An Introduction to Wi-Fi®

019-0170 • 090409-B

The latest revision of this manual is available on the Rabbit Web site, www.rabbit.com, for unregistered, free download.

An Introduction to Wi-Fi®

Part Number 019-0170 • 090409–B • Printed in U.S.A.

Trademarks

Rabbit and Dynamic C® are registered trademarks of Digi International Inc.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance

Table of Contents

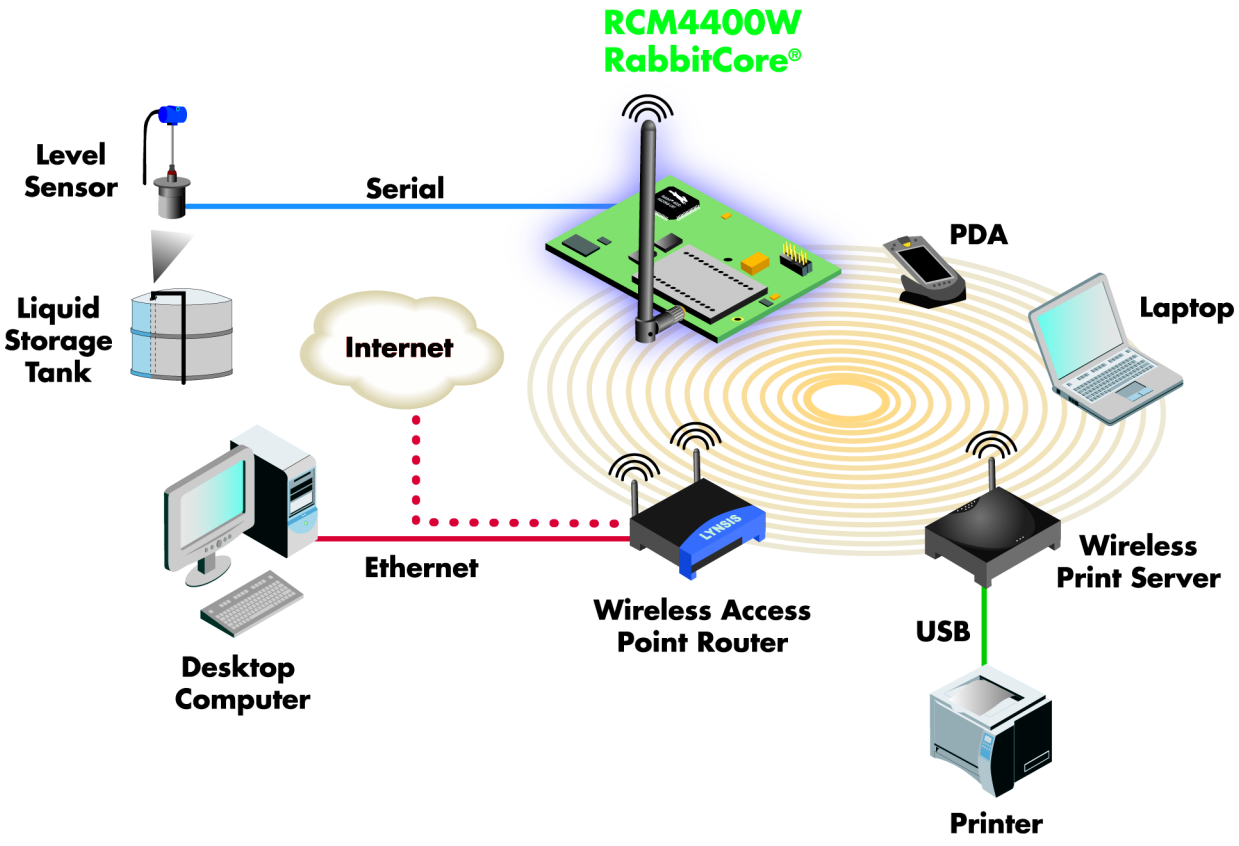
1. OVERVIEW

This manual is intended for embedded systems engineers and support professionals who are not familiar with wireless networking from a theoretical or implementation point of view. The components, organization, and operation of Wi-Fi networks will be presented. There is an emphasis on security issues and the available security protocols.

Wi-Fi is the name given by the Wi-Fi Alliance to the IEEE 802.11 suite of standards. 802.11 defined the initial standard for wireless local area networks (WLANs), but it was considered too slow for some applications and so was superseded by the extensions 802.11a and 802.11b, and later by 802.11g (with the release of 802.11n still pending).

At its most basic, Wi-Fi is the transmission of radio signals[1]. Wireless Rabbits offer the embedded systems engineer many benefits in a wide range of applications. Figure 1 illustrates the Rabbit's role in a sensor monitoring application.

Figure 1. Wireless Local Area Network Connected to the Internet



1. When asked to describe radio, Albert Einstein replied, "You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."

1.1 Benefits of Wi-Fi

What are the benefits of Wi-Fi over a more traditional wired network? In particular, what are the benefits for an embedded system application? To begin with, if you study the diagram in Figure 1, you can see the enormous flexibility that a wireless connection brings to an embedded application. The addition of wireless provides more choices for monitoring, control and the dissemination of information. Practically speaking, remote locations become more accessible and costs drop.

The following list summarizes some of the benefits of a Wi-Fi network.

- **Wireless Ethernet**. Wi-Fi is an Ethernet replacement. Wi-Fi and Ethernet, both IEEE 802 networks, share some core elements.
- **Extended Access**. The absence of wires and cables extends access to places where wires and cables cannot go or where it is too expensive for them to go.
- **Cost Reduction**. As mentioned above, the absence of wires and cables brings down cost. This is accomplished by a combination of factors, the relatively low cost of wireless routers, no need for trenching, drilling and other methods that may be necessary to make physical connections.
- **Mobility**. Wires tie you down to one location. Going wireless means you have the freedom to change your location without losing your connection.
- **Flexibility**. Extended access, cost reductions, and mobility create opportunities for new applications as well as the possibility of creative new solutions for legacy applications.

1.2 Wi-Fi Embedded System Applications

The reach of wireless communication in embedded systems continues to grow. Forrester Research, a company that focuses on the business implications of technology change, has reported that in a few short years, up to 95% of devices used to access the Internet will be non-PC devices that use an embedded system.

There are many applications for embedded devices with a Wi-Fi interface:

- Industrial process and control applications where wired connections are too costly or inconvenient, e.g., continuously moving machinery.
- Emergency applications that require immediate and transitory setup, such as battlefield or disaster situations.
- Mobile applications, such as asset tracking.
- Surveillance cameras (maybe you don’t want them easily noticed, cables are difficult to hide).
- Vertical markets like medical, education, and manufacturing.
- Communication with other Wi-Fi devices, like a laptop or a PDA.

2. IEEE 802.11 SUITE OF STANDARDS

This chapter discusses the concepts and characteristics specified in the IEEE 802.11 standard. 802.11 is a packet protocol that defines data transmission and manages location-independent network access using radio signals.

Wi-Fi is a physical/link layer interface, as is Ethernet. The layers above the physical and data link layers include TCP/IP. On a practical level, this means that all Rabbit sample programs and customer applications for TCP/IP that are run on an Ethernet interface will also run on a Wi-Fi interface.

2.1 Architecture

This section discusses the architectural components defined by the 802.11 standard. The architecture describes the structure and organization of the network. This knowledge informs various tasks, such things as selecting the right operating mode to suit your application or completing an effective site survey for the physical location of the network.

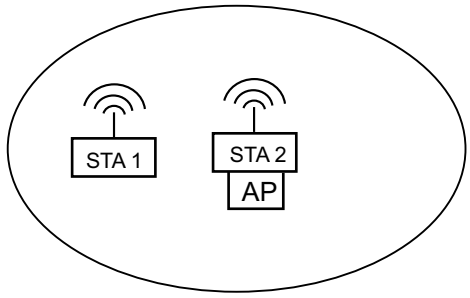
2.1.1 Basic Components

All wireless devices that join a Wi-Fi network, whether mobile, portable or fixed, are called wireless stations (STAs). A wireless station might be a PC, a laptop, a PDA, a phone, or a Rabbit core module. When two or more STAs are wirelessly connected, they form a basic service set (BSS). This is the basic building block of a Wi-Fi network.

A BSS is a set of STAs controlled by a single coordination function (CF). The CF is a logical function that determines when a STA transmits and when it receives.

The BSS shown in Figure 2.1 is an example of the simplest Wi-Fi network possible: two wireless stations. The oval shape around them roughly represents the coverage area.

Figure 2.1

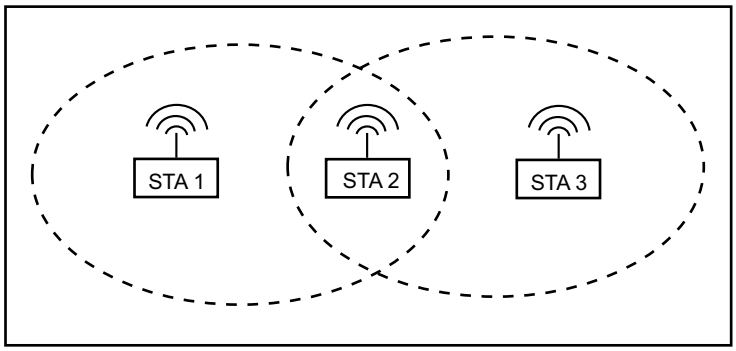


BSS

While a circle may represent the idealized coverage area of a single radio, it is not very accurate in real world situations. Environmental factors cause dramatic variations to the coverage area. For example, a STA with an omnidirectional antenna placed in the corner of a building may have most of its coverage area outside the building and in the adjacent parking lot.

Not all STAs in a BSS can necessarily communicate directly. Consider Figure 2.2. STA 1 and 3 are mutually out of range, thus require use of STA 2 to relay messages.

Figure 2.2



2.1.2 Operating Modes

This section discusses the two operating modes specified in the IEEE 802.11 standard: infrastructure mode and ad-hoc mode. Each one makes use of the BSS, but they yield different network topologies.

The operating mode is selected during the configuration of the wireless station (see Chapter 5 for more details); all wireless stations must select an operating mode before attempting to create or join a Wi-Fi network.

2.1.2.1 Ad-Hoc Mode

The independent BSS (IBSS) is the simplest type of 802.11 network. Wireless stations communicate directly with one another using the ad-hoc operating mode. Such a network follows a peer-to-peer model.

A BSS operating in ad-hoc mode is isolated. There is no connection to other Wi-Fi networks or to any wired LANs. Even so, the ad-hoc mode can be very useful in a number of situations. Because an ad-hoc network can spring up anywhere, it is especially useful in situations that demand a quick setup in areas that do not have any infrastructure, such as emergency sites and combat zones.

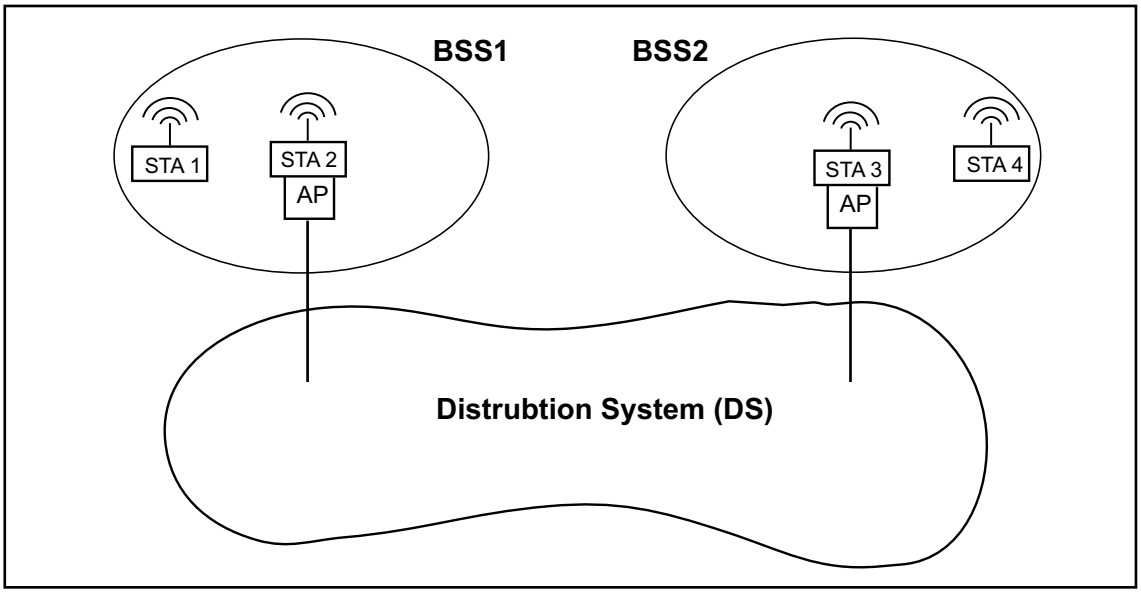
As another example of the usefulness of ad-hoc Wi-Fi, consider that it is now common for people to have their laptops with them in business meetings, in airports waiting for flights, or even at their local coffee hang-out. Operating in ad-hoc mode, people can easily and quickly form a network to do things like share large files or anything else they may want to do cooperatively.

2.1.2.2 Infrastructure Mode

The infrastructure operating mode requires that the BSS contain one wireless access point (AP). An AP is a STA with additional functionality. A major role for an AP is to extend access to wired networks for the clients of a wireless network. The exact services specified by 802.11 for APs are listed in Section 2.3.

All wireless devices trying to join the BSS must associate with the AP. An AP provides access to its associated STAs to what is called the distribution system (DS). The DS is an architectural component that allows communication among APs; this concept is represented pictorially in Figure 2.3.

Figure 2.3 APs Communicate Using the DS



The IEEE 802.11 specification does not define any physical characteristics or physical implementations for the DS. Instead, it defines services that the DS must provide. The services are discussed in Section 2.3.2.

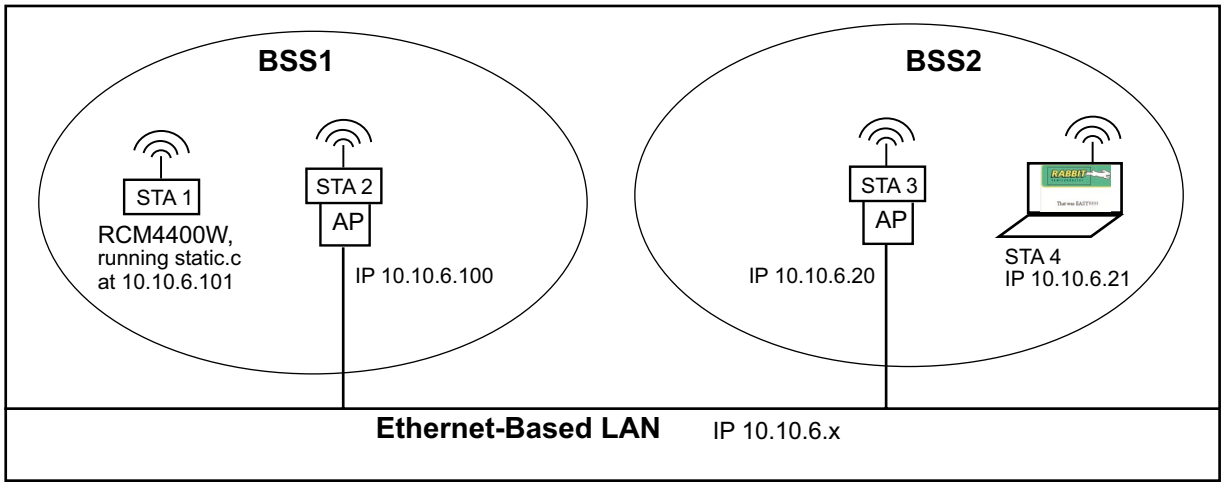
The DS medium comprises the physical components of a specific DS implementation, e.g., coaxial cabling or fiber optic cabling.The DS medium is logically different from the wireless medium (WM). Thus, the addresses used by the AP on the wireless medium and the addresses used on the DS medium do not have to be the same. See Figure 3.2 for an illustration of this logical difference.

All wireless communication to or from an associated STA goes through the AP when the network is configured to use infrastructure mode. This setup is similar to the host/hub model (or “star topology”) used frequently in wired networks. In the 802.11 specification, both AP (“hub”) and “host” are called wireless stations or STAs.

To make this concept more clear we will look at a concrete example using these architectural components. In Figure 2.4 we are concerned with a subnet of 10.10.6.x. In this example, the Rabbit-based device is running static.c, one of the TCP/IP sample programs that comes with Dynamic C. The Rabbit serves a static web page that is then viewable from the laptop that has joined a separate Wi-Fi network, BSS2, on the same subnet as the Rabbit.

A wireless station that created or joined a BSS on that subnet would be able to communicate with any other wireless station on that subnet. The AP acts as a wireless hub or switch.

Figure 2.4 Test Network Set-Up of Wireless AP Communication



Another architectural component described by 802.11, called a portal, is also needed for the access to another system to occur. This construct is like a doorway. It is what bridges a wireless LAN to a wired LAN. In a practical sense, this means that all data going to an 802.11 network from an non-802.11 network must pass through this doorway.

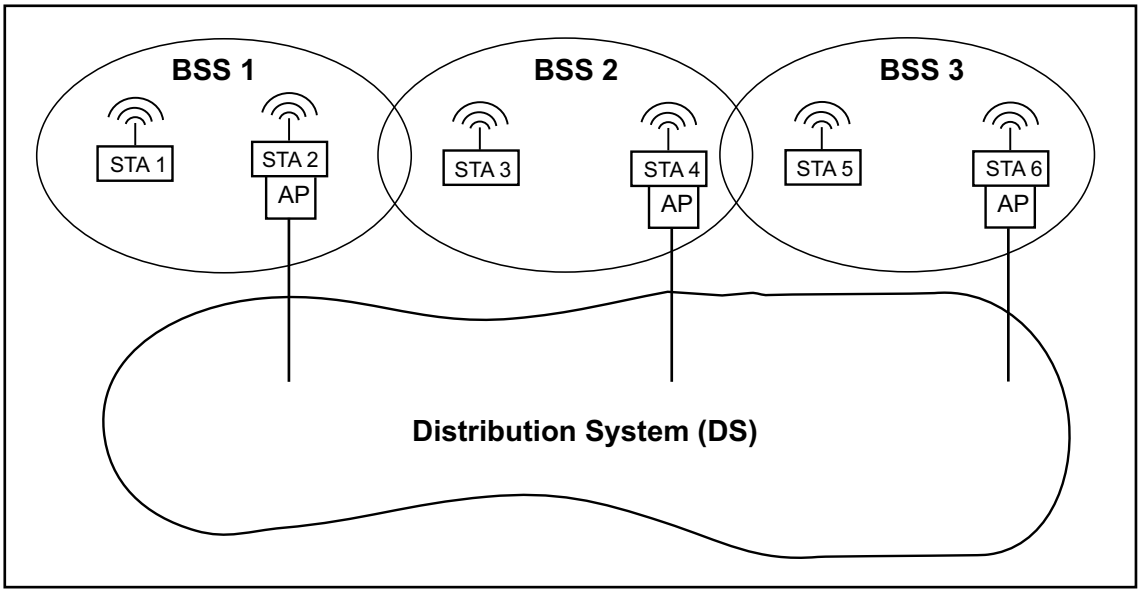
The portal and DS access functionality can be implemented in the same device (an access point), and typically are, but there is no requirement in the IEEE 802.11 standard that this must be the case.

2.1.3 Extended Service Set

A common distribution system (DS) and two or more BSSs create what is called an extended service set (ESS). An ESS is a Wi-Fi network of arbitrary size and complexity. In Figure 2.5 is a representation of an ESS comprised of BSS 1, 2 and 3. The distribution system is not part of the ESS.

The distribution system enables mobility in a Wi-Fi network by a method of tracking the physical location of STAs, thus ensuring that frames[1] are delivered to the AP associated with the destination STA. Mobility means a wireless client can move anywhere within the coverage area of the ESS and keep an uninterrupted connection. However, please note that since the 802.11 specification does not specify how the DS works, APs from different vendors may not work well with each other to provide an uninterrupted connection.

Figure 2.5 ESS



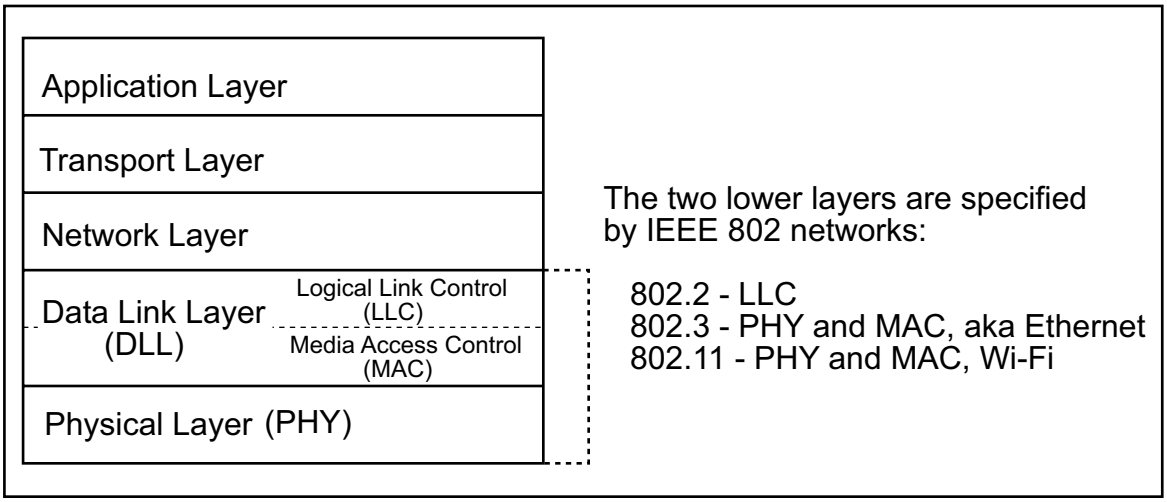
The network name, or SSID, must be the same for all APs participating in the same ESS.

1. For more information on frames, see Section 2.4.

2.2 Five-Layer TCP Model

802.11 and its extensions (a, b, g, etc.) define two layers in the five-layer TCP model: the physical layer and the data link layer. These are the same two layers that are defined by 802.3 (Ethernet). The data link layer is actually made up of two layers: media access control (MAC) and logical link control (LLC). The IEEE 802.11 specification defines the MAC sublayer.

Figure 2.6 5-Layer TCP Model



2.2.1 IEEE 802.11 Physical Layer (PHY)

There are several physical layers described in the 802.11 specification and its extensions. The PHY is responsible for such things as modulation methods, encoding schemes and the actual transmission of radio signals through space. Most of the information pertaining to these topics is well beyond the scope of this manual.

PHY implementations operate in specific bands. A band defines the frequencies allocated for particular applications. Many Wi-Fi devices are designed for use in the Industrial, Scientific and Medical (ISM) band. The ISM band is for license-free devices; regulatory requirements demand that license-free devices use spread-spectrum technology. Direct sequence spread spectrum (DSSS) PHYs are the most widely deployed at this point in time.

2.2.2 IEEE 802.11 Medium Access Control Layer (MAC)

The 802.11 MAC layer is technically a sublayer of the data link layer (DLL). It rides above the physical layer, controlling transmission of data and providing interaction with a wired backbone, if one exists. The MAC layer also provides services related to the radio and mobility management.

To move data packets across a shared channel, the MAC layer uses CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), which is very similar to the strategy used in 802.3 MAC layers: CSMA/CD (Collision Detection). They are both peer-to-peer protocols, but unlike CSMA/CD, which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.

The 802.11 MAC layer is required to appear to a logical link control (LLC) layer as an IEEE 802 LAN, thus Wi-Fi and Ethernet both use MAC addresses in the same format, i.e., 6 octets that are globally unique.

2.3 Services Specified by IEEE 802.11

The IEEE 802.11 standard does not define any specific implementations. Instead, nine services are specified that all implementations must provide. The services are summarized here and some of them have links to other sections where the service is described in more detail.

2.3.1 Station Services (SS)

All 802.11 compliant wireless stations (STAs) must implement the four station services defined in the IEEE specification. Remember that STAs include APs and wireless routers with AP functionality (see Section 3.2.3.1).

The services are:

- Authentication - A wireless station needs to be identified before it can access network services. This process is called authentication. It is a required state that comes before the STA may enter the association state. See Section 4.2.1, Section 4.3.1 and Section 4.3.2 for more information on authentication options.
- Deauthentication - This service voids an existing authentication.
- Privacy - A wireless station must be able to encrypt frames in order to protect message content so that only the intended recipient can read it. See Section 4.2.2 and Section 4.3.3 for more information on encryption options.
- MAC Service Data Unit (MSDU) Delivery - An MSDU is a data frame that must be transmitted to the proper destination.

2.3.2 Distribution System Services (DSS)

A wireless station that functions as an access point must implement the four station services plus the distribution system services listed here:

- Association - This service establishes an AP/STA mapping after mutually agreeable authentication has taken place between the two wireless stations. A STA can only associate with one AP at a time. This service is always initiated by the wireless station and when successfully completed enables station access to the DSS.
- Reassociation - This service moves a current association from one AP to another AP.
- Disassociation - This service voids a current association.
- Distribution - This service handles delivery of MSDUs within the distribution system; i.e., the exchange of data frames between APs in an extended service set (ESS).
- Integration - This service handles delivery of MSDUs between the distribution system and a wired LAN on the other side of a portal. Basically this is the bridging function between wireless and wired networks.

2.3.3 State Variables

Each wireless station maintains two state variables, one for authentication and one for association. A wireless station is authenticated or unauthenticated. Once in an authenticated state, the STA is either associated or unassociated.

These variables create three states:

- State 1: Unauthenticated and unassociated.
- State 2: Authenticated, not associated.
- State 3: Authenticated and associated.

The state of the wireless station determines which MAC frames are admissible. This information could be useful when debugging with a packet sniffer.

2.4 802.11 Frame and Message Types

Three types of MAC frames (MPDUs) traverse a wireless LAN: control, data, and management. Each of the services described in Section 2.3 are carried by one or more of these frame types.

A MAC frame has up to four, but usually three, address fields. Each address field is the same format as an IEEE 802 MAC address. The following five address types are used:

- BSS Identifier (BSSID) - Identifies the AP of an infrastructure BSS. For an IBSS (ad hoc network) this is a locally-administered random number.
- Destination Address (DA) - Identifies the final recipient(s) of the frame.
- Source Address (SA) - Identifies the initial source of the frame.
- Receiver Address (RA) - Identifies the immediate recipient AP(s) on the wireless DS.
- Transmitter Address (TA) - Identifies the AP that transmitted the frame onto the wireless DS.

Whether a frame contains three or four addresses depends on the settings for “To DS” and “From DS” in the Frame Control field of the MAC frame. The fourth address field is special case; it is only used when the distribution system (DS) is wireless.

Table 2-1. MAC Frame Address Fields

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	n/a
0	1	DA	BSSID	SA	n/a
1	0	BSSID	SA	DA	n/a
1	1	RA	TA	DA	SA

Addr 1: this is always the recipient address, which is the wireless station in the BSS who is the next receiver of the frame.

Addr 2: this is always the wireless station that is physically transmitting the frame.

Addr 3: this is either the original source address or the intended destination address.

Addr 4: this is the final source address for a frame that is both transmitted and received on a wireless distribution system.

In the above table, the first row defines the address fields for frames traveling between an access point and its associated stations. The second and third rows define the address fields for frames traveling between an access point and the distribution system. The fourth row defines the special case of when the immediate addresses for both transmitting and receiving are via a wireless distribution system, thus requiring two additional address fields for the final source and destination addresses.

2.5 IEEE 802.11a/b/g/n Standards

This section compares Wi-Fi characteristics of the different 802.11 networks. The characteristics themselves are discussed in Section 3.1.

Table 2-2. Comparison of 802.11 Networks

Wi-Fi Parameter	IEEE 802.11 Protocols			
	802.11a	802.11b	802.11g	802.11n[a]
Operating Frequency	5.3 GHz and 5.8 GHz	2.4 GHz		2.4 GHz or 5 GHz
Average Signal Range[b]	~30 to 35 m			~60 to 70 m
Available Bandwidth per Channel	~20 to 22 MHz			20 or 40 MHz
Data Rate (Max.)	54 Mbps	11 Mbps	54 Mbps	248 Mbps (2 streams)
Typical Throughput for Max Data Rate	18 to 22 Mbps	6 Mbps	18 to 22 Mbps	74 Mbps
Modulation Technique	OFDM	CCK or DSSS	OFDM	OFDM using MIMO and CB
Channels	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	1-11		3 non-overlapping channels in ISM frequency band at 2.4 GHz 12 non-overlapping UNII channels in 5 GHz frequency band with and without CB
Special Considerations	Higher frequency signals have more trouble with physical obstruction	2.4 GHz subject to interference from: Bluetooth products, cordless phones, microwaves, radar, remote controls, ZigBee networks, etc.		

a. not finalized
b. dependent on physical environment

2.6 Some 802.11 Add-Ons

This section summarizes some of the additional specifications from IEEE 802 groups.

- 802.11e - defines a set of Quality of Service enhancements that are of critical importance to applications that cannot tolerate delays, such as streaming multimedia or voice over IP.
- 802.11i - security extension, see Chapter 4.0 for details.
- 802.11p - adds support for data exchange between high-speed vehicles and between vehicles and roadside infrastructure.

3. WIRELESS LAN BASICS

This chapter discusses various topics of interest to those creating or joining wireless LANs. There are several decisions to make when deploying a Wi-Fi network. Since the original 802.11 specification that came out in 1997, which operated in the 2.4 GHz range at low data rates of 1-2 Mbps, several extensions have expanded the available choices. The marketplace has also responded to customer demand by offering devices that combine 802.11 extensions into one device.

The topics included in this chapter are things to consider in relationship to the requirements of your application.

3.1 Wi-Fi Characteristics

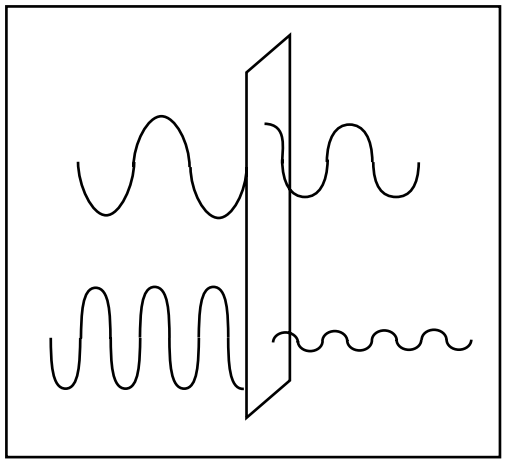
The physical characteristics summarized in Table 2-2 allow you to compare the different 802.11 extensions (802.11a/b/g/n) with one another. This section describes basic characteristics that are common to all Wi-Fi networks.

3.1.1 Operating Frequency

There are two signaling frequencies currently used by Wi-Fi networks:

- 2.4 GHz - Comprises 14 channels, each with a bandwidth of approximately 20 to 22 MHz operating in the ISM band. 802.11b/g networks operate in the 2.4 GHz band. It is a crowded frequency because many devices other than 802.11 devices operate in it. For example, Bluetooth as well as many consumer products such as microwaves, telephones, garage door openers, baby monitors, etc.
- 5 GHz - Comprises 13 channels, each with a bandwidth of approximately 20 MHz operating in the U-NII band. 802.11a networks operate in the 5 GHz band. Currently, this band is less crowded than 2.4 GHz, but this is likely to change as the wireless market continues to grow.

Higher frequency signals have higher attenuation passing through obstacles than do lower frequency signals. This is because some of the energy of the electromagnetic field transfers into the material of the obstacle (cement walls, foliage, etc.) which reduces the strength of the signal.



3.1.2 Signal Strength and Range

Putting aside the topic of RF interference for a moment, it can be said that received signal strength is a function of the power output of the transmitter, the frequency used, the distance travelled by the signal, and the path loss that occurs before the signal is received.

Received signal strength, and thus usable range, can vary from moment to moment because propagation characteristics are dynamic and unpredictable. This means that small changes in the environment can result in huge changes to Rx signal strength.

The critical thing is received signal-to-noise ratio. Noise is a function of interfering source strength, proximity, and bandwidth. Additionally, all receivers contain an inherent noise source caused by fundamental physical processes such as random thermal motion of charge carriers. In practice, Rx signal-to-noise ratio (SNR) is required for higher transmission speed. SNR is more important than absolute Rx signal strength.

Tips for improving SNR:

- Position wireless AP or router in a good spot. Off the floor to start and as far away as possible from any known sources of interference.
- Use a high-gain antenna, especially on the AP, but also on STAs with marginal SNRs. Antennas provide gain with very little additional noise of their own. Use directional antennas to help filter out interfering noise sources.

3.1.3 Data Rate and Throughput

The terms data rate and throughput are sometimes used interchangeably. In this manual, the term data rate will be used to discuss the theoretical peak data rate, whereas throughput will be used to describe the actual number of data bits transmitted per second through the wireless medium. Throughput is diminished by protocol overhead, client competition/collisions, and retransmissions. As you can see in Table 2-2, the typical throughput is about half of the peak data rate. This slowdown is caused by the overhead of 802.11 packets.

802.11 requires positive and timely acknowledgement of each frame transmitted. Unlike wired Ethernet, where the chance of interference is relatively small, 802.11 anticipates a high probability of interference, hence more overhead is required to deal with this challenge.

Also, unlike wired Ethernet, 802.11 allows selection of transmission speed so that less favorable SNRs may be overcome by using slower data rates (as slow as 1 mbit/sec). Choosing a suitable slower data rate may result in an improved overall throughput over attempting a higher data rate which is bogged down with retransmissions.

An assessment of the throughput required for any particular application is a precursor to any decision about which 802.11 standard to use. The requirements of many embedded applications are satisfied with the relatively slower speed of 802.11b.

There are several things to consider in order to determine the throughput needed by an application.

- What type of traffic will traverse the network?
- Is the traffic steady or intermittent?
- Does the application require low latency?
- What error rate is acceptable?

Table 3-1 lists the data rates supported by the IEEE 802.11 standards.The initial 802.11 specification defined two data rates: 1 and 2 Mbps. These low rates were inadequate for some applications, which spurred the development of 802.11 standards with faster data rates. But, keep in mind that faster is not always better. The 1 Mbps data rate is more than adequate for many Rabbit-based applications. And, it is arguably the most robust data rate for industrial applications in general.

Note that Wi-Fi devices will dynamically adjust the data rate.

Table 3-1. Data Rates Supported by IEEE 802.11 Standards

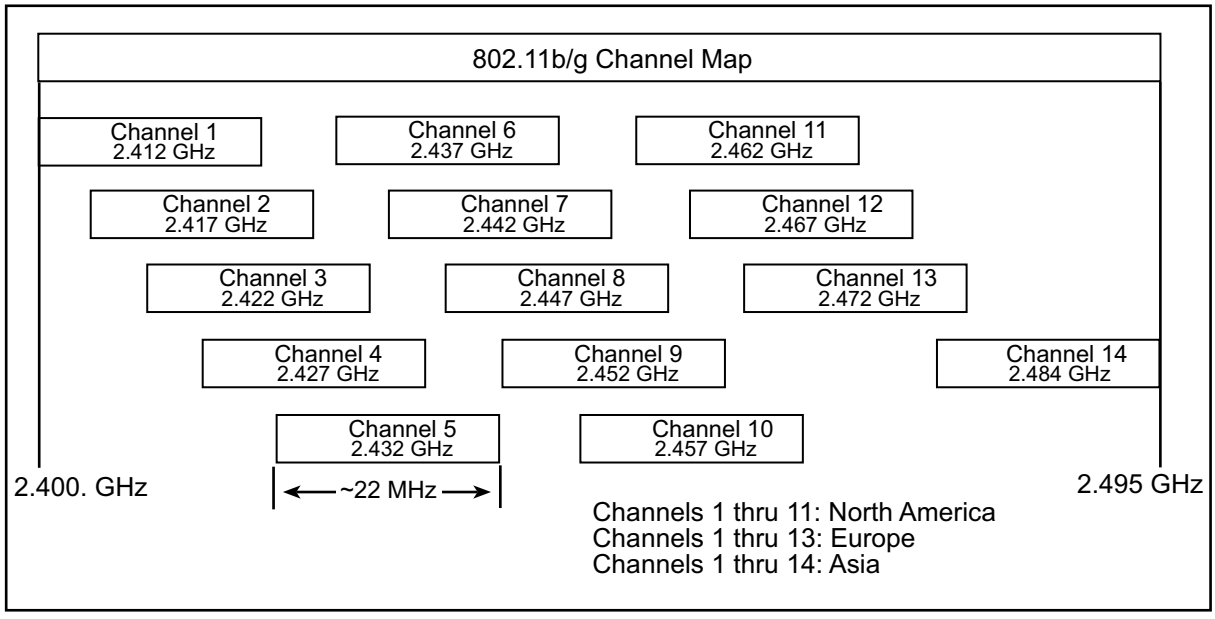
802.11 Extension	Supported Data Rates
802.11	1, 2 Mbps
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps 6, 12, and 24 Mbps are mandatory
802.11b	1, 2, 5.5, 11 Mbps
802.11g	1, 2, 5.5, 11, 6, 9, 12, 18, 22, 24, 33, 36, 48, 54 Mbps 1, 2, 5.5, 11, 6, 12 and 24 Mbps are mandatory 22 and 33 Mbps are typically not supported
802.11n	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 121.5, 130, 144.44, 270, 300 Mbps

3.1.4 Channels

Direct communication between wireless stations, whether it be in an ad-hoc network or an infrastructure network, happens on a channel: a specified frequency band for the travel of electromagnetic signals.

Rabbit products (like the RCM4400W) support the 2.4 GHz range of the ISM band. As shown in Figure 3.1, there are three non-overlapping channels available in North America: 1, 6 and 11. Non-overlapping allows for simultaneous use of the channels in the same physical area without causing interference.

Figure 3.1 ISM Band



The channel is set during configuration of the access point or wireless router. On the wireless station, the channel is selected during a scan of available networks. See Section 3.2.2 for more information on network scanning.

Rabbit hardware does not have support for channels in the 5 MHz range, but for the sake of completeness, the valid channel identifiers and their center frequencies are listed in Appendix A.

3.1.5 Speed Needs

Though faster speeds are available when using Rabbit hardware, most applications can meet their requirements with the slower speeds. Consider the following statements about the relatively slow speed of the 1 Mbps data rate:

- latency hardly different from higher rates for short packets
- most robust
- never gets slower
- fast enough for most sensor/control applications
- universally supported by old equipment

These are all good reasons to use the 1 Mbps option, but when using existing infrastructure use OFDM rates if you need to avoid slowing other users of the network.

3.2 Creating or Joining a Network

All Wi-Fi networks have a name and will communicate on a specific channel frequency. Together, the name and channel allow multiple wireless networks to be present within the same physical space.

3.2.1 Configuration Parameters

An access point, or a wireless router acting as an access point, is typically configured with a utility program provided by the manufacturer of the device.

Wireless clients such as a Rabbit-based device are typically configured via the software application running on the wireless device. The Dynamic C software package that comes with Rabbit-based hardware provides many sample applications to run on Wi-Fi capable Rabbit boards.

Each wireless station, both clients and access points, must be configured in the following ways:

- **Operating Mode** - there are two options for the operating mode: infrastructure and ad-hoc. See Section 2.1.2 for a detailed explanation of these two modes. Any Wi-Fi capable device can create or join a Wi-Fi network operating in ad-hoc mode.

  Only an access point or router can create a Wi-Fi network operating in infrastructure mode. Embedded devices like the RCM4400W do not create such networks, they join them.

- **Operating Channel** - the 802.11 extension in use (a, b, g, n...) and country regulatory agencies determine the channels available to the network.

  Which channel should be used? For access points that are within range of one another, set each one to a different channel to avoid interference from one another. With 802.11b/g networks, typically channels 1, 6, and 11 are selected because they do not overlap, thus ensuring enough frequency separation to avoid collisions; however, other channels may be used by adjacent networks in crowded environments.

  Some access points allow automatic setting of the channel based on what is already in use.

- **Network Name** - the Service Set IDentifier (SSID) is essentially the name of a Wi-Fi network. Some networks broadcast their SSIDs to wireless devices in range. Other networks disable the broadcast of the network's SSID[1]. An example of an of SSID is "WiFiRabbit". Most access points and wireless routers have a default SSID, such as "LinkSys" or "admin". SSIDs are up to 32 bytes long, and may be any binary character; however, it is recommended to use ASCII names to enable operation with buggy implementations.

An access point or wireless router has additional configuration parameters to consider that are the same as those for Ethernet. These options (IP addresses, etc.) are explained in the *TCP/IP User's Manual, Vol 1*.

The most interesting configuration parameters are related to security. The topic of security is discussed in Chapter 4 and Rabbit specific configuration information is given in Chapter 5.

1. This was a feeble attempt at improving security; however, there are far superior ways of restricting access, so now it is recommended to always broadcast the network SSID.

3.2.2 Scanning for a Network

This section discusses what a network scan is and how it is used to join a network. Basically, a scan is a search for available networks within range of the scanning device. To be considered Wi-Fi compatible, a device must be able to scan for available networks. The device can be directed to search on a particular channel or all channels. Likewise, a wireless device can search for a particular SSID or it can be directed to "not care" about the SSID of the network.

Access points transmit management MAC frames called beacons for the purpose of announcing their network to any interested Wi-Fi device in range. Beacon frames are what the wireless device is looking for when it passively scans. Active scanning is used to shorten the time spent waiting for beacons for each potential SSID. Beacons from an AP are typically sent every 100 ms, but an AP will respond immediately to an active probe request from a STA.

Dynamic C comes with a sample program, `WiFiScan.c`, that initiates a scan and reports on up to 16 Wi-Fi networks in range of the wireless Rabbit-based device. This sample program is located in `.../Samples/WiFi/` where Dynamic C was installed. A Wi-Fi scan will briefly interrupt network connectivity, since the scan must iterate through all the available channels.

3.2.3 Wireless Access Points and Routers

This section gives some information about access points and routers used in Wi-Fi networks.

The 802.11 specification defines an access point (or, AP, for short) as a wireless station (STA) that provides access to the distribution service (DS). A wireless router that claims to be 802.11 compliant also provides access to the distribution service because it contains AP functionality. (A full list of the services provided by STAs and APs are listed in Section 2.3.)

3.2.3.1 AP vs. Router

The key difference between an access point and a router is that routers allow wireless clients access to multiple networks and strictly speaking APs allow access to a single network. However, in practice many APs these days have routing capabilities.

Figure 3.2 Typical SOHO Wireless Router

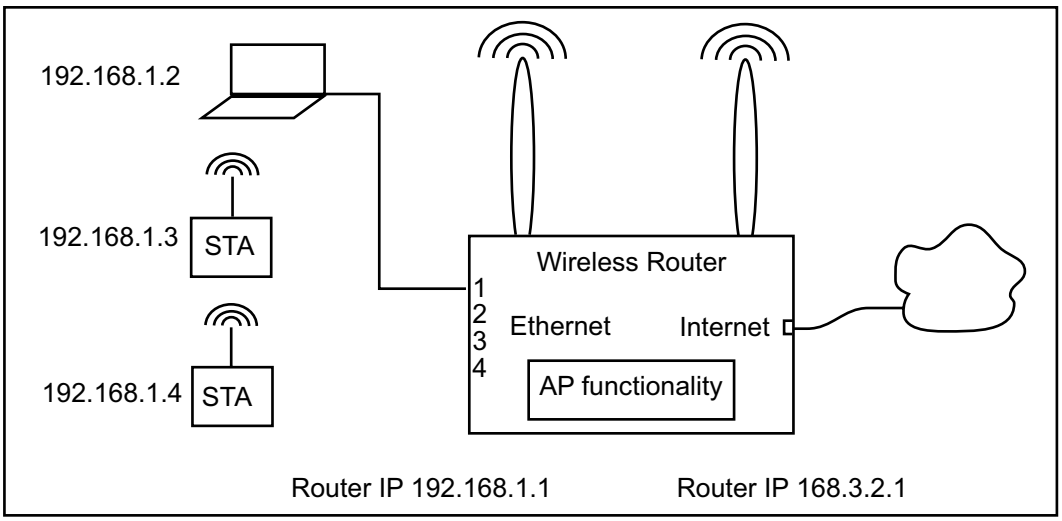


Figure 3.2 shows an AP with routing capabilities that is typically the setup for wireless routers used in small office and home office (SOHO) networks. The subnet addresses fall within the range 192.168.1.x, with a subnet mask of 255.255.255.0. Some high-end routers may support multiple subnets on the Ethernet side, but typically a wireless router has one public IP address on the Internet side and one private (i.e., not routable on the Internet) IP address on the other side.

In Figure 3.2, the box marked “AP functionality” provides the interface between the wireless devices and the wired Ethernet. It could just as easily provide an interface between the wireless devices and PPP or have no bridging responsibilities at all, providing only a controlling function for the wireless devices.

Wireless routers often have more functionality than an access point in addition to being able to route across subnets. Here is a list of possible features a wireless router may implement:

- DHCP Server
- NAT / Firewall Protection
- VPN Pass-Through
- RIP1
- DMZ Support
- Built-in DSL or Cable Modem

There are wireless access points on the market that have some of the added functionality typically associated with routers, such as DHCP servers. See Appendix A.2 for a list of manufacturers of wireless routers and access points.

3.2.3.2 Fat and Thin APs

Fat APs are part of a distributed architecture, in that they operate independently of one another. They are access points that have the full AP functionality physically present in the device. Fat APs have the intelligence to control traffic flow, manage the association of wireless stations, and enforce security policies.

Thin APs are part of a centralized architecture. They function more like Ethernet hubs, having little intelligence themselves and passing responsibility to a central switch or controller.

You might see or hear the terms “fat AP” and “thin AP” used more loosely, namely to differentiate between APs that have lots of features (NAT, VPN, etc.) compared to those that have fewer.

3.2.3.3 AP Client Capacity

The client capacity number you may see on the data sheet of an access point or router is an upper boundary of the number of client associations that an AP allows and does not take into account the various factors that frequently exist in a deployed network that will bring that number down. This section will not discuss the client capacity for specific APs. Instead it will discuss those things that affect the client capacity of APs in general.

There are many factors that taken together determine the number of clients that can simultaneously connect to an access point. Keep in mind, there is a difference between the number of clients that can sustain a connection to an AP and the number of clients that can do so without degrading throughput to an unacceptable degree.The following items can affect the number of client associations:

- *Limit placed by device manufacturer.* The device may have a hard-coded limit on the number of associations that it will allow.
- *Channel capacity.* Since channels are shared resources, the sum of all traffic cannot exceed the channel's capacity.
- *Client-configured security options*. Selecting Open authentication will typically allow for more clients than selecting a configuration that includes TKIP.
- *Application complexity.* Data transactions, bursty in nature, have less stringent requirements for service than the more complex applications, such as video or voice.

The number of clients associated with an AP has a direct impact on the network throughput, since all communication must go through one device. It is well-documented that as the number of client associations increase, aggregate throughput decreases.

3.3 Network Planning and Maintenance

It is straight-forward and relatively easy to join an existing network; for instance, it is easy to go to a cafe and access the Internet using a wireless laptop and the cafe’s WLAN. Deploying your own wireless network requires much more up front work. At minimum, there needs to be consideration of:

- *Physical Location*. The physical location of a wireless network has a major influence on it. Everything from atmospheric conditions to buildings and trees may change the strength and direction of RF signals. Information about the network’s physical location may include such things as floor plans or blueprints. It should also include any available information about other potential networks that are in the same location or range.
- *Coverage Area*. This is the area wherein a client can expect to be able to sustain a connection with an access point at a minimum data rate. RF signal propagation is unpredictable, which makes the coverage area somewhat unpredictable as well. There are differences in the coverage area when the network is outside versus inside. Obstacles and interference affect coverage area, as does the transmit power of the access point.

  The coverage area for the highest link rate is the smallest and for the lowest link rate it is the largest. The coverage area is sometimes referred to as a cell in the wireless LAN.
- *Bandwidth Requirements*. Getting this part of the design right will enhance the experience of using the network. How much bandwidth is required, where is it required, and when is it required, are all questions that need to be answered. Bandwidth is affected by the number of associated stations, client con-

tention, collisions, physical channel errors, application requirements and protocol overhead. Some of these factors can be mitigated, others, such as physical channel errors and protocol overhead, are just the cost of doing business.

- *Security Requirements*. The over-the-air transmissions in wireless networks introduce security risks not present in wired networks. With the release of IEEE 802.11i, there are now strong security options available for Wi-Fi networks. This subject is explored in Chapter 4.

3.3.1 Wireless Site Survey

The purpose of a site survey is to gather information so as to properly position the access points and determine whether any sources of interference are present that will affect performance of the network. A goal of the site survey is to assist in an effective network design that will provide maximum reliable coverage and capacity at minimum cost. Site surveys can also be done after the network is in place, with the goal of troubleshooting or optimization.

A site survey is done by walking around the physical location with a laptop or handheld device like a PDA and running site survey software which measures radio signals and interference. The measurements are taken at different places within the desired coverage area. There are site survey programs available for free download on the web. Some hardware vendors also offer free site survey software with purchase of their hardware. Complete site survey packages can be purchased, along with the services of trained professionals who will do all the work.

The need for a site survey depends on the size of the coverage area, as well as the obstacles and interference that exists there. Medium to large-scale networks will benefit from one, as will networks located in areas with high interference or with demanding application requirements.

3.3.2 Types of RF Interference

There are many factors that can interfere with RF signals in a Wi-Fi network. Networks using the 2.4 GHz band have more potential sources of interference than networks operating in the 5 GHz band. This is because the 2.4 GHz band is more crowded with consumer electronics and has fewer non-overlapping channels than the 5 GHz band.

Items causing RF interference will be identified in a good site survey. The following list includes some known sources of interference:

- Other 802.11 networks.
- Bluetooth devices.
- Consumer electronics: cordless phones, wireless cameras, garage door openers, baby monitors. Older microwaves may cause interference, but in general microwaves are shielded well.
- Building materials: metal, brick, concrete (wood, plaster, and glass don’t affect RF transmissions enough to worry about)
- Environmental factors: dense foliage, large bodies of water, extreme weather.

The fast and continued growth of Wi-Fi and other wireless implementations means that RF interference is a challenge that will only become greater in the years to come. Interference issues should be adequately addressed during the design of the network.

3.3.3 Minimizing or Eliminating RF Interference

IEEE 802.11 does not specify how to deal with interference.

You can minimize or eliminate some sources of interference. The first thing to do is identify all interfering RF signals. This can be done with a site survey, a visual inspection, and/or talking to people in the vicinity. The following list contains some good rule-of-thumb suggestions:

- *AP Position*. Wireless routers and APs should be placed as high as possible. They should be placed as far away as possible from metal, concrete, stone, water heaters, water tanks, large house plants, and even large CD collections.
- *Channel Selection*. Changing the channel for your network may eliminate interference from networks transmitting in your vicinity.
- *Good Cell Coverage.* Ensure the wireless LAN has strong signals throughout the areas where users will need it.
- *Transmit Power Setting*. The transmit power of the AP should be set to reach only the desired coverage area. Besides being less likely to interfere with your neighbors wireless LAN, a smaller coverage area will be less likely to exhibit the hidden node problem. The hidden node problem is when clients on opposite sides of the AP are unable to “hear” one another. This allows the clients to transmit at the same time, thus increasing the chance of a collision.
- *Define an RF Policy.* Where possible, define, and thus limit, the devices allowed in the coverage area. Minimize other wireless devices in the coverage area. For example, newer microwave ovens produce less noise than older models. Ask yourself questions like: is the wireless video camera really necessary or can a wired replacement fit the bill just as well?

3.3.4 Tools and Tasks

Certain tools are necessary in order to maintain a wireless network. You need the ability to capture 802.11 frames and display throughput. You also need test equipment that measures radio parameters, such as SNR.

- Network monitoring - through alerts
- Performance monitoring - review access point activity for average and peak use.
- Inspect APs visually - they are easily moved and may be left in vulnerable positions by 3rd parties

4. WIRELESS LAN SECURITY

Securing communication and services in wireless networks is a complex problem. There are several areas of concern. A wireless device needs to have some way to reliably prove its identity and to reliably confirm the identity of the device on the other end of the connection. Without cables and Ethernet jacks, this is not as straightforward as it once was. The fact that no obvious physical connection is required to send and receive packets brings up questions regarding the ability of others to not only read legitimate packets but also to be able to interject their own. These activities may or may not be malicious, but in all cases they should be handled by the security components of the network.

This chapter presents a description of the different security components, as well as an explanation of how they work together.

4.1 Security Goals and Strategies

There are three goals that must be met to have a successful security strategy in a wireless network:

- Mutual Authentication
- Private Communication
- Data Integrity

The goal of mutual authentication is to make sure that both the client and AP are who they say they are. Both parties have an interest is verifying identities since either side can cause trouble for the other. Typically the AP is a gatekeeper for access to other network resources and regardless of the relative importance of the resource, be it family photos from last year's vacation or the database from a major bank detailing customer account information, access to that resource needs to be controlled by the proper authority.

On the other side, there is a need for the AP to authenticate itself because rogue APs can do substantial damage by stealing passwords from unsuspecting clients and causing denial-of-service attacks.

The goal of privacy addresses the challenge of sending information through open space, which is accessible to everyone, friend and foe alike. Strong encryption algorithms and dynamic key derivation strategies solve this problem. The goal of integrity means that the data is intact when it is received. The protocols used for mutual authentication, privacy and integrity will be discussed in more detail throughout this chapter.

The original IEEE 802.11 specification provided a security strategy known as WEP, which was quickly found to be flawed. Even so, it is discussed in Section 4.2 because it was widely implemented in Wi-Fi networks and is still in use today. Section 4.3 discusses the next generation of security strategies, popularly known as WPA and WPA2. They are both based on the IEEE 802.11i specification. Strictly speaking, the terms WPA and WPA2 are certification programs offered by the Wi-Fi Alliance.

4.2 Wired Equivalency Privacy

The original IEEE 802.11 specification introduced Wired Equivalency Privacy (WEP). As the name implies, WEP was supposed to ensure the same security as exists for a wired connection. Unfortunately, it does not. But even though it is easily broken, WEP is still worth using. Why? Because WEP is broken like a lock is broken after someone kicks in your front door. There is no question that the lock did not keep out the intruder who showed up on your porch, but your garden variety burglar is not that energetic and is looking for an easier mark, someone who has left their door unlocked or even open.

In other words, if WEP is all you have access to, then by all means use it. Meanwhile, be aware that there are several security limitations with this method.

- No mutual authentication - only clients can authenticate, not access points. This can lead to rogue APs.
- No user-level authentication - static WEP key stored on device. This is a problem if the device is stolen or otherwise accessed without permission.
- Reuse of static key - the key used for authentication and encryption is the same.

4.2.1 Authentication Modes

The original IEEE 802.11 specification defined two modes for authentication: Open and Shared Key. A wireless client must select one of these two modes.

- **Open Authentication** - This is basically no authentication. There is no exchange of identifying information before the client is allowed to join the ad-hoc network or associate to the access point in the case of an infrastructure network.
- **Shared Key Authentication** - In this authentication mode, both sides of the connection know the value of a shared secret called a key. Knowledge of the key is delivered by some method outside of 802.11. Shared Key mode requires the use of WEP.

  Please note that Shared Key mode is NOT the same thing as the pre-shared key discussed later in Section 4.3.2.1.

4.2.2 Static WEP Encryption

WEP is used not only for authentication, but for encryption as well. As a matter of fact, the same key is used in both processes.

Encryption is done using a static shared key that is preconfigured on all access points and clients. The process of manual distribution of keys makes changing the key time-consuming and thus likely to be left undone. Using a stale key value increases the risk of eavesdropping and tampering with data.

The standard calls for a 40-bit WEP key, though some implementations now use a 104-bit value. The WEP key is added to a 24-bit initialization vector and so is sometimes referred to as 64- or 128-bit WEP, respectively. The initial 40-bit restriction was due to government rules regarding the export of cryptographic technology. Either way, 40- or 104-bit, the WEP key can be cracked in a short period of time.

4.2.3 Integrity

An Integrity Check Value (ICV), encrypted with WEP, provides data integrity when implementing the original 802.11 specification. The process is based on the CRC-32 algorithm. CRC is excellent at detecting noise and common transmission errors, but not that good as a cryptographic hash. In other words, it protects against random errors, but not malicious attacks.

One of the main problems is that the payload of the wireless frame can be altered undetected without even knowing the WEP key.

4.2.4 Flaws with WEP Authentication and Encryption

The following is a list of known issues that cause WEP to be easily broken or not well-maintained.

- WEP does not provide for mutual authentication.
- The same WEP key is used for authentication and encryption.
- The WEP key (40 bits) is too short to survive a brute force attack, and, in any case, there are known weaknesses in RC4 which makes any key crackable.
- The WEP initialization vector (IV) at 24 bits is too short to avoid collisions within a short time frame. This results in XORed messages with the same IV, giving hackers more information to use in their analysis of plaintext differences.
- WEP does not provide for dynamic key generation and management.
- There is no real data integrity when using a checksum value.

After WEP was recognized as wholly flawed, a new solution was needed to address the security issues that remained. The result was the IEEE 802.11i specification.

4.3 IEEE 802.11i (WPA and WPA2)

Prior to the ratification of 802.11i by the IEEE, Wi-Fi Protected Access (WPA) was released by the Wi-Fi Alliance as a firmware upgrade to WEP-based systems. WPA is based on the third draft of 802.11i, whereas WPA2 is based on the final, ratified version.

Authentication, access control and key management are the same in WPA and WPA2; however, the mechanisms used to ensure data integrity and confidentiality are different.

4.3.1 “802.11 Authentication”

You must use the Open Authentication mode defined in the original 802.11 specification in order to use WPA or WPA2. Shared Key mode requires the use of WEP.

When using WPA or WPA2, the term “802.11 Authentication” is a bit misleading. It’s like walking up to a wall and saying “hello” and someone on the other side says “hello” back. There has been no identification, no exchange of information, nothing except for an informal announcement that you are there and that your existence has been noticed. At this point, 802.11 Open Authentication is complete.

It is also at this point that there are choices as to which way to go. One possibility is to require nothing more. In this case, the wall is gone and the STA has unimpeded access to the services offered by the AP. A

safer choice is to add the authentication protocols defined in 801.11i to run on top of 802.11 Authentication. These protocols are discussed in the next section.

4.3.2 802.11i Authentication Options

The IEEE 802.11i specification defines two modes of operation: “Personal” and “Enterprise.” The authentication method used by a Wi-Fi network differs between these two modes, as shown in Table 4-1.

Table 4-1. Comparison of 802.11i Operation Modes

	Personal Mode	Enterprise Mode
WPA	Authentication: PSK Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC
WPA2	Authentication: PSK Encryption: AES-CCMP	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP

The ability to pre-authenticate to an AP in order to save time is a feature of WPA2, but is not allowed in WPA. Pre-authentication is not covered in this manual.

On the Rabbit, both WPA and WPA2 are supported in Personal mode. Dynamic C 10.54 along with the Rabbit Embedded Security Pack Module version 3.01[1] introduces support for Enterprise mode authentication. Note that Enterprise mode requires a lot more code and memory resources, so it should be used only when required.

Since these security measures have little if any impact on the target network application, it is recommended initially to develop applications with no security options enabled, only enabling the desired options when close to actual deployment.

This is not to say that security should be added as an afterthought in the design cycle, since there are many complex issues to deal with in the initial design, such as certificate and key management. Where possible, there should be as much separation as possible between the core application and the security management, so that each subsystem can be implemented with minimum interference and inconvenience.

1. The version number is written on the label of the software CD.

4.3.2.1 WPA-PSK and WPA2-PSK

When operating in Personal mode, the use of a pre-shared key (PSK) for authentication is mandatory. Knowledge of the PSK is what authenticates the wireless station. This knowledge is gained through the process of both sides using the PSK to generate encryption keys and then being able to successfully encrypt and decrypt their shared communication.

The PSK is generated in a predictable way from a passphrase that can be from 8 to 63 ASCII characters. Alternatively, the PSK can be directly specified as a 32-byte binary number. When composing the passphrase, keep the following suggestions in mind:

- don't use real words (such passphrases can be cracked using a dictionary attack)
- don't use names or dates associated with you (e.g., a pet's name, your child's birthday, etc.)
- use a random combination of case, letters, and digits
- use at least 20 characters
- passphrase-to-PSK generation takes 10's of seconds, so ensure your application generates the PSK only once from the passphrase+SSID and thereafter uses the binary PSK

The pre-shared key is not related to the Shared Key authentication mode, which uses a WEP key. Regardless of whether you are using a WEP key or a WPA PSK, it must be preconfigured on the devices that want to communicate with one another. This means that the key distribution problem is still an issue. This mode of operation is only suitable for smaller networks, and even there, be aware of the temptation to keep stale passphrases for much longer than is advisable.

To encrypt a network with WPA Personal/PSK you provide your AP not with an encryption key, but rather with a passphrase between 8 and 63 characters long or a binary PSK of 256 bits. Using a technology called TKIP (for Temporal Key Integrity Protocol), the PSK is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. (Although WEP also supports passphrases, it does so only as a way to more easily create static keys).

This is a much better scheme overall because even if one key is cracked, it does not compromise the entire session. And the knowledge of individual keys does not reveal the "master key."

4.3.2.2 IEEE 802.1X

When operating in Enterprise mode, IEEE 802.1X provides a framework for port-based access control to wireless network resources. 802.1X is a Layer 2 protocol (i.e., IP addresses have not been assigned yet) whose purpose is to prevent unauthorized access to services offered by a System, such as a Wi-Fi network.

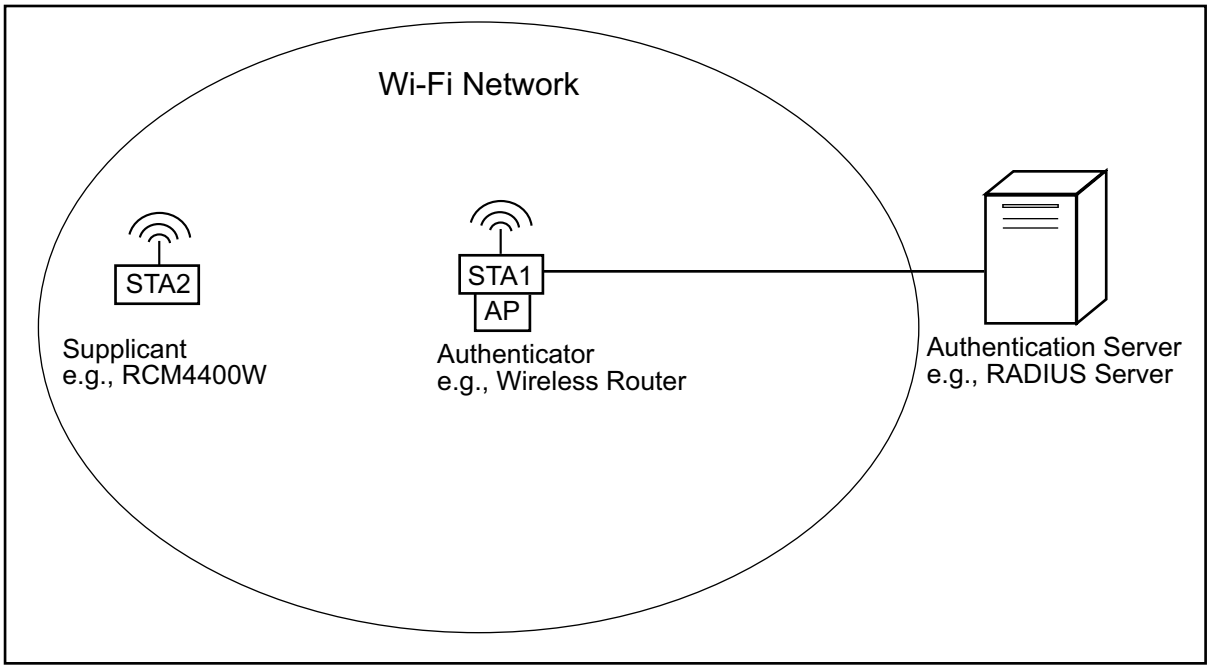
4.3.2.2.1 IEEE 802.1X Architecture

802.1X is composed of three main components:

- Supplicant - this role is adopted by a device that wants to access resources provided by the Authenticator.
- Authenticator - this role is adopted by a device that wants to restrict access to its resources to those wireless stations that can prove their identity.
- Authentication Server - this role is adopted by the device that performs the authentication function that validates the Supplicant's identity.

The Supplicant role and the Authenticator role can be implemented in the same device. Similarly, the Authenticator role and the Authentication Server role can be implemented in the same device. To simplify this discussion, it is assumed that the three roles reside in three different devices, as shown in Figure 4.1.

Figure 4.1 Illustration of IEEE 802.1X Architecture



In a Wi-Fi network, the Supplicant is typically a wireless station attempting to join an infrastructure network. The Authenticator (which is typically an AP) passes authentication communication it receives from the Supplicant to the Authentication Server. The Authentication Server is where the Supplicant's credentials are checked. The result of authentication, success or failure, is passed to the Authenticator. Based on the authentication results, access to the Wi-Fi network is allowed or denied.

4.3.2.2.2 Port-Based Access

802.1X uses the concept of controlled and uncontrolled ports for both the Supplicant and the Authenticator. The controlled port is blocked for regular data traffic until an 802.1X authentication procedure completes successfully on the uncontrolled port.

802.1X is based on EAP (Extensible Authentication Protocol). After an association takes place between two STAs (either peers or an AP and STA) the EAP authentication can be initiated by either the Supplicant or the Authenticator. The Supplicant can send a “Start” packet, which will cause an EAP request from the Authenticator, but the Authenticator may also send an EAP request without receiving a “Start” from the Supplicant.

Figure 4.2 EAP Authentication within 802.1X

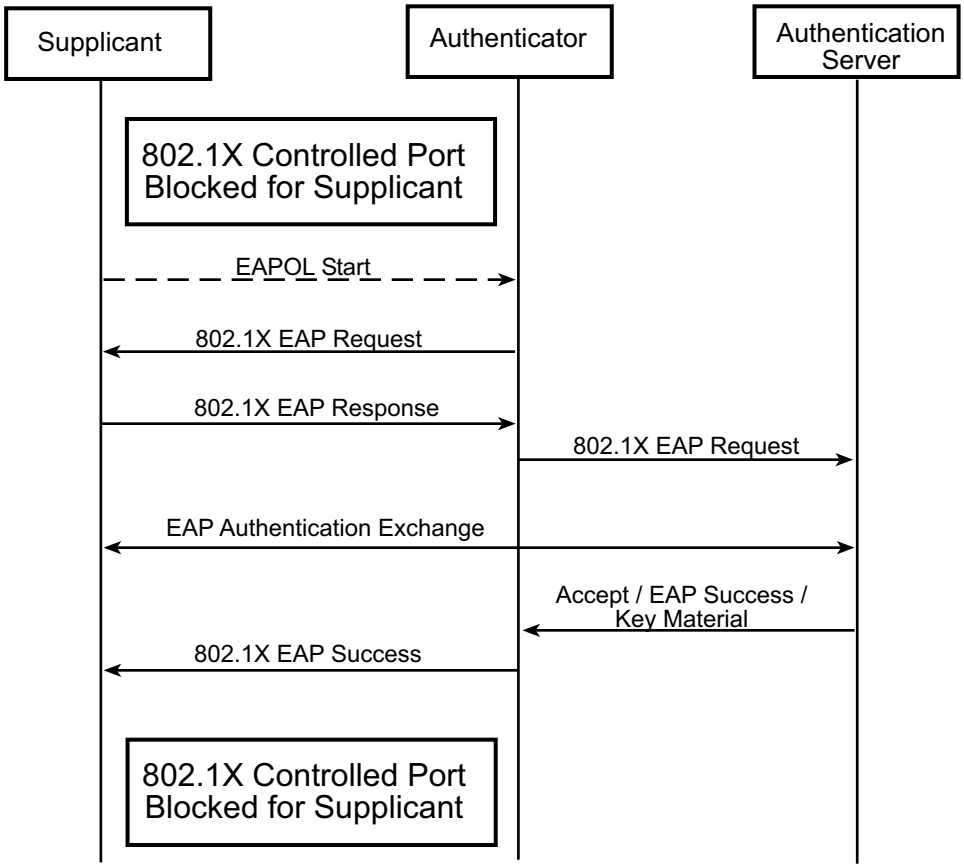


Figure 4.2 follows the EAP authentication process ending in success. As shown, the controlled port is still in an unauthorized state. The 4-way handshake must complete before the entire 802.1X authentication process is complete. Essentially, the 4-way handshake is a series of four messages passed between the Supplicant and the Authenticator for the purpose of:

- confirming freshness of the Pairwise Master Key (PMK)
- exchanging nonces in order to derive fresh Pairwise Transient Keys (PTKs) from the shared PMK
- generating the group temporal key (GTK) if necessary

PMKs, PTKs, and other keys are described in Section 4.3.3.

Note that the PSK bypasses EAP authentication and goes directly to the 4-way handshake. At the end of the 4-way handshake, the Supplicant and the Authenticator have proven their identities to one another in a secure manner, the 802.1X controlled port is now put into an authorized state, which means regular traffic is allowed and both sides have the symmetric transient keys that will be used to encrypt the data.

Details regarding the 4-way handshake can be found in the IEEE 802.11i specification. This four-way handshake occurs whenever you connect to a WLAN using WPA or WPA2. It also occurs periodically thereafter, whenever the AP decides to refresh transient keys.

4.3.2.2.3 Communication Protocols

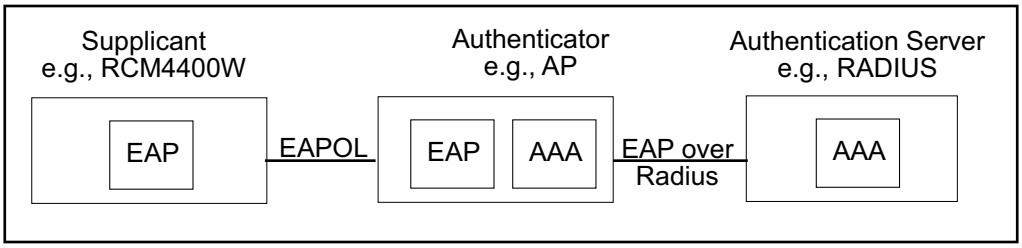
IEEE 802.1X defines an EAP frame that is an encapsulated form of EAP. EAP encapsulation depends on higher-layer transport protocols to travel between source and destination addresses. There are several ways EAP can be encapsulated:

- EAP over LAN (EAPOL)
- EAP over RADIUS

To communicate with the back-end authentication server 802.1X recommends the use of what is called the Authentication, Authorization and Accounting protocol (AAA). The 802.1X specification does not define the AAA protocol; RADIUS, a widely deployed back-end authentication server, is an example of an AAA server.

Figure 4.3 illustrates the relationship between 802.1X devices and the communication protocols they implement.

Figure 4.3 Communication Protocols Used in an 802.1X System



For insomniacs, and other interested parties, details regarding the EAP conversation can be found in both the IEEE 802.1X specification and IETF RFC 3748, the document that defines EAP.

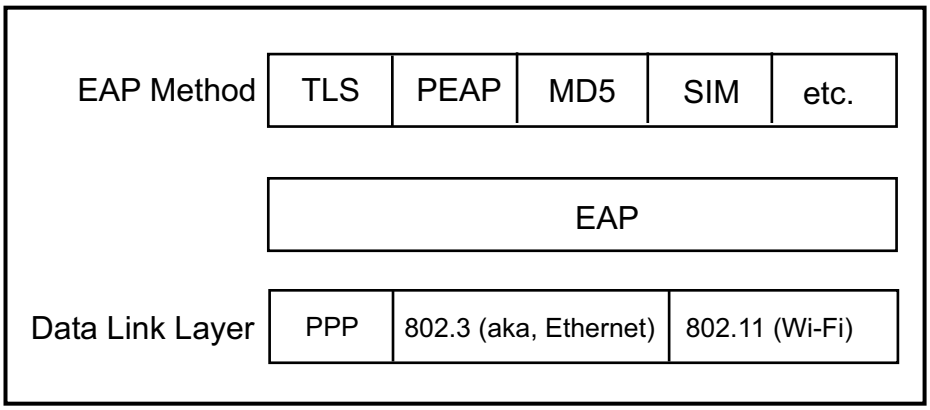
EAP provides an authentication framework, meaning that it does not define how users are authenticated, but provides a means for the actual authentication algorithm to be agreed upon and executed.

4.3.2.3 EAP Methods

EAP authentication algorithms, known as “methods,” are the work horses in this multi-layered security scheme, as they perform the actual authentication and key derivation functions. The different methods correspond to different credential types, such as digital certificates, username/password schemes, token cards, mobile network secrets (GSM and UMTS) and the use of public/private keys.

The chosen EAP method determines if mutual authentication is supported. A list of registered EAP methods can be found at: http://www.iana.org/assignments/eap-numbers. Not all EAP methods are appropriate for wireless networks. The requirements for EAP methods when used in wireless LANs are stated in RFC 4017. The credential types need not be symmetrical for mutual authentication between two wireless stations to succeed. An EAP method that defines key derivation must do so either directly in its specification or thru a reference to another specification. Any method that defines key derivation, must also support mutual authentication.

Figure 4.4 EAP Architecture



Many of the EAP methods use a client/server model of communication, which basically means that an application on one device, the client, makes a request from an application on the another device, the server.

When discussing mutual authentication of client and server in an 802.1X system, please note that the server that is being authenticated is the device known as the Authenticator. This is true even if the Authenticator is acting as a pass-thru device, as shown in Figure 4.1.

Section 4.3.2.3.1, “EAP-TLS” and Section 4.3.2.3.2, “PEAPv0/EAP-MSCHAPv2” discuss two popular client/server methods, both of which will be supported by Wi-Fi Rabbits.

4.3.2.3.1 EAP-TLS[1]

EAP used with Transport Level Security (TLS) is widely deployed in wireless devices. It is considered among the most secure methods available.

Some of the EAP-TLS security claims are:

- Mutual Authentication with Public-Key Cryptography
- Protected Ciphersuite Negotiation
- Key Management Capabilities

Mutual Authentication with Public-Key Cryptography

EAP-TLS implementations must support TLS v1.0, a certificate-based authentication protocol. In this EAP method, digital certificates are used for authentication of both client and server. This method binds a trusted identity with a public key. The public key is then used by others to encrypt messages to be sent back to the owner of the public key, the only entity that possesses the private key which will decrypt the message.

A good description of how a digital certificate works to ensure the identity of its owner is available at: http://en.wikipedia.org/wiki/Public_key_certificate.

For readers interested in more information about certificates, the *Rabbit Embedded Security Pack Manual* discusses details about the underlying theory such as the trust model, as well as the more hands-on matters of certificate creation and distribution.

Protected Ciphersuite Negotiation

The security claim of protected ciphersuite negotiation refers to the ability of the EAP method to negotiate the ciphersuite used to protect the EAP conversation, as well as to protect the integrity of said negotiation.

Protected ciphersuite negotiation is not related to negotiation of ciphersuites for encrypting application data after the authentication process has completed, i.e., regular data traffic. The 802.11 Beacon and Probe Response frames sent by APs state the security parameters available, including the ciphersuites used for encrypting application data, (such as TKIP and CCMP). Agreement about which security parameters to use is implied as each side in the 802.11 association responds by continuing the conversation after receiving the security parameters offered by the other side.

1. Defined in RFC 2716bis, which obsoletes RFC 2716

Key Management Capabilities

As part of the TLS handshake, the client generates a pre-master secret and encrypts it with the server's public key. Since only the server can decrypt the pre-master secret, the client (Supplicant) and server (Authentication Server) both generate a shared master secret from it. The master secret ultimately yields the following cryptographic parameters:

- MSK - Master Session Key, also known as the AAA-key. See Figure 4.5.
- EMSK - Extended Master Session Key, reserved for future use.
- IV - Initialization Vector, only needed for bulk ciphers.

After EAP authentication succeeds, the Authentication Server exports the MSK and IV (if created) to the Authenticator.

4.3.2.3.2 PEAPv0/EAP-MSCHAPv2

The same processes defined in the TLS protocol that are made use of by EAP-TLS also apply to PEAPv0/EAP-MSCHAPv2; namely:

- Mutual Authentication using Asymmetric Methods
- Protected Ciphersuite Negotiation (see Section 4.3.2.3.1)
- Key Management Capabilities (see Section 4.3.2.3.1)

For the sake of brevity, PEAPv0/EAP-MSCHAPv2 is commonly referred to as PEAP,[1] in this document and elsewhere. EAP-MSCHAPv2 is also known as "Microsoft Challenge Handshake Protocol."

Note that there is a version number after "PEAP." The same PEAP version number must be installed on all 802.1X devices. The is important because different versions are not compatible. For example, if only PEAPv0 is installed on the client and only PEAPv1 is installed on the AP, these two devices will not work together. Note that this does not mean that PEAP clients and servers can not each support multiple versions of the protocol. For example, if the client has only PEAPv0 installed and the AP has PEAPv0 and PEAPv1, communication can occur using PEAPv0 on both devices.

Mutual Authentication using a Server Certificate and Username/Password

PEAP is a two-step process. Step one is the creation of an outer authentication method, which is always a TLS tunnel. Step two is the inner authentication method that will make use of the TLS tunnel. The inner authentication method has to be an EAP method. The forward slash in the method name separates the outer method from the inner method; i.e., outer_method/inner_method.

This strategy creates an encrypted channel (which is the outer authentication method) that enables the use of an inner authentication method that will be made much more secure because it is traveling on an encrypted channel. Passive eavesdropping is a serious and common threat on wireless devices. The use of PEAP allows enterprises to make use of existing resources like the well known password-based login.

1. Strictly speaking, PEAP stands for Protected EAP. This acronym turned word is also used to refer to PEAPv1/EAP-GTC, etc.

The server authenticates itself to the peer using a digital certificate in the same manner as EAP-TLS. But unlike EAP-TLS, the peer uses another EAP type to authenticate itself to the server, in this case MS-CHAPv2. This is a challenge-based username/password authentication protocol. It allows a user to access the network from any client machine as long as they know a valid username/password. This method can be useful in its convenience, but is vulnerable if the username/password is compromised.

This brings up at least two questions for an embedded applications engineer:

1. How does the embedded application come into possession of the username/password?
2. Is it better to authenticate users or devices?

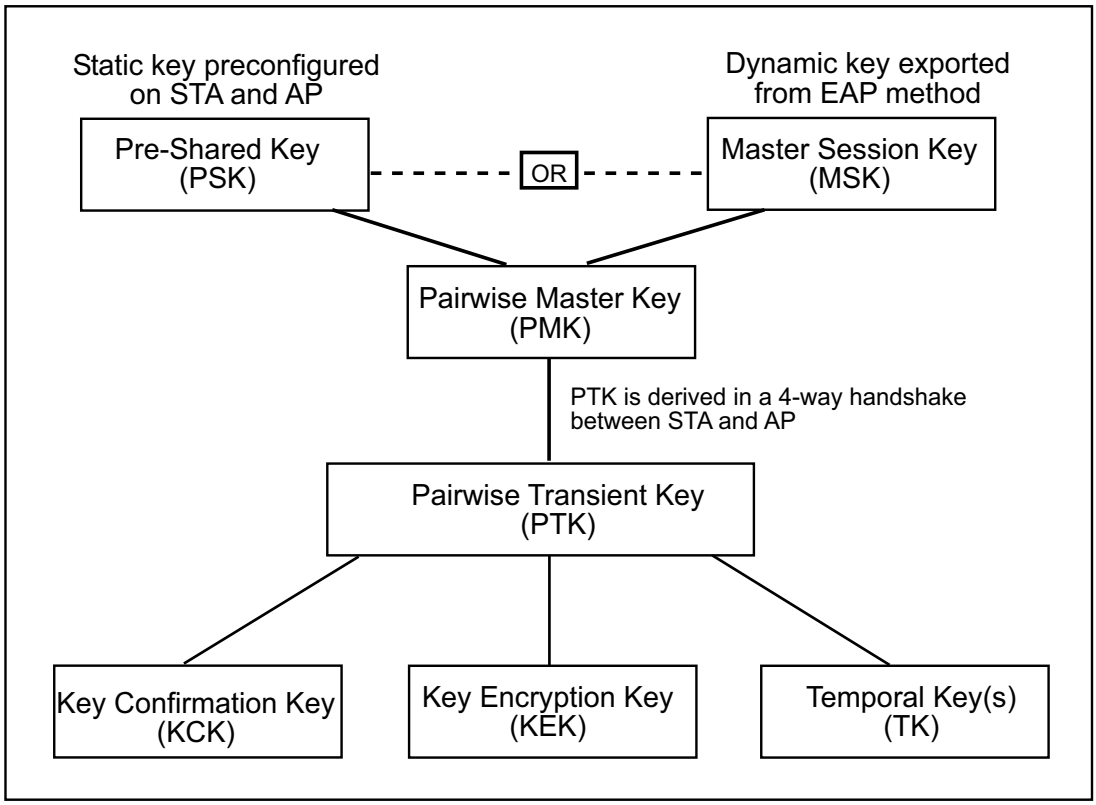
The answer to both of these questions is that it depends. It depends on the application and other system constraints. For example, if the embedded device is in a location that is easy to access, it might have any number of interfaces (touch screens, keypads, etc.) that allow users to easily input their credentials. If the device is not easily accessible, it might make more sense, for some situations, to authenticate the device instead of individual users. These considerations are beyond the scope of this manual given the diversity of the applications market.

4.3.3 802.11i Encryption and Data Integrity Options

The flaws with encryption and data integrity that exist when using WEP have all been addressed in the IEEE 802.11i specification, with both WPA and WPA2. The specific algorithms for these two standards are discussed in Section 4.3.3.1 and Section 4.3.3.2.

The authentication framework used by WPA and WPA2 is the same and thus the key derivation scheme that provides keying material for encryption is similar. The cipher keys used in the encryption protocols are derived from the Pairwise Master Key (PMK). This keying material is derived from either a statically defined pre-shared secret or a dynamically derived value that was exported during the EAP authentication process. A high-level look at the unicast key derivation is shown in Figure 4.5. Keys are also derived for multicast and broadcast packets, but that is not shown in the figure.

Figure 4.5 Wi-Fi Key Hierarchy



PSKs allow both the supplicant and the authenticator to share a common, statically configured key. Like static WEP keys, if a device is compromised, all wireless devices will have to be re-configured with a new key. But, unlike static WEP keys, using the PMK to derive a PTK eliminates the need for every device to use the same encryption key.

The keys shown at the bottom of Figure 4.5 are used during the 4-way handshake (KCK, KEK) and for data encryption (TK).

Encryption and data integrity methods differ between WPA and WPA2. WPA encryption is based on the RC4 stream cipher but with some major improvements over how it was employed by WEP. WPA2 encryption is based on the 128-bit block cipher AES, which is cryptographically stronger than RC4.

4.3.3.1 WPA

The original motivation for WPA was that it could replace WEP with only a firmware upgrade. This worked well with large number of legacy devices running WEP that would otherwise have needed a hardware upgrade to run WPA2.

4.3.3.1.1 TKIP

Temporal Key Integrity Protocol (TKIP) is mandatory for WPA implementations. It is optional for a WPA2 implementation. Even though TKIP is based on RC4, the same cipher used by WEP, it is a superior security protocol.

Table 4-2. Reasons TKIP is Better than WEP

WEP Weakness	TKIP Strength
Short IV, only 24 bits.	Longer IV, 48 bits
Static pre-shared key used for all frames pertaining to a connection	Dynamically derived keys used on a per-frame basis.
No replay protection	IV is used as a frame counter to provide replay protection.
Uses same pre-shared key for authentication and encryption.	Pre-shared keys (always 256 bits in length) are used to generate Pairwise Transient Keys (PTKs) instead of being used directly for encryption.
Inadequate data integrity algorithm.	Uses a Message Integrity Code (MIC) for data integrity.

Ciphers use very long pseudo random sequences. However, the sequences are not truly random. They follow a predefined deterministic pattern so that the receiver can predict the next number and thus decode the data in the channel. Because the sequence is not truly random, statistical analysis can be used to crack the code if enough packets are collected.

The WEP implementation seeds RC4 with a static key that stays the same for the entire connection. It is only a matter of time before the code is cracked. In fact a 40-bit key can be discovered in seconds. The 104-bit key takes a little longer.

The TKIP implementation does not use a static key and therefore an eavesdropper is unable to collect enough packets to expose the key value. The only vulnerability so far is a dictionary attack, which fails if the passphrase is sufficiently robust.

Although there are no known successful attacks on TKIP using 802.1X and RADIUS, there may be applications that require an even higher level of security. The AES-based encryption used in WPA2 is considered among the most secure encryption algorithms available today.

4.3.3.1.2 Michael

TKIP includes a Message Integrity Check (MIC) named Michael. Michael is a one-way cryptographic hashing algorithm, sometimes referred to as a keyed hash function.

The original WEP design did not protect against packet forgeries and other active attacks. According to the IEEE 802.11i specification, the vulnerabilities that existed under WEP include:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

Michael does not thwart these attacks by itself; however, a MIC failure is always noticed and allows TKIP to enact countermeasures, such as alerting the system administrator, changing the PTK or even shutting down the network.

4.3.3.2 WPA2

WPA2 is based on the final draft of the IEEE 802.11i specification. At the time of this writing, it is the strongest wireless security standard available.

WPA2 includes an Intrusion Detection System (IDS)[1] which protects against Denial-of-Service attacks.

4.3.3.2.1 CCMP

Counter Mode (**C**TR) with **C**BC-**M**AC **P**rotocol (CCMP) is mandatory for WPA2[2]. It is also one of the more confusing acronyms we have. CTR is the first "C" in CCMP; it refers to an operating mode of AES. AES is the cipher used in place of RC4. It is considered one of the most secure bulk data encryption algorithms available. The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity and authentication.

In summary:

- For encryption: CCMP uses AES operating in counter mode
- For packet authentication and integrity: CCMP uses CBC-MAC

4.4 Security Trade-Offs

As with all things, there is a trade-off to be made between security (good) and overhead (bad). Getting the balance right requires careful consideration of the goals of the system and the price which the end user is willing to pay to achieve those goals.

1. IDS is unrelated to the Tamper Detect feature that was introduced in the Rabbit 4000 microprocessor.
2. TKIP is optional for WPA2.

5. RABBIT WI-FI CONFIGURATION

This chapter contains information about configuring Rabbit-based boards that have Wi-Fi interfaces. There are a variety of options that must be chosen carefully to match the security and performance criteria of the embedded application, bearing in mind that the deployment environment of the Wi-Fi network will affect both security and performance.

5.1 Hardware and Software Requirements

To exercise the Wi-Fi components of a Rabbit-based board there needs to be another wireless device with which to communicate. Either the Rabbit will be part of an ad-hoc network or an infrastructure network.

This means that beyond a host machine running Dynamic C 10.xx or later and a Rabbit-based target board with a Wi-Fi interface, you will need another wireless station (e.g., a laptop) to create an ad-hoc network. An access point is needed to create an infrastructure network. Remember that all wireless devices on the same network must have compatible 802.11 extensions. For example, an 802.11a access point will not be seen in a scan by a 802.11b device. Compatible interfaces does not necessarily mean using the same 802.11 extension. For example, 802.11g devices can understand transmissions from 802.11b devices.

5.2 Configuration Macros and Default Conditions for Wi-Fi Rabbits

As mentioned in a previous chapter, all sample programs for Ethernet-enabled Rabbits will run on Wi-Fi Rabbits. The same library, `/Lib/Rabbit4000/tcpip/tcpconfig.lib`, serves to configure both types of interfaces using the same macro, namely `TCPCONFIG`.

Most Wi-Fi applications will define `TCPCONFIG` to "1" to use static IP addresses or "5" to use DHCP. If `TCPCONFIG` is not defined, it will default to "0" with the assumption that all configuration will be done at runtime. From within Dynamic C, pressing Ctrl+H with the cursor on `TCPCONFIG` will bring up a description of all its pre-defined values, which will include PPP interfaces and custom configurations.

Starting with Dynamic C 10.40, a number of configuration macros were deprecated, with appropriate warnings given when they are encountered during compilation. The remainder of this section categorizes and lists the configuration macros required for a Wi-Fi application, along with any default values.

5.2.1 TCP/IP Parameters

As with an Ethernet interface, a Wi-Fi interface is configured with a netmask and some static IP addresses for the device, the gateway and possibly a DNS server. The corresponding configuration macros are:

_PRIMARY_STATIC_IP (default "10.10.6.100")
This macro is the IP address of the host, i.e., the Rabbit target. If DHCP is enabled, this address can be used as a fallback address in case of DHCP failure.

_PRIMARY_NETMASK (default "255.255.255.0")
This macro is the netmask, the part of the address that distinguishes machines on the host's network from machines on other networks.

MY_GATEWAY (default "10.10.6.1")
This macro is the IP address of the router that connects the host's network to the rest of the world.

MY_NAMESERVER (default "10.10.6.1")
This macro is the IP address of the host's DNS server.

5.2.2 Wi-Fi Specific Parameters

The macros described in this section are only useful with a Wi-Fi interface. They set critical parameters that determine with which network the Rabbit will associate. Also, some of the configuration macros affect performance in busy or noisy environments.

IFC_WIFI_MODE (default `IFPARAM_WIFI_INFRASTRUCTURE`)
This macro selects the operating mode for the network; either infrastructure or ad-hoc. Valid values are:

- `IFPARAM_WIFI_ADHOC` - In this mode, the Rabbit can create an ad-hoc network or can associate with another STA within range that is already part of an ad-hoc network. Currently, WEP cannot be used in ad-hoc networks.
- `IFPARAM_WIFI_INFRASTRUCTURE` - In this mode, the Rabbit can associate with an access point within range.

IFC_WIFI_SSID (default "rabbitTest")
This macro is the Service Set Identifier (SSID), which is also considered the network name. An empty string will allow the Rabbit to associate with a network regardless of its SSID. SSIDs are up to 32 bytes long and may be any binary string, which can include any byte value (including non-printable characters and null). The recommendation is to use ASCII text strings for compatibility with other wireless devices.

All other devices on your wireless network (including your access point or wireless router) must have the exact same SSID.

IFC_WIFI_CHANNEL (default 0)

This macro identifies the channel the network uses for its wireless communication. The default value of 0 allows the Rabbit to associate with a network communicating on any valid channel, and so is usually appropriate in an infrastructure network because which channel is being used is determined by the AP.

In an ad-hoc network, setting this macro is mandatory. If you set it to 0, the Rabbit will keep scanning until it finds an existing ad-hoc network with the matching `IFC_WIFI_SSID`. In this case, you must set at least one STA to a definite channel, otherwise all STAs will search forever, with no STA able to make the decision as to which channel to use.

In addition to 0, the valid channel values for this macro are:

- 1-11 in North America
- 1-13 in Europe
- 1-14 in Japan (the RCM4400W cannot access channel 14)

Valid channels depend on the region selected by `IFC_WIFI_REGION`.

IFC_WIFI_REGION (default `IFPARAM_WIFI_REGION_AMERICAS`)

This macro limits the channel range and maximum transmit power to be consistent with the restrictions of the selected regulatory region. Valid parameters for this command are listed below, along with the channel ranges and maximum transmit power allowed for each region:

- `IFPARAM_WIFI_REGION_AMERICAS` - Americas, including the US (ch. 1-11, <20 dBm)
- `IFPARAM_WIFI_REGION_AUSTRALIA` - Australia (ch. 1-11, <16 dBm)
- `IFPARAM_WIFI_REGION_CANADA` - Canada (ch. 1-11, <20 dBm)
- `IFPARAM_WIFI_REGION_CHINA` - China (ch. 1-11, <16 dBm)
- `IFPARAM_WIFI_REGION_EMEA` - Europe, Middle East, Africa (ch. 1-13, <16 dBm)
- `IFPARAM_WIFI_REGION_FRANCE` - France (ch. 10-13, <16 dBm)
- `IFPARAM_WIFI_REGION_ISRAEL` - Israel (ch. 3-11, <16 dBm)
- `IFPARAM_WIFI_REGION_JAPAN` - Japan (ch. 1-13, <14 dBm)
- `IFPARAM_WIFI_REGION_MEXICO_INDOORS` - Mexico indoors (ch. 1-11, <16 dBm)
- `IFPARAM_WIFI_REGION_MEXICO_OUTDOORS` - Mexico outdoors (ch. 9-11, <16 dBm)

Running the sample program `\Samples\WiFi\Regulatory\region_compiletime.c` will list the maximum transmit power allowed based on both regulatory region and board type.

IFC_WIFI_ROAM_BEACON_MISS (default 20)

This macro sets the number of beacons that must be missed contsecutively in order to trigger scanning for a better access point, i.e., one with a stronger signal.

IFC_WIFI_ROAM_ENABLE (default 1**)**

This macro turns roaming on or off. Roaming is enabled when the macro is defined to 1.

IFC_WIFI_FRAG_THRESHOLD (default 0, no fragmentation)
This macro sets the fragmentation threshold. Frames (or packets) that are larger than this threshold are split into multiple fragments. This can be useful on busy or noisy networks. The value of this macro can be between 256 and 2346, or 0 for no fragmentation.

IFC_WIFI_RTS_THRESHOLD (default 2347, no RTS/CTS)
This macro sets the RTS threshold, which is the frame size at which the RTS/CTS mechanism is used. This is sometimes useful on busy or noisy networks, but should be weighed against the increased overhead. The value of this macro can be between 1 and 2347.

5.2.3 Security Configuration Macros

The configuration macros described in this section enable authentication and encryption protocols. The macros supported by Dynamic C 10.54 and later versions that control Enterprise mode authentication are not described here; interested readers should refer to the *TCP/IP User's Manual Vol. 1* and the *Rabbit Embedded Security Pack Manual*. Both documents are available online from this page:

www.rabbit.com/products/dc/docs.shtml

WIFI_USE_WPA (defaults to undefined)
This macro is required for WPA and WPA2. Defined by itself, it will enable WPA with TKIP encryption.

```
#define WIFI_USE_WPA
```

WIFI_AES_ENABLED (defaults to undefined)
This macro when defined with WIFI_USE_WPA will enable WPA2 with CCMP encryption.

```
#define WIFI_USE_WPA
#define WIFI_AES_ENABLED
```

IFC_WIFI_AUTHENTICATION (default IFPARAM_WIFI_AUTH_ANY)
This macro specifies the authentication mode to use for this Wi-Fi network. It accepts a combination (with multiple values OR'd together) of the following values:

- IFPARAM_WIFI_AUTH_ANY - Use any available method.
- IFPARAM_WIFI_AUTH_OPEN - Use 802.11 Open Authentication mode.
- IFPARAM_WIFI_AUTH_SHAREDKEY - use 802.11 Shared Key authentication mode; requires the use of a WEP key. See the IFC_WIFI_WEP_* commands below for instructions on setting WEP keys.

If you #define WIFI_USE_WPA, more authentication methods are available:

- IFPARAM_WIFI_AUTH_WPA_PSK - use WPA-PSK; operating in 802.11i Personal mode requires the use of WPA-PSK for authentication. See the IFC_WIFI_WPA_PSK_* commands below for instructions for setting the pre-shared key.
- IFPARAM_WIFI_AUTH_WPA_8021X - use 802.11i Enterprise mode. This authentication operating mode is available with the Rabbit Embedded Security Pack.

The default value of “use any method” means that if the Rabbit associates with a wireless device that only implements WEP, then that is the method that will be used. Have the following code in your application:

```
#define WIFI_USE_WPA
#define IFC_WIFI_AUTHENTICATION IFPARAM_WIFI_AUTH_WPA_PSK
```

to limit the Rabbit’s associations to those devices that have better security than WEP.

IFC_WIFI_ENCRYPTION (default `IFPARAM_WIFI_ENCR_NONE`)
This macro specifies the type of encryption used. It accepts the parameters listed here. Multiple parameters may be OR’d together.

- `IFPARAM_WIFI_ENCR_ANY` - use any type of encryption.
- `IFPARAM_WIFI_ENCR_NONE` - no encryption used, this is the default condition. Currently, this option is required for ad-hoc networks.
- `IFPARAM_WIFI_ENCR_WEP` - use WEP encryption (see `IFC_WIFI_WEP_KEYNUM`, etc., to set WEP keys).

Define the macro `WIFI_USE_WPA` to compile in code for WPA.

- `IFPARAM_WIFI_ENCR_TKIP` - use TKIP encryption (WPA)

Define both `WIFI_USE_WPA` and `WIFI_AES_ENABLED` to compile in code for WPA2.

- `IFPARAM_WIFI_ENCR_CCMP` - use CCMP encryption (WPA2)

> **NOTE:** TKIP and CCMP are not supported in ad-hoc mode.

IFC_WIFI_WEP_KEYNUM (default 0)
This macro selects the WEP key to use for encryption. Valid values are 0, 1, 2, or 3, corresponding to the key set by `IFC_WIFI_WEP_KEYx_HEXSTR` or `IFC_WIFI_WEP_KEYx_BIN`. See the WEP key macros below; one or more need to be defined to make use of `IFC_WIFI_WEP_KEYNUM`.

IFC_WIFI_WEP_KEY0_BIN
IFC_WIFI_WEP_KEY1_BIN
IFC_WIFI_WEP_KEY2_BIN
IFC_WIFI_WEP_KEY3_BIN (defaults to undefined)
These macros set the WEP keys to use for WEP encryption. These keys can be either 40-bit or 104-bit (i.e., 5 bytes or 13 bytes). They must be defined as a comma-separated list of byte values. At least one of the WEP key macros must be defined in order to use WEP encryption. Specifically, the WEP key selected (`IFC_WIFI_WEP_KEYNUM`) must be defined and it must match the key used on all other devices in the network.

IFC_WIFI_WEP_KEY0_HEXSTR
IFC_WIFI_WEP_KEY1_HEXSTR
IFC_WIFI_WEP_KEY2_HEXSTR
IFC_WIFI_WEP_KEY3_HEXSTR (defaults to undefined)

These macros set the WEP keys to use for WEP encryption. These keys can be either 40-bit or 104-bit (i.e., a string of either 10 or 26 hex characters). At least one of the WEP key macros must be defined in order to use WEP encryption. Specifically, the WEP key selected (`IFC_WIFI_WEP_KEYNUM`) must be defined and it must match the key used on all other devices in the network.

If both `IFC_WIFI_WEP_KEY#_HEXSTR` and `IFC_WIFI_WEP_KEY#_BIN` are defined for a particular key, the HEX version will be used.

Example of setting a 13-byte key via a hex string:

```
#define IFC_WIFI_WEP_KEY0_HEXSTR "0123456789abcdef0123456789"
#define IFC_WIFI_WEP_KEYNUM 0
```

Example of setting a 5-byte key via a hex string:

```
#define IFC_WIFI_WEP_KEY1_HEXSTR "0123456789"
#define IFC_WIFI_WEP_KEYNUM 1
```

Example of setting a 13-byte key via an array of bytes:

```
#define IFC_WIFI_WEP_KEY2_BIN \
0x01,0x23,0x45,0x67,0x89,0xab,0xcd,0xef,0x01,0x23,0x45,0x67,0x89
#define IFC_WIFI_WEP_KEYNUM 2
```

Example of setting a 5-byte key via an array of bytes:

```
#define IFC_WIFI_WEP_KEY3_BIN 0x01,0x23,0x45,0x67,0x89
#define IFC_WIFI_WEP_KEYNUM 3
```

IFC_WIFI_WPA_PSK_HEXSTR

This macro sets the WPA pre-shared key value using a 64-char hex string.

IFC_WIFI_WPA_PSK_PASSPHRASE

This passphrase is hashed with the target SSID to generate the 64-char hex string for the WPA PSK.

WPA (TKIP) and WPA2 (CCMP) encryption both require a passphrase or a key. This macro allows you to define a passphrase with an ASCII string. The Wi-Fi driver will expand the passphrase into a key using a standard algorithm. This process takes up to about 20 seconds. The same passphrase must be configured on all devices on the same Wi-Fi network.

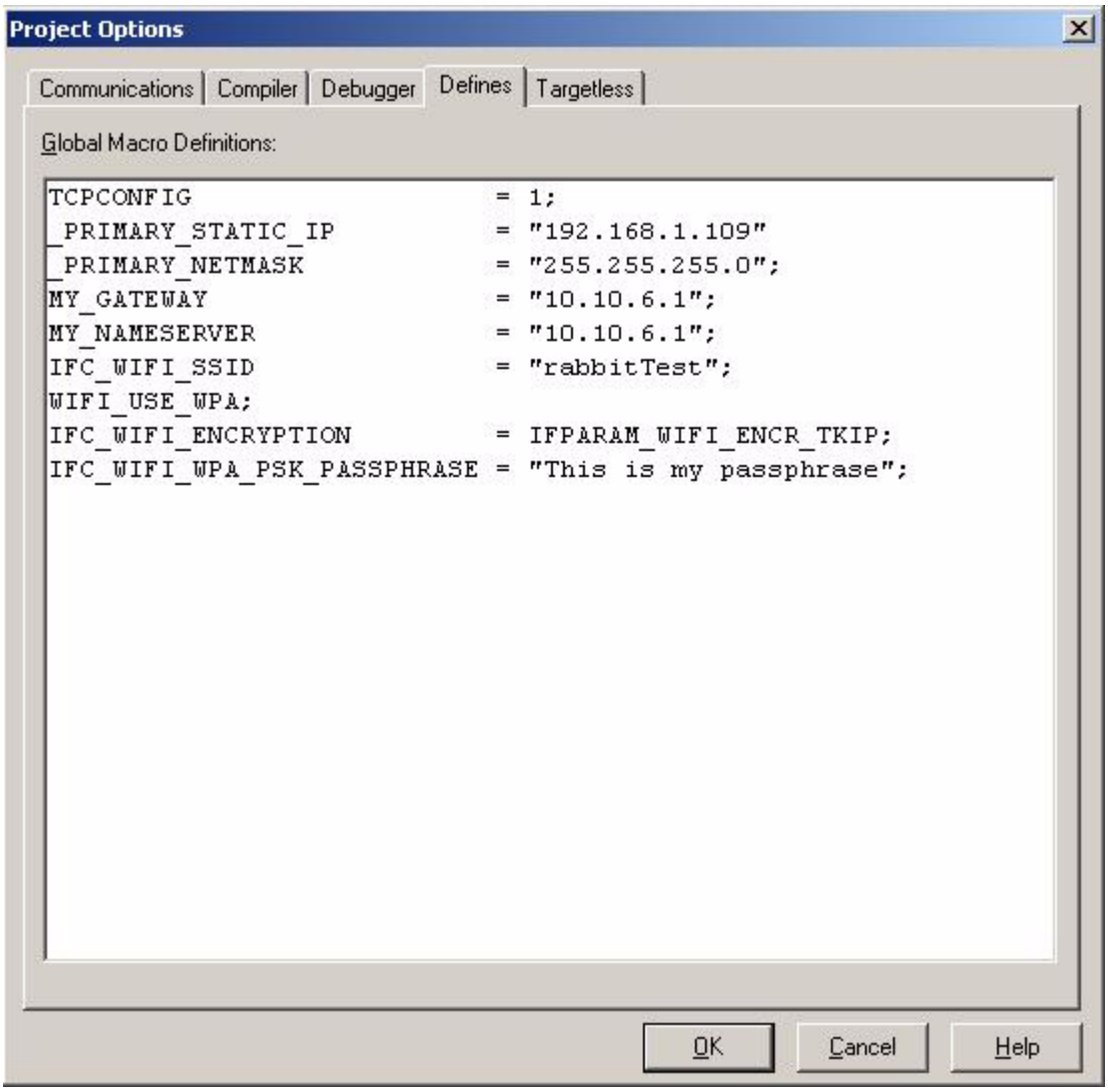
Given the considerable length of time it takes to create the PSK from the passphrase, you should use `IFC_WIFI_WPA_PSK_HEXSTR` instead of `IFC_WIFI_WPA_PSK_PASSPHRASE` to set the key.

5.3 Compile-Time Configuration

As described in Section 5.2 many configuration macros are given default values in `tcpconfig.lib`. These macros can be overridden at compile time by defining them in the “Defines” tab of Dynamic C or from within the application program before the #use "dcrtcp.lib" line.

The example in Figure 5.1 shows how to override the default configuration values using the “Defines” tab.

Figure 5.1 Infrastructure, WPA/TKIP Encryption



Note that several of the configuration macros (`IFC_WIFI_ROAM_ENABLE`, etc.) are missing in the above example because the default values were used. Also note that you can choose to use the hex value of the passphrase.

There are various websites that will take an SSID and passphrase and will calculate the value of the hex key. This website: http://www.wireshark.org/tools/wpa-psk.html, was used to create a hex key for the Wi-Fi network described in Figure 5.1.

To specify the hex key for “rabbitTest” with the passphrase “This is my passphrase” add the following line in the “Defines” tab in place of IFC_WIFI_WPA_PSK_PASSPHRASE:

```
IFC_WIFI_WPA_PSK_HEXSTR =
"ab66b943ae08979d83e9d42dc8f5e67d4504d61ae415590436f917d146ed9497";
```

It is important to type the SSID and passphrase in accurately; the smallest difference will change the generated hex value. For example, using the same SSID (rabbitTest) but with two spaces after “This” and before “is” in the passphrase, resulted in a different hex value being generated:

```
"acd499971c0a6fd85ea551d07ca0065d62592816ad228afc16f93573bf88915b"
```

The reason to use a hex value for the PSK instead of a passphrase is to save time during the association/authentication process. Although passphrases are easier to type, it takes 15-17 seconds (15 on RCM4400W, 17 on RCM5400W) to calculate the PSK using a passphrase. However, long hex values are difficult to remember and to type without error, which is not the case with a passphrase.

5.4 Runtime Configuration

Prior to Dynamic C 10.40, Wi-Fi configuration options were set at runtime using the wifi_ioctl() function. This function is thoroughly documented in the *TCP/IP User’s Manual, Vol 1* and also via the Function Lookup feature in Dynamic C. wifi_ioctl() is deprecated starting with Dynamic C 10.40 in favor of the general configuration function ifconfig().

The first parameter for ifconfig() identifies an interface. Subsequent parameters are predefined commands that are polymorphic (like printf() parameters). Many of the commands themselves take parameters. Multiple commands may be passed in a single call to ifconfig() using a comma-separated list. The list must be terminated using the command IFS_END, even if there is only one command in the list. For example, the following line enables DHCP services on the Wi-Fi interface:

```
ifconfig(IF_WIFI0, IFS_DHCP, 1,IFS_END);
```

Some of the ifconfig() commands require that the interface be brought down beforehand. The code below shows one way of ensuring that the interface is completely down.

```
ifdown(IF_WIFI0);
while (ifpending(IF_WIFI0) != IF_DOWN) {
   printf(".");
   tcp_tick(NULL);
}
printf("...Done.\n");
```

If the interface is brought down temporarily, it will be brought up again before return; however, any open sockets will have been aborted.

The Wi-Fi specific commands for ifconfig() are listed in Section 5.4.1, along with any parameters, default values or conditions that apply.

5.4.1 Wi-Fi Commands for ifconfig()

The naming convention is `IFS_WIFI_*` for setting Wi-Fi configuration options with `ifconfig()` at compile time. Almost all "set" commands have a counterpart of the form `IFG_WIFI_*` that gets the current settings for the selected configuration option.

The `ifconfig()` commands for Wi-Fi configuration are grouped below by category.

5.4.1.1 Basic Network Configuration

There are three configuration options that largely define and characterize a Wi-Fi network. They are the SSID, the communication channel and the operating mode. All of these commands require that the interface be brought down.

IFS_WIFI_SSID

Sets the SSID (i.e., network name); takes two parameters, length and buffer. Since the SSID can contain any byte (including nulls), it's necessary to provide the length along with the SSID. The maximum length for an SSID is 32 bytes.

See the Dynamic C function `wifi_ssid_to_str()` for creating a null-terminated, printable version of the SSID, with nulls and non-printable characters (byte values 0x00-0x20 and 0x7F-0xFF) replaced with "?".

IFS_WIFI_CHANNEL

Sets communication channel; takes argument of type int; valid values are : 1-11 in North America; 1-13 in Europe; 1-14[1] in Japan. See the description for `IFC_WIFI_CHANNEL` for information on the use of "0" for the channel number.

IFS_WIFI_MODE

Sets the operating mode; takes one of the two parameters below:

- `IFPARAM_WIFI_ADHOC` (Currently, WEP cannot be used in ad-hoc networks.)
- `IFPARAM_WIFI_INFRASTRUCTURE`

5.4.1.2 Network Performance

There are two configuration commands that alter the network's performance in a noisy environment or when there are hidden nodes (i.e., wireless devices in the same network that are out of range of one another).

IFS_WIFI_FRAG_THRESHOLD

Sets the fragmentation threshold in bytes; takes one parameter in the range 256-2346. Smaller frames stand a better chance of avoiding collisions.

IFS_WIFI_RTS_THRESHOLD

Sets the request-to-send (RTS) threshold; takes one parameter in the range 1-2347. When there are hidden nodes, using RTS/CTS to avoid collisions can improve throughput.

1. The RCM4400W cannot use channel 14.

5.4.1.3 Active Scanning

This command will not cause the interface to be brought down, but it will briefly interrupt communication on each channel that it scans.

IFS_WIFI_SCAN

Initiates an active scan of all valid channels for the selected regulatory region. A pointer to a scan callback function is passed as the only parameter.

```
ifconfig(IF_WIFI0, IFS_WIFI_SCAN, scan_callback, IFS_END);
```

The callback function must have the following function prototype:

```
root void scan_callback (far wifi_scan_data *data);
```

When the scan has completed, the scan callback function is called. A Wi-Fi scan can be done without taking the interface down, but it will briefly interrupt the network connectivity as it scans the channels on the wireless network.

The scan data is provided to the callback function in its “data” parameter. The scan data includes the number of detected access points and for each one, its SSID, channel number, MAC address and maximum transmission rate, as well as the AP signal strength received by the Rabbit. Up to 16 networks can be reported on with this command.

5.4.1.4 Roaming

There are several commands that affect roaming.

IFS_WIFI_ROAM_ENABLE

Boolean value that enables/disables roaming. Roaming is enabled by default.

IFS_WIFI_ROAM_BEACON_MISS

Sets number of consecutive lost beacons that it takes to trigger a roaming event.

IFS_WIFI_MULTI_DOMAIN

Boolean value enables multi-domain capability for use with APs that implement 802.11d; enabling support for IEEE 802.11d on the access point causes the AP to reveal which country it is operating in. Client stations then use this information for multi-country roaming.

If the interface is up when the multi domain command is run, the interface will be taken down and then brought back up after other `ifconfig()` options have been processed (essentially when `ifconfig()` gets to `IFS_END`).

5.4.1.5 Transmit Power Options

There is one `ifconfig()` command that sets the maximum transmit power for the Wi-Fi Rabbit.

IFS_WIFI_TX_POWER

Sets the maximum transmit power of the Rabbit, taking into account regulatory region and board type; valid parameters are in the range 0-15. These numbers are in dBm units and roughly map like this: 0 = ~0 dBm, 1 = ~1 dBm, 2 = ~2 dBm, etc.

Run the program `\Samples\WiFi\Regulatory\region_compiletime.c` to determine the maximum transmit power allowed both with your Rabbit-based board and in the region in which it will be operating. These two limits will differ, the one for board type being lower. It is not possible to set the maximum transmit power to a value higher than what the Rabbit allows. If such an attempt is made, the maximum transmit power will be set to the highest value allowed by the Rabbit.

If "15" is passed to `IFS_WIFI_TX_POWER`, the Rabbit's transmit power will be at its maximum no matter which regulatory region it is operating in.

5.4.1.6 Regulatory Regions

There is one `ifconfig()` command that sets which regulatory region is considered by the software.

IFS_WIFI_REGION

Limits the channel range and maximum transmit power to be consistent with the restrictions of the selected regulatory region. Valid parameters for this command are listed below, along with the channel ranges and maximum transmit power allowed for each regulatory region. Setting this option at runtime requires the interface to be brought down.

- `IFPARAM_WIFI_REGION_AMERICAS` - Americas, including the US (ch. 1-11, <20 dBm)
- `IFPARAM_WIFI_REGION_AUSTRALIA` - Australia (ch. 1-11, <16 dBm)
- `IFPARAM_WIFI_REGION_CANADA` - Canada (ch. 1-11, <20 dBm)
- `IFPARAM_WIFI_REGION_CHINA` - China (ch. 1-11, <16 dBm)
- `IFPARAM_WIFI_REGION_EMEA` - Europe, Middle East, Africa (ch. 1-13, <16 dBm)
- `IFPARAM_WIFI_REGION_FRANCE` - France (ch. 10-13, <16 dBm)
- `IFPARAM_WIFI_REGION_ISRAEL` - Israel (ch. 3-11, <16 dBm)
- `IFPARAM_WIFI_REGION_JAPAN` - Japan (ch. 1-13, <14 dBm)
- `IFPARAM_WIFI_REGION_MEXICO_INDOORS` - Mexico indoors (ch. 1-11, <16 dBm)
- `IFPARAM_WIFI_REGION_MEXICO_OUTDOORS` - Mexico outdoors (ch. 9-11, <16 dBm)

Running the sample program `\Samples\WiFi\Regulatory\region_compiletime.c` will list the maximum transmit power allowed based on both regulatory region and board type.

5.4.1.7 Data Rates

There is one `ifconfig()` command that sets the maximum transmit data rate it is possible to negotiate.

IFS_WIFI_TX_RATE

Sets the maximum data rate, as a multiple of 100 kbps. Use the macros below, or their integer equivalents. Note that some speeds are only available on 802.11g hardware. (The RCM4400W supports an 802.11b interface. The RCM54xxW, RCM5600W, and BL5S220 support both 802.11b and 802.11g.)

Macro Name	Integer Value	Data Rate
IFPARAM_WIFI_TX_RATE_ANY	0	Any mutually negotiated rate from this table.
IFPARAM_WIFI_TX_RATE_1	10	1.0 Mbps
IFPARAM_WIFI_TX_RATE_2	20	2.0 Mbps
IFPARAM_WIFI_TX_RATE_5_5	55	5.5 Mbps
IFPARAM_WIFI_TX_RATE_6	60	6.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_9	90	9.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_11	110	11.0 Mbps
IFPARAM_WIFI_TX_RATE_12	120	12.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_18	180	18.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_24	240	24.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_36	360	36.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_48	480	48.0 Mbps (802.11g)
IFPARAM_WIFI_TX_RATE_54	540	54.0 Mbps (802.11g)

5.4.1.8 Security Configuration Commands

The `ifconfig()` commands in this section control the selection of authentication, encryption and data integrity protocols.

5.4.1.8.1 Authentication Options

Although authentication and encryption are separate ideas, in practice, they work together. If the wireless Rabbit uses a pre-shared key for authentication, the encryption process succeeding is how each device knows that the other device shares the same secret. Likewise, the encryption protocols require keying material, which is acquired as a result of authentication, either using 802.1X or by the definition of a pre-shared key.

IFS_WIFI_AUTHENTICATION

Sets the authentication mode. The valid parameters are:

- `IFPARAM_WIFI_AUTH_ANY` - Default value. This includes all available modes.
- `IFPARAM_WIFI_AUTH_OPEN` - Effectively disable authentication.
- `IFPARAM_WIFI_AUTH_SHAREDKEY` - WEP authentication. A WEP pre-shared key must be defined when using Shared Key authentication; see Section 5.4.1.8.2.

Defining the macro `WIFI_USE_WPA` makes available more authentication modes:

- `IFPARAM_WIFI_AUTH_WPA_PSK` - Personal mode authentication. A pre-shared key must be defined when using WPA-PSK authentication; see Section 5.4.1.8.3.
- `IFPARAM_WIFI_AUTH_WPA_8021X` - Enterprise mode authentication. This feature is available in the Rabbit Embedded Security Pack Module starting with Dynamic C 10.54. When operating in Enterprise mode, there are additional configuration commands related to the EAP method used. For more information on these commands, refer to the *TCP/IP User's Manual, Vol. 1* and/or the *Rabbit Embedded Security Pack Manual*. You can also look up the function description for `ifconfig()` from within Dynamic C to view all of the function's commands and any related command parameters.

5.4.1.8.2 WEP Pre-Shared Keys

An application can #define up to four WEP keys to use for authentication, encryption, or both. Only one key at a time can be used.

IFS_WIFI_WEP_KEYNUM

Selects which WEP key is active, valid range is 0 to 3. Only one key at a time can be active.

IFS_WIFI_WEP_KEY_BIN

Sets the value for the indicated WEP key. This command takes three parameters; the first parameter is an integer that identifies the WEP key being defined (range is 0-3); the second parameter is the key size: 5 or 13 bytes; and the third parameter is the WEP key value.

```
const byte MY_WEPKEY_BIN[] = { 0x01, 0x23, 0x45, 0x67, 0x89 };
...
ifconfig (IF_WIFI0,
          IFS_WIFI_WEP_KEY_BIN, 0, 5, MY_WEPKEY_BIN
          IFS_END)
```

IFS_WIFI_WEP_KEY_HEXSTR

Sets WEP key value (10 or 26 char hex string). This command takes two parameters; the first parameter is an integer that identifies the WEP key being defined (range is 0-3); the second parameter is the WEP key value.

```
ifconfig (IF_WIFI0,
          IFS_WIFI_WEP_KEY_HEXSTR, 0, "0123456789ABCDEF0123456789",
          IFS_END)
```

5.4.1.8.3 WPA Pre-Shared Keys

Unlike WEP, only one pre-shared key can be defined for WPA-PSK authentication. There are three ways to define the pre-shared key.

IFS_WIFI_WPA_PSK_PASSPHRASE

Sets WPA PSK by hashing the passphrase and target SSID.

```
ifconfig(IF_WIFI0,
         IFS_WIFI_WPA_PSK_PASSPHRASE, "my bad passphrase",
         IFS_END);
```

Please note that if the SSID changes, the passphrase will need to be set again.

IFS_WIFI_WPA_PSK_HEXSTR

Sets WPA PSK using 64-char hex string. With the passphrase "my bad passphrase" and the SSID "rabbit", the hex string is:

```
char * const my_wpakey_hex =
"aa475492a3b03f0b71df0957fd388d02cfe10af49fe0062b542c06181e75d087";
...
ifconfig(IF_WIFI0,
         IFS_WIFI_WPA_PSK_HEXSTR, my_wpakey_hex,
         IFS_END);
```

IFS_WIFI_WPA_PSK_BIN

Sets WPA PSK using a 32-byte array.

```
const byte my_wpakey_bin[] = {0xaa, 0x47, 0x54, 0x92, 0xa3, 0xb0,
         0x3F, 0x0B, 0x71, 0xDF, 0x09, 0x57, 0xFD, 0x38, 0x8D, 0x02,
         0xCF, 0xE1, 0x0A, 0xF4, 0x9F, 0xE0, 0x06, 0x2B, 0x54, 0x2C,
         0x06, 0x18, 0x1E, 0x75, 0xD0, 0x8};
...
ifconfig(IF_WIFI0,
         IFS_WIFI_WPA_PSK_BIN, my_wpakey_bin,
         IFS_END);
```

5.4.1.8.4 Encryption and Data Integrity Protocols

The encryption protocols require keying material, which is acquired as a result of authentication, either using 802.1X or by the definition of a pre-shared key.

IFS_WIFI_ENCRYPTION

Sets the encryption and data integrity protocols that will be acceptable to the Rabbit. The default is no encryption enabled. This command automatically resets the interface.

The macro `WIFI_USE_WPA` must be defined for support of TKIP or CCMP to be available. Valid parameters for the `ifconfig()` encryption command are:

- `IFPARAM_WIFI_ENCR_ANY` - Use any of the supported encryption protocols. If WEP, TKIP or CCMP is used, the appropriate pre-shared key must be defined.
- `IFPARAM_WIFI_ENCR_NONE` - Default condition. Currently, this option is required for ad-hoc networks.
- `IFPARAM_WIFI_ENCR_WEP` - Use WEP for encryption and CRC for data integrity. Define at least one WEP key and make it active; see Section 5.4.1.8.2.
- `IFPARAM_WIFI_ENCR_TKIP` - Use TKIP for encryption and Michael for data integrity. A pre-shared key must be defined when using this protocol; see Section 5.4.1.8.3.
- `IFPARAM_WIFI_ENCR_CCMP` - Use AES in Counter Mode for encryption and CBC-MAC for data integrity. A pre-shared key must be defined when using this protocol; see Section 5.4.1.8.3.

5.4.1.9 Status and Region Commands

These `ifconfig()` commands report back information on state and operating parameters.

IFG_WIFI_STATUS

This command returns information about the Rabbit device and its Wi-Fi network into a user-supplied buffer.

```
auto wifi_status status_info;
...
ifconfig (IF_WIFI0, IFG_WIFI_STATUS, &status_info, IFS_END);
```

After the command `IFG_WIFI_STATUS` successfully returns, the buffer contains the following: the Rabbit's associative state, SSID, channel number, transmit/receive rates and signal information.

IFG_WIFI_REGION_INFO

This command returns information about the Rabbit's currently set regulatory region into a user-supplied buffer.

```
auto wifi_region region_info;
...
ifconfig (IF_WIFI0, IFG_WIFI_REGION_INFO, &region_info, IFS_END);
```

After the command `IFG_WIFI_REGION_INFO` successfully returns, the buffer contains the following: region identifier, channel range, maximum transmit power allowed in region and maximum transmit power allowed for Rabbit board type.

IFG_WIFI_BSSID

Gets the MAC address of the access point that the Rabbit device is associated with. In an ad-hoc network, the BSSID is generated from a random number by the STA that created the IBSS.

5.5 Sample Programs

Dynamic C comes with many sample programs that demonstrate features of Wi-Fi Rabbit boards. Many of them are located in the `\Samples\WiFi\` folder where you installed Dynamic C. Others are in Wi-Fi board-specific folders, e.g., `\Samples\RCM4400w\tcpip\pingled.c`.

A summary of Wi-Fi sample programs, along with more general TCP/IP ones, is available online:

www.rabbit.com/documentation/SamplesRoadmap/tcpip-roadmap.pdf

APPENDIX A. ADDITIONAL WI-FI INFORMATION

This appendix is provided as a convenience for readers who want more information about wireless networking.

A.1 Links to Specifications

This section provides links to the IEEE and IETF specifications relevant to Wi-Fi networks.

- IEEE 802.11: http://standards.ieee.org/getieee802/802.11.html
- IEEE 802.11i: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
- IEEE 802.1X: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf
- The EAP Specification: http://www.ietf.org/rfc/rfc3748.txt (obsoletes RFC 2284)
- The TLS Specification: http://tools.ietf.org/html/rfc2246.
- The EAP-TLS Specification: http://www.faqs.org/rfcs/rfc2716.html
- EAP Method Requirements for WLANs http://www.faqs.org/rfcs/rfc4017.html
- MSCHAPv2 http://www.faqs.org/rfcs/rfc2759.html

A.2 Manufacturers of Wireless Routers and APs

This section provides links to the websites of some of the major wireless router/AP manufacturers.

- D-Link - www.dlink.com
- LinkSys - www.linksys.com
- Netgear - www.netgear.com

A.3 More Information

Any good search engine will bring up a wealth of information on Wi-Fi. Here are some websites that may be useful:

- The web site of Bruce Schneier, a world-renowned computer security expert: http://www.schneier.com/
- Utility for generating WPA hex key from WPA passphrase: http://www.wireshark.org/tools/wpa-psk.html
- Matthew Gast's protocol poster that gives a pictorial summary of 802.11: http://www.oreillynet.com/wireless/2005/05/20/graphics/802.11Poster.pdf

We make two book recommendations for readers interested in a more detailed and comprehensive treatment of 802.11 and/or wanting a deeper understanding of security issues in embedded systems:

- Gast, Matthew S. (2005). *802.11 Wireless Networks, The Definitive Guide*, 2nd ed. Cambridge: O'Reilly
- Stapko, Timothy (2007). *Practical Embedded Security.* Elsevier Science & Technology

A.4 International Regulatory Standards

The nature of RF creates a need for regulations to ensure that all devices "play nicely with one another." The result is the existence of regulatory bodies in different countries that create and enforce rules in their respective geographic regions.

Table 1: International Regulatory Standards

Country	Regulatory Agency
Canada	RSS-210
European Union	European Radiocommunications ero.dk EN 301-328
Japan	Ministry of Internal Communications soumu.go.jp Std. 66 and Std. 33a
United States	Federal Communications Commission fcc.gov FCC Part 15.247

The Rabbit Wi-Fi modules have already been certified for use in many regions.

APPENDIX B. GLOSSARY OF TERMS AND ACRONYMS

There is a fair amount of obscure terminology used to describe the numerous details of wireless networking. It's unavoidable. The sheer volume of information demands some linguistic shortcuts. To counter any confusion that may exist this chapter provides a list of acronyms and other terms used in this manual and in other Wi-Fi reference material.

802.11

802.11 is the IEEE specification for wireless LANs that was ratified in 1999.

802.11-2007, which includes a, b, g, i and others, was ratified in 2007.

802.11i

802.11i is the IEEE specification for wireless LAN security standards that was ratified in 2004.

802.1X

802.1X is the IEEE specification for an authentication protocol ratified in 2001. It was designed for both wireless and wired LANs to authentication users at login with the use of an authentication server, typically RADIUS.

AAA

Authentication, Authorization and Accounting. This describes the processes for controlling access to network resources, enforcing policies, auditing usage, and providing billing information for services. These processes are typically run by one server, e.g., a RADIUS server.

Ad-hoc Mode

This is one of two operating modes defined in the IEEE 802.11 specification. The architecture resulting from using this mode is a network where all wireless stations make peer-to-peer connections and there is no access point to grant Internet or wired LAN services. (See Infrastructure Mode)

AP

Access Point. An AP is a bridging device. In the 802.11 standard it is defined as a wireless station (STA) that provides access to distribution services via a wireless connection to associated stations. Typically an AP has a fixed location and provides access to wireless clients to a wired LAN and/or the Internet.

Bandwidth

Transmission capacity of the channel. In radio communications the bandwidth is the range of frequencies occupied by a modulated carrier wave.

BER

Bit Error Rate. Percentage of bits with errors divided by the number of bits transmitted.

bridge

A bridge connects two networks. An access point is a layer 2 bridge between the wireless network and the wired one.

BSS

Basic Service Set. This is a basic building block for wireless LANs. See Section 2.1.1 for more details.

BSSID

Basic Service Set Identifier. This term is defined by IEEE 802.11. In infrastructure mode, it is the MAC address of the access point in a BSS. The BSSID uniquely identifies each BSS.

In ad-hoc mode, the BSSID identifies the IBSS. It is locally administered and generated from a 46-bit random number.

A BSSID of all 1s indicates a broadcast BSSID (may only be used during probe requests).

CCA

Clear Channel Assessment. This check measures the amount of energy in the air before any client transmits.

CCK

Complementary Code Keying. CCK is a modulation technique; it is a "single carrier" waveform, meaning that the transmission of data is done by modulating a single radio frequency. The preamble, header and payload of a packet are all transmitted using CCK modulation in an 802.11b network.

CCMP

Counter-Mode/CBC-MAC Protocol. This protocol provides confidentiality of data by using AES in counter mode. Authentication and integrity are accomplished via Cipher Block Chaining Message Authentication Code (CBC-MAC).

CCMP is also known as WPA2 encryption.

cell size

Coverage area of a single access point.

CF

Coordination Function. The CF is a single logical function that determines when a wireless station (STA) in a Wi-Fi network transmits and when it receives.

channel

A channel in a Wi-Fi network corresponds to a frequency range in the ISM or U-NII band.

commodity network

Network made up of off-the-shelf components.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance. This is a media access method used by 802.11 networks as the packet transmission protocol. This differs from Ethernet, which uses "Collision Detection."

CTS

Clear-to_Send. This is part of the hardware flow control method used by Wi-Fi networks to reduce collisions.

data rate

The data rate of a channel is also known as the channel capacity or throughput. Shannon's Law states that the maximum data rate that a channel can support is proportional to the product of its bandwidth and signal-to-noise ratio.

DHCP

Dynamic Host Configuration Protocol. A scheme for assigning IP addresses at runtime.

DLL

Data Link Layer. DLL is layer two of both the 7-layer OSI model and the 5-layer TCP/IP model.

DNS

Domain Name System. This is a system that includes a process for translating human-readable domain names (e.g., www. rabbit.com) into IP addresses.

DS

Distribution System. This is the architectural component that is used to interconnect BSSs by allowing communication between APs.

DSS

Distribution System Service. This is a service provided by the DS. See Section 2.3.2 for more details.

DSSS

Direct-Sequence Spread Spectrum. One of the PHYs specified in 802.11 Std., with data rates of 1 and 2 Mbps. DSSS uses a modulation technique that is resistant to interference.

EAP

Extensible Authentication Protocol. EAP is an authentication framework, not a specific authentication method. Some of the authentication methods it allows are:

- EAP-TLS is the original EAP authentication protocol
- PEAPv0/EAP-MSCHAPv2 is the technical term for what people most commonly refer to as "PEAP." Whenever the word PEAP is used, it almost always refers to this form of PEAP.

  Next to EAP-TLS, PEAPv0/EAP-MSCHAPv2 is the second most widely supported EAP standard in the world.

EAPoL

Extensible Authentication Protocol over LAN. This is a way to encapsulate EAP messages included in the 802.1X specification.

EAP Server

The ultimate endpoint conversing with an EAP client. It might be the AP or it might be a back-end server like a RADIUS server.

ESS

Extended Service Set. This is an 802.11 network of arbitrary size and complexity. An ESS is made possible by the DS and BSSs. An ESS requires intercommunication between APs.

FHSS

Frequency-Hopping Spread Spectrum. One of the PHYs specified in 802.11 Std.

FIPS

Federal Information Processing Standard. - 140-2 requirement, which is a government security criterion.

frame

This term refers to a formatted block of information that traverses a network.

FSL

Free Space Loss. This is a measure (in dB) of how much the signal has weakened over a given distance.

HMAC

Hash Message Authentication Code. A type of message authentication code.

HR/DSSS

High Rate/Direct Sequence Spread Spectrum. An extension of the DSSS PHY; it adds data rates of 5.5 Mbps and 11 Mbps.

IAS

Internet Authentication Service. An IAS server is the Microsoft implementation of RADIUS.

IBSS

Independent Basic Service Set. This is a BSS that stands alone, i.e., not connected to an AP, thus no access to a wired network.

ICV

Integrity Check Value.

IETF

Internet Engineering Task Force. This organization, an open, international community of network designers and others, has the stated primary goal: “make the Internet work better.”

Infrastructure Mode

One of two operating modes defined in the IEEE 802.11 specification. Requires an access point.

ISM Band

Industrial, Scientific, Medical Band. This is a slice of the radio-frequency spectrum. The ISM band has three ranges:

- 902-928 MHz
- 2400-2483 MHz
- 5725-5780 MHz

MD5

Message Digest 5. This is a crypto secure hash.

MIC

Message Integrity Code. This is sometimes referred to as “Message Integrity Check”. Either way, it is used to validate the integrity of data.

MIMO

Multiple-Input/Multiple-Output. A system that has more than one transmit antenna and more than one receive antenna for handling multiple data streams simultaneously.

MPDU

MAC Protocol Data Unit. A fragmented MSDU.

MSDU

MAC Service Data Unit. The MAC layer accepts a packet called a MSDU from higher layers, adding headers and trailers to the frame that will be passed to the PHY.

MSK

Master Session Key. This value is derived between the Supplicant and the Authentication Server and is given to the Authenticator. It is at least 64 octets in length. It is used to derive session keys for encryption.

Keying material that is derived between the EAP peer and server and exported by the EAP method.

NAT/NAPT

Network Address (and Port) Translation. This protocol allows multiple devices on a private network to share a single public IP address.

NEMA

National Electronics Manufacturers Association. This association, among other things, rates sealed enclosures that may be used for access points located in areas subject to extreme temperatures, heavy dust exposure, etc. The enclosures are referred to as NEMA enclosures.

nonce

A single use value. The word itself is derived from “a piece of nonsense, used once.”

PAE

Port Access Entity. This is defined in the IEEE 802.1X specification as the protocol entity associated with a network port. The protocol functionality is supported for supplicants, authenticators, or both.

passphrase

A passphrase is similar to a password, in that they are both a sequence of text used to control access to a resource. A passphrase is typically longer than a password in order to provide added security.

PEAP

(See PEAPv0/EAP-MSCHAPv2 on page 61.)

PRF

Pseudo-Random number Function. This is the function that generates the MSK, as well as other key derivations.

PHY

Physical Layer. This term refers to the first layer of both the 7-layer OSI model and the 5-layer TCP/IP model.

PKI

Public Key Infrastructure. This is no single device, but rather it is the idea that a trusted third-party can verify the identities of parties involved in an Internet transaction. PKI implements a trust hierarchy using digital certificates and registration authorities. A good analogy is that of the driver's license. It is issued by the government (the trusted third-party) and verifies your identity when you engage in certain transactions with individuals or businesses.

PMK

Pairwise Master Key. This key is derived in one of two ways: in Enterprise mode, the PMK is generated by the RADIUS server and given to the AP so as to derive more keys. In Personal mode, the PMK is generated by both the STA and the AP, usually by combining the PSK and some nonces.

PSK

Pre-Shared Key. This is a shared secret, which is some piece of data previously given to two parties using a secure channel. The original derivation of the PSK is system-dependent: it may be a password, a passphrase, or a hex string; however, in the WPA context, the PSK is always a 256-bit binary quantity.

PTK

Pairwise Transient Key. This is the key established by the four-way handshake (The four-way handshake is an important element of the authentication process). The PTK is divided into other keys that are each used for specific purposes.

OFDM

Orthogonal Frequency-Division Multiplexing. This is a modulation method; data is transmitted in parallel on many narrow bands divided from available bandwidth.

QoS

Quality of Service. This defines a level of performance in a data communications system, such as a Wi-Fi network. Typically there are multiple parameters that determine the QoS, such as the reliability of data transmission, which might include a minimum data rate and/or a guaranteed transmission time for high priority applications. Another important performance parameter is the error rate.

RADIUS

Remote Authentication Dial In User Service. This is the de facto standard for dedicated authentication servers.

RC4

Rivest Cipher 4. The most widely-used stream cipher. In particular it is used by WEP and TKIP encryption.

RF

Radio Frequency. Traditionally RF is frequencies from a few kHz to ~ 300 GHz. The following link is the RF allocation chart:

```
http://www.ntia.doc.gov/osmhome/allochrt.pdf
```

RSA

Rivest-Shamir-Aldeman. This is a public-key cryptographic algorithm; it is based on the assumption that it is difficult to factor the product of two large primes.

RSN

Robust Security Network. This term is defined in the IEEE 802.11i specification as a network that allows only robust security network associations (RSNAs). It is a synonym for WPA2.

RSNA

Robust Security Network Association. An association between devices that was established using the 802.11i 4-way handshake.

RTS

Request-to-Send. This is part of the hardware flow control method used by Wi-Fi networks to reduce collisions.

scanning

The process of looking for and identifying wireless LANs.

SSID

Service Set IDentifier. This is one of main configuration parameters of a Wi-Fi network. It is also used as the name of the network.

STA

Short for wireless station. This is an addressable entity defined in 802.11 as a wireless computing device that is mobile, portable or fixed.

TKIP

Temporal Key Integrity Protocol. An encryption protocol included in the IEEE 802.11i specification.

TKIP is also known as WPA encryption.

TLA

Three Letter Acronym. Why? We needed just one more to make an even number.

TLS

Transport Layer Security. TLS is a cryptographic protocol, as is its predecessor, SSL.

TSK

Transient Session Key. These keys are used to protect data exchanged after EAP authentication has successfully completed. The TKIP and CCMP ciphersuites derive the TSKs from the PMK.

U-NII Band

Unlicensed-National Information Infrastructure Band. This is a slice of the radio-frequency spectrum.

WEP

Wired Equivalent Privacy. This is the original security strategy defined by the IEEE 802.11 specification.

Wi-Fi

This is the name given to the IEEE 802.11 suite of standards by the Wi-Fi Alliance. Some people believe that Wi-Fi is short for Wireless Fidelity. It isn't.

Wi-Fi Alliance

This organization is a global, non-profit group of industry leaders created to drive the adoption of a single standard for wireless LANs. They do certification testing for the Wi-Fi brand. They also provide up-to-date information to consumers.

WLAN

Wireless Local Area Network. According to the IEEE 802.11 specification, a WLAN is:

"A system that includes the distribution system (DS), access points (APs), and portal entities. It is also the logical location of distribution and integration service functions of an extended service set (ESS). A WLAN system contains one or more APs and zero or more portals in addition to the DS."

WPA

Wi-Fi Protected Access. Wi-Fi Alliance name for the third draft of the IEEE 802.11i specification.

WPA2

Wi-Fi Protected Access 2. Wi-Fi Alliance name for the final draft of the IEEE 802.11i specification.

INDEX

M

N

O

P

R

S

T

W