi.org/discover-wi-fi/wi-fi-home-design
- WFA Members: The MRD's and Test Plans

4. Compliance Notation

shall	This word or the adjective "***required***" means that the item is an absolute requirement of this document.
shall not	This phrase means that the item is an absolute prohibition of this document.
forbidden	This word means the value specified shall never be used.
should	This word or the adjective "*recommended*" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighted before choosing a different course.
should not	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
may	This word or the adjective "*optional*" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.
deprecated	Use is permissible for legacy purposes only. Deprecated features may be removed from future versions of this document. Implementations should avoid use of deprecated features.

5. Abbreviations and Definitions

5.1. Abbreviations

ACS	auto configuration server
ACS	auto channel selection
AP	access point
BPSK	binary phase shift keying
BSS	basic service set
BSSID	basic service set identifier
CSMA/CA	carrier sense multiple access with collision avoidance
CPE	customer premises equipment
CPU	central processing unit
CRC	cyclic redundancy check
dB	decibel
dBm	decibel milliwatt
DBC	dual band concurrent
DCF	distributed coordination function
DFS	dynamic frequency selection
DOCSIS	Data-Over-Cable Service Interface Specifications
DRS	data rate shifting
DS	downstream
DSL	digital subscriber line
DSSS	direct sequence spread spectrum
FHSS	frequency hopping spread spectrum
FSPL	free space path loss
GHz	gigahertz
GUI	graphical user interface
GW	gateway
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of things
IP	Internet protocol
IPDR	Internet protocol detail record
ISBE	International Society of Broadband Experts
ISI	inter-symbol interference
ISM	industrial, scientific, and medical
IT	information technology
ITU	International Telecommunication Union
KPI	key performance indicator
LAN	local area network
LED	light emitting diode
LTE	long term evolution
MAC	media access control
Mb/s (Mbps)	megabits per second
MCS	modulation and coding scheme
MDU	multiple dwelling unit
MHz	megahertz
MIMO	multiple input multiple output

MoCA	Multimedia over Coax Alliance
MSO	multiple system operator
MU-MIMO	multi-user MIMO
ns	nanosecond
OBSS	overlapping basic service set
OD	outdoor
OFDM	orthogonal frequency division multiplexing
OUI	organizationally unique identifier
PC	personal computer
PHY	physical layer
PIN	personal identification number
QAM	quadrature amplitude modulation
QPSK	quadrature phase shift keying
RDK	reference design kit
RF	radio frequency
RSSI	received signal strength indicator
RX	receive (also receiver)
SCTE	Society of Cable Telecommunications Engineers
SNMP	Simple Network Management Protocol
SNR	signal-to-noise ratio
SSID	service set identifier
STA	station
TV	television
TX	transmit (also transmitter)
U-NII	unlicensed national information infrastructure
US	upstream
USB	universal serial bus
VoIP	Voice over Internet Protocol
VPN	virtual private network
WFA	Wi-Fi Alliance
WMM	Wi-Fi Multimedia
WPS	Wi-Fi protected setup

5.2. Definitions

access point (AP)	A device or circuit that provides an interface between a wired local area network and radio transmitter/receiver circuitry to enable over-the-air transmission of data to and from various Wi-Fi capable devices.
amplitude	The signal level, or more specifically, the power of an electromagnetic signal.
attenuation	See *loss*.
decibel (dB)	A logarithmic-based expression of the ratio between two values of a physical quantity, typically power or intensity. The decibel provides an efficient way to express ratios which span one or more powers of the logarithmic base, most commonly 10. Mathematically, the ratio of two power levels P_1 and P_2 in decibels is $dB = 10\log(P_1/P_2)$.
decibel milliwatt (dBm)	Unit of power, defined as decibels relative to 1 milliwatt, where 0 dBm equals 1 milliwatt. Mathematically, $dBm = 10\log_{10}$(value in mW/1 mW).

frequency	The number of times (typically per second) that a repetitive event happens; that is, the rate of oscillation of an electromagnetic signal. Frequency is measured in units of hertz, which is the number of cycles or waves per second.
gain	An increase in the power of a signal or signals, usually measured in decibels. Expressed mathematically, $G_{dB} = 10\log_{10}(P_{out}/P_{in})$, where G_{dB} is gain in decibels, P_{out} is output power in watts, P_{in} is input power in watts, and $P_{out} > P_{in}$. When signal power is stated in dBmV, $G_{dB} = P_{out(dBmV)} - P_{in(dBmV)}$.
gigahertz (GHz)	A unit of frequency equal to one billion (10^9) hertz. See also *hertz*.
hertz (Hz)	A unit of frequency equivalent to one cycle per second.
interference	A collective term that describes unwanted signals, noise, intermodulation distortion, or other disturbance that may degrade or otherwise change the quality or performance of a desired signal or signals.
loss	A decrease in the power of a signal or signals, usually measured in decibels. Expressed mathematically, $L_{dB} = 10\log_{10}(P_{in}/P_{out})$, where L_{dB} is loss in decibels, P_{in} is input power in watts, P_{out} is output power in watts, and $P_{out} < P_{in}$. When signal power is stated in dBmV, $L_{dB} = P_{in(dBmV)} - P_{out(dBmV)}$.
megahertz (MHz)	A unit of frequency equal to one million (10^6) hertz. See also *hertz*.
multipath	A phenomenon in which an electromagnetic signal from a transmitter travels via more than one route to the receiver. For example, a Wi-Fi signal transmitted from an access point might travel directly to the receiver, and some of the same transmitted signal might also be reflected by nearby objects before arriving a fraction of a second later at the receiver.
radio frequency (RF)	That portion of the electromagnetic spectrum from a few kilohertz to just below the frequency of infrared light.
signal-to-noise ratio (SNR)	A general measurement of the ratio of signal power to noise power, usually expressed in decibels.
service set identifier (SSID)	An up to 32-character string of letters and/or numbers used to name a wireless network.
Wi-Fi	A term that describes technology that uses over-the-air radio waves for wireless local area networking based on IEEE 802.11.

6. Introduction

6.1. Wi-Fi Introduction

Wi-Fi is a term that describes technology that uses over-the-air radio waves for wireless local area networking. Wi-Fi enabled devices – which implement the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards – have become almost ubiquitous in homes, businesses, and elsewhere, functioning as extensions of wired networks.

In its simplest form, a Wi-Fi network includes a device called an access point (AP) or wireless router (or wireless gateway), which provides an interface between a wired local area network (LAN) and radio transmitter/receiver circuitry to enable over-the-air transmission of data to and from various Wi-Fi capable devices (also called clients or stations); refer to Figure 1. Wi-Fi APs can be standalone devices connected to cable modems and digital subscriber line (DSL) modems using a length of Ethernet cabling,

or built-in to those modems. Wi-Fi capable user devices such as smart phones and tablets, laptops, desktop personal computers, printers, smart TVs, and so on use a built-in wireless adapter to communicate with the access point. Older equipment – especially older desktop PCs – that doesn't have a built-in wireless adapter can often use an external wireless adapter that plugs in to an available Ethernet port or universal serial bus (USB) port.

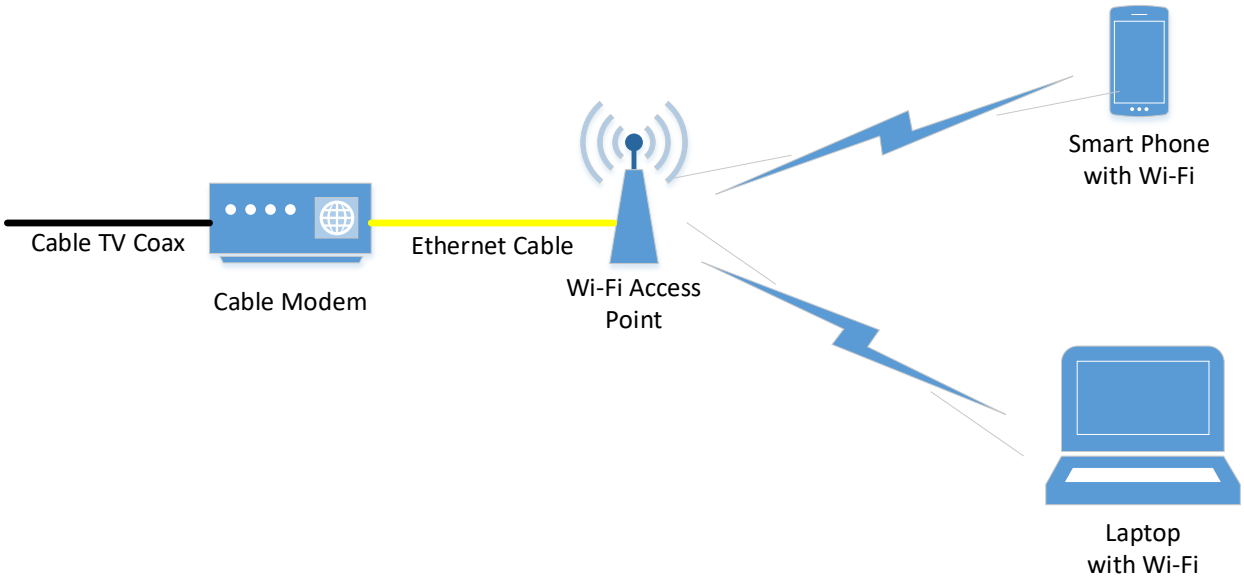

Figure 1 - Example of a simple Wi-Fi network

Wi-Fi technology most commonly uses the 2.4 GHz and 5 GHz radio frequency (RF) bands for wireless transmission of data. As such, Wi-Fi operation is subject to the usual impairments that affect over-the-air radio communications: weakening or blockage of the signal over distance, and as it passes through walls, floors, doors, furniture, and other obstructions in the signal path; reflections – also called multipath (similar to ghosting in analog TV pictures); and interference from other services or devices – including other Wi-Fi devices – operating on or near the same frequency. One example of the latter is interference from microwave ovens, which operate in the same 2.4 GHz band that Wi-Fi uses. Some baby monitors and cordless phones also operate in the 5GHz spectrum.

Additional information about Wi-Fi is available online at https://computer.howstuffworks.com/wireless-network.htm and https://en.wikipedia.org/wiki/Wi-Fi and http://wi-fi.org.

A significant percentage of a cable company's service calls is related to Wi-Fi problems. Section 6.7 of this document lists the top 10 home user Wi-Fi issues reported by cable operators. In general, the reported issues can be categorized into three major areas: subscriber education, Wi-Fi RF performance issues, and wireless network congestion.

It is probably useful to begin by considering the top sources of wireless discontent and then to consider how those sore points can be addressed and hopefully avoided altogether.

The Wi-Fi radio signals occupy unlicensed spectrum in the 2.4 GHz and 5 GHz bands. Allocations for industrial, scientific and medical (ISM) equipment in these bands have been useful for low power local area wireless networks based on Wi-Fi technology. There is no protection from interference in these bands so Wi-Fi device operation near microwave ovens, baby monitors, and Bluetooth devices, which also use this unlicensed spectrum, may result in impaired performance.

6.2. Wi-Fi Data Rates and Client Performance

Wi-Fi data rate is the connection rate from Wi-Fi client to serving access point. The throughput is the total amount of data transferring from access point to Wi-Fi client at any moment in time. The 802.11 standards offer data rate shifting (DRS) to manage availability of the Wi-Fi link under changing RF interference and client density conditions in the earlier 802.11g specifications.

Similar to modulation profiles in DOCSIS, the 802.11n specification introduced high throughput (HT) multiple modulation profiles with the potential to support simultaneous encoded streams which means multiple transmit and receive capabilities with per-stream unique modulations possible.

802.11n also introduced for the first time, Wi-Fi channel operation over 20 MHz and 40 MHz of radio frequency. These modulation profiles are known as modulation coding scheme (MCS).

The MCS is determined by radio capabilities in terms of simultaneous radio stream processing capability and the potential to independently modulate these streams.

For example, MCS 0 supports one spatial stream, modulated using BPSK at ½ coding rate and offers 7.2 Mb/s in 20 MHz or 15 Mb/s in 40 MHz on a 400 ns guard interval.

The mobile phone located somewhere near or on you is usually a single spatial stream or 1x1 capable device and typically supports 802.11n or 802.11ac in 20 MHz channels.

At the high end of 802.11n, MCS 31 employs four simultaneous spatial streams, at 64-QAM, 5/6 coding rate, offering 289 Mb/s in 20 MHz and 600 Mb/s in 40 MHz on a 400 ns guard interval.

The 802.11ac standard further enhanced MCS operations by introducing very high throughput (VHT) multiple modulation profiles with the potential to support up to eight simultaneous encoded streams. It specifies wider RF bandwidths up to 160 MHz, more MIMO spatial streams up to eight, downlink multi-user MIMO up to four clients, enabling use of nulls in airtime to establish up to streams, each to a 1x1 client device, and high-density modulation up to 256-QAM. A full list of MCS values for 802.11ac may be viewed at http://www.mcsindex.com.

802.11n			Data Rate (MHz)								802.11ac
HT	Spatial	Modulation & Coding	Data Rate	Data Rate	Data Rate	Data Rate	Data Rate	Data Rate	Data Rate	Data Rate	VHT
MCS	Streams		GI = 800 ns	SGI = 400 ns	GI = 800 ns	SGI = 400 ns	GI = 800 ns	SGI = 400 ns	GI = 800 ns	SGI = 400 ns	MCS
Index			20 MHz	20 MHz	40 MHz	40 MHz	80 MHz	80 MHz	160 MHz	160 MHz	Index
0	1	BPSK 1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	0
1	1	QPSK 1/2	13	14.4	27	30	58.5	65	117	130	1
2	1	QPSK 3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	2
3	1	16-QAM 1/2	26		54	60	117	130	234	260	3
4	1	16-QAM 3/4	39	43.3	81	90	175.5	195	351	390	4
5	1	64-QAM 2/3	52	57.8	108	120	234	260	468	520	5
6	1	64-QAM 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	6
7	1	64-QAM 5/6	65	72.2	135	150	292.5	325	585	650	7
n/a	1	256-QAM 3/4	78	86.7	162	180	351	390	702	780	8
n/a	1	256-QAM 5/6	n/a	n/a	180	200	390	433.3	780	866.7	9
8	2	BPSK 1/2	13	14.4	27	30	58.5	65	117	130	0
9	2	QPSK 1/2	26	28.9	54	60	117	130	234	260	1
10	2	QPSK 3/4	39	43.3	81	90	175.5	195	351	390	2
11	2	16-QAM 1/2	52	57.8	108	120	234	260	468	520	3
12	2	16-QAM 3/4	78	86.7	162	180	351	390	702	780	4
13	2	64-QAM 2/3	104	115.6	216	240	468	520	936	1040	5
14	2	64-QAM 3/4	117	130.3	243	270	526.5	585	1053	1170	6
15	2	64-QAM 5/6	130	144.4	270	300	585	650	1170	1300	7
n/a	2	256-QAM 3/4	156	173.3	324	360	702	780	1404	1560	8
n/a	2	256-QAM 5/6	n/a	n/a	360	400	780	866.7	1560	1733.3	9
16	3	BPSK 1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195	0
17	3	QPSK 1/2	39	43.3	81	90	175.5	195	351	390	1
18	3	QPSK 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	2
19	3	16-QAM 1/2	78	86.7	162	180	351	390	702	780	3
20	3	16-QAM 3/4	117	130	243	270	526.5	585	1053	1170	4
21	3	64-QAM 2/3	156	173.3	324	360	702	780	1404	1560	5
22	3	64-QAM 3/4	175.5	195	364.5	405	n/a	n/a	1579.5	1755	6
23	3	64-QAM 5/6	195	216.7	405	450	877.5	975	1755	1950	7
n/a	3	256-QAM 3/4	234	260	486	540	1053	1170	2106	2340	8
n/a	3	256-QAM 5/6	260	288.9	540	600	1170	1300	n/a	n/a	9
24	4	BPSK 1/2	26	28.9	54	60	117	130	234	260	0
25	4	QPSK 1/2	52	57.8	108	120	234	260	468	520	1
26	4	QPSK 3/4	78	86.7	162	180	351	390	702	780	2
27	4	16-QAM 1/2	104	115.6	216	240	468	520	936	1040	3
28	4	16-QAM 3/4	156	173.3	324	360	702	780	1404	1560	4
29	4	64-QAM 2/3	208	231.1	432	480	936	1040	1872	2080	5
30	4	64-QAM 3/4	234	260	486	540	1053	1170	2106	2340	6
31	4	64-QAM 5/6	260	288.9	540	600	1170	1300	2340	2600	7
n/a	4	256-QAM 3/4	312	346.7	648	720	1404	1560	2808	3120	8
n/a	4	256-QAM 5/6	n/a	n/a	720	800	1560	1733.3	3120	3466.7	9

Figure 2 - MCS Rates for 802.11n and 802.11ac (up to 4 of 8 spatial streams)

Receive sensitivity is the measurement of the receiver's ability to demodulate the transmission at a given level above the noise floor of the operating channel. The negotiated throughput from client to access point can be related to the receive signal strength indication (RSSI) value, which in part drives modulation coding scheme (MCS) selection.

The highest mutually supported MCS value is, generally speaking, the best throughput the access point and client can achieve. From the perspective of understanding conditions related to per-client Wi-Fi performance, the current RSSI and negotiated MCS are key performance indicators.

6.3. Wi-Fi Provisioning

Two examples of Wi-Fi provisioning used by the cable industry include TR-069 and Web Protocol Adapter or “WebPA.” More information about these two can be found at the following link:

https://en.wikipedia.org/wiki/TR-069

Wi-Fi Data collection and PNM is enabled through WFA's Data Elements https://www.wi-fi.org/discover-wi-fi/specifications

In-depth information about these (and other) provisioning methods is beyond the scope of this document.

6.4. Power Management

Coordinated power management of both the beacon and all wireless communication from an access point becomes a key building block to managing Wi-Fi experience when multiple uncoordinated home devices are offering Wi-Fi connectivity. Note the coordinated mesh systems (Wi-Fi EasyMesh™) self-manage these power issues.

The further a client is from its access point, the lower its overall bandwidth will be and beacon overreach issues start to happen.

As the distance increases, there is less signal energy to overcome the surrounding noise and interference in the channel. Further, because the power output of most modern clients is less than that of the access point, at a certain distance the access point will no longer be able to receive the transmissions back from the client.

Looking once again at the use of TR-069 or webPA and their current objects related to Wi-Fi Radio and SSID operations there are some useful parameters that can be set. In TR-069 Device Wi-Fi Radio {i} offers visibility to Operating Frequency Band, Channel, Operating Channel Bandwidth and may offer Wi-Fi Associated Device information including Downlink and Uplink data rate, Signal Strength and Retransmission.

This information is valuable as part of the back office in terms of historical knowledge and possibly snapshot reports that may assist in troubleshooting certain issues. Essentially, we can learn how much bandwidth at a given moment in time was available at the radio, a general sense if there were some quality concerns from retransmission values however we are unable to understand why the radio is operating at the bandwidth advertised.

6.5. 802.11ac

More and more subscribers are demanding improved connectivity from their wireless home network. Streaming video, voice over Wi-Fi, gaming, and other interactive applications are driving the need for more reliable wireless connectivity within the home/business. Broadband subscribers are more connected than ever, and their bandwidth requirements and number of connected devices continue to increase. In fact, the average user in the United States had 7.4 connected devices in 2014 and that number is projected to grow to 13.8 by 2019[2]. With the increased demand being placed on subscribers' Wi-Fi networks, broadband service providers and their subscribers are routinely installing 802.11ac devices to enhance wireless performance. 802.11ac, the fifth generation of Wi-Fi, was developed to provide faster and more scalable wireless networks, with performance commensurate with wired gigabit Ethernet networks. This section highlights some of the advantages of 802.11ac technology, describe how 802.11ac differs from other 802.11 technologies, and identifies potential issues that may be experienced by technicians deploying 802.11ac devices in the subscriber's home/business.

[2] Cisco, (2015) *VNI Global IP Traffic Forecast, 2014 – 2019 www.cisco.com/c/en/us/solutions/service=provider/visual-networking-index-vni/index.html*

6.6. Field Performance Observations

Since 802.11ac is backwards compatible with legacy 802.11a/n 5 GHz bands, those clients will still be able to connect to APs that have been migrated to 802.11ac. Unlike 802.11n, 802.11ac operates using only the 5 GHz band. This being the case, 5GHz coverage area typically is reduced since the 2.4 GHz band coverage that 802.11n users are accustomed to, has better range and propagation than the 5 GHz band. Dual-band clients also operate at 802.11n using the 2.4 GHz band.

Another potential issue subscribers can face with 802.11ac is limited client support. Most laptops, tablets, and smartphones released prior to 2014 do not support 802.11ac and while many device vendors began deploying devices with 802.11ac support in 2014, there are still many devices being offered to consumers that do not support the technology.

Post-installation testing should be completed to ensure coverage is adequate and to verify appropriate speed and throughput are achieved on the wireless network. Technicians ability to test 802.11ac may be limited if their existing devices do not support 802.11ac technology and in many case technicians will need to be re-tooled in order to properly support 802.11ac. Since 802.11ac cannot be deployed on existing 802.11n chipsets, technicians test equipment and tablets will likely need to be replaced to allow for proper testing and support of 802.11ac.

6.7. Common Home User Wi-Fi Issues

The following is a list of typical home Wi-Fi user issues, in no particular order.

1. Lost Wi-Fi password or reset password requests (security)
2. Configuration of SSID (network name)
3. Range / coverage issues (proper AP placement)
4. Login / access to gateway / router
5. Slow or low speeds (closely related to range issues)
6. Intermittent wireless connections
7. Cannot connect wirelessly - all clients
8. Cannot connect wirelessly - single client
9. Customer does not know how to set up a Wi-Fi network
10. Customer is not familiar with setting up a new Wi-Fi client device

These issues can generally be separated into a few larger buckets: customer education, customer care, Wi-Fi RF issues, and Wi-Fi congestion issues.

Customer education and customer care come up in Wi-Fi discussions because the cable subscriber is relatively uninformed about how the services actually work, and often parts of the setup experience are not optimal. These problems may require multiple steps to resolve. For example, education of the service provider's personnel is important so that they can determine the subscriber's issues and can explain to the subscriber how to resolve the issues. Technology can also address some of the issues. For example, a simple issue, such as a forgotten password, may be addressed with a web-based self-help portal for the subscriber.

Wi-Fi RF issues such as poor range or coverage can be more difficult to resolve since they may stem from decisions made during the initial installation of the Wi-Fi AP / gateway, or they may have been caused by changes that the subscriber has made within the environment since the initial Wi-Fi installation. Initial installation issues can often be addressed with customer facing training by service provider technical personnel. For subscriber self-installs, as well as troubleshooting later subscriber-driven changes, web-based self-help tools for consumers can help minimize the operational impacts of these issues. Such tools improve the quality of experience with services such as Wi-Fi and empower the subscriber to resolve

some of their own wireless related issues. Some range-based coverage issues may require the deployment of additional equipment to improve coverage. Examples of additional equipment include Multi-AP (EasyMesh) devices or extenders.

Finally, Wi-Fi congestion caused by other Wi-Fi subscribers, other unlicensed wireless equipment, and environmental noise sources contribute to the last major category of Wi-Fi issues. These issues can be difficult to address in a vacuum because they may be caused by elements that neither the operator nor the consumer can control. Further they can be intermittent or time-of-day dependent. For example a Wi-Fi network setup be a technician in the morning may work fine, but when neighbors return home in the evening and begin stream, congestion can dramatically increase. Good monitoring tools and troubleshooting training will help to identify congestion-related problems and ideally guide the subscriber into other Wi-Fi configurations that may provide better performance.

7. Wi-Fi Quality of Experience

7.1. Categories of Wi-Fi related Issues / Common Install Related Issues

7.1.1. Equipment Placement

Poor access point or gateway placement can cause many problems with respect to range and coverage within the premises. Access point location has a big impact on Wi-Fi performance in the home, and this must be considered during the installation. The range of AP transmission/reception is limited and can be hindered by obstructions in the signal path or by interference generating home appliances. Many decisions made by different customers or an installation technician can lead to a poorly-placed AP. An installation technician may simply place the AP in the easiest location to access an existing coax outlet. Subscriber's performing a "self-install" likewise may be reluctant to run additional coax, maybe at additional cost, to position the AP at a more optimal location at the premises. They may not even understand where the AP should be more optimally located. A subscriber may also find the AP device aesthetically unpleasing or not fitting in with their chosen decor, requesting that the hardware be placed "out of sight."

Hidden hardware will unlikely be in the optimum location because proximity to dense material, such as concrete block walls or dense hardwood furniture, can compromise propagation of the RF signal. Sometimes the height of AP may also result in coverage issues. A customer may want the GW/AP out of sight, perhaps on the floor behind the TV or in the utility cupboard.

To address these problems, a two pronged approach is recommended:

1. Educate the Customer on the realities of Wi-Fi. – Customers expect seamless Wi-Fi throughout the home, centralized AP placement is required. There are several apps and other tools available for testing and troubleshooting Wi-Fi installations, including signal strength and throughput.
2. Training is needed for installation technicians
    a. Perhaps even more important would be a tool that a technician can use to help explain why a given location is not necessarily the best location for optimum performance. If the tool can be built as an app for a smart phone, then a consumer doing a self-installation can also be encouraged to use the app.

If a consumer knows that a certain location is probably going to cause problems, they may be motivated to consider other locations. When Wi-Fi was a novelty, it was hard to convince a customer that a little trouble was worth it in improved performance. Now that Wi-Fi performance is valued by the customers and their families, it should be getting easier to demonstrate the improvements even small changes in AP location can make.

7.1.2. Wi-Fi Channel Assignment

Aside from the physical impediments faced by an AP due to its position within a residence, Wi-Fi performance may also be strongly influenced by the RF environment within the residence. The AP itself may see other APs, called overlapping BSSs (OBSS) in Wi-Fi speak, but just as significantly the clients connecting to that AP spread throughout the residence may also see interference from OBSSs.

The effects of Wi-Fi congestion are the result of access mechanisms within the Wi-Fi protocols. The lowest layers of Wi-Fi channel allocation protocols attempt to share the air fairly. A Wi-Fi device will listen before transmitting, and if a transmission fails, will back off before attempting another transmission. Another important feature is that of modulation and coding used and it depends on RSSI, SNR, and error stats, but the selection and adjustment is internal to the device. When transmissions of their Wi-Fi devices attempt to use the same RF channel, progressive back off events can limit the channel throughput substantially. If an OBSS from another Wi-Fi network is at a low level, the attempted transmissions may still take place, but due to the reduced SNR (other network transmissions are seen as noise), data throughput will be lower when the OBSS is active.

Uneducated users and technicians often mistake the channel bandwidths of 2.4 GHz Wi-Fi as non-overlapping. Bad channel configuration choices can affect other Wi-Fi networks nearby. In the 2.4 GHz band, only channels 1, 6 and 11 are non-overlapping in North America. In the EU, channel 12 or 13 may also be available. A person who assigns their AP to channel 3 in the mistaken hope of avoiding his neighbors on the other channels will actually interfere with users on both channels 1 and 6 (and vice-versa). Sometimes, a customer may be able to ask for a little cooperation with their neighbors to only use channels 1, 6, & 11 and to optimize the settings of those channels between neighbors - a little explanation may go a long way if everyone can understand that distributing channel assignments benefits everyone.

While these points apply most directly to the 2.4 GHz band, the increasing usage of 802.11ac devices in the 5 GHz band will also cause congestion and overlap issues to crop up. It’s important for consumers to realize that if they fix their 5 GHz channel bandwidth at 80 MHz, for example, that another user may overlap by 20 MHz or 40 MHz and reduce their 80 MHz throughput substantially. Some access points will automatically shift their bandwidth usage to whatever is available, while others will treat any signal as a reason to back off and try again later. Good auto-channel selection is desirable. Also, APs that support DFS (dynamic frequency selection) channels are desirable. Otherwise, if APs don’t support DFS channels, there is a very limited number of channels left for them to operate on (only channels 42 and 155 in North America, for 80 MHz), so, there is a higher chance there will be co-channel OBSS that interferes with each other.

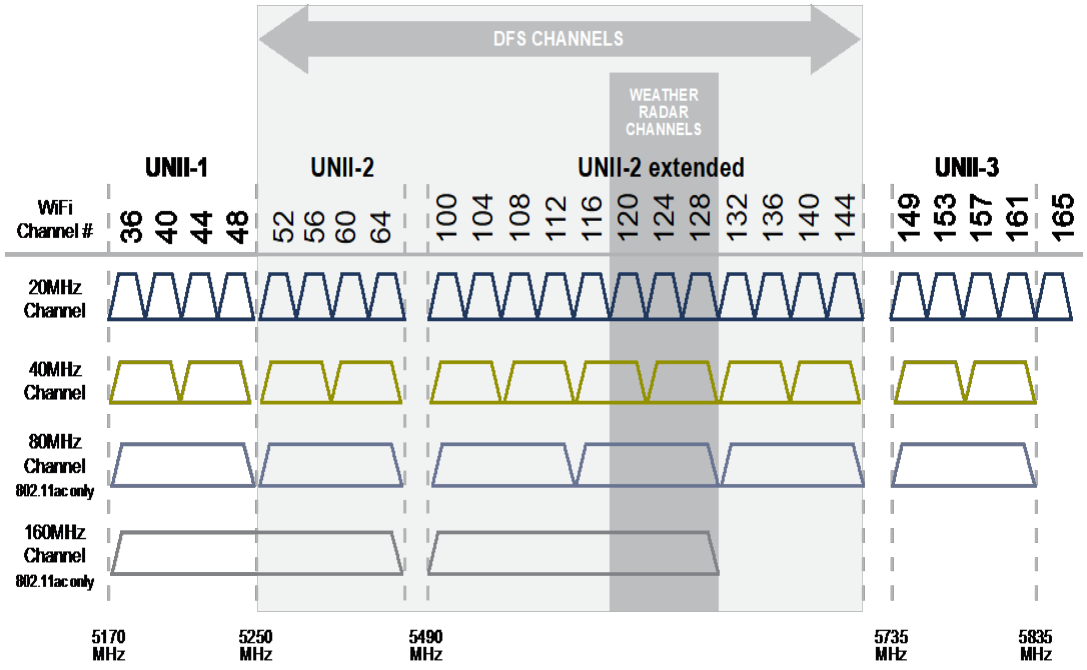

Figure 3 -5 GHz Channel Bands

As more devices are deployed with 5 GHz, we may learn more lessons about the best deployment methods for channel width selection and automatic channel adjustments.

7.2. User Experience View

Broadband providers' current marketing Wi-Fi often make claims like "our most powerful Wi-Fi yet" suggesting that performance will be better than before in the furthest corners of the subscriber's home. Subscribers often have no technical understanding of Wi-Fi and expect the maximum advertised throughputs at maximum advertised range. Most consumers never understand the range versus speed tradeoff for wireless - why should they be expected to understand the same for Wi-Fi? Subscribers increasingly have more untethered devices in their homes and may not have updated their broadband service for many years or may have older access point or gateway hardware that may not even support sufficient depth of Internet address handling.

In 2015, it was common for typical homes to have at least seven wireless devices and four wired. It is expected for the number of wireless devices to double or triple due to IoT devices. IP addressing in the home that cannot reliably handle over 120 devices will be obsolete shortly.

7.3. Two types of service provision deployment

As mentioned earlier, two main types of service provision deployment are common for Wi-Fi.

7.3.1. Provider managed install

With this approach, there has largely been a feedback directly to the provider when wireless problems occur resulting in fault reports and additional costs for the provider to rectify these as best they can. The provider may (eventually) send out a "super-tech" to go and analyze the problem and attempt to optimize the installation using "free" and off-the-shelf tools such as mobile phone signal strength apps. Alternately,

the provider may simply offer Wi-Fi extenders that in their simplest form just reduce overall throughput to half by occupying at least twice as many timeslots for each transmission.

Some providers may choose to offer secondary access points perhaps connected via MoCA or "powerline" (e.g., HomePlug AV2) communication to the master gateway. These have the advantage of offering additional bandwidth without compromising the original access point, provided a second non-overlapping channel is available. Also, the technician may need a little knowledge to correctly position and configure these devices.

In 2018. Providers began to aggressively install mesh Wi-Fi systems with multiple coordinated access points. This was bolstered by the availability of Wi-Fi Alliance's EasyMesh standard and certification for Multi-AP.

7.3.2. Consumer Self-install

To avoid the need for the service provider to visit to the end-user's home, equipment such as set-tops, cable modems, and Wi-Fi APs can be sent by mail for the end user to install and configure or made available for sale (or pickup) at retail kiosks. In particular, the default configuration or capability of the in-home wireless equipment may not always be optimum, though algorithms in the equipment's firmware do attempt to analyze the area and choose the optimum channel. Basic instructions for optimum placement are included but often a lot of trial and error is needed to improve this. The "obvious" location near the center of the home is not always best for many reasons. The end-user may be reluctant or unable to run additional cabling from the network termination point to a more optimum location for the AP.

Cable operators should consider providing more comprehensive instructions with recommendations for optimal AP placement and other setup issues. Alternatively a provider can recommend a mesh or EasyMesh system. The following guidelines can be used by subscribers for self-installs as well as by cable company installers and technicians.

For best Wi-Fi coverage, try to place the wireless gateway or AP close to where Wi-Fi capable devices are or will be most frequently used. For best Wi-Fi reception and minimal interference, the wireless gateway/AP should be located in an open area away from exterior walls, metal surfaces, microwave ovens and windows (do not place it inside of a cupboard, closet, file cabinet, or other enclosed area). Once the wireless gateway is in the best location in the home, it's time to plug it in and power it up.

Note: If you are replacing a modem currently connected in the home, be sure to unplug that device from the cable or coaxial outlet and plug the new wireless gateway/AP (often built in to the new modem) into that same coaxial outlet. If you do not have an existing modem set up, simply plug the new modem into the main cable or coaxial outlet in the home.

The wireless gateway or wireless router makes it easy to set up the Wi-Fi network and adjust its settings. Once you set up the network, you can wirelessly access the Internet and other services from your computer, laptop, game system and more. You can find out how to set up a wireless network with these simple steps.

Before you can access your provider's services or the Internet through your wireless gateway, you'll need to make sure it's properly connected. Please check that:

Your wireless gateway is connected to the Internet through the cable connector on the back panel with a coaxial cable (labeled "F" in Figure 4)

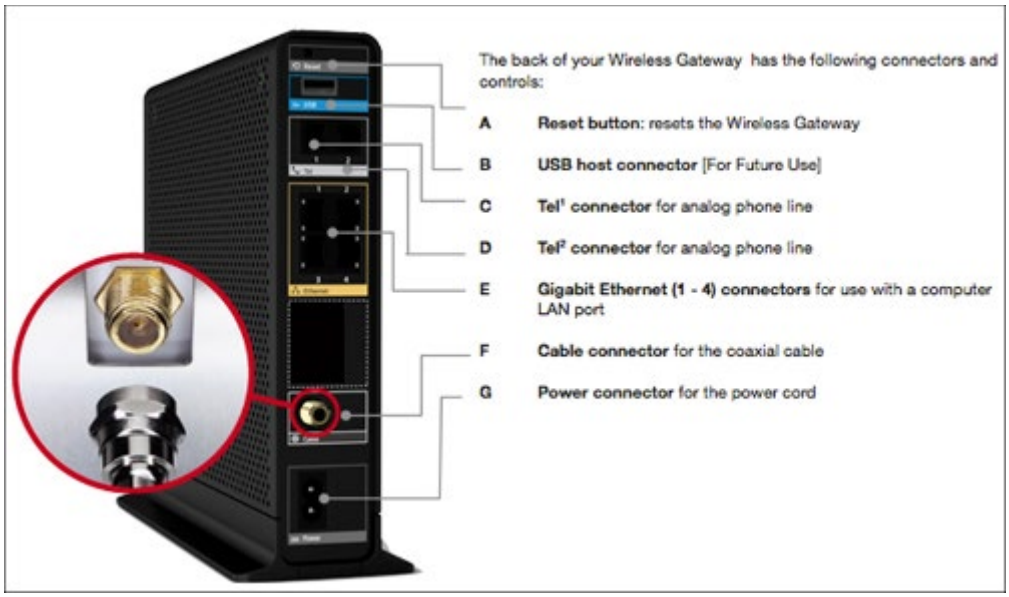

Figure 4 -Wireless gateway connections and controls

Wireless gateway back panel features are:

- Reset button for resetting the wireless gateway
- USB host connector [for future use]
- Tel1 connector for analog phone line
- Tel2 connector for analog phone line
- Gigabit Ethernet (1-4) connectors for use with a computer LAN port
- Cable connector for the coaxial cable
- Power connector for the power cord

Check your specific make and model regarding light indicators, etc., which may be different than what is shown in Figure 4 and Figure 5. Ensure the following: the wireless gateway is plugged in to a power source through the power connector with the provided power cord. The power, US/DS, and online LED indicators on the front panel are steadily lit. This may take several minutes after plugging in your wireless gateway.

Figure 5 - Front view of wireless gateway

7.3.3. Activating Your Wireless Gateway

Now you are ready to activate your cable company's services and your wireless gateway. Generic activation information is provided below and specific activation information may be available from the cable company's web site (refer to the gateway's printed instructions).

Once you have installed your wireless gateway/AP and established a temporary Internet connection, you are ready to activate your Internet/voice service.

Once connected, if you're not automatically presented with an Activation Welcome screen:

1. Open a web browser (such as Chrome, Safari, Internet Explorer, etc.) on your device and go to {provider site}. Next, click Continue.
2. Enter your account number and phone number (if you received a self-installation kit, the account number can be found on the activation information card inside the kit.). You can also authenticate your account by signing in with your service provider username. If you've already created a username, skip steps 3 through.
3. Create a username and password. If you have moved and are transferring your service(s) to a new address, click "Sign-in" with your existing username.
4. Choose a security question and answer (answer must be 3-25 characters long and is case-sensitive) and check the box that you agree to the Terms and Privacy Policy, then click "Continue".
   - Note: Your username provides access to your account settings and services. It will also become your email address prefix, similar to [Username]@{service provider.net. Feel free to use it as your

primary email account or as a spare. It is recommended that you print or write down this important information.

5. Click "Continue" to proceed from the Connection Established screen.
6. After you receive the "Device Activated" screen, your gateway may reboot. It should be all set when the power, US/DS and online lights on the front of the gateway stop blinking and remain solid for one minute, and the Wi-Fi light(s) start flashing.

Notes:

- You can continue to use the default Wi-Fi network name and password on your device, but it is highly recommended that you change your Wi-Fi network name and password to something easy for you to remember.
- Depending on the type of gateway you have, you may be required to create a new Wi-Fi network name and password as part of the activation process.

7.4. Qualifying CPE

For maximum trust any test solution must be capable of testing via the existing or newly installed gateway device. Showing the technician's equipment working at extreme far range is all well and good, but customers want assurance that their own equipment will work, maybe not as quickly (see below), and that they will have coverage in the home where they need it.

Some providers are now suggesting that their set top boxes for high and ultra-high definition video streaming can be connected wirelessly, reducing the need for additional cabling at the time of installation or encouraging a self-install. If the initial installation attempt does not work, what visibility is there from the customer's perspective or from the provider's perspective as to what to try next? Troubleshooting steps are provided elsewhere in this document.

7.5. Customer Education

Customers often expect the hardware they bought many years ago, perhaps only offering 802.11b capability, to keep on working or even to be improved in performance by updating their gateway/AP. While older equipment will generally still work, they do not understand that operating older equipment will inevitably occupy more timeslots that could carry much higher data rates using more modern modulation profiles and expanded channel widths. Education that older hardware really does need replacing is important.

8. Installation, Configuration and Management

8.1. Common Residential / Commercial Deployment Models

- Wi-Fi Gateway
- Wi-Fi Gateway with EasyMesh Controller and multiple EasyMesh Agents (APs)
- Wi-Fi Gateway with Repeater/Extender
- Wi-Fi Gateway with Secondary Device (Dual AP)
- Wi-Fi Gateway and Wi-Fi Peripheral
- Wi-Fi Gateway and Managed Broadband Router
- Wi-Fi Gateway and Wi-Fi Video AP
- Wi-Fi Gateway and outdoor (OD) Wi-Fi Gateway
- Community Wi-Fi Gateway

8.2. Example Wi-Fi Home

The average North American home will have almost a dozen Wi-Fi client devices active today. Many industry disruptions such as Internet of Things (IoT) will drive per subscriber Wi-Fi device counts much higher, with some predicting this device count is set to double in just three years.

There are also many different and often simultaneous use cases for Wi-Fi service occurring in the typical home. Telework VPN and VoIP traffic, Over-The-Top IP Video, Gaming, home automation and security, and general web surfing may all be actively competing for radio airtime.

The placement of these clients varies and is usually not fixed with perhaps the exception of home automation and security and perhaps gaming consoles. This poses a real challenge as we consider today's Wi-Fi deployment models beginning with Wi-Fi enabled DOCSIS Gateways.

8.3. Wi-Fi Deployment Models - Gateway Deployment Model (Single AP)

A common scenario in many deployments is the use of a DOCSIS 3.0 or 3.1 cable modem gateway with embedded Wi-Fi access point. The install technician likely locates the gateway near the utility panel or closest to drop entry point to avoid in home coax runs and splitters. There are several disadvantages to this approach depending on the device and the circumstances of the customer premise.

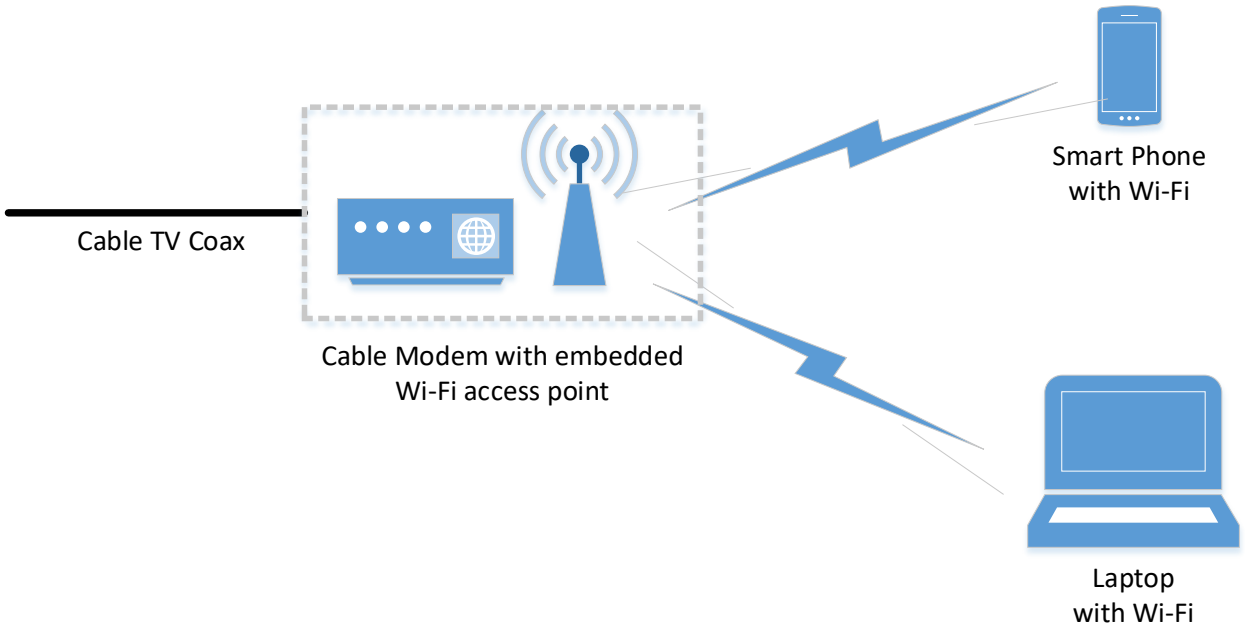

Figure 6 - Single AP Model

Beyond the DOCSIS side functions of the gateway itself, there are often several variations between vendors in the offered features and functions for the Wi-Fi access point. The radio itself may implement 802.11 g/n or ac functionality.

These may be in the form of single band 2.4 GHz or dual-band 2.4 GHz and 5 GHz or dual-band concurrent 2.4 GHz – 5 GHz simultaneous radio operation.

The number of simultaneous transmit and receive functions commonly vary from 2x2 to 3x3 in 802.11n mode with MIMO (Multiple Input Multiple Output) processing on each spatial stream. Depending on

manufacturer, the transmit power of the gateway access point may range for example from 20dBm to 26dBm.

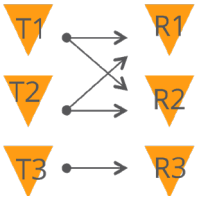

Figure 7 - 3x3 MIMO

Customers often expect to have more than one logical Wi-Fi network or SSID to use. Often customers are seeking a secondary SSID for Guests or to apply different security for kids' devices from that of the parents' devices.

Operators often have an SSID for use by local technician or possibly as part of an overall public HotSpot service model.

When the DOCSIS cable modem gateway is a Dual Band Concurrent (DBC) device, the logical Wi-Fi SSID configuration follows to both the 2.4 GHz and 5 GHz radios.

Dual band concurrency has become popular as the overcrowding in the 2.4 GHz ISM band is at an all-time high and the need to avoid spurious noise in that region such as microwave oven and Bluetooth devices.

8.4. Wi-Fi Deployment Models - Gateway + Secondary Device (Dual AP)

To address coverage issues commonly found in single-family homes or encountered in high noise environments, a secondary access point can be deployed within the customer premise. The secondary access point is usually back hauled from the DOCSIS Gateway over MoCA, PowerLine, or other in premise physical layer options.

The main drawback to Dual AP model when deployed by the cable operator is the need to manage radio resources effectively. The DOCSIS Gateway access point may have a -24 dBm transmit power. The secondary access point may also be equally as powerful. It is expected that the access points themselves should use their own auto-channel selection algorithm to tune to the best channel possible. However, there is no relationship between the Gateway access point, and the secondary access point from a radio resource management perspective or relation to client devices in the subscriber premise.

If the DOCSIS Gateway was to choose 2.4 GHz Ch1 operation, and the secondary access point chose 2.4 GHz Ch6, there will be significant side channel energy between Ch1 and Ch6. This side channel or roll off energy becomes additive noise from each access point's perspective. While these are non-overlapping channels in terms of center frequency, there is energy present from Ch1 into Ch2 and Ch3 in decrements of ½ of transmit power per side channel. The second access point in Ch6 center frequency may hear noise from the portions of Ch2 and Ch3 its receiver might sense. Thus, it is advantageous to configure the channels on the APs to be as far apart as practical.

8.5. Mesh / EasyMesh / Multi-AP

The growth in connected devices and streaming services that rely on Wi-Fi connectivity in the home has resulted in the need for smarter Wi-Fi networks that provide extended, uniform coverage. Service providers need to be able to deploy full coverage networks that intelligently manage resources with minimal user intervention and to be highly scalable, enabling users to easily add wireless APs where needed.

Since 2017, proprietary mesh products have become available and in 2018 standardized EasyMesh products have become available for service provider deployment. Wi-Fi CERTIFIED EasyMesh™ brings a standards-based approach to Wi-Fi networks that utilize multiple access points (APs), combining the benefits of easy to use, self-adapting Wi-Fi with greater flexibility in device choice that comes with interoperable Wi-Fi CERTIFIED™ devices. Wi-Fi EasyMesh™ networks employ multiple access points that work together to form a unified network that provides smart, efficient Wi-Fi throughout the home and outdoor spaces.

Wi-Fi EasyMesh is very simple to install and use. Network setup and device onboarding involves minimal user intervention. Once established, the network self-monitors to ensure optimized performance. Leveraging mechanisms from Wi-Fi CERTIFIED Agile Multiband™, Wi-Fi EasyMesh can guide devices to the AP providing the best service for that device. Wi-Fi EasyMesh networks can also modify the network's structure based on changing conditions to provide a consistent experience.

Wi-Fi EasyMesh brings these capabilities to home and office Wi-Fi networks:

- Flexible design: Allows for best placement of multiple APs providing extended coverage
- Easy setup: Delivers automatic device onboarding and configuration
- Network intelligence: Self-organizing and self-optimizing network collects information and responds to network conditions to maximize performance
- Effective load balancing: Guides devices to roam to the best connection and avoid interference
- Scalability: Enables addition of Wi-Fi EasyMesh APs from multiple vendors

8.6. Community Wi-Fi

Another growing type of Wi-Fi service that deserves mention because it has some unique issues: Hotspot or Community Wi-Fi service. In this case an MSO is providing Internet access services over Wi-Fi facilities that may be shared within a home user (e.g. Community Wi-Fi) or may be provided by a public Wi-Fi access point (Hotspot).

9. Assesment and Installation Process

9.1. Five Step Installation Process

The following five-step process can be used as a reference for a comprehensive and repeatable Wi-Fi home deployment procedure:

1. Assess
2. Install
3. Site Survey
4. Adjust and Retest
5. Record, Store and Report

9.1.1. Assess

The first step in the installation process is to assess the customer's residence. Technicians should be trained on the assessment process. The assessment process encompasses identifying the type of house (building materials, possible sources of interference) and layout, as well as a questionnaire on how Wi-Fi will be used (how many devices, usage pattern, number of simultaneous users, IoT). The assessment process will guide the best placement and configuration for the Wi-Fi Gateway/Access Point.

It is recommended to provide technicians with a survey questionnaire listing the questions for site assessment.

- Where is the cable feed?
    - The purpose is to determine the location of the Cable Modem and whether it is an appropriate location for the Wi-Fi Gateway. Very often when the Cable Modem and Wi-Fi Gateway are included in the same device, leaving no choice to the technician for device placement without running additional coax.
- What kind of home construction?
    - The purpose is to determine the type of building material and the corresponding Wi-Fi signal attenuation, as well as the possible sources of RF Signal obstruction. Refer to section 10.2.2 for a list of common building materials and attenuation.
- What is the layout?
    - The purpose is to determine whether a single or multiple levels need to be covered and the distance to the furthest point that need to be covered by the Wi-Fi signal. For example, does the customer expect Wi-Fi coverage on their patio? This information will have to be taken into account during the site survey. Refer to section 10.1 for site survey information.
- How close are other houses/tenants?
    - The purpose is to determine the potential sources of Wi-Fi interference. Refer to section 10.2.1 for definition of Wi-Fi interference.
- What are the possible sources of non-Wi-Fi interference?
    - The purpose is to determine the possible sources of non-Wi-Fi interference and their impact on the Wi-Fi signal. Refer to section 10.2.3 for the list of common sources of non-Wi-Fi interference

The following questions should guide the technician's assessment of customer's usage pattern:

- What kind of application(s) will be used?

    - The purpose is to determine the throughput needs for each application. Refer to section 9.2 for typical bandwidth usage of common applications
- What are the rooms where these applications will be used?
    - The purpose is to determine the rooms where to most throughput usage will be needed, these rooms will need to be covered during the site survey. Refer to section 10.1 for site survey information.
- How many devices and what kind?
    - Determine how many Wi-Fi devices are used around the subscriber's home and if they are used simultaneously, this will help determine the throughput needs to be addressed during the site survey.
      It is also important to note if the client devices used by the customer are of older generation and therefore educate the customer about Wi-Fi system capacity throughput limitations of older generation devices. Refer to section 6.2 for customer education information.
- Are home automation, security cameras or IoT devices used?
    - The purpose is to determine if home automation, security cameras or IoT Wi-Fi devices are used around the house. While typical IoT device throughput needs may be fairly low, the devices are often located at boundary locations around the house. Similarly, security cameras may be several Mbps and often still at boundary locations. These locations will need to be surveyed for coverage during the site survey. Refer to section 10.1 for site survey information.

9.1.2. Install

For Wi-Fi gateway installation process refer to sections 7.3.1 and 9.3.

9.1.3. Site Survey

For site survey information refer to section 10.1.

9.1.4. Adjust and Retest

If the site survey uncovers throughput or latency performance issues, the technician should make any needed changes or adjustments, such as switching to a less congested Wi-Fi channel or moving the Wi-Fi gateway to a better location, then repeat the site survey step to ensure that the changes were effective. (See section 10.3.2 for methods of congestion evaluation including time of day effects.) Technicians should educate customers that Wi-Fi operating conditions may change based on a variety of factors after the finalized site survey.

For information about remedial steps to be taken to improve Wi-Fi performance refer to section 10.3.

This step can be omitted if the site survey is successful on the first attempt.

9.1.5. Record, Store and Report

With all the rooms and locations now passing the site survey, the technician should get the customer's approval and finalize the installation.

The customer immediately could receive an email with a Wi-Fi 'Birth Certificate', documenting the test results in each room and location.

The test results of each Wi-Fi site survey should be recorded for future reference in case of revisits and made available for call center operators in case of incoming support calls.

9.2. Typical Throughput Usage for Common Applications

For the purpose of capacity planning, the following guidelines can be used to determine the throughput requirements for the home being surveyed, these values could be used as thresholds to determine the pass/fail criteria during an active site survey (see section 10.1.4).

These guidelines can be used to compute the average throughput requirements for the home by evaluating the number of simultaneous applications in use and the number of Wi-Fi enabled devices in the home:

Application Type	**Typical Application Throughput in Mbps**
Standard Definition (SD) Video Call	0.6 to 0.7
High Definition (HD) Video Call	2 to 3
Video Conference	1 to 5
Audio Streaming	< 1
Standard Definition (SD)Video Streaming	2 to 3
High Definition (HD) Video Streaming	5 to 8
4K Video Streaming	25

An alternative approach to capacity planning is to simplify the evaluation is by choosing conservatively high numbers based on a simple rubric such as the number of occupants or size of the home. For example:

- Two Wi-Fi video devices per occupant
- Five Wi-Fi IoT devices per occupant

To adequately model the video device consumption, a 4K HEVC stream consuming 30 Mb/s is assumed. The number of IoT devices is important as well since a single AP can often become overloaded, driving up latency times, if more than 30 or 35 devices are connected to it.

The Wi-Fi Certified Home Design program simplifies the evaluation by choosing conservatively high numbers based on the size of the home. For example:

- One Wi-Fi device (including IoT devices) per 50~100 square feet
- One Wi-Fi video device per 300~500 square feet

Since sharing of the Wi-Fi channels with neighbors is unavoidable, the capacity numbers should be doubled to account for the overlapping BSSs (OBSS)

Simplifying the numbers, the simplistic capacity calculation can be met by dividing the square footage by 5, expressed in Mbps. This capacity number needs to be met at all locations in the home and adjacent areas such as patio, garages, and backyards

9.3. In Home Wi-Fi - Best Practices

The following guidelines can be used to determine the Wi-Fi gateway/AP placements and configurations:

1. Whenever possible, place AP in a central location of the Wi-Fi devices.
    a. The AP placement guiding principle should be to place it where Wi-Fi coverage is needed most for mobile devices use i.e. laptops, tablets, and smartphones.
    b. Hardwire stationary streaming devices, that are bandwidth intensive (Smart TVs, streaming video players, gaming stations, etc.) should have their own AP. This will allow you to free up Wi-Fi channel capacity to connect more mobile Wi-Fi devices. This will also improve Wi-Fi performance.
2. Never Use 40 MHz channel bonding on 2.4 GHz. Wi-Fi uses shared spectrum and there are only three non-overlapping channels available in 2.4 GHz. Wi-Fi uses “Listen Before Talk” protocol. Usually devices with signal level above -85 dBm are heard. Bonding channels can result in unnecessary packet collisions, retries and poor Wi-Fi performance for devices operating in these channels. If Channels must be bonded for higher throughput, consider using 5 GHz channels
3. Use 5 GHz channels when possible. The 5 GHz frequency band has many more channels available (UNII-1 and UNII-3) than 2.4 GHz channels. Educate customer to purchase dual band devices that support 5 GHz band and configure them to prefer using 5 GHz.
4. Always set max Tx power on the 5 GHz radio. Run Wi-Fi speed tests at different areas of the house and verify coverage. Run speed tests using a suitable application on a smart phone or embedded in field test equipment.
5. If co-channel interference is a concern, for example in MDUs, consider lowering Tx power. Verify coverage by running speed tests in different areas of the house to be certain that there are no coverage holes.
6. Configure the fewest number of SSIDs per frequency band on the access point. Every SSID defined on a channel generates beacons every 10^{th} of a second. This results in saturated airspace and high channel utilization that causes poor Wi-Fi performance. Figure 15 illustrates the impact of cleaning up unused SSIDs

Figure 8 - SSIDs and Low Rates Consume Air Time

7. To extend Wi-Fi signal coverage in areas consider using MoCA, wireless extenders or wireless mesh (e.g. EasyMesh) solutions.
8. Recommendations to Mitigate Wi-Fi and ZigBee interference in ISM

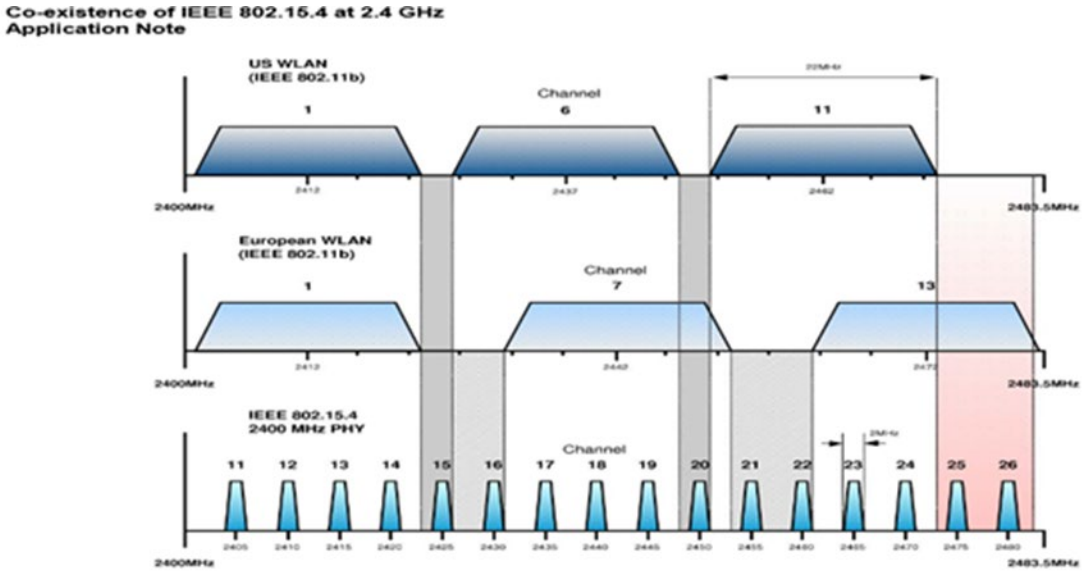

Figure 9 - LR-WPAN vs Non-Overlapping WLAN Channel Allocations

1. **Switch ZigBee to channel 25**
    a. Will fix interference from Wi-Fi in almost all scenarios

2. **Switch 2.4 GHz to 20 MHz channel width**
    a. This can affect Wi-Fi throughput but shouldn't have a huge impact
    b. Most Client devices are designed to default to 20 MHz channel width
    c. Industry Best practices recommends ***NOT*** to use channel bonding in 2.4 GHz band

d. Use 5 GHz[1] for higher throughput devices.

3. **Watch out for Interference from other non-Wi-Fi devices in 2.4 or 5 GHz band**
   a. Baby monitors
   b. Analog Security Cameras
   c. Cordless phones
   d. Bluetooth devices etc.

4. **Increase the physical separation between the AP and ZigBee devices**
   a. Should lower the interference

5. **Adjust / Decrease (Tx) output power of 2.4 GHz radio**
   a. Will impact range of Wi-Fi Signal
   b. Can lower interference with other devices in ISM

10. Survey and Troubleshooting Tools

To assess Wi-Fi networks, technicians and IT professionals often utilize site-survey tools. There are a wide variety of site survey tools available on the market today to provide insight into the performance of such networks. In this section, we discuss the types of tools available and discuss their advantages and pitfalls as Wi-Fi networks continue to evolve to support more bands, users, and applications.

10.1. Site Survey

A Wi-Fi site survey tools is used to ensure the Wi-Fi signal's coverage and performance throughout the facility being surveyed.

There are three main types of site surveys: Passive, Active, and Predictive, site survey's results are often collected and displayed in the format of Wi-Fi coverage map, also called Heat Map.

10.1.1. Heat Map

During the site survey, the active or passive site survey software records a set of performance metrics. These measurements can be a recorded map, commonly called "Heat Map". The heat map records the Wi-Fi signal's coverage based on the signal level threshold (ex: -72 dBm). Site survey software often allows the user to upload a floorplan file for the site. The floorplan file needs to be calibrated to determine the scale. This can be done by a manual process whereby the user enters distances in meters or feet or automatically using a GPS.

When a floor plan of the site is not easily available, as it would often be the case for residential deployments, the site survey software can provide other means of recording location. For example, naming and storing the measurement points by the room being surveyed (e.g. Living Room, Dining Room) or providing a "blank canvas" map.

During the survey, the technician performs a site walkthrough, carrying the site survey equipment. The site survey equipment will either automatically record measurements at regular intervals or the technician will select when to make the measurement. The walkthrough path should be decided in agreement with

[1] 5 GHz has 23 non-overlapping channels compared to just 3 in 2.4 GHz. Channels can be bonded in 5 GHz with a much lower risk of interference.

the customer so that all the areas where the Wi-Fi signal will be used are covered during the walkthrough. Customers should be prompted about desired coverage in non-traditional locations such as bathrooms, garages, outdoors, etc. It may also be advisable to verify signal coverage in a room with its doors and windows closed to reflect the worst case scenario.

At the end of the survey, a heat map will be produced reflecting the walkthrough path and Wi-Fi coverage areas. The criteria selected to create the heat map will vary depending on the service provider's requirement. They can include a signal coverage map showing the received signal strength or Signal-to-Noise Ratio for a "passive" site survey or Upload+Download throughput rates for an "active" site survey. Heat Map survey software generally allows adjustment to the color coding to reflect the service provider's selected service acceptance thresholds.

10.1.2. Predictive Site Survey

A Predictive site survey uses a software program to pre-determine the quality of the Wi-Fi signal based on the site plan and algorithmic models of the behavior of the RF waves in the environment. The models include RF signal attenuation by building material type and RF signal propagation by Access Point/Antenna type and model.

Predictive site surveys are commonly used for large commercial deployments, but generally out of scope for existing home deployments. Wi-Fi Certified Home Design uses predictive site surveys for new home deployments. The next sections will focus on Passive and Active site surveys.

10.1.3. Passive Site Survey

In this configuration, devices such as tablets, smartphones, or PCs host software that can be used in mobile or static configurations to assess coverage and performance on a point-to-point basis. Oftentimes, this manifests in the user launching an app, executing a test, and then viewing the results. Some applications enable the user to walk around and take measurements such as RSSI over time and overlay this information on a floor plan. Both active and passive site survey include a site walkthrough, the purpose of these surveys is to determine if the placement and configuration of the Access Point or Access Points provide the required level of coverage. In a passive site survey, the test device passively listens to the Wi-Fi signal received and records a set of RF metrics during the site walkthrough. In a passive survey, the test device is not associated to the access point under test.

A passive site survey can be performed with a site survey application running on a PC/Tablet or phone or with a dedicated test equipment hardware or adapter.

The site passive site survey application "scans" the RF environment and provides metrics related to the quality of the signal received from one or multiple Access Points.

Depending on the passive site survey's software capability one or more of these metrics will be collected - the list below is representative of the metrics collected during a passive site survey:

- Signal Level in dBm – Indicates the received signal strength
- RSSI (Received Signal Strength Indicator) or Signal Quality – Vendor proprietary metric often on a scale from 0 to 100 or in dBm
- Noise Level in dBm – Indicates the background noise level
- SNR Level in dB – Indicates the Received Signal's to Noise Ratio

- RF Availability or Utilization – Indicates the % of time the RF channel is available or busy, often used to determine the RF channel congestion
- RF Spectrum Analysis – Detects sources of non-Wi-Fi Interference (requires Spectrum Analyzer hardware)
-

It is important to determine ahead of the survey, the criteria necessary for the survey to be successful. For example, the service provider may require a minimum Signal level or SNR to be measured in all the surveyed locations for the site survey to be considered successful. The threshold values and the type of metrics being collected may vary amongst service providers or SLA being provided and is therefore out of scope for this document.

It is important to survey both the 2.4 GHz and 5 GHz frequency bands, as the RF signal properties are not the same for the 2 Wi-Fi frequency bands.

A Non-Wi-Fi source of interference can degrade the signal quality. If interference from non-Wi-Fi device(s) is suspected, it is recommended to use a spectrum analyzer.

If the site survey is not successful refer to section 11.2 Common Sources of Performance Degradation.

10.1.4. Active Site Survey

In an active site survey, the test device is actively associated to the Access Point under test and acts like a Wi-Fi client. This survey most closely emulates the end user's service experience. In this configuration, Wi-Fi test sensor devices can be placed in a distributed fashion in multiple areas where Wi-Fi devices are expected to operate, for example a Family room where the TV will be streaming video or a Home office. During a test, the Wi-Fi test devices can be instructed to load the network in a variety of ways to emulate the expected traffic load. For Wi-Fi networks in particular, this method can more accurately approximate the expected environment because the sensor devices act as proxies for the actual devices in a fully operational network. Simultaneous loading of the network with the distributed sensors can reproduce real world conditions such as channel contention and traffic congestion, identifying not only potential RF coverage issues but capacity considerations on both the wireless network and the wired-side backhaul as well.

An active site survey can be performed with a site survey application running on a PC/Tablet or phone or perform performance testing like Ping test or Upload and Download speed tests.

Depending on the active site survey's software capability one or more of these metrics will be collected, the list below is representative of the metrics collected during an active site survey:

- Wi-Fi PHY Rates – Indicates the PHY rates at which the client device associates to the AP under test
- Packet Loss/ Packet Retransmission – Indicates the quality of the data transmission
- Upload and Download throughput rates (speed test)
- Jitter – Indicates the packet jitter experienced by the test data, some applications like voice are sensitive to jitter
- Latency – Indicates the latency experienced by the test data, some applications like voice and video are sensitive to latency

It is important to note, when testing Upload/Download speed tests to a remote server that the performance may be affected by the speed test server itself or its internet access, therefore it is not recommended to

perform performance tests to a public Internet based server, unless this server's access is controlled by the service provider. If the goal is to estimate the true network's Wi-Fi performance, it is advisable to keep the responder speed test device local to the network under test.

Just as in the case of the passive site survey, it is important to establish prior to the survey, the criteria necessary for the survey to be successful. For example, the service provider may require a minimum Upload and/or Download throughput rates to be achieved in all the surveyed locations for the survey to be successful. The threshold values and the type of metrics collected may vary amongst service providers or SLA being provided and is therefore out of scope for this document.

If the site survey is not successful refer to section 10.2 Common Sources of Performance Degradation.

10.2. Common Sources of Performance Degradation

10.2.1. Interferers: Adjacent and Co-channel

For Wi-Fi networks, interference is perhaps one of the most challenging problems encountered. When a Wi-Fi network is configured to operate on a particular channel or band, it often has to contend with other networks to access the same channel. Consider the case of a suburban neighborhood where all the houses purchase Internet service and deploy a Wi-Fi router. In the 2.4 GHz band, for example, there are three 20 MHz non-overlapping channels in the United States that can support Wi-Fi operation. While limitations on the transmit power of any device in the band inherently reduce the amount of interference possible, it is clear that for a particular house, its neighbors are likely to interfere on some level. Compounding this issue is the fact that each deployment often operates independently when choosing a particular channel to operate—when in reality, coordinated frequency planning in this case would benefit the entire neighborhood. Indeed, frequency planning is employed heavily in cellular networks to maximize capacity and increase spectral reuse. However, because the 2.4 GHz band is unlicensed, market forces are not driving to support coordinated frequency planning. Thus, we live with the chance that our neighbors' emissions will interfere with our own.

In the case of Wi-Fi- interference, we can encounter multiple cases where other devices that are not part of our network can interfere: these other devices can emit signals within our own channel directly, known as co-channel interference, or they can emit signals in adjacent or overlapping channels with our own known as adjacent channel interference.

The Distributed Coordination Function (DCF) of 802.11 requires that both physical and virtual carrier sensing are employed for all Wi-Fi-compliant devices, and this sensing will aid in reducing the probability of a collision between the emissions of otherwise co-interfering devices. However, there is a limit to this capability—for devices will choose to emit after a back off period and interframe spacing defined by 802.11. For co-channel interferers, devices can use the virtual carrier sensing function to determine the amount of time remaining for a particular frame emitted from a device before it ceases transmission and will adjust their timing for transmission to take this into account. However, for adjacent or overlapping channel interference the physical carrier sensing function may provide more value—unfortunately, it cannot determine for how long the incumbent energy is expected to remain in the air, so it is less efficient at sharing the medium compared to the virtual carrier sensing function.

Complicating matters is the fact that Wi-Fi networks often exhibit cyclical traffic patterns throughout the day, so congestion becomes a function of time as well. While vendor access points often utilize a variety of methods to detect congestion, because each AP operates independently (and sometimes with its own tools compared to another vendor) the optimization choices they make may or may not be useful to maximize performance.

10.2.2. Sources of RF Obstruction Loss

Building materials and home furnishings can cause attenuation of the Wi-Fi signal's RF strength. Depending on the type of material, the impact can be severe and cause a large attenuation of the signal's strength. In extreme cases, the RF signal can be completely blocked. Care should be taken to identify these sources of physical interference and place the Wi-Fi gateway/AP away from these physical interferers.

The following list can be used to identify the most common sources of physical interferers found in homes:

- Large kitchen appliances
- Aquariums
- Tile and Stone surfaces
- Metal Screens
- Large screen TV
- Steel or Security doors

The following table lists the common building materials and the associated impact on the RF Signal's strength:

Table 1 - Building Materials and the Associated Impact on the RF Signal

Material	2.4 GHz Frequency Band Signal Attenuation	5 GHz Frequency Band Signal Attenuation
Concrete 203 mm (8") Without rebar	35 dB	55 dB
Concrete 203 mm (8") with rebar 140mm On Center	31 dB	53 dB
Concrete 203 mm (8") with rebar 70 mm On Center	37 dB	56 dB
Masonry Block (concrete block) 203 mm (8")	11 dB	15 dB
Masonry Block (concrete block) 406 mm (16")	18 dB	27 dB
Masonry Block (concrete block) 609 mm (24")	30 dB	39 dB
Dry lumber 38 mm (1.5")	3.3 dB	4 dB
Dry lumber 76 mm (3")	4.7 dB	8 dB
Dry lumber 152 mm (6")	8.5 dB	20 dB
Brick 89 mm (1 brick)	5.5 dB	15 dB
Brick 178 mm (2 bricks)	7.5 dB	32 dB
Brick 267 mm (3 bricks)	10.5 dB	32 dB
Glass panels 6 mm (1/4")	1.4 dB	1 dB
Glass panels 13 mm (1/2")	3.4 dB	0 dB
Drywall 6 mm (1/4")	0.6 dB	0 dB
Drywall 13 mm (1/2")	0.6 dB	0 dB

Source: EMF Shielding by Building Material U.S. National Institute of Standards and Technology (NIST) and the University of the German Federal Armed Forces 2012 (updated 2017).

10.2.3. Sources of Non Wi-Fi Interference

When the FCC opened up the 2.4GHz RF spectrum for non-regulated use, Wi-Fi 802.11 standard equipment was not the only technology to adopt this frequency band. Numerous types of equipment also communicate on this frequency band without adhering to the 802.11 standard. A few very common examples are:

- Baby monitors
- Cordless phones
- Wireless cameras
- Wireless audio devices
- Bluetooth devices
- Security systems
- Microwave ovens
- Zigbee devices

All these devices constitute sources of non Wi-Fi interference. They emit frequencies in the 2.4GHz band either on a single static frequency (e.g. Zigbee), they are frequency hopping across the entire spectrum (e.g.Bluetooth) or continuously emitting across the entire spectrum (e.g. a microwave oven).

These interferers do not follow the 802.11 protocols rules, so interference can start while Wi-Fi devices are in the middle of a transmission and last for an unknown duration. When non-Wi-Fi interference occurs, the destination will receive the transmission with errors or will not receive the transmission at all and require retransmission. In some cases, it will attempt to continue operation in the presence of non-Wi-Fi interference by automatically switching to a lower data rate, which slows the use of wireless applications.

And in the worst case, if the interference source is strong and constant, the Wi-Fi devices will hold communications until the interfering signal goes completely away.

Technicians should pay close attention to sources of non-Wi-Fi interference, because they are often the most serious source of poor Wi-Fi performance.

In addition, phone or tablet based Wi-Fi Applications cannot detect sources of non-Wi-Fi interference unless they are fitted with a specialized spectrum analyzer, because these sources of non-Wi-Fi interference do not obey 802.11 protocol rules nor broadcast 802.11 messages.

10.3. Troubleshooting Methods

To comprehensively troubleshoot a network, it is desirable to employ a method that can identify which layer or layers of the protocol stack the problem is occurring first, and then provide deeper knowledge to direct the user to the correct resolution. Unfortunately for Wi-Fi networks, the number of variables is large, and as such the potential solution recommendation should be chosen quite carefully to maximize success.

For Wi-Fi networks, there are multiple causes for performance problems that occur at the different layers:

10.3.1. RF signal performance

Wi-Fi devices and access points are limited in their maximum transmission power and have limits to their associated receiver sensitivity. Propagation of radio waves through the wireless medium causes

attenuation. Devices often experience both small-scale and large-scale fading behavior, which can result not only in performance degradation as a function of distance, but also as a function of time. Furthermore, signal performance is impacted by noise and interference, of which interference can also exhibit a time-varying component. The best mitigation techniques involve AP placement or using multiple mesh APs.

10.3.2. Congestion

Wi-Fi devices on a single network must share the wireless medium to transmit and receive data. This sharing occurs by way of a protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Devices will sense the wireless medium for existing energy or Wi-Fi transmissions, and will use this information to reduce the probability of collisions. For networks with light loading and a small number of devices, this works well. However, when the network must share its channel with other networks or scale to increase the number of devices on its own, problems may arise, especially in periods where the traffic load increases. When traffic load increases, each device may be sending or receiving more packets-and these packets must still traverse the same wireless medium. Often interfering traffic has a time of day impact. A particular customer's deployment that works well in the morning in a particular room in a house may not perform so well after the neighbor kids get home from school.

Identifying the source of issues is a critical component of resolving congestion, and even then, the recommendations can be numerous. In the case of supporting more devices on a single network, sometimes it is desirable to deploy another access point with additional backhaul capacity-other times, it may be simply changing to a different channel that hosts less active co-channel devices. This is highly customer-specific and requires a thorough understanding of the cause and desired performance before a recommendation can be made.

On the issue of congestion, a powerful method for troubleshooting is to passively capture packets on the network. Packet capture can enable a rich set of data to provide performance metrics such as utilization, error rate, retransmissions, and efficiency. However, technician devices cannot often support packet capture due to several constraints: customer privacy, memory or storage limitations, and algorithm development required to support full-scope analysis. Still, there are some ways to indirectly measure these metrics, including counting cyclic redundancy check (CRC) errors incident at a measurement point, or keeping track of the number of retransmitted packets over the total number of packets transmitted for a particular client. Once again, in the case of a single-point measurement, this can be useful to identify issues, but in a multi-point client test, these measurements could be taken for the total number of sensors, which would result in a more comprehensive data set to provide deeper analysis across the entire deployment. Sometimes clients that are on the edge of a building may be impacted by network congestion resultant from other devices on other networks in adjacent buildings while clients that are in the middle of the building are only within range of their host AP and other clients on the same network.

10.3.3. Configuration

Residential gateways can often be configured in different ways to support Wi-Fi operation. One such example is the "mixed-mode" Wi-Fi configuration that is often a default on most gateways. In this case, mixed-mode enables the widest compatibility between older devices and the newest smartphones, but it can sometimes come at the expense of inefficiency. In the case of heavily-loaded networks, the performance hit to throughput can be in the tens of percent, as older devices take more time on the wireless channel to send the same amount of data compared to the newest devices. In this case, it may be reasonable to recommend that a customer deploy two APs simultaneously, one of which serves 802.11n -capable devices on a particular channel configuration, and another which serves older and slower 802.11b/g devices on another channel. In this case, the offloading of the different devices on different

channels could result in a significant performance increase to both. Of course, gateways or mesh systems must support this feature to be effective.

10.3.4. Placement

To troubleshoot these issues on a network, consider the two primary methods for site surveys—in the case of single-point testing, edge-of-coverage issues could be identified and potentially remedied. However, most single-point testing systems cannot simultaneously address edge-of-coverage issues for an entire building at once (unless there are multiple technicians walking around). Compounding the issue is the fact that the network loading during such tests may not represent the typical operation during customer use. In the case of multi-point testing, these issues could be identified at once and a suggestion on moving the AP or deploying an additional one could take these inputs together to provide a result that may be more accurate. However, it is important to note that the placement of the clients in a multi-point test matters—in the case of projecting edge-of-coverage performance, it is important to place the client in an area where marginal coverage has been observed, so the performance can be more fully characterized for analysis.

10.3.5. Tools Technician Domain

For Wi-Fi issues, field technicians rely on easy-to-use tools that give them actionable results quickly. These devices are necessarily portable, so they can be easily transported between field sites and deployed as needed. Technicians often utilize a combination of devices—these could include a tablet or PC with cellular data service that reaches back to the corporate network to access customer information, a variety of handheld test tools used to assess Wi-Fi performance at a single point, or a multi-client solution in a suitcase form factor that could be used to assess Wi-Fi performance in a distributed, simultaneous fashion. Refer to section10.1 Site Survey for a description of side survey methods and tools.

10.3.6. Tools Remote Customer Service Domain

Customer service agents are often the first responders during troubleshooting matters. For Wi-Fi issues, these agents may be able to access the customer's residential gateway and help address issues remotely. During the course of a service call, the agent may be able to reset the gateway, perform a limited series of tests to assess congestion from the gateway's point of view, or command the gateway to change to another channel, amongst other potential features. These features are often provider-specific, and different providers develop different sets of features to employ. However, many problems in the Wi-Fi domain cannot be solved by leveraging diagnostic tools from a gateway point of view—such as edge-of-coverage issues in a building. However, these tools can help guide technicians once they are deployed at the customer site.

10.3.7. Tools Self Care Domain

Some customers prefer to administer as much of their own Wi-Fi network as they can—and as such, providers often enable customers to set the parameters of their residential gateways to address this issue. For those customers who have technical knowledge of Wi-Fi and networking concepts, utilizing some diagnostic tools within the gateway's software may enable them to identify and remedy their own issues. Oftentimes, however, these tools require a working knowledge of network protocols and radio frequency concepts. Unfortunately, some customers may start adjusting parameters without full knowledge of what each parameter means, and this could result in further degradation of network performance.

Other tools available to customers include over-the-Internet speed tests, where the customer simply directs their web browser to a site that can test the connection. It is important to educate the customer about the limitations of these tests, as the performance of the speed tests to a remote server may be affected by the performance of the speed test server itself or its Internet access, this is why it is not

recommended to perform performance tests to a public Internet based server, unless this server's access is controlled by the carrier or embedded in the gateway.

Customers can also often access a variety of freeware applications through their smartphones, tablets, or PCs—and utilize these to diagnose their own issues. Such applications for Wi-Fi could include functionality that lists the number of SSIDs after a channel scan, or even provides a full-packet capture capability such as Wireshark. For customers in the "Expert" category of proficiency, these can yield great insights to improve performance, but the level of sophistication is oftentimes a huge barrier to entry.

11. Wi-Fi Trends

This section discusses new trends in Wi-Fi technology.

11.1. 802.11ax

Started in 2014, the IEEE 802.11ax standard is scheduled to be completed and Wi-Fi Certified program to launch in 2019, with expected PHY rates up to 10 Gbps and operation in the 2.4 GHz and 5 GHz frequency bands. The IEEE High Efficiency Wireless LAN working group's stated objective for the standard is to achieve improvement of spectrum efficiency to enhance the system throughput/area in high density scenarios of APs and/or STAs such as stadiums, shopping centers, or airports.

Unlike past Wi-Fi standards, 802.11ax is not only focusing on pure theoretical high speed, but also on providing enough capacity in environments with a high density of clients. This is intended to enhance the user's quality of experience, with the goal of providing an average throughput per user at least four times better than 802.11ac in dense environments.

802.11ax achieves these goals using the following technologies:

- 1024-QAM: Introduction of MCS 10 and 11 using 1024-QAM, providing respectively up to 1081 Mbps and 1201 Mbps per stream on a 160 MHz channel.
- OFDMA (orthogonal frequency-division multiple access): Used in 4G LTE and MoCA networks, OFDMA technology provides frequency-multiplexed access to multiple simultaneous users, by dividing the Wi-Fi frequency channels into smaller sub-channels and assigning them to multiple users.
- MU-MIMO: The multi-user MIMO technology first introduced in the 802.11ac standard is now mandatory in the 802.11ax standard. It allows the devices to beamform traffic to multiple concurrent users. The standard supports sending up to eight simultaneous MIMO transmissions. The standard also introduces uplink MU-MIMO which allows client devices to transmit concurrently to the AP in some conditions.

Some manufacturers have announced pre-standard 802.11ax chipset support and several other manufacturers are already including this technology in their consumer Wi-Fi access points or routers.

802.11ax is backwards compatible with 802.11 a/b/g/n/ac standards, supporting interoperability with older Wi-Fi clients, although they are not able to take full advantage of the benefits and features of the newer technology.

For the most up to date list of 802.11ax devices refer to the following web page:
https://wikidevi.com/wiki/List_of_802.11ax_Hardware.

The Wi-Fi Alliance has introduced a new designation for Wi-Fi products and networks that support 802.11ax Wi-Fi technology. This new generation will be named Wi-Fi 6, referring to the 6th generation

of Wi-Fi products. This generational naming is also extended to identify the previous Wi-Fi major generations:

Wi-Fi 5 to identify devices that support 802.11ac technology and Wi-Fi 4 to identify devices that support 802.11n technology.

The Wi-Fi Alliance is also introducing new logos and certification programs to reflect these changes.

For additional information refer to the Wi-Fi Alliance web site: https://www.wi-fi.org/

Appendix A – Wi-Fi Background Material

All the way back in 1980, the Institute of Electrical and Electronics Engineers (IEEE) founded the 802 standards group which specifies a family of local and metropolitan area networks. The approved use of 2.4 GHz ISM (Industrial Scientific and Medical) band frequencies dates back to the mid 1980's and early pre-802.11 uses of these channels were introduced in the early 1990's. From this early IEEE work the Ethernet standard in 802.3 was formed and eventually, the 802.11 working group defined what we commonly refer to as Wi-Fi today.

In 1999 the Wi-Fi Alliance was formed to establish 802.11 interoperability certifications.

The 802.11 standards contain an impressive collection of specifications. The 1997 initial definition of the specification enabled Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSS) radio modes.

One of the most commonly discussed issues in Wi-Fi as it pertains to Wi-Fi quality is channel crowding in the 2.4 GHz ISM band. Frequency Hopping Spread Spectrum (FHSS) with lofty 1MB/s to 2MB/s data rates were possible in the earliest days of 802.11. However, FHSS is only using a small portion of the spectrum at a time by varying the carrier as a method to mitigate noise. The enterprise network market were the early adopters of this technology and by the late 1990's was pushing for much higher bandwidth.

802.11 working group introduced higher coding rates in 1999 as part of 802.11b to the 2.4 GHz ISM band using Direct Sequence Spread Spectrum. Channel overlap now became a more significant topic. While DSSS was sampling more of the 22MHz channel offering 11 Mb/s, it was also spreading its energy across the entire channel width.

The 802.11 working group introduced 802.11a at the same time as 802.11b, which was the first consumer Wi-Fi radio standard to use the 5 GHz U-NII (Unlicensed National Information Infrastructure) channel space.

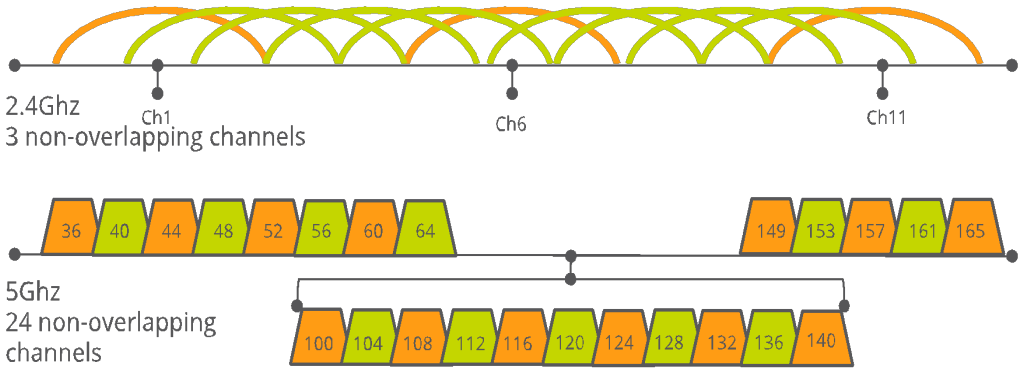

Figure 10 - North American Wi-Fi Channels 2.4 GHz 5 GHz

802.11a brought with it the use of OFDM (Orthogonal Frequency Division Multiplexing) which offers a much higher bit/Hz coding efficiency as well as increased immunity from Inter-Symbol-Interferers (ISI), enhancing immunity from reflection effects. 802.11a offered BPSK, QPSK, 16-QAM and 64-QAM modulations, which were achieved relative to client association. As attractive as 802.11a's 54Mb/s was at the time, its use was mainly found in the enterprise network space given cost associated with silicon at the time.

In 2003 the average consumer was finally introduced to the advantages of OFDM in the 2.4 GHz ISM band from 802.11g standard definition. This newest member of the 802.11 physical layer standards offered backward compatibility with 802.11b, and the opportunity to achieve 54Mb/s in 20 MHz channels. Supporting backward compatibility at the time was key to achieving mass-market adoption of this silicon. Today however we would prefer there is no use of 802.11b given the additive noise an 802.11b radio will introduce across multiple nearby 802.11g operating 2.4 GHz channels. For this reason, 11 years later this backward compatibility is a topic for improving customer Wi-Fi experience. One common misconfiguration is for DOCSIS Gateway access points to be configured in 802.11b/g compatible mode. This can cause the access point to down-select DSSS operation, which lowers efficiency and adds noise to side channels when mixed with other 802.11g clients.

In 5 GHz, Wi-Fi has 4 distinct bands of allocation for Wi-Fi use, called the UNII bands. Each band has distinctive power and usage restrictions. Generally, UNII-1 and UNII-3 are the easiest to use but have slightly lower power levels that the UNII-2 and UNII-2-Ext bands. The UNII-2 bands overlap with military and weather radar users. Devices in those bands must be prepared to immediately halt transmissions and switch to another band whenever radar usage is detected, though a device may return later if no further usage is seen. This issue is primarily a concern near military bases and some coastal areas.

It was in 2009 that bonding in Wi-Fi became a reality. 802.11n introduced the use of 20MHz channels with option to bond an addition channel, using OFDM across 40 MHz of continuous channel space. 802.11n introduced Multiple Input Multiple Output (MIMO) spatial streaming. Multiple simultaneous transmit and receive combinations became possible as did alternate modulation schemes across streams. The Modulation Coding Scheme (MCS) defined modulation type, coding rate and allowable mix-modulation schemes. Additional sub-carriers and control of Guard Interval allowed for additional peak throughput performance per channel.

Data rates could now range from 54 Mb/s to upwards of 600MB/s and use either 2.4 GHz or 5 GHz.

802.11n was a stunning advancement in Wi-Fi technology creating the framework for advanced IP service delivery throughout the customer premise. Subsequent standards from 802.11 such as the

802.11ac standard allow 80MHz and 160MHz channel use modulated up to 256-QAM using anywhere from 1 to a maximum of 8 antennas. 802.11ac features are generally entering the market in a series of waves with the Wi-Fi Alliance defining expected capabilities for each wave.

In this brief background of 802.11b/g/n/ac physical layer, it is important to mention that there are many additional 802.11 working group efforts. 802.11 family of standards encompass QoS (802.11e), Inter-Access Point messaging (802.11f), Dynamic Frequency Selection (DFS) for radar detection/avoidance (802.11h), security (802.11i), Radio Resource Management (802.11k RRM), Fast Transition (802.11r), Mesh interfaces (802.11s), and HotSpot services (802.11u).

Appendix B – Troubleshooting Tips

Issue	Resolution
Range	Strive to place the access point centrally in the home/premises, both vertically and laterally, and ensure that the antennas are pointed so that there are no nulls (end of antennae) pointing at key coverage areas
	Switch AP to one with more antennas/MIMO capability
	Add additional APs to cover remote parts of home, e.g. basements, outdoor suites/garages, etc.
	Ensure that there are no key blockages near the AP like chimneys, refrigerators, metal shelves, or similar
Throughput / Speed	If the customer is using their own wired router (either combined with Wi-Fi or a separate wired router between the AP and the cable modem), ensure it can handle the packets per second rate required of the speed tier selected.
	General home router configuration issues that rob speed: disable logging, etc.
	Old connected Wi-Fi devices using older Wi-Fi spec such as 802.11a/b/g/n
	Run wired Ethernet connections to TVs, desktops, security cameras, etc. so that video fixed end devices do not take up Wi-Fi capacity
Interference	e.g. microwave ovens, wireless cameras, Wi-Fi devices operating on overlapping channels, etc.
	Don’t put AP’s in kitchen, or on a wall opposite the kitchen wall with the microwave! Likewise, baby monitors and other Wi-Fi home devices
Congestion	i.e. too many users or devices using same channels
	Select Wi-Fi channels with lower levels of other users
	Upgrade to a dual or tri-band AP
Location of Wi-Fi devices	e.g. building construction/materials, which is related to location; location not optimized for maximum coverage in dwelling
	Similar to range above, minimize the number of concrete block/stone walls between the AP and key usage areas (living room, den, bedroom, etc.)
Lost or forgot login credentials	Use TR-069 to allow customers to reset their passwords w/o having to call a person.
Cable subscriber education	Educate on the basics of Wi-Fi
	Show the customer the speed test results when wired to the Cable Modem, then reconnect the Wi-Fi AP/router and repeat the test over Wi-Fi, to highlight differences depending on where in the house.

Appendix C – Monitoring

Popular Monitoring Parameters

1. BSSID and SSID
2. Number of clients per BSS
3. MCS and RSSI for each client

4. Current operating channel
5. Current channel bandwidth
6. Tx Power
7. Minimum allowed rate
8. Environment scan summary (neighboring AP and their channels and other information)
9. BSS security mode
10. Maximum number of associated clients

Appendix D – RF Fundamentals

RF Fundamentals (Scatter, Reflection, Multipath, Diffraction, etc.)

RF Propagation

Free space path loss (FSPL) is the signal loss from the isotropic spreading of the electromagnetic wave. The ideal FSPL is in open air where direct line of sight occurs from client to access point. This line of sight is known as the Fresnel Zone that are concentric ellipsoids of radiated energy. Loss increases as a square of distance and frequency.

$$L_{fs}(dB) = -10\log\left[\frac{\lambda^2}{(4\pi)^2 d^2}\right] = 20\log\left[\frac{4\pi d}{\lambda}\right]$$
$$= 32.45 + 20\log_{10} d_{Km} + 20\log_{10} f_{MHZ}$$
$$= 36.58 + 20\log_{10} d_{mi} + 20\log_{10} f_{MHZ}$$

One of the main issues for most Wi-Fi deployments is the lack of the ideal clear line-of-sight. A Wi-Fi signal is weakened as it travels through the air and further impeded as it propagates through physical objects such as building materials. The impact of these obstructions depends on where in the fresnel zone they have occurred, in addition to the operating frequency.

There are many conditions present within indoor structures that impede 2.4 GHz and 5 GHz RF signal. The ITU model for Indoor Attenuation[3]is a high level attempt to characterize the impacts of transmission through common building materials based on frequency.

$$\mathrm{L} = 20log\ f + Nlog\ d + Pf(n) - 28$$

The ITU Indoor Attenuation path loss model defines L as the total path loss, f is frequency in MHz, d is distance in meters. N is the distance power loss coefficient, n is the number of floors between transmitter and receiver and $Pf(n)$ is the floor loss penetration factor. The ITU has a table of values for power loss coefficient *N,* $Pf(n)$ accounts for floor loss values, which differ by frequency band and type of construction, illustrated in ITU Recommendation P.1238-7-201202.

2.4 GHz Channel 6 Indoor Attenuation at 35 feet

[3] ITU Indoor Propagation Model http://www.itu.int/rec/R-REC-P.1238/en

$$L = 20log\ (2437) + 28log\ (10.6) + 5(1) - 28 = 73.44\ dB$$

5 GHz Channel 56 Indoor Attenuation at 35 feet

$$L = 20log\ (5280) + 28log\ (10.6) + 7(2) - 28 = 124.16\ dB$$

This 50.72 dB of propagation difference between these two frequencies is one factor in overall Wi-Fi subscriber quality across the customer premises.

RF Interference can be defined as when another signal such as an 802.11 modulated (data-carrying) event occurs, or an un-modulated non-802.11 or non-data carrying signal enters the receiver.
In addition to interference, multipath occurs when a reflection of an RF wave arrives at the receiver. The results of multiple copies of the same signal are beneficial in 802.11n-based systems where the use of OFDM can be applied to re-constitute the modulated signal.

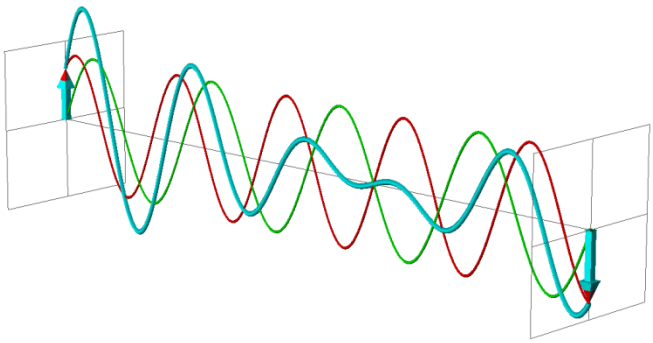

Figure 11 - 802.11n Multi-path