SoftAP Functionality

Revision History

Revision	***Date***	***Change Description***
43XX-AN801-R	09/15/09	**Added:** • "SoftAP Basics" on page 2. **Updated:** • "SoftAP Security" on page 5. • "Chipset AP Configuration" on page 6.
43XX-AN800-R	07/29/09	Initial release.

Broadcom Corporation
5300 California Avenue
Irvine, CA 92617

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The BCM43XX wireless LAN (WLAN) chips (BCM4325, BCM4329, and BCM4319) are usually used in devices that connect to home networks, Wi-Fi® hot spots, and workplace networks. These devices operate as a station, or STA, which can connect to a single wireless router/access point (AP) that is typically hardwired at a fixed location.

The retail market wireless router/AP know-how that Broadcom has acquired during its eight-plus years of leadership and innovation has been applied to traditional STA chips in the form of SoftAP technology which enables a STA to behave like a wireless router/AP.

USES OF SOFTAP TECHNOLOGY

Broadcom® WLAN chips can now be found on a wide range of mobile devices, including smartphones, feature phones, personal media players, and digital cameras. As WLAN proliferates onto more and more such devices, use cases for SoftAP technology become compelling.

CELLULAR TETHERING

Many smartphones have high-bandwidth cellular data connections using technologies such as HSPA, UMTS, EVDO, and so on. In addition to providing access to network-based services from the phone itself, many carriers want to enable their customers to use the connection for other WLAN-enabled devices, such as computers and handheld video games.

For other devices to connect to the cellular phone, the WLAN chipset must be configured for SoftAP operation. Multiple WLAN-enabled devices can then connect to the cellular phone and share the connection. This capability is known as tethering.

Several other protocols are required, however, before the WLAN-enabled devices can successfully share a connection with the cellular phone. These protocols include DHCP (for giving associated devices their own IP address) and Network Address Translation (NAT). These protocols are layer-3 protocols that exist entirely above the Broadcom SoftAP implementation.

For major operating systems, most of these additional protocols and applications are freely available. For instance, Windows Mobile® 6.1 and later has native support for Internet Connection Sharing (ICS). ICS uses DHCP, NAT, and routing technology to share a cellular connection with another device. By default, as shipped, the Windows Mobile support is targeted at Bluetooth® tethering using the PAN profile. A device manufacturer should work with Microsoft to modify the default configuration to work with the Broadcom SoftAP solution.

In the Linux® environment, tethering solutions have been part of standard Linux distributions for some time. These freely available solutions can be integrated onto customer platforms to perform the desired sharing.

Broadcom will also be offering a collection of software called the SoftAP Host Support Library (HSL), which is described later. The HSL can be used to implement much of the needed functionality for a cellular tethering solution.

On-the-Go Gaming

Network gaming has become an important feature of home video game consoles. This feature has migrated to handheld video games and other devices such as smartphones and personal media players. SoftAP technology supports the setting up of multiplayer video game sessions, even when a user is away from a WLAN access point.

Unlike tethering, many of the protocols such as NAT and routing are not required for local gaming. DHCP, however, is required for a seamless user experience across multiple diverse devices. The Broadcom SoftAP HSL can be used to implement the needed functionality for on-the-go gaming.

Wi-Fi Peer-to-Peer

The Wi-Fi organization is developing a specification for easy communication of WLAN devices without the need for a fixed AP. This new specification is likely to use SoftAP technology to achieve this functionality. As this specification matures towards ratification, Broadcom SoftAP technology will be used.

Broadcom will be providing a comprehensive host-side Point-to-Point (P2P) library to simplify implementation as the specification matures.

SoftAP Basics

Broadcom SoftAP implementations inherit most of their configuration and operating parameters from Broadcom-based retail router designs, though some parameters are scaled down for the smaller, mobile platform market.

Table 1: SoftAP Features

Feature	***Description***
Stations supported	8
Station power save support	IEEE and WMM-PS
Security	Open, WEP, WPA-PSK (TKIP), and WPA2-PSK(TKIP+AES)
WEP keys supported	4
SSID broadcast disable	Yes
Allow/deny list	Yes, through MAC address filtering
Association station list	Yes
Limit station associations	Yes, the maximum = 8.

Power Savings in SoftAP Implementations

In a traditional WLAN network with a fixed AP, the AP is not involved with its own power savings, but does provide functionality to allow for associated devices to save power.

In a SoftAP implementation, the device acting as the AP is often a mobile, battery-powered device, and thus might have to do things above and beyond what is done by a traditional AP.

POWER SAVINGS FOR ASSOCIATED DEVICES

The SoftAP implementation allows associated devices to go into standard IEEE 802.11 power save mode. When a device indicates it is in power save mode, the SoftAP begins to buffer packets for the device so that it can sleep and conserve power.

Additionally, the Broadcom SoftAP supports Wi-FI WMM® power save mode. This newer power save mode is optimized for devices that support voice/video via WMM and is fully supported by the SoftAP implementation.

Note that because of limited on-chip memory, if an associated device sleeps for long periods of time or if multiple devices go to sleep, some packets may be lost. This will not result in catastrophic errors, but might adversely affect overall network performance.

POWER SAVINGS FOR THE SOFTAP DEVICE

Standard IEE 802.11 and Wi-Fi specifications do not provide protocols that allow for an AP to go into power save mode. Broadcom, however, has been developing and is continuing to develop mechanisms to prevent a device operating as a SoftAP from draining the device battery too quickly.

Application-Optimized Devices

The BCM43XX devices have been optimized for low-power device applications. Mechanisms such as CPU offloading, optimized low-power radios, and so on enable the BCM43XX devices to draw significantly less power than traditional WLAN devices.

Broadcom Opportunistic Power Savings

The BCM43XX chips are able to put the device automatically into low-power states when it is determined that the wireless channel is being used by other devices. This feature is called Opportunistic Power Savings (OPS).

OPS is not enabled by default, but can be enabled at any time by the ops_en IOVAR. Once enabled, the SoftAP OPS algorithm will:

1. Monitor packets being sent on the channel.
2. Process those packets directed towards the MAC address of the SoftAP chipset.
3. Calculate packet durations and disable the SoftAP’s radio if a received packet is:
   a. Not directed to the MAC address of the SoftAP chipset.
   b. Of sufficient length to allow for radio disable/enable times.

   Because the medium is being used for other purposes, it is safe to disable the radio because no other devices can send during this time.
4. Reenable the radio in time to receive a packet following a packet which led to the radio being turned off.
5. Go back to step 1.

When OPS is being used, the SoftAP chipset is able to save power without any interaction from the host and without the need for any protocol overhead to the associated devices.

Wi-Fi Peer-to-Peer Notice of Absence

Once ratified, the Wi-Fi Peer-to-Peer specification will likely provide for the device acting as the AP to schedule times when it will be unavailable. These absence times can be used for the SoftAP device to turn off portions of the chip for the purposes of saving power.

SoftAP Software Components

For the BCM43XX chips, the vast majority of the functionality required to implement a SoftAP solution is implemented in the firmware that is executed by the on-chip processor. Consequently, the software and CPU load on the host is relatively small.

There are several pieces to a fully functional SoftAP implementation as described in this section and shown in Figure 1. Any chip-specific details regarding the implementation are noted.

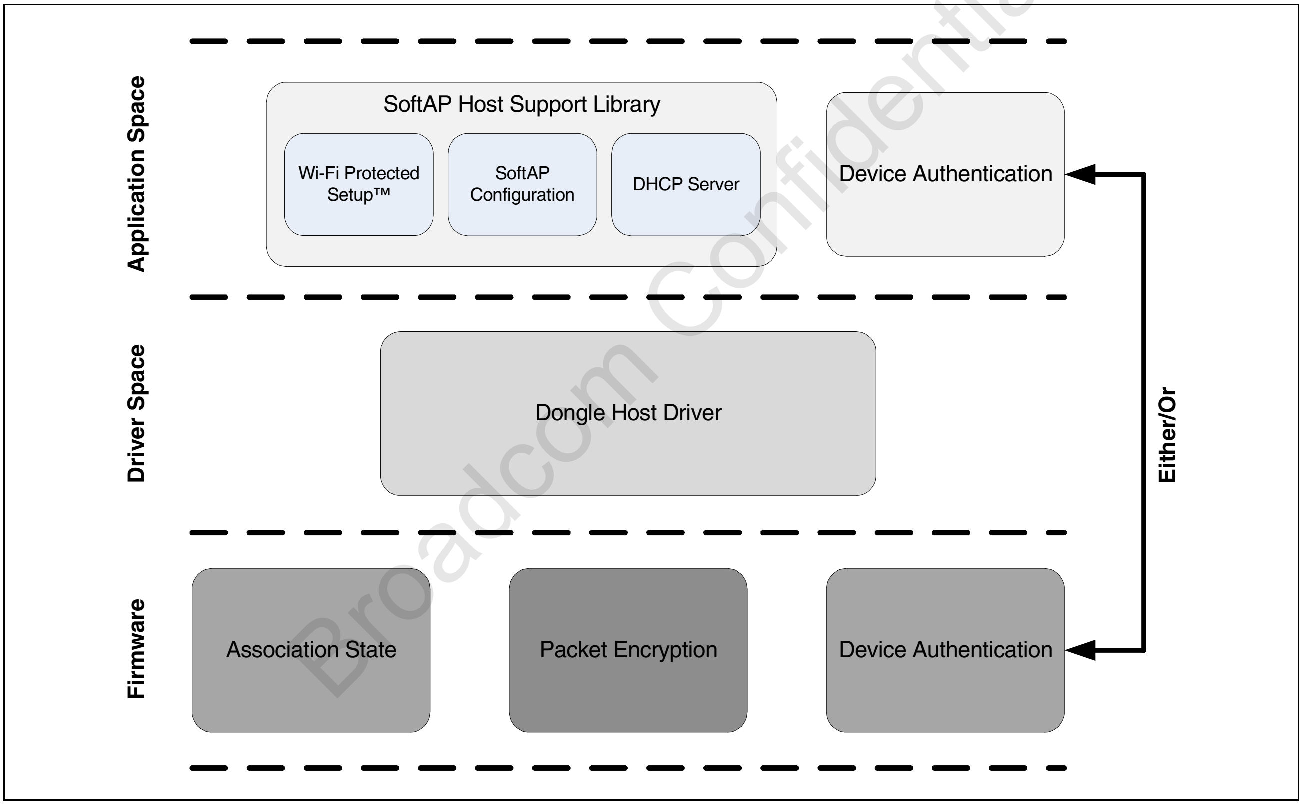

Figure 1: SoftAP Implementation Topology

Firmware

The bulk of the IEEE 802.11 MAC functionality is implemented in device firmware. The firmware is code that is downloaded to the device by the Dongle Host Driver (DHD) at initialization time and is executed by the on-chip processor.

Many different firmware files are delivered with a chipset software package. If the target device requires SoftAP support, a firmware file with SoftAP support must be downloaded to the chipset. The firmware binary file must have an *ap* in the filename, such as sdio-g-cdc-reclaim-wme-ap.bin

DONGLE HOST DRIVER AND FIRMWARE

All BCM43XX implementations have to have a lightweight device driver called the Dongle Host Driver, or DHD. The DHD is implemented in the native network driver format for the target operating system. Because the IEEE 802.11 MAC implementation exists on the firmware, the DHD is extremely lightweight and places very little burden on the host operating system.

The primary purpose of the DHD is to take network packets from the upper layer protocol stacks and send them over the bus interface, usually SDIO or USB.

SOFTAP HOST SUPPORT LIBRARY

The SoftAP HSL is intended to make initialization and run-time configuration of a SoftAP chipset easier to implement. Configuration can all be handled via IOCTL calls, and free or OS-provided DHCP and WPS libraries can be used. The HSL is provided as an alternative to simplify the implementation.

The HSL performs the following tasks:

- Implements library functions to initialize a SoftAP implementation on the platform. This includes the setting of parameters such as the SSID, channel, security settings, and so on.
- Configures security settings by interfacing to the WPA™ authenticator, whether it is in the firmware or on the host.
- Interfaces to a Broadcom-provided WPS library for the purposes of implementing PBC and/or PIN Wi-Fi Protected Setup™ configuration of clients.
- Implements a Broadcom-developed lightweight DHCP library so that connected devices are given an IP address.

Because of system-level complexities and differences, the HSL does not implement the NAT/routing capabilities needed for a complete tethering implementation. Broadcom software applications engineers can work with customers to tie the Broadcom-provided and OS/third party-provided components together.

The HSL comes with library-specific documentation regarding the details of its specific API.

SOFTAP SECURITY

The goal of Broadcom's SoftAP technology is to provide mechanisms for easy wireless connections, primarily for mobile devices that are away from traditional access points. It is not intended to pass traditional Wi-Fi AP certification tests.

SoftAP technology provides many features found in stand-alone access points, such as support for IEEE and WMM-PS power save, multiple connected clients, full WEP64/128, and WPA/WPA2-AES/TKIP security. Because of the target applications, however, these limitations apply:

- WDS inter-AP bridging is not supported.
- IEEE 802.1X security is not supported.

Association State Machine

Any IEEE 802.11 AP is required to keep the state associated with the devices that are connected to it. This includes the association state, transmission rate, statistics, and so on. For the BCM43XX chips, all of this is implemented and stored within the device firmware. This approach reduces the burden on the host and spares the host from having to deal with AP management states.

Packet Encryption

On secure networks, the packets to and from the AP are encrypted. Either WEP, TKIP, or AES encryption can be used, depending on the network. All encryption types are handled in the device firmware in the SoftAP implementation so that the host is not burdened with this CPU-intensive operation.

Station Authentication

WPA-PSK and WPA2-PSK security implementations must implement authentication routines to be sure that associating STA devices have the proper network credentials.

The authentication code, which is fairly large, can exist either on-chip (called the in-driver authenticator) or implemented as an application on the host (called the host-side authenticator), depending on the other device features required.

If IEEE 802.11n support (for the BCM4329 and BCM4319) is not included, then all authentication functionality can be included in the firmware. This approach simplifies the overall platform porting effort. For most use cases, such as cellular tethering, this approach is a perfectly acceptable trade-off because the speed of the cellular interfaces today are limited and cannot take advantage of the increased bandwidth of an IEEE 802.11n connection. In this case, when SoftAP support is needed, the device would download IEEE 802.11g-only firmware to the chipset. Once SoftAP support is no longer required, IEEE 802.11n firmware can then be downloaded.

Whether the authentication function resides in the firmware or on the host, the load on the host CPU is still very low, as authentication is an infrequent event, only happening when a new device joins the network.

Wi-Fi Protected Setup

Wi-Fi Protected Setup™ (WPS) is a protocol defined by the Wi-Fi Alliance® to ease configuration of devices onto secure networks, such as a SoftAP network using WPA/WPA2-PSK security. In the BCM43XX SoftAP implementation, the WPS registrar is implemented on the host platform. As with station authentication, WPS is an infrequent event and thus puts very little load on the host CPU.

SoftAp Configuration

Chipset AP Configuration

As with standard STA mode, BCM43XX chipsets are configured via a series of IOCTL commands (for testing purposes, the wl utility can be used for SoftAP configuration).

For a complete reference to all of the wl commands and IOCTLS, refer to the 80211-TI20X-R and 80211-AN30X-R application notes available from the docSAFE tab of the Broadcom Customer Support Web site at http://support.broadcom.com/Core/Home/Main.aspx.

The following command sequence can be used as a template for bringing up a SoftAP on the primary WLAN interface.

```
/* enable SoftAP mode */
wl mpc 0
wl down
wl ap 1

/* Set operating channel */
wl channel x

/* For open authentication, no security */
wl wsec 0
wl wpa_auth 0

/* OR for WEP security */
wl wsec 1
wl addwep 0 xxxxxxxxxx
wl wpa_auth 0

/* OR for WPA-Personal security */
wl wsec x               /* 2 for TKIP, 4 for AES , 6 for both*/
wl set_pmk xxxxxxxxx    /* raw 64-byte HEX PMK */
wl wpa_auth x           /* 4 for WPA-PSK, 128 for WPA2-PSK, 132 for both */

/* set maximum allowed connections */
wl maxassoc x           /* Maximum of 8 */

/* set allow/deny MAC address list */
wl macmode x            /* 0 = disable, 1 = allow, 2 = deny */
wl mac xx:xx:xx:xx:xx:xx [xx:xx:xx:xx:xx:xx …]

/* if desired, disable SSID broadcast */
wl closed x             /* 0 = open, 1 = hidden */

/* enable the BSS */
wl ssid xxxxx           /* set SSID, enable BSS */
```

HOST-SIDE AUTHENTICATOR CONFIGURATION

As mentioned earlier, the authenticator required for WPAWPA2-PSK security might need to exist in application space on the host processor.

Host-side authenticator configuration is handled via calls to the SoftAP HSL.

FAQ

Q: Are there specific Broadcom WLAN chips that can support SoftAP operation?

A: Although this documents focuses on specific ships, all Broadcom devices can be configured for SoftAP operation.

Q: What is the additional host load (memory, CPU) to support SoftAP mode?

A: For most configurations, there is no additional load. All AP management code is implemented within the device firmware itself. Depending on the other features required on the solutions, the WPA-PSK authentication code might need to run on the host platform in user space. This activity will consume approximately an additional 200 KB of flash and host memory.

Q: Can devices associated with the SoftAP go into power save mode?

A: Yes, both IEEE and WMM-PS power save modes are supported.

Q: How does SoftAP compare to ad hoc mode?

A: SoftAP has the following distinct advantages over ad hoc mode:

- SoftAP allows for the associated devices to go into power save mode.
- SoftAP supports WPA2-level encryption, making the connection much more secure.
- Wi-FI CERTIFIED™ devices must limit the data rates to IEEE 802.11b levels. SoftAP can use full IEEE 802.11g or IEEE 802.11n rates.

Broadcom Corporation

5300 California Avenue
Irvine, CA 92617
Phone: 949-926-5000
Fax: 949-926-5203