

Wireless#

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.



PrepLogic

Be Prepared. Be Confident. Get Certified.



Joel Barrett - Author
Jimmy Donohue - Technical Editor

Introduction

Radio frequency (RF) technologies are constantly changing. This study guide was developed, first, to comply with the objectives for the Wireless# exam, and second, as a general reference for “all things related to wireless networking.” In six months or more, some standards and solutions will change, but expect the base level of knowledge required to master them to remain the same.

The following are some basic terms and concepts you’ll need to understand prior to reading this study guide:

- Standards and drafts – In most cases, when we refer to drafts and standards in this book, we’re referring to IEEE documents, such as IEEE 802.11b. The whole IEEE process for creating a standard is similar to what the US government goes through to change a bill into a law. There are seven steps the IEEE implements in the standard setting process: securing sponsorship, requesting project authorization, assembling a Working Group, drafting the Standard, balloting (75% approval required), review committee, and last, the final vote. This process usually takes at least 18 months to complete. Drafts are documents that describe the rules by which vendors, developers, and manufacturers must comply when creating products for the identified technology; however, a draft is not the final version. A draft is the version before the document becomes accepted as the standard. Drafts are like alpha or beta versions of software; the standard is the final version. A standard may be altered or amended in the future, but not without majority voting consent of the members of that Working Group. Some amendments can amend both the standard and other amendments.
- Layer 1, layer 2, and layer 3 – these refer to the lowest layers of the OSI model. The OSI model is a way to develop interoperable systems. For networking systems, almost everything revolves around the OSI model. In fact, there are four more layers above Layer 3. You don’t have to have a deep understanding of the OSI model to learn the topics in this study guide, but it does help. Starting with layer 3 (L3) and working down to layer 1 (L1), here are descriptions of what each layer does in regard to basic networking and wireless networking equipment.
 - ▶ Layer 3 (L3) is the Network layer. This is where the network comes together. Upper layer applications exchange messages with layer 3. IP addressing and subnetting occur here. L3 is where you’ll find routers, wireless routers, and L3 switches (switches capable of routing packets). L3 and IP subnetting allow one network to talk to other networks, including the Internet. L3 exchanges packets with L2.
 - ▶ Layer 2 is the Data Link layer, or MAC. It is made of the Media Access Control (MAC) and the Logical Link Control (LLC) sublayers. L2 is where access points (APs), switches, and bridges exist. Devices use MAC addresses here. Devices in L2 can’t do routing; that’s left up to L3. L2 exchanges frames with L1.
 - ▶ Layer 1 (L1) is the Physical layer, or PHY. This is where all hardware and cabling fall. L1 exchanges electromagnetic representations of ones and zeros with the medium. Bits become electrons, photons (for fiber networks), or RF (for wireless networks). The PHY won’t be discussed much in this study guide because delving into bit-level analysis is beyond the scope of most of the conversations. However, many of the devices used in wireless networks will be discussed.
- Protocol stack – The OSI model breaks down different functions and capabilities into seven separate layers. You can’t get to the bottom layer, without going through the other layers first. The protocols that make each layer, or stack, interoperable, are referred to as the protocol stack.
- Terms associated with IEEE 802.11 technologies – IEEE 802.11b and .11g operate in the same frequency (2.4 GHz) and, since .11g is backwards compatible with .11b, the two are often merged

together as “802.11b/g” or “802.11bg.” Sometimes you’ll even see “802.11abg” referring to the lower-layer technologies involved in Wi-Fi solutions: 802.11a and 802.11b/g.

- Usage of meters and kilometers versus feet and miles – Like many scientific communities, radio people primarily use the metric system when discussing range and distances. Ham radio operators typically refer to the frequency ranges they are able to use in meter, centimeter, or millimeter terms. For example, the 144-148MHz ham radio range is called the 2-meter ham band and the 50-54MHz range is called the 6-meter band. These meter distances refer to the wavelength of the frequency. A wavelength is the distance a radio wave travels in the time of one cycle. The metric system is more globally accepted than American standard measurements and, since RF is a solution used worldwide, you need to understand it in global terms. All measurements in this study guide are described in metric terms. You can use the following for a rather generic understanding of conversions: one centimeter is about .4 inches, one meter is about 3.3 feet, five meters is about 16 feet, 10 meters is about 33 feet, 100 meters is about 330 feet, and one kilometer is about .6 miles.
- Usage of “antenna” and “antennas” – It is acceptable by the IT and RF industry to use “antennas,” rather than “antennae,” when referring to more than one antenna on a wireless device.
- Wireless clients – Clients are the combined hardware and software solutions that work together to help your computer, PDA, etc. get connected to the wireless network. Some devices have embedded clients, like Windows XP’s Wireless Zero Config or a Sony PSP’s wireless client. Other devices or operating systems get software installed either before or during the hardware install. You can’t just plug in a PC Card and expect everything to start working, unless the system came preconfigured to do so. The client software lets you configure the necessary parameters so your computer can connect. If security restrictions are enabled on the WLAN, you’ll have to configure them in the client software before being allowed to transmit data across the WLAN.
- Low Latency – This is basically the ability to get data across a communication link as fast as possible. A low latency connection for wireless layer 2 links is typically less than 150 milliseconds (ms). That means that your packets traverse the communication link in less than .15 of a second. This is most important in voice networks where humans can detect delays (drops) of 200ms or higher. Worse rates may be acceptable for cellular calls, but they are unacceptable for business IP telephony systems. This is why it is important to have low latency in enterprise-capable wireless network solutions.
- SOHO, SMB, and Enterprise solutions – Small Office/Home Office (SOHO) locations are small and usually have solutions geared for less than 25 users. Small-to-Medium Business (SMB) solutions can range from 10 to about 150 users. Enterprise solutions can scale to hundreds, thousands, or tens of thousands of users. There are many vendors and manufacturers that play in the SOHO and SMB spaces, of which only a few can handle the enterprise space. Due to the entry-level nature of this study guide, most discussions will concentrate on SOHO or SMB solutions.

IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is a household name in scientific, telecommunication, medical, and information technology groups. The organization is commonly referred to as “the IEEE,” pronounced “eye-triple-e.” IEEE members work together to create draft documents and standards, or formal publications.

These standards are typically based on protocols that enable different products to communicate with each other. Equipment manufacturers and software developers use these protocols and standards to create interoperable products. The process the IEEE uses to create standards is quite formalized and comes from over 100 years of experience. It is important to be familiar with the IEEE because many of the solutions described in this study guide come from well known IEEE standards and amendments, such as IEEE 802.11 (WLAN and Wi-Fi), 802.15.1 (Bluetooth), 802.15.4 (ZigBee), and 802.16 (WiMAX).

It is also important to know that the IEEE does not enforce standards, nor is the IEEE a governing body. Manufacturers and developers are not required to comply with IEEE standards, but it is their voluntary compliance that helps advance the industries in which the IEEE contributes.

Standards boards that are similar to the IEEE are the Federal Communication Commission (FCC), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), Industry Canada (IC), and Association of Radio Industries and Businesses (ARIB).

Wi-Fi Alliance

The Wi-Fi Alliance is a global trade organization that performs product certifications to guarantee interoperability with other Wi-Fi Certified products. There are over 200 member companies and over 2000 Wi-Fi certified products on the market today. The Wi-Fi Alliance also helps promote the use of Wi-Fi-enabled products and solutions.

The Wi-Fi Alliance verifies products operate within compliance specifications for these IEEE standards:

- 802.11 - 1999
- 802.11b
- 802.11a
- 802.11g
- 802.11i
- 802.11h
- 802.11d
- 802.11e

NOTE: This list is sorted chronologically. Some of these standards (802.11b, g, and a) are OSI Physical Layer (L1) technologies, while others are add-ons to other Layer 2 Wi-Fi capabilities (802.11i, h, d, and e).

Wi-Fi product security capabilities are tested for compliance to Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and Extensible Authentication Protocol (EAP) mechanisms. Certification tests also now validate that products are compliant with Wi-Fi Multimedia (WMM) Quality of Service (QoS) and WMM Power Save capabilities.

Wi-Fi has become synonymous with Wireless Local Area Networks (WLANs). Whenever wireless comes up in conversation, if it doesn't have to do with cellular-based technologies, then the term Wi-Fi can't be far behind.

Technology Fundamentals

As mentioned previously, it is important to understand the OSI model when working with any networking solution, especially Wi-Fi. For example, understanding where Wi-Fi operates within the OSI model will help keep you from creating security holes due to missing encryption or from implementing too much security by having encryption in two places when you only need it in one.

We discussed how the OSI model maps to networking technologies, but here is a brief overview of how it maps to WLAN solutions. The Physical layer (L1) is where frequencies, modulations and channels, as well as radio power levels are defined. Almost all Wi-Fi devices operate in the Physical and Data Link (L2) layers. This is important to understand. For example, if you apply L2 encryption using WPA and then also use IPsec security at L3, you have an extremely secure network but with a high overhead cost. Encryption processing decreases throughput. If you have multiple encryption operations, it will have a negative impact on WLAN capabilities. For Wi-Fi devices, the MAC sublayer in the Data Link layer is very different than what is found in Ethernet solutions. The MAC layer allows device addressing, packet fragmentation, Quality of Service implementation, and other functions usually found in higher layers for wired networking equipment. Almost all the Wi-Fi features covered in this study guide are found in the Data Link layer.

Layer 3, the Network layer, is where most people think their WLAN starts. This is because IP addressing is done here and most people tend to take lower level protocols for granted. Most Wi-Fi devices don't rely on Network layer protocols; however, there are a few that do, such as wireless routers and Enterprise Wireless Gateways (EWG).

Wi-Fi networks are typically made up of access points and client stations. An access point, or AP, is the heart of most wireless networks. Most APs operate only at Layers 1 and 2, but some provide routing functionality and therefore also operate at Layer 3. In traditional Wi-Fi networks, traffic passes through the AP headed either to a client device or the wired network. A client is usually software on a device with a wireless network card that enables a wireless connection to an AP and then uses that connection to pass data to another device. Clients are most often laptops, PDAs, or other computers, but they can also be devices like wireless print servers or range extenders.

Within the Wi-Fi network, there are other terms that are consistently used. "Service Set Identifier," or SSID, is the name assigned to the WLAN. "Association" is one of several client processes used to join the WLAN. "WPA," "802.1X," and "802.11i" all refer to security. The wired network that connects access points is sometimes referred to as the "Distribution System."

Frequencies/Channels used

There are two primary radio frequency (RF) spectrums used in Wi-Fi today. They are the 2.4 GHz (gigahertz) ISM band for 802.11b/g and the 802.11a 5 GHz UNII bands. ISM stands for “Industrial, Scientific and Medical,” and defines areas in the radio spectrum that are free for unlicensed use. You don’t need to obtain a license to use them, as you do for most RF spectrums. Many devices, such as garage door openers, baby monitors, microwave ovens, cordless phones, and hospital equipment, use ISM. These devices can create interference and noise for Wi-Fi systems but must be accommodated since the spectrum is unlicensed. Some wireless equipment is completely incompatible with other devices, which is why Wi-Fi certification is so important. It lets the buyer know there is at least a required level of compatibility between Wi-Fi branded products; products from one vendor will work well with products from another.

The 2.4 GHz band, as specified by the Federal Communication Commission (FCC) in the United States, starts at 2.400 GHz and goes to 2.500 GHz. This is a 100 million Hertz (MHz) band. The FCC also specifies power output limits. The IEEE uses these “rules” to build the IEEE 802.11b and 802.11g standards. However, the IEEE left room at the top end of the spectrum, and only went to 2.4835 GHz. This is to separate 2.4 GHz devices from those operating in the 2.5 GHz spectrum.

Both 802.11b and 802.11g use the 2.4 GHz spectrum. However, 802.11b uses direct-sequence spread spectrum modulation while 802.11g uses orthogonal frequency division multiplexing modulation. There are 14 channels defined for Wi-Fi use in the 2.4 GHz spectrum.

The idea behind any spread spectrum technology is to use low power signals that are spread across the frequency range. For example, an 802.11b signal is spread across 22 MHz with each channel based around a center frequency. The signal carries bits of information used to recreate the data at the receiver. Each signal requires a five-channel separation between center channels to keep from overlapping one another. The maximum number of channels that can be used simultaneously out of the 14 is three. In the United States, the accepted practice is to use channels 1, 6, and 11, but any combination will work as long as the channels in use are five or more channels apart (e.g., 2 and 8; or 1, 7, and 13). However, there are regional restrictions in place that limit the channels available for individual countries. For the United States, only channels 1 through 11 are available for use. Some countries have only one channel available; some have all 14. Wi-Fi devices purchased for use must comply with the rules and regulations of the country where they’ll be operating. In other words, you can’t purchase an access point in the United States and legally operate it in another country without modifications to RF power and channel use, unless the RF restrictions in that country allow for that.

IEEE 802.11b uses HR/DSSS (High-Rate/Direct Sequence Spread Spectrum) as its DSSS modulation type. OFDM is Orthogonal Frequency Division Multiplexing and is also the name of the PHY described by 802.11a. The OFDM type for 802.11g is referred to as ERP (Extended Rate PHY). OFDM is used to put data in the signals of 802.11g and .11a transmissions. IEEE 802.11b that uses DSSS can only manage up to a maximum of 11 Mbps data rate, while 802.11g can achieve speeds of 54 Mbps data rate using OFDM.

NOTE: Data rate and throughput are usually thought of as being the same thing, but they are very different. The data rate reported by wireless client software only refers to the amount of data passing through the card and into the machine.

The data rate reported by your wireless client is what the card perceives as the highest possible data rate connection available.

For example, say you have a single 802.11g AP with one 802.11g client associated. With the client about a meter away and no other interfering devices present, the client software will almost definitely connect at the highest data rate of 54M bps. If you start a file transfer from a machine on the wired side of the network to the wireless client and use a wired-side utility to check the amount of data being transferred, the throughput you receive will be much less than 54M bps.