11. WLAN Operational Description

Within USA :
- WLAN : 2.4GHz 802.11 b/g/n
- BT : v4.0

Although the chipset documentation may indicate possible functions,
The following have been permanently hardware disabled in this device
and cannot be enabled by the end user or service provider :

(BT)
HS compliant : Not Supported

(WLAN)
5GHz Features : Not Supported
Channel Bonding in 2.4GHz : Not Supported

(FM Radio)
FM Transmitter
RDS - AF : Not Supported

SM-G130HN BT/WIFI RF BLOCK DIAGRAM

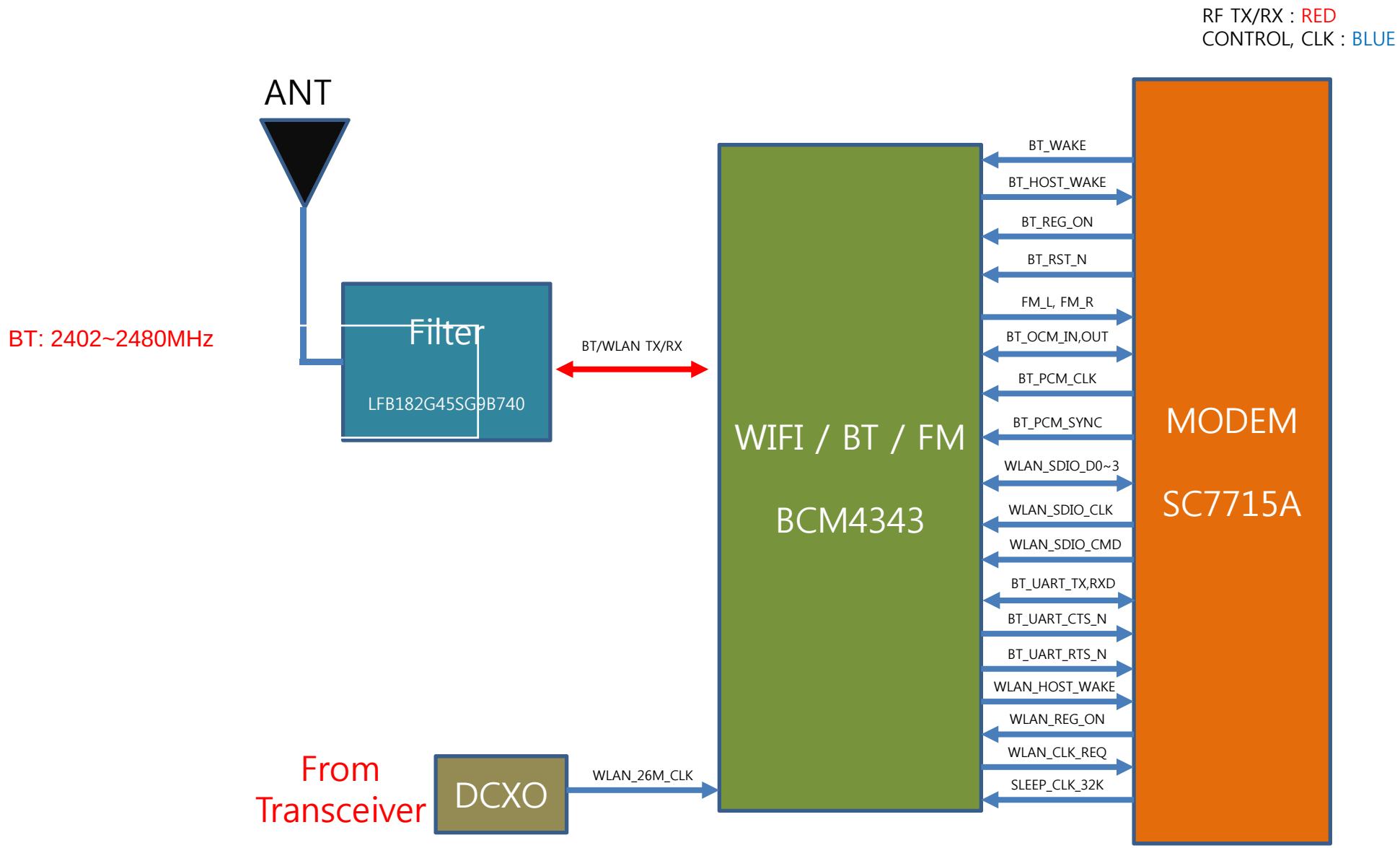
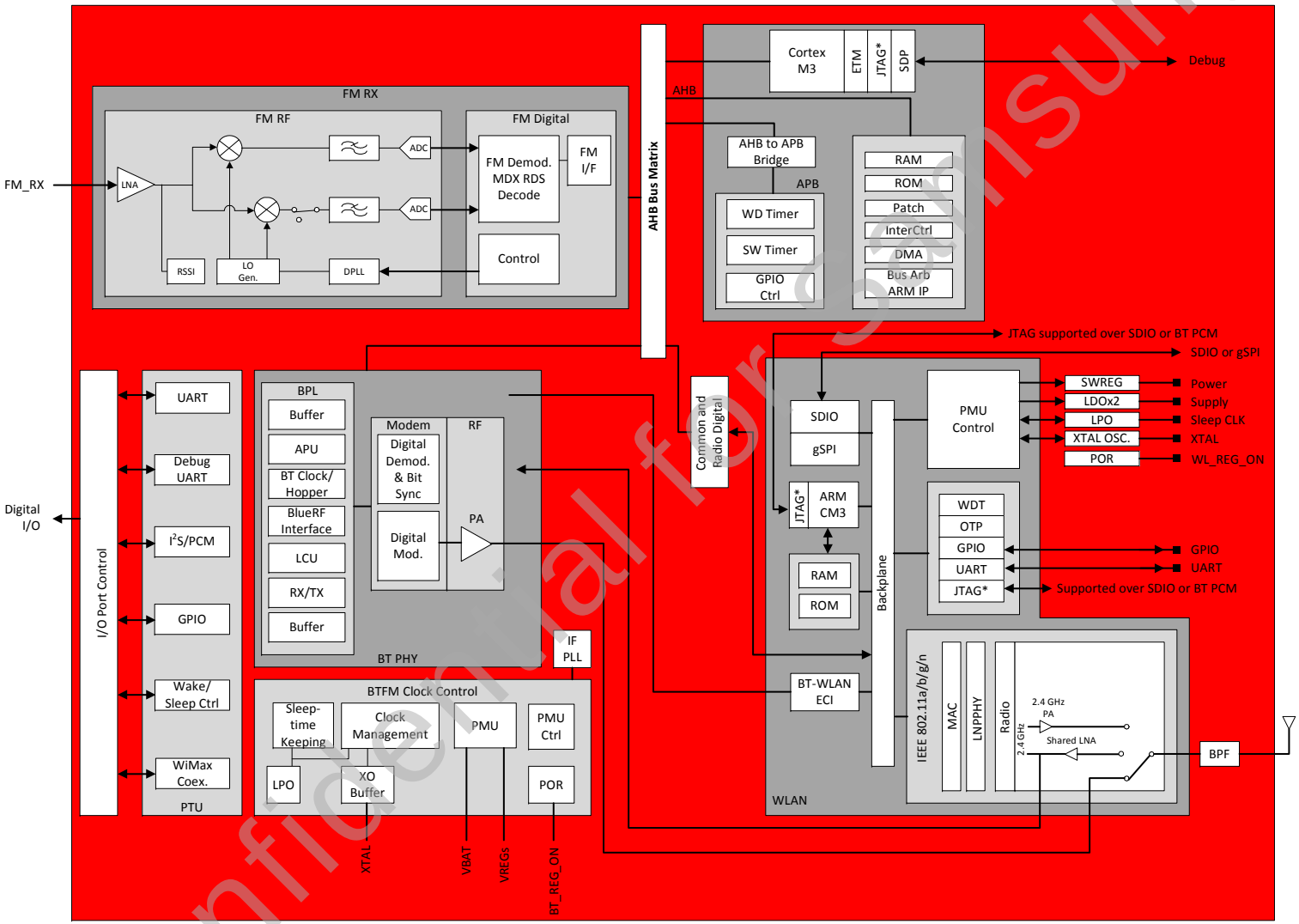


Figure 2: BCM4343S Block Diagram



* Via GPIO configuration, JTAG is supported over SDIO or BT PCM

Section 4: WLAN System Interfaces

SDIO v2.0

The BCM4343S WLAN section supports SDIO version 2.0. for both 1-bit (25 Mbps) and 4-bit modes (100 Mbps), as well as high speed 4-bit mode (50 MHz clocks—200 Mbps). It has the ability to map the interrupt signal on a GPIO pin. This out-of-band interrupt signal notifies the host when the WLAN device wants to turn on the SDIO interface. The ability to force control of the gated clocks from within the WLAN chip is also provided.

SDIO mode is enabled using the strapping option pins. See Table 18 on page 92 for details.

Three functions are supported:

- Function 0 standard SDIO function. The maximum block size is 32 bytes.
- Function 1 backplane function to access the internal System-on-a-Chip (SoC) address space. The maximum block size is 64 bytes.
- Function 2 WLAN function for efficient WLAN packet transfer through DMA. The maximum block size is 512 bytes.

SDIO Pin Descriptions

Table 4: SDIO Pin Descriptions

SD 4-Bit Mode		*SD 1-Bit Mode*		*gSPI Mode*	
DATA0	Data line 0	DATA	Data line	DO	Data output
DATA1	Data line 1 or Interrupt	IRQ	Interrupt	IRQ	Interrupt
DATA2	Data line 2	NC	Not used	NC	Not used
DATA3	Data line 3	NC	Not used	CS	Card select
CLK	Clock	CLK	Clock	SCLK	Clock
CMD	Command line	CMD	Command line	DI	Data input

Figure 10: Signal Connections to SDIO Host (SD 4-Bit Mode)

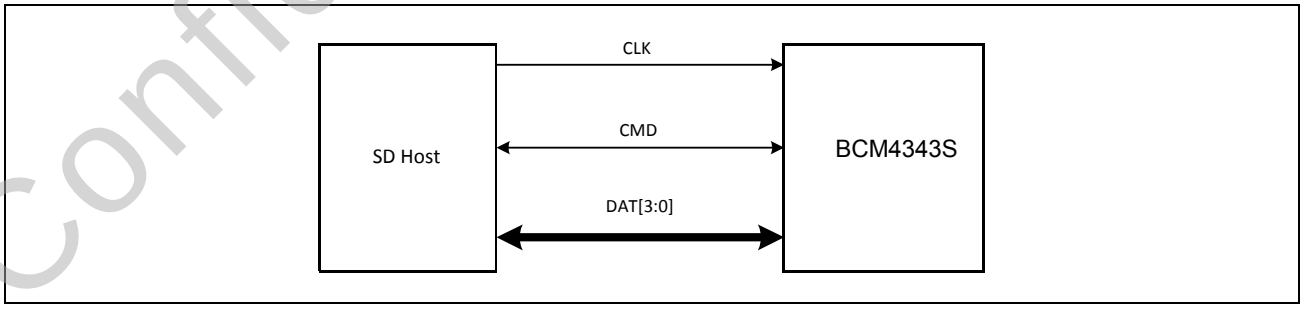
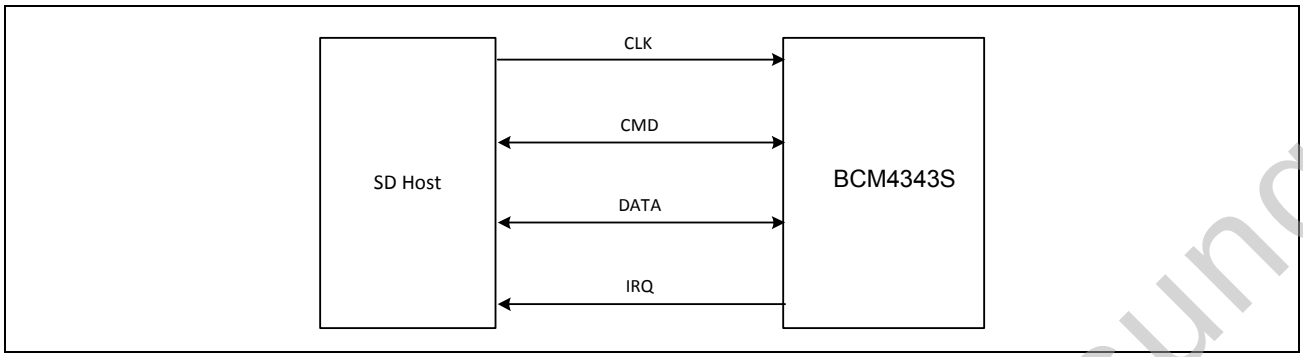


Figure 11: Signal Connections to SDIO Host (SD 1-Bit Mode)



Section 5: Wireless LAN MAC and PHY

MAC Features

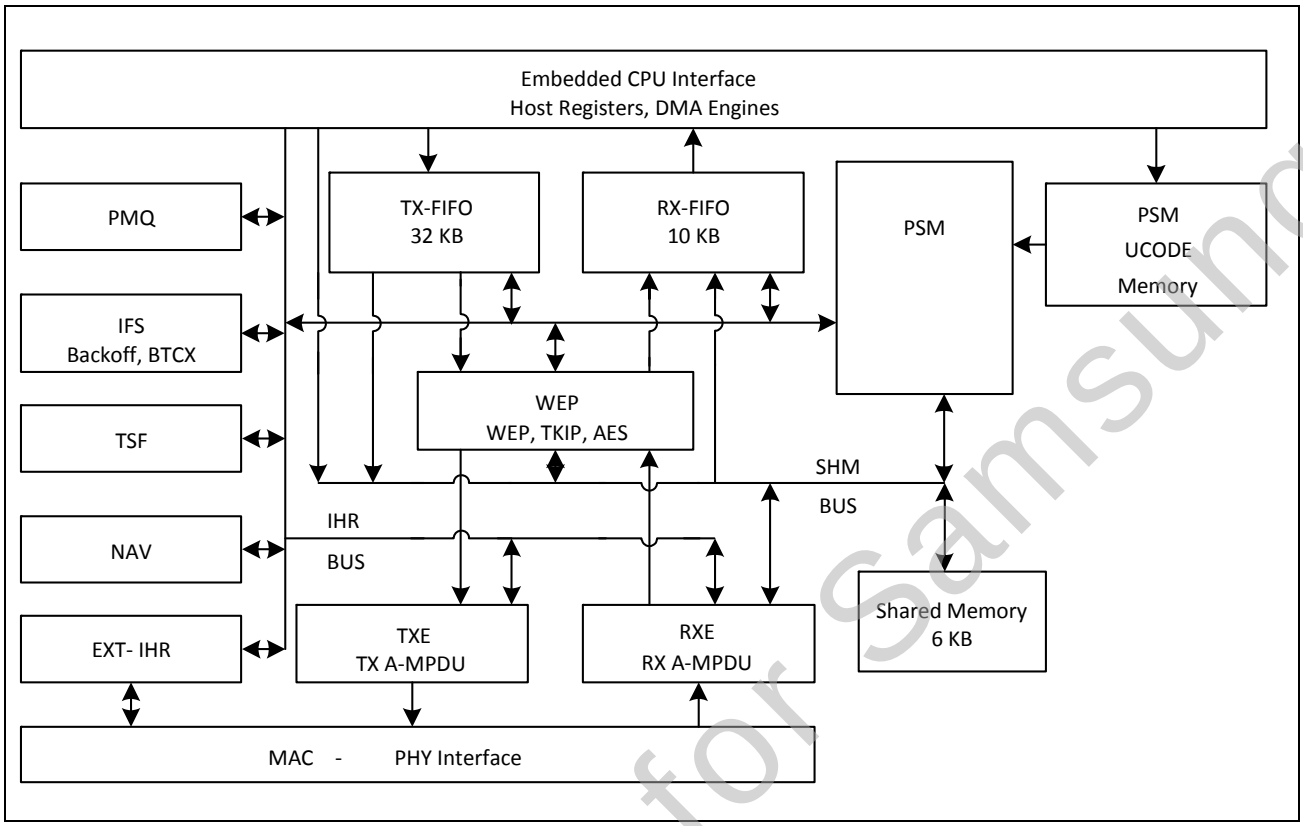
The BCM4343S WLAN MAC supports features specified in the IEEE 802.11 base standard, and amended by IEEE 802.11n. The salient features are listed below:

- Transmission and reception of aggregated MPDUs (A-MPDU).
- Support for power management schemes, including WMM power-save, power-save multipoll (PSMP) and multiphase PSMP operation.
- Support for immediate ACK and Block-ACK policies.
- Interframe space timing support, including RIFS.
- Support for RTS/CTS and CTS-to-self frame sequences for protecting frame exchanges.
- Back-off counters in hardware for supporting multiple priorities as specified in the WMM specification.
- Timing synchronization function (TSF), network allocation vector (NAV) maintenance, and target beacon transmission time (TBTT) generation in hardware.
- Hardware off-load for AES-CCMP, legacy WPA TKIP, legacy WEP ciphers, WAPI, and support for key management.
- Support for coexistence with Bluetooth and other external radios.
- Programmable independent basic service set (IBSS) or infrastructure basic service set functionality
- Statistics counters for MIB support.

MAC Description

The BCM4343S WLAN MAC is designed to support high throughput operation with low-power consumption. It does so without compromising on Bluetooth coexistence policies, thereby enabling optimal performance over both networks. In addition, several power-saving modes that have been implemented allow the MAC to consume very little power while maintaining network-wide timing synchronization. The architecture diagram of the MAC is shown in Figure 19 on page 44.

Figure 19: WLAN MAC Architecture



The following sections provide an overview of the important modules in the MAC.

PSM

The programmable state machine (PSM) is a microcoded engine that provides most of the low-level control to the hardware to implement the IEEE 802.11 specification. It is a microcontroller that is highly optimized for flow-control operations, which are predominant in implementations of communication protocols. The instruction set and fundamental operations are simple and general, which allows algorithms to be optimized until very late in the design process. It also allows for changes to the algorithms to track evolving IEEE 802.11 specifications.

The PSM fetches instructions from the microcode memory. It uses the shared memory to obtain operands for instructions, as a data store, and to exchange data between both the host and the MAC data pipeline (via the SHM bus). The PSM also uses a scratch-pad memory (similar to a register bank) to store frequently accessed and temporary variables.

The PSM exercises fine-grained control over the hardware engines by programming internal hardware registers (IHR). These IHRs are collocated with the hardware functions they control and are accessed by the PSM via the IHR bus.

The PSM fetches instructions from the microcode memory using an address determined by the program counter, an instruction literal, or a program stack. For ALU operations, the operands are obtained from shared memory, scratch-pad memory, IHRs, or instruction literals, and the results are written into the shared memory, scratch-pad memory, or IHRs.

There are two basic branch instructions: conditional branches and ALU-based branches. To better support the many decision points in the IEEE 802.11 algorithms, branches can depend on either readily available signals from the hardware modules (branch condition signals are available to the PSM without polling the IHRs) or on the results of ALU operations.

WEP

The wired equivalent privacy (WEP) engine encapsulates all the hardware accelerators to perform the encryption and decryption, as well as the MIC computation and verification. The accelerators implement the following cipher algorithms: legacy WEP, WPA TKIP, and WPA2 AES-CCMP.

Based on the frame type and association information, the PSM determines the appropriate cipher algorithm to be used. It supplies the keys to the hardware engines from an on-chip key table. The WEP interfaces with the transmit engine (TXE) to encrypt and compute the MIC on transmit frames and the receive engine (RXE) to decrypt and verify the MIC on receive frames. WAPI is also supported.

TXE

The transmit engine (TXE) constitutes the transmit data path of the MAC. It coordinates the DMA engines to store the transmit frames in the TXFIFO. It interfaces with WEP module to encrypt frames and transfers the frames across the MAC-PHY interface at the appropriate time determined by the channel access mechanisms.

The data received from the DMA engines are stored in transmit FIFOs. The MAC supports multiple logical queues to support traffic streams that have different QoS priority requirements. The PSM uses the channel access information from the IFS module to schedule a queue from which the next frame is transmitted. Once the frame is scheduled, the TXE hardware transmits the frame based on a precise timing trigger received from the IFS module.

The TXE module also contains the hardware that allows the rapid assembly of MPDUs into an A-MPDU for transmission. The hardware module aggregates the encrypted MPDUs by adding appropriate headers and pad delimiters as needed.

RXE

The receive engine (RXE) constitutes the receive data path of the MAC. It interfaces with the DMA engine to drain the received frames from the RX FIFO. It transfers bytes across the MAC-PHY interface and interfaces with the WEP module to decrypt frames. The decrypted data is stored in the RX FIFO.

The RXE module contains programmable filters that are programmed by the PSM to accept or filter frames based on several criteria such as receiver address, BSSID, and certain frame types.

The RXE module also contains the hardware required to detect A-MPDUs, parse the headers of the containers, and disaggregate them into component MPDUS.

IFS

The IFS module contains the timers required to determine interframe space timing including RIFS timing. It also contains multiple back-off engines required to support prioritized access to the medium as specified by WMM.

The interframe spacing timers are triggered by the cessation of channel activity on the medium, as indicated by the PHY. These timers provide precise timing to the TXE to begin frame transmission. The TXE uses this information to send response frames or perform transmit frame-bursting (RIFS or SIFS separated, as within a TXOP).

The back-off engines (for each access category) monitor channel activity, in each slot duration, to determine whether to continue or pause the back-off counters. When the back-off counters reach 0, the TXE gets notified so that it may commence frame transmission. In the event of multiple back-off counters decrementing to 0 at the same time, the hardware resolves the conflict based on policies provided by the PSM.

The IFS module also incorporates hardware that allows the MAC to enter a low-power state when operating under the IEEE power-saving mode. In this mode, the MAC is in a suspended state with its clock turned off. A sleep timer, whose count value is initialized by the PSM, runs on a slow clock and determines the duration over which the MAC remains in this suspended state. Once the timer expires, the MAC is restored to its functional state. The PSM updates the TSF timer based on the sleep duration, ensuring that the TSF is synchronized to the network.

The IFS module also contains the PTA hardware that assists the PSM in Bluetooth coexistence functions.

TSF

The timing synchronization function (TSF) module maintains the TSF timer of the MAC. It also maintains the target beacon transmission time (TBTT). The TSF timer hardware, under the control of the PSM, is capable of adopting timestamps received from beacon and probe response frames in order to maintain synchronization with the network.

The TSF module also generates trigger signals for events that are specified as offsets from the TSF timer, such as uplink and downlink transmission times used in PSMP.

NAV

The network allocation vector (NAV) timer module is responsible for maintaining the NAV information conveyed through the duration field of MAC frames. This ensures that the MAC complies with the protection mechanisms specified in the standard.

The hardware, under the control of the PSM, maintains the NAV timer and updates the timer appropriately based on received frames. This timing information is provided to the IFS module, which uses it as a virtual carrier-sense indication.

MAC-PHY Interface

The MAC-PHY interface consists of a data path interface to exchange RX/TX data from/to the PHY. In addition, there is a programming interface, which can be controlled either by the host or the PSM to configure and control the PHY.

PHY Description

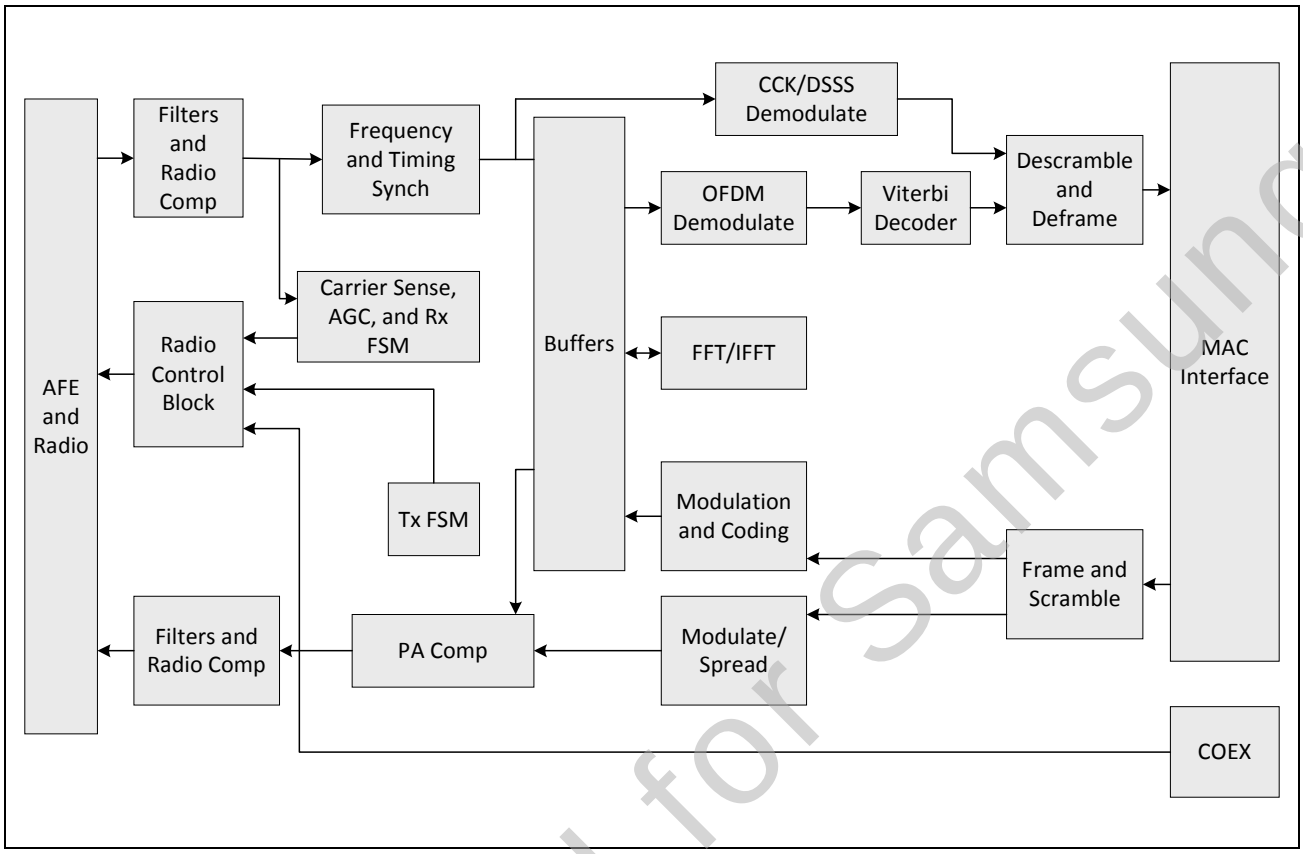
The BCM4343S WLAN digital PHY is designed to comply with IEEE 802.11b/g/n single stream to provide wireless LAN connectivity supporting data rates from 1 Mbps to 96 Mbps for low-power, high-performance handheld applications.

The PHY has been designed to meet specification requirements in the presence of interference, radio nonlinearity, and impairments. It incorporates efficient implementations of the filters, FFT, and Viterbi decoder algorithms. Efficient algorithms have been designed to achieve maximum throughput and reliability, including algorithms for carrier sense/rejection, frequency/phase/timing acquisition and tracking, and channel estimation and tracking. The PHY receiver also contains a robust IEEE 802.11b demodulator. The PHY carrier sense has been tuned to provide high throughput for IEEE 802.11g/IEEE 802.11b hybrid networks with Bluetooth coexistence.

PHY Features

- Supports the IEEE 802.11b/g/n single-stream standards.
- Supports explicit IEEE 802.11n transmit beamforming.
- Supports optional Greenfield mode in TX and RX.
- Supports IEEE 802.11h/d for worldwide operation.
- Algorithms achieving low power, enhanced sensitivity, range, and reliability.
- Algorithms to maximize throughput performance in the presence of Bluetooth signals.
- Automatic gain control scheme for blocking and nonblocking application scenarios for cellular applications.
- Closed-loop transmit power control.
- Designed to meet FCC and other regulatory requirements.

Figure 20: WLAN PHY Block Diagram



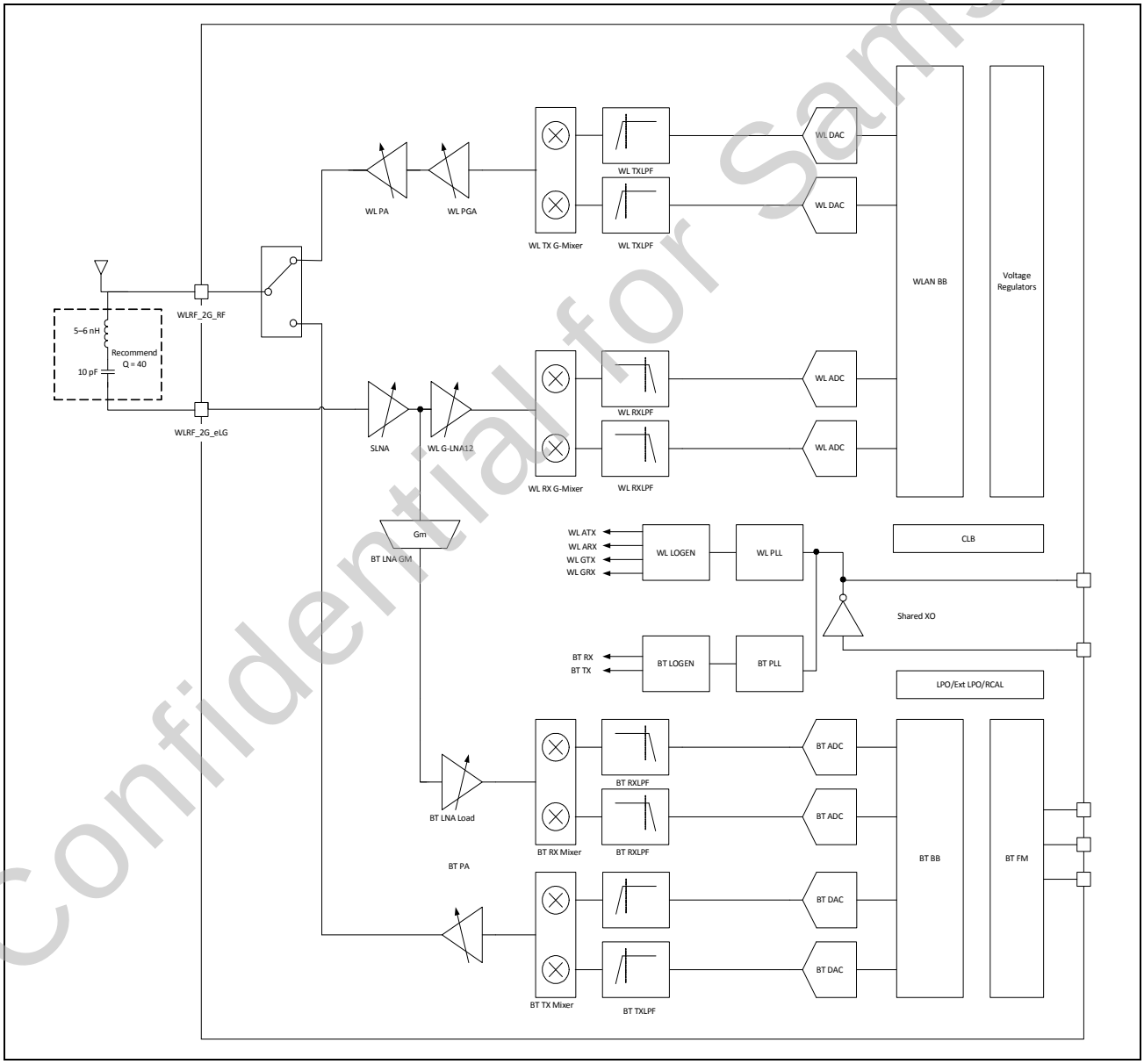
The PHY is capable of fully calibrating the RF front-end to extract the highest performance. On power-up, the PHY performs a full calibration suite to correct for IQ mismatch and local oscillator leakage. The PHY also performs periodic calibration to compensate for any temperature related drift, thus maintaining high-performance over time. A closed-loop transmit control algorithm maintains the output power at its required level and can control TX power on a per-packet basis.

Section 6: WLAN Radio Subsystem

The BCM4343S includes an integrated WLAN RF transceiver that has been optimized for use in 2.4 GHz Wireless LAN systems. It is designed to provide low power, low cost, and robust communications for applications operating in the globally available 2.4 GHz unlicensed ISM band. The transmit and receive sections include all on-chip filtering, mixing, and gain control functions. Improvements to the radio design include shared TX/RX baseband filters and high immunity to supply noise.

Figure 21 shows the radio functional block diagram.

Figure 21: Radio Functional Block Diagram



Receive Path

The BCM4343S has a wide dynamic range, direct conversion receiver. It employs high-order on-chip channel filtering to ensure reliable operation in the noisy 2.4 GHz ISM band.

Transmit Path

Baseband data is modulated and upconverted to the 2.4 GHz ISM band. A linear on-chip power amplifier is included, which is capable of delivering high output powers while meeting IEEE 802.11b/g/n specifications without the need for an external PA. This PA can be powered directly from VBAT, thereby eliminating the need for a separate PALDO. Closed-loop output power control is integrated.

Calibration

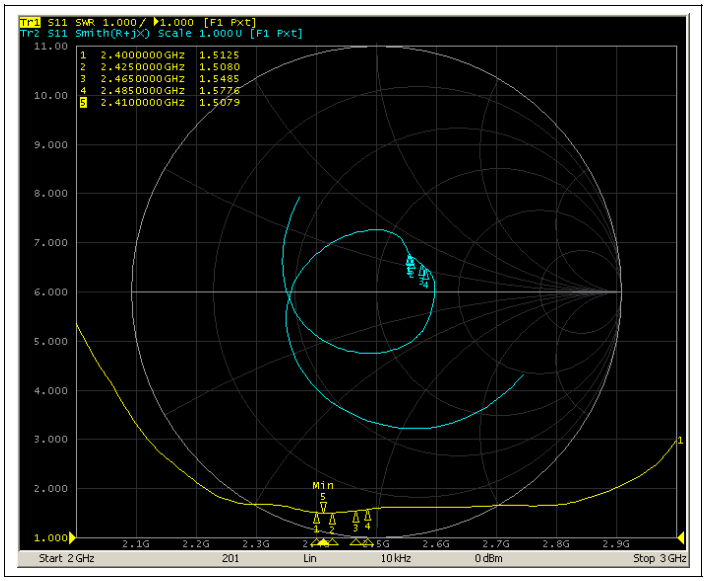
The BCM4343S features dynamic on-chip calibration, eliminating process variation across components. This enables the BCM4343S to be used in high-volume applications because calibration routines are not required during manufacturing testing. These calibration routines are performed periodically during normal radio operation. Automatic calibration examples include baseband filter calibration for optimum transmit and receive performance and LOFT calibration for leakage reduction. In addition, I/Q calibration, R calibration, and VCO calibration are performed on-chip.

4. 전기적 특성

4.1-1 시료 실장 측정

항 목				특 성
Frequency Range [MHz]				2400 ~ 2485
SWR [Max]				3.0 : 1 (Typ 2.5 : 1)
Input Impedance [Ω]				50 Ohm
Polarization				Linear
Gain [dBi]	Total Gain (Peak / Avg) [dBi]			-3.35 / -8.06
	Azimuth	Theta	Peak	-3.11
			Average	-6.47
		Phi	Peak	-6.55
			Average	-12.21
	Elevation 1	Theta	Peak	-2.74
			Average	-6.41
		Phi	Peak	-1.37
			Average	-7.40
	Elevation 2	Theta	Peak	-12.81
			Average	-18.88
		Phi	Peak	-1.26
			Average	-6.39

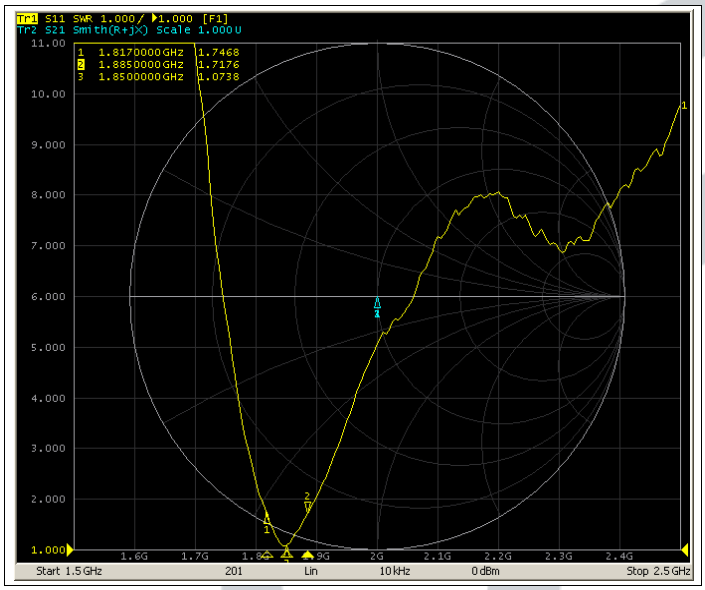
4.2 시료 실장 측정 그래프



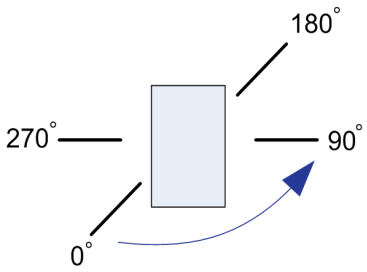
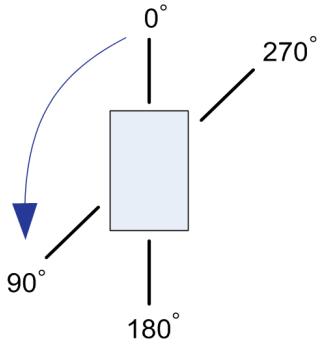
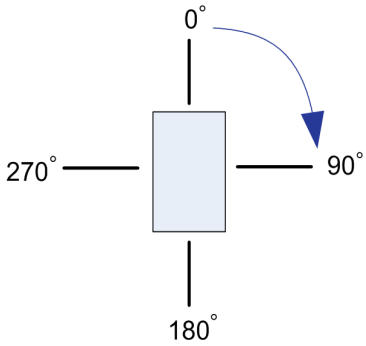
4.3 수동 지그 측정

항 목	특 성
Frequency Range [MHz]	1817 ~ 1885
Lower Frequency (1817MHz) SWR [Min~Max]	1.2 ~ 2.2 : 1 (Ref 1.7 : 1)
Upper Frequency (1885MHz) SWR [Min~Max]	1.2 ~ 2.2 : 1 (Ref 1.7 : 1)

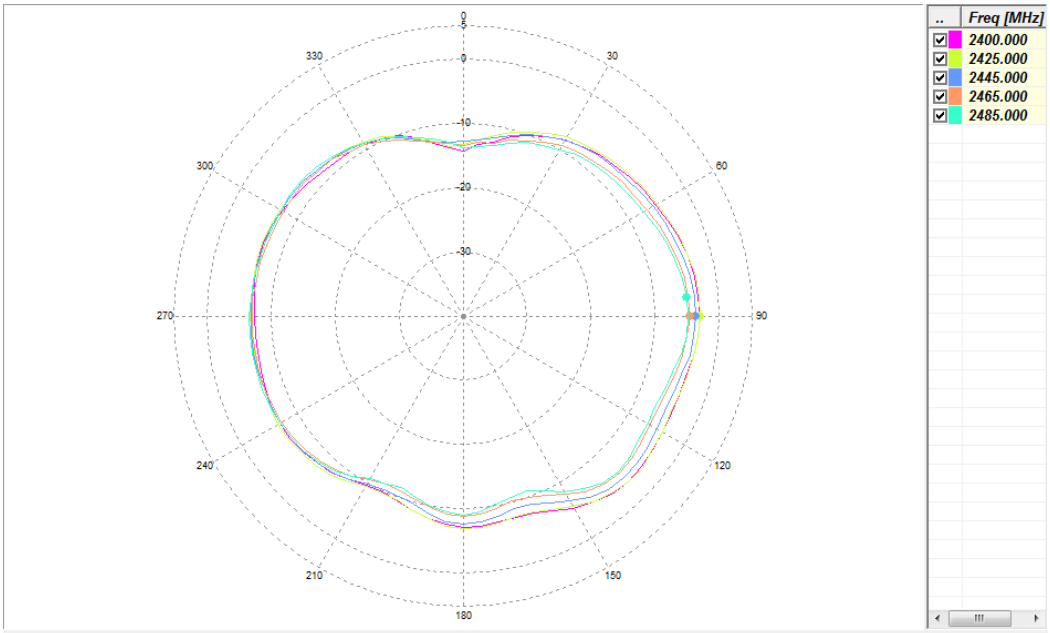
4.4 수동 지그 측정 그래프 CTF



4.5-1 방사 패턴

Azimuth Plane	Elevation1 Plane	Elevation2 Plane
		
Theta	Vertical field of measured plane	
Phi	Horizontal field of measured plane	

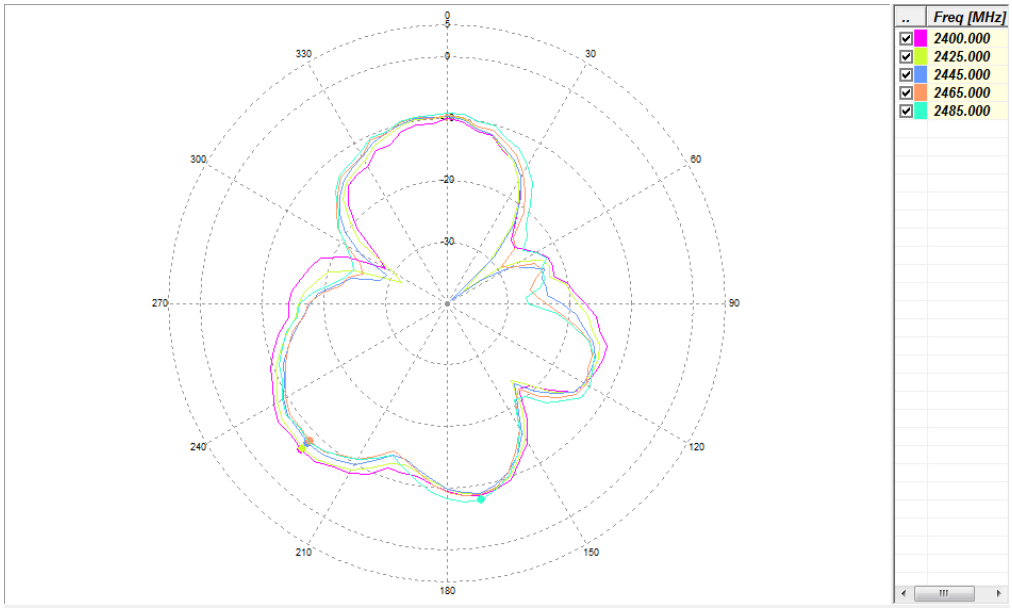
Azimuth Theta



H-Plan [Horizontal]

Frequency[MHz]	PeakValue	Theta[deg]	Phi[deg]	MinValue	Theta[deg]	Phi[deg]	3D Avg[dBi]	Gain[dBi]	Efficiency[%]
2400.000	-3.21	90	90	-14.33	90	0		-6.66	21.69
2425.000	-3.11	90	90	-13.59	90	355		-6.47	22.66
2445.000	-3.83	90	90	-12.85	90	355		-7.07	19.76
2465.000	-4.76	90	90	-13.44	90	0		-7.83	16.59
2485.000	-5.05	90	85	-13.85	90	0		-7.92	16.24

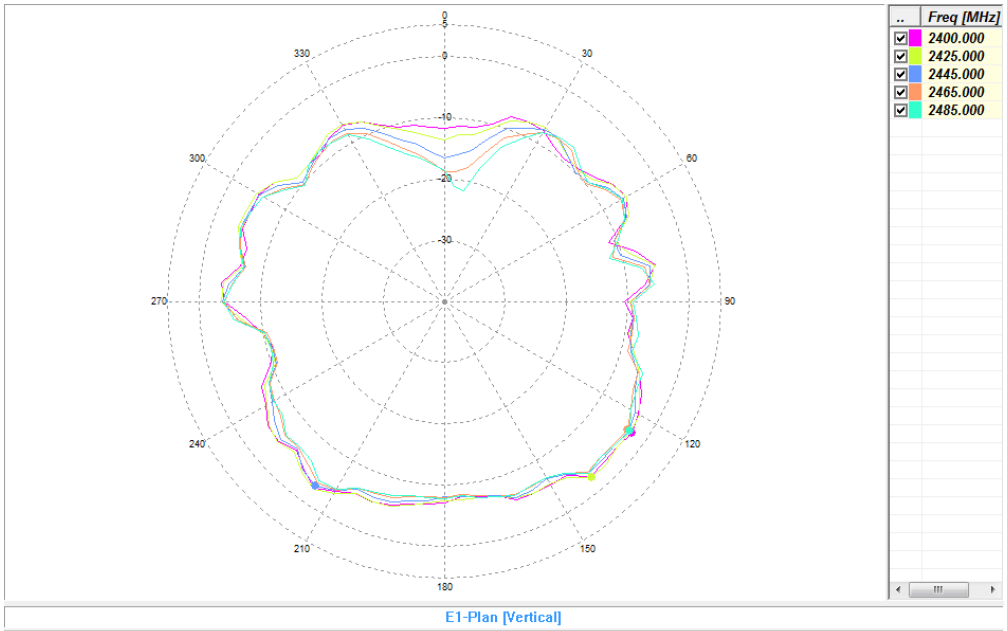
Azimuth Phi



H-Plan [Vertical]

Frequency[MHz]	PeakValue	Theta[deg]	Phi[deg]	MinValue	Theta[deg]	Phi[deg]	3D Avg[dBi]	Gain[dBi]	Efficiency[%]
2400.000	-6.55	90	225	-28.46	90	300		-12.21	6.12
2425.000	-6.96	90	225	-36.63	90	50		-12.57	5.65
2445.000	-8.15	90	225	-39.18	90	50		-13.11	5.00
2465.000	-8.44	90	225	-29.27	90	55		-13.08	5.03
2485.000	-7.81	90	170	-27.21	90	85		-12.49	5.75

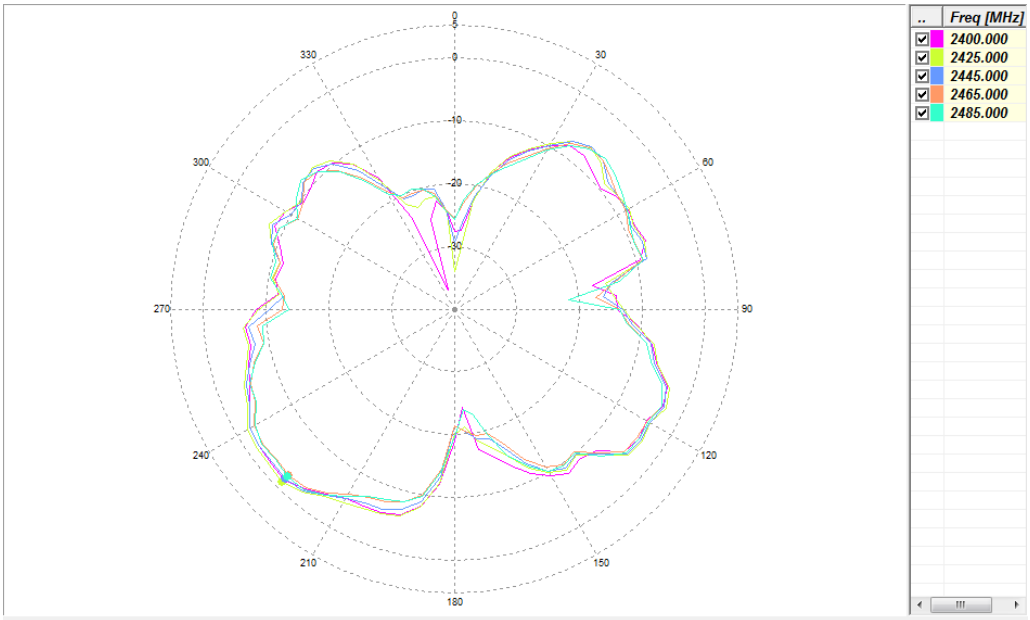
Elevation1 Theta



E1-Plan [Vertical]

Frequency[MHz]	PeakValue	Theta[deg]	Phi[deg]	MinValue	Theta[deg]	Phi[deg]	3D Avg[dBi]	Gain[dBi]	Efficiency[%]
2400.000	-2.76	125	0	-11.82	0	0		-6.52	22.38
2425.000	-2.74	140	0	-13.70	0	0		-6.41	22.98
2445.000	-3.32	215	0	-16.48	0	0		-7.01	20.02
2465.000	-3.65	125	0	-18.83	0	0		-7.44	18.15
2485.000	-3.20	125	0	-21.53	10	0		-7.36	18.46

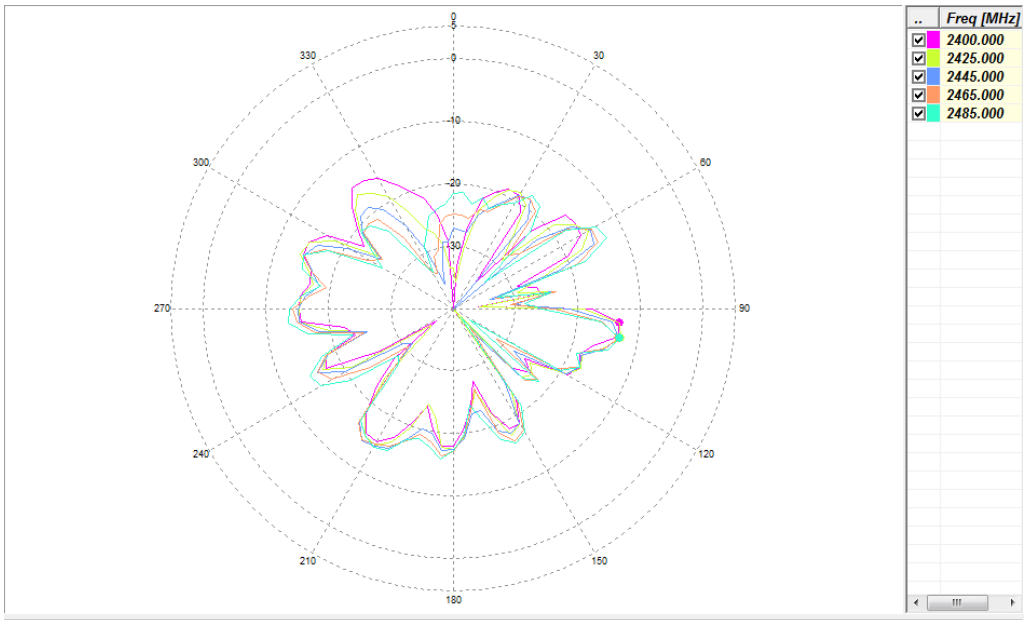
Elevation1 Phi



E1-Plan [Horizontal]

Frequency[MHz]	PeakValue	Theta[deg]	Phi[deg]	MinValue	Theta[deg]	Phi[deg]	3D Avg[dBi]	Gain[dBi]	Efficiency[%]
2400.000	-1.83	225	0	-36.55	340	0		-7.85	16.52
2425.000	-1.37	225	0	-33.87	0	0		-7.40	18.31
2445.000	-1.92	225	0	-29.25	0	0		-7.80	16.69
2465.000	-2.68	225	0	-25.51	0	0		-8.46	14.36
2485.000	-2.39	225	0	-25.72	0	0		-8.30	14.91

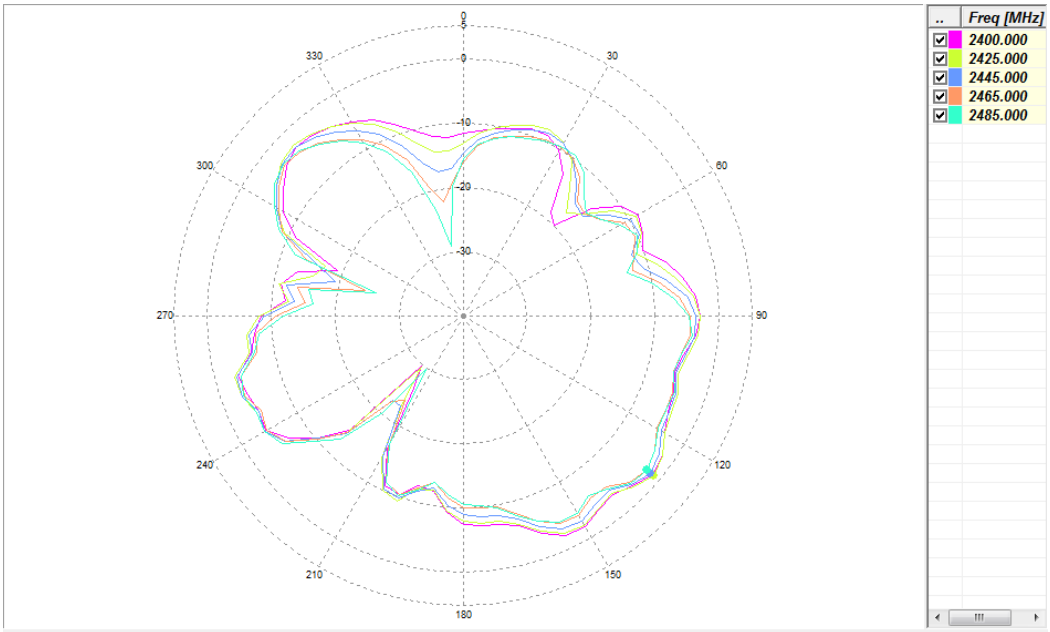
Elevation2 Theta



E2-Plan [Vertical]

Frequency[MHz]	PeakValue	Theta[deg]	Phi[deg]	MinValue	Theta[deg]	Phi[deg]	3D Avg[dBi]	Gain[dBi]	Efficiency[%]
2400.000	-13.31	95	90	-43.45	0	90		-18.77	1.44
2425.000	-12.81	100	90	-42.49	140	90		-18.88	1.40
2445.000	-13.19	100	90	-42.42	45	90		-19.03	1.36
2465.000	-13.23	100	90	-35.99	140	90		-19.01	1.37
2485.000	-13.05	100	90	-38.11	140	90		-18.39	1.56

Elevation2 Phi



E2-Plan [Horizontal]

Frequency[MHz]	PeakValue	Theta[deg]	Phi[deg]	MinValue	Theta[deg]	Phi[deg]	3D Avg[dBi]	Gain[dBi]	Efficiency[%]
2400.000	-1.62	130	90	-29.73	220	90		-6.54	22.29
2425.000	-1.26	130	90	-29.64	220	90		-6.39	23.06
2445.000	-1.90	130	90	-22.88	215	90		-6.97	20.18
2465.000	-2.61	130	90	-24.17	285	90		-7.74	16.94
2485.000	-2.61	130	90	-29.80	215	90		-7.66	17.26

5. 시험 방법

5.1 SWR/Return loss

Network Analyzer를 이용하여 SWR / Return loss를 측정하며 표본 샘플을 선별, 수동 지그 측정 또는 자동화 검사장비를 이용하여 양품과 불량품을 선별한다.

	시료 측정 조건	수동 지그 측정 조건
Network Analyzer	Agilent HP8753E	Agilent E5071C
Cable	RF cable (300 mm)	RF cable (300 mm)
Test condition