Driving the wireless future™

The Atheros Chipset for 108Mb/s Wireless LANs

Bill McFarland, Director of Algorithms and Architecture

ATHEROS™
COMMUNICATIONS

Outline

WLAN Tutorial

- Market & Regulatory
- Standards
  - Modulation overview
  - MAC overview (QoS)
  - Throughput and system capacity
  - Security

Chipset Overview

- Client MAC/Baseband chip
- 2.4 GHz and 5 GHz analog chips
- Integrated Access Point chip
- Measured performance

WLAN Market

WLAN is rapidly growing and shifting towards 5 GHz/802.11a

- 2002 InStat market report predicts (millions of units):

WLAN Type	2002	2004	2006
802.11b (2.4GHz)	12.8	25.2	23.6
802.11a (5GHz)	0.7	6.5	16.3
Dual mode, dual band	0.7	7.0	29.3

- Laptops are currently the primary driver
- Future drivers include
  - Hotspot/WAN access (cell phones / PDAs)
  - Home/consumer electronics, particularly digital video

Unlicensed spectrum for WLAN has been allocated on a country/ regional basis

- 2.4-2.483 GHz (83 MHz total) has been available in most counties for many years
- Many countries have created much larger allocations at 5 GHz in the past few years:

Region	5.15-5.25	5.25-5.35	5.47-5.725	5.725-5.825	Total (MHz)
USA	200mW	1W		4W	300
Europe	200mW	200mW	1W		455
Japan	200mW				100
Asia Pacific, including Korea, Hong Kong, China, Singapore, New Zealand, Australia	200mW (Singapore, Australia, NZ)	200mW (Singapore, Australia, NZ, Taiwan)		100mW to 1W (all, at various power levels)	300

More spectrum = higher data rates and larger overall system capacity

- Radio is fundamentally a shared medium
- Current 2.4 GHz systems are limited to only 3 independent 11 Mb/s channels
- Current 5 GHz systems have >13 54 Mb/s channels

Currently, the only WLAN standards that matter are created in IEEE 802.11. Work is ongoing on numerous enhancements:

- **802.11**: Original standard provided for 1 and 2 Mb/s PHY layer, CSMA/CA MAC, adopted in 1997
- **802.11a**: enhancement to provide 54Mb/s in the 5 GHz band, adopted 1999
- **802.11b**: enhancement to provide 11Mb/s in the 2.4 GHz band, adopted 1999
- **802.11d**: Changes for international regulatory compliance, adopted 2001
- **802.11e**: Enhancements to the MAC to provide QoS through prioritized CSMA and advanced polling techniques, still in debate
- **802.11f**: Recommended practices for Inter-access point communication, nearly completed
- **802.11g**: PHY layer enhancement to provide 54Mb/s in the 2.4GHz band, still in debate
- **802.11h**: Enhancements to 802.11a to help with regulatory compliance in Europe, still in debate
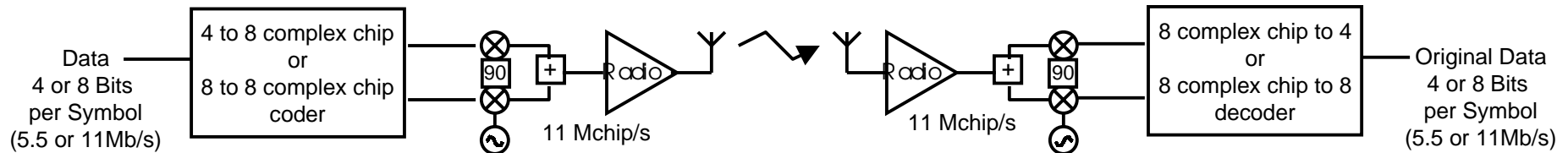- **802.11i**: Enhancements for greater security, still in debate

Modulation (DSSS and CCK)

802.11: Direct Sequence Spread Spectrum (DSSS, 1 & 2 MB/s)
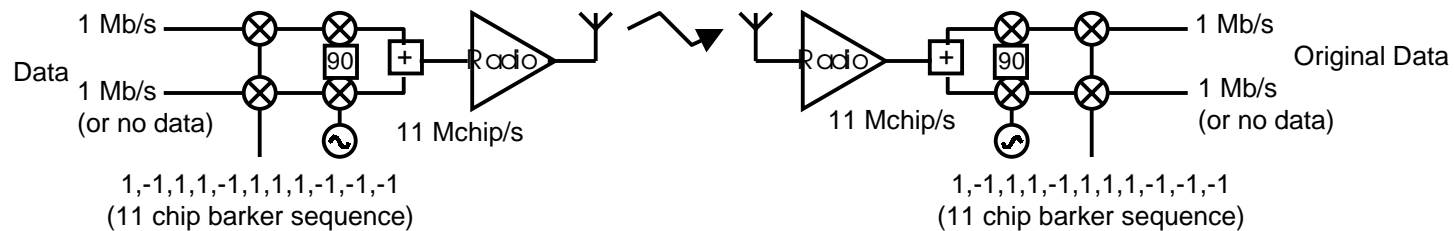
- Not really CDMA, only one station in a cell transmits at a time
- Spreading done to meet regulatory rules, and provide some added robustness to multi-path (echoes)

802.11b: Complementary Code Keying (CCK, 5.5 & 11 Mb/s)
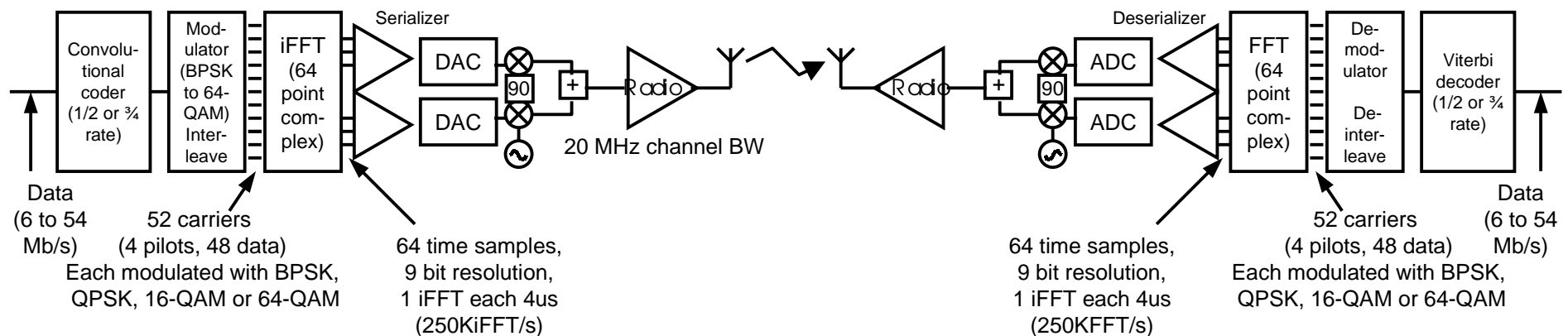

- Code expansion is small, and code is not optimal. Coding gain is limited to ~2 dB.
- Equalizer is required to deal with multi-path, computational load is proportional to the square of the data rate

Modulation (OFDM)

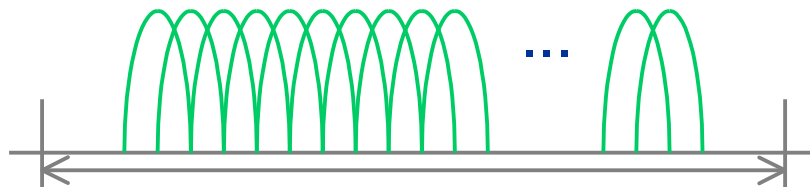## 802.11a: Orthogonal Frequency Division Multiplexing (OFDM)

Data (6 to 54 Mb/s)

52 carriers (4 pilots, 48 data) Each modulated with BPSK, QPSK, 16-QAM or 64-QAM

64 time samples, 9 bit resolution, 1 iFFT each 4us (250KiFFT/s)

20 MHz channel BW

64 time samples, 9 bit resolution, 1 iFFT each 4us (250KFFT/s)

52 carriers (4 pilots, 48 data) Each modulated with BPSK, QPSK, 16-QAM or 64-QAM

Data (6 to 54 Mb/s)

- Data rate on each carrier is very low; multi-path echoes are short compared to the symbol time. No time domain equalizer is required.

- The iFFT and FFT are very efficient. The computational load is proportional to $(R/2)*\log_2(R)$, where R is the data rate (compared to R^2 for an equalized system)

- A strong convolutional code (½ rate or ¾ rate) creates redundancy across the carriers that resists interference and frequency selective channels (coding gain >5dB)

- Orthogonal spacing of the carriers allows a high data rate in a narrow channel bandwidth (54Mb/s in a 20 MHz channel)

- Atheros Turbo mode doubles the data rate (and consumed bandwidth), providing 108Mb/s in 40MHz channels
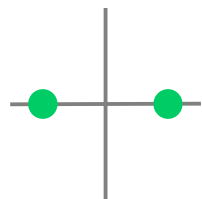
OFDM (52 carrier signals)

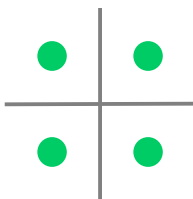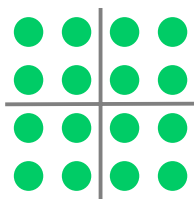Each carrier is modulated
with data according to one of:

BPSK

QPSK

16QAM

64QAM

6 Mb/s	12 Mb/s	24 Mb/s	48 Mb/s
(1/2 rate code)	(1/2 rate code)	(1/2 rate code)	(2/3 rate code)
or	or	or	or
9 Mb/s	18 Mb/s	36 Mb/s	54 Mb/s
(3/4 rate code)	(3/4 rate code)	(3/4 rate code)	(3/4 rate code)

Lower data rates support longer range.
Radios automatically change data rates as required to maintain connection.

X_1 *

Time

X_2 *

X_3 *

X_4 *
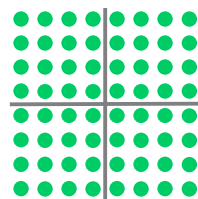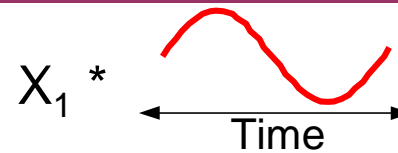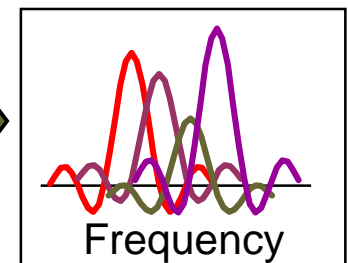
Symbol

- Different data per tone (via FFT)
- Multipath just scales tones
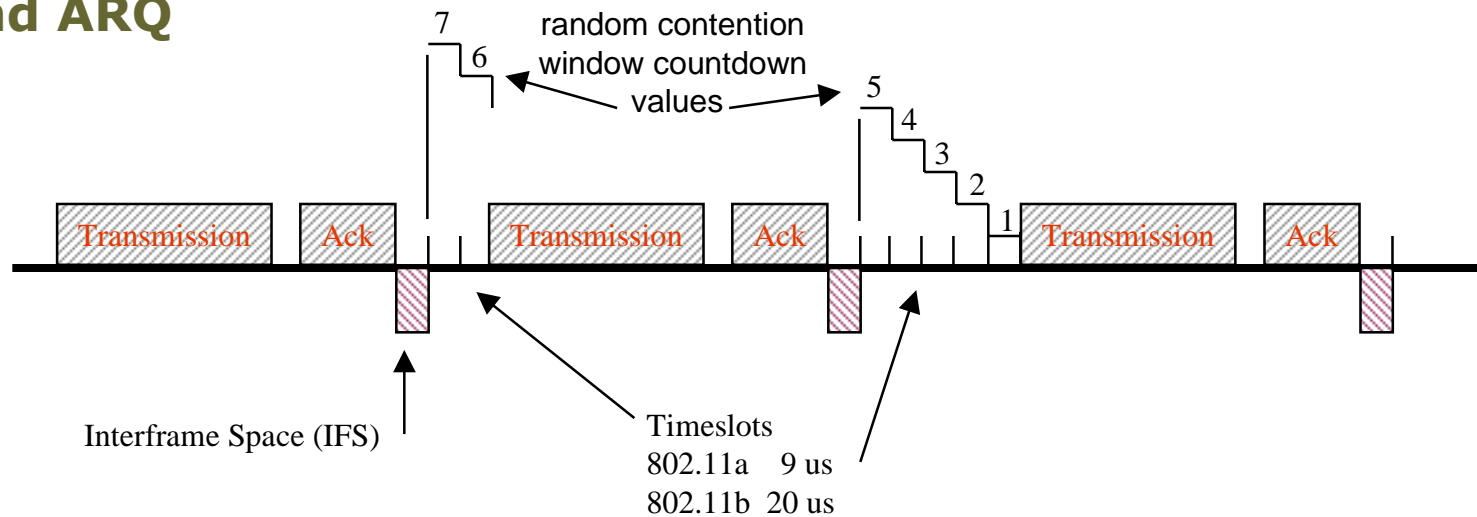- Tones remain orthogonal even with multipath

Frequency

As transmitted

Frequency
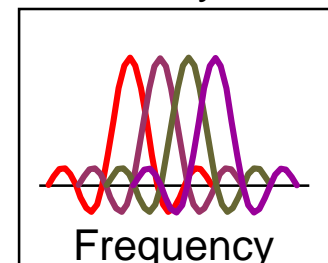
As received
after echoes in channel
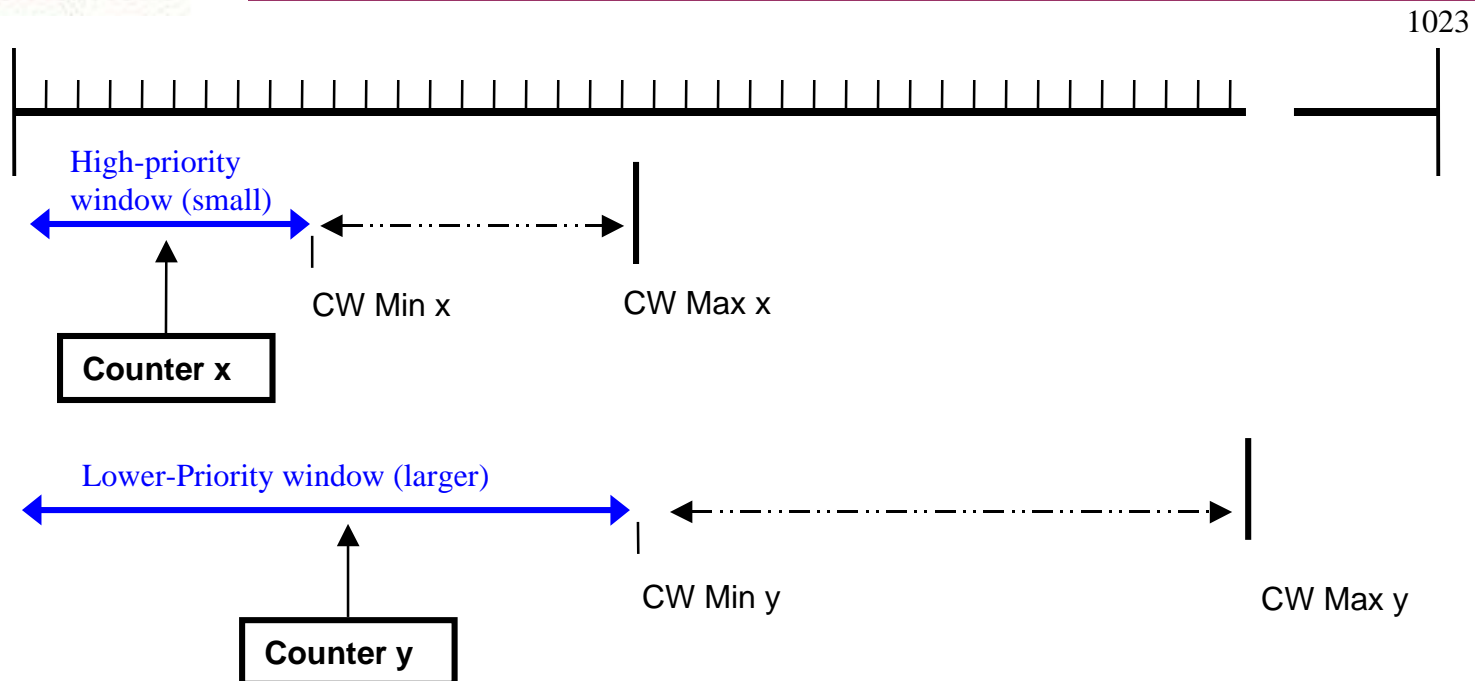
Media Access Control (DCF)

Basic MAC is listen before talk, with slotted random backoff, and ARQ

- It is more expensive to build radios that transmit and receive at the same time. Therefore it is hard to detect collisions.
- Normal packet loss rates are much higher in radio than in wired systems.
- Use of ARQ (Acknowledgements) at the PHY layer greatly increases robustness, but degrades throughput.

MAC Enhancements for QoS (EDCF)

1023

High-priority window (small)

CW Min x   CW Max x

Counter x

Lower-Priority window (larger)
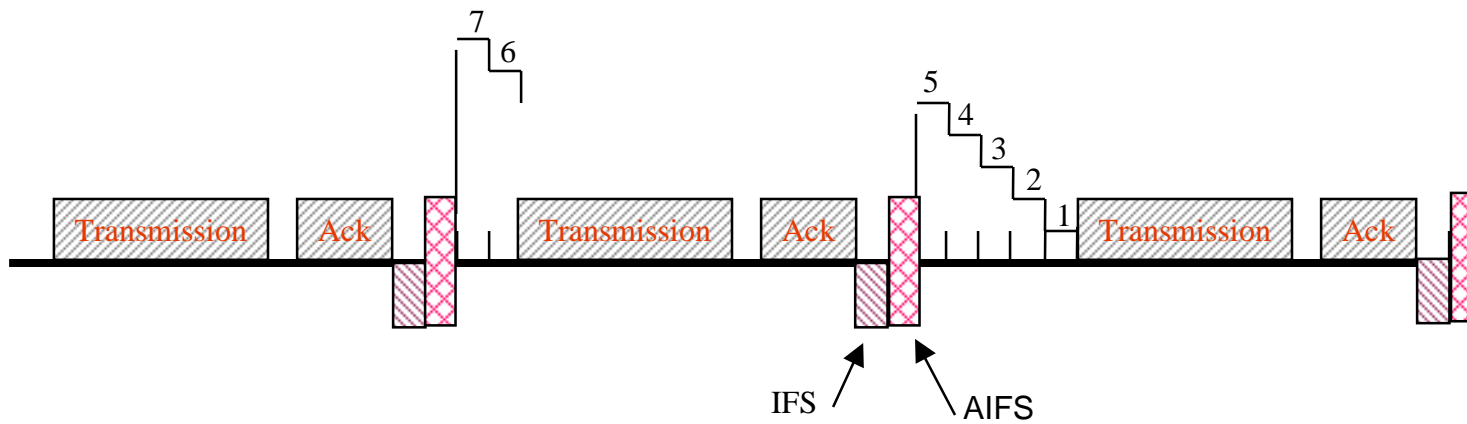
CW Min y   CW Max y

Counter y

EDCF has 8 counters and 8 pairs of (CW Min, CW Max) values, one for each of the 802.1p Traffic Class (TC) priority levels. TC 0 is lowest priority, TC 7 is highest.

High-priority >> small window >> greater access

Exemplifies the IETF concept of Differentiated Service (DIFFSERV).

IFS

AIFS

AIFS value for each priority class extends the IFS spacing.
Timeslot counting is delayed by the AIFS amount.

AIFS=1 is shown in the picture.

EDCF (3)

- EDCF defines three "knobs"
    - CW Min adjusts contention algorithm
    - CW Max bounds retransmission backoff window
    - AIFS inhibits access by traffic class
- 802.11e draft defines default values
- Defaults may be overwritten by AP via Beacon
- Effects
    - small AIFS values have large effect on latency
    - CW Min values control contention probability
        - adjust for small, medium, large number of stations within TC
        - adjust for gross differentiation between TCs
    - slow-acting adaptation to traffic is feasible
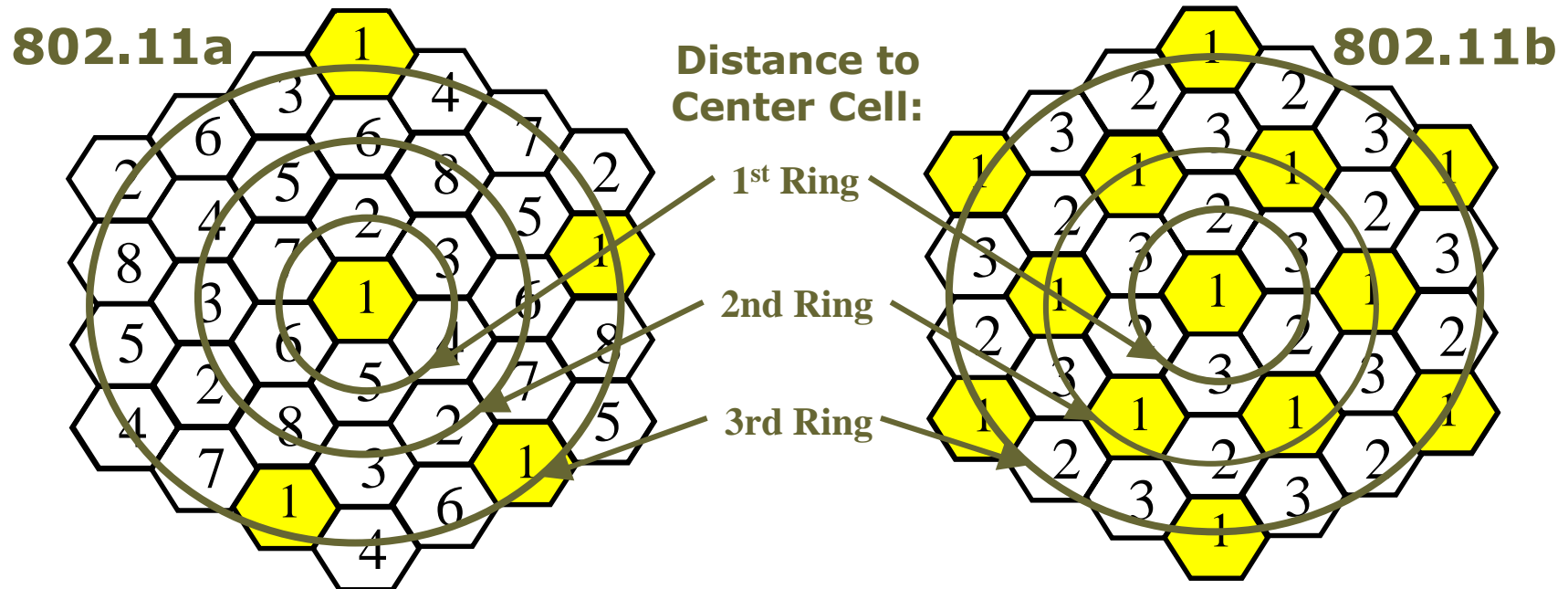
What is System Capacity?

System Capacity is total <u>throughput</u> in a multi-cell deployment

$$\text{System Capacity} = \text{Number of Cells} \times \text{Cell Throughput} \times \text{CCI Penalty}$$

Co-Channel Interference (CCI) Penalty depends on:

- Number of Cells
- Cell Diameter

Higher System Capacity

802.11a

802.11b

Distance to Center Cell:

1st Ring

2nd Ring

3rd Ring

- Large areas with 802.11a will suffer less Co-Channel Interference (CCI) than with 802.11b – resulting in higher system capacity
- Many cell systems can also include multi-story deployments
- Interference can come from other neighbors in multi-dwelling units

14

Average Cell Throughput Comparison
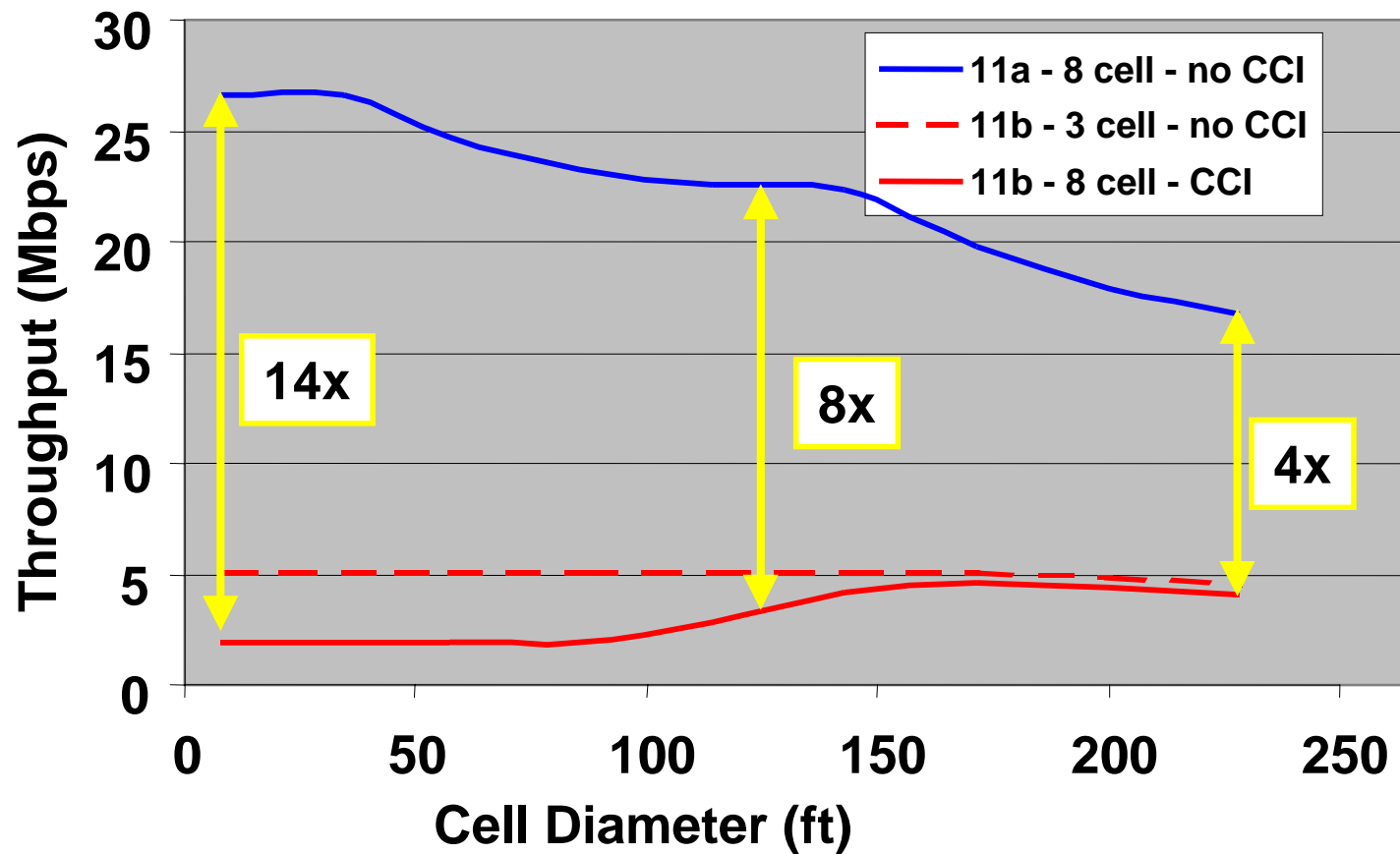
Throughput and System Capacity

Mode →	Atheros Turbo	11a & 11b overlaid	11a	OFDM at 2.4GHz	50/50 mix 11g/11b	11b
Raw data rate (Mb/s)→	108	54 & 11	54	54	54 & 11	11
Single Cell throughput UDP	54.3	37.6	30.5	30.5	9.9	7.1
Single CellS throughput TCP/IP	42.5	30.3	24.4	24.4	7.9	5.9
# of Channels available	5 (US)	12/3 (US) 19/3 (EU)	12 (US) 19 (EU)	3	3	3
UDP System Capacity	212.5 (US)	387 (US) 601 (EU)	366 (US) 580 (EU)	91.5	29.7	21.3

- All values in Mb/s, operation at the maximum PHY layer rate assumed
- 11b results assume short preamble mode
- Mixed 11b/11g assumes short preamble with legacy RTS/CTS
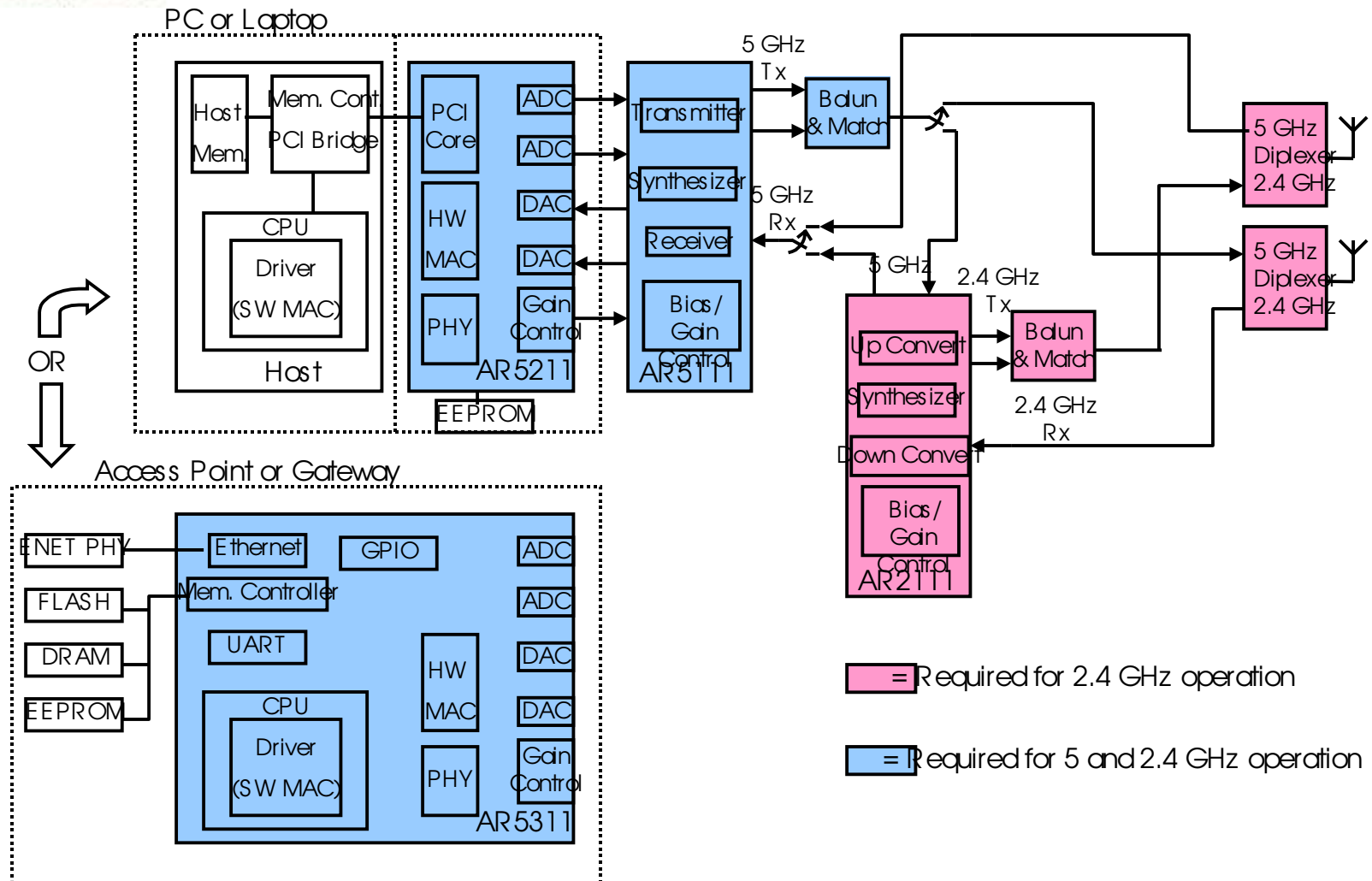
802.11 Security

Link Layer Encryption

- **WEP (Wired Equivalent Privacy):** The original simple encryption method, based on RC4. No longer considered secure since several attacks are known. Provides privacy only, no integrity check.

- **TKIP (Temporal Key Exchange Protocol):** A "fix" for WEP that scrambles the key between packets and adds a message integrity check to prevent spoofing. 802.11 considers this a temporary fix.

- **AES (Advanced Encryption Standard):** NIST standard symmetric block cipher intended to replace DES. It is considered to be "military strength" and includes an integrity check. This is the long term solution chosen by 802.11.

System level Security

- **802.1x:** A general purpose and extensible framework for authenticating users and generating/distributing keys for encryption.

- **SSN/RSN (Simple Secure Network):** A recipe for authentication based on 802.1x, bridging between an 802.11 base station and an authentication server in the network.
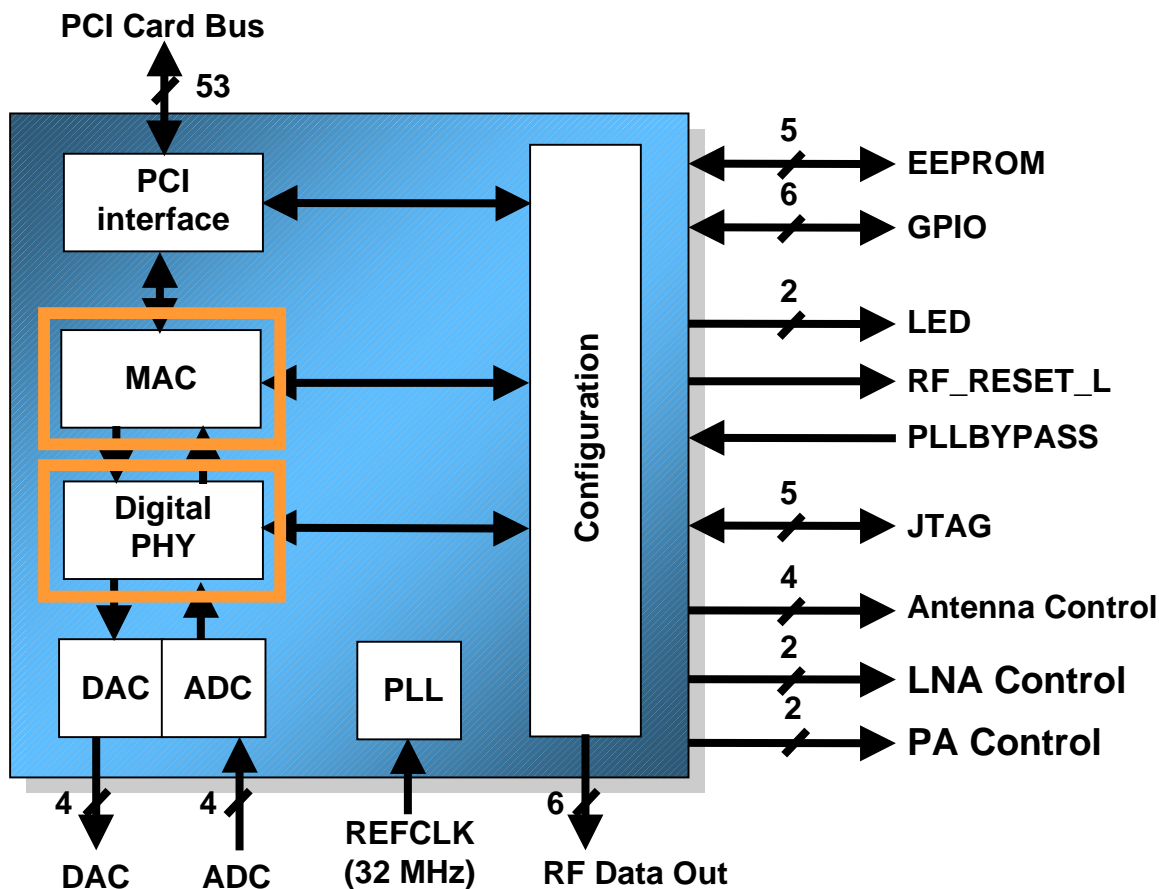
Chipset Overview

PC or Laptop

Host Mem.
Mem. Cont
PCI Bridge
CPU
Driver (SW MAC)
Host

PCI Core
HW MAC
PHY
AR5211
EEPROM

ADC
ADC
DAC
DAC
Gain Control

Transmitter
Synthesizer
Receiver
Bias/Gain Control
AR5111

5 GHz Tx
5 GHz Rx

Balun & Match

5 GHz Diplexer 2.4 GHz
5 GHz Diplexer 2.4 GHz

Up Convert
Synthesizer
Down Convert
Bias/Gain Control
AR2111

2.4 GHz Tx
2.4 GHz Rx

Balun & Match

OR

Access Point or Gateway

ENET PHY
FLASH
DRAM
EEPROM

Ethernet
Mem. Controller
UART
CPU
Driver (SW MAC)

GPIO
HW MAC
PHY

ADC
ADC
DAC
DAC
Gain Control
AR5311

= Required for 2.4 GHz operation

= Required for 5 and 2.4 GHz operation

18

AR5211 Baseband IC

PCI Card Bus

53

- PCI interface
- MAC
- Digital PHY
- DAC
- ADC
- PLL
- Configuration

EEPROM — 5
GPIO — 6
LED — 2
RF_RESET_L
PLLBYPASS
JTAG — 5
Antenna Control — 4
LNA Control — 2
PA Control — 2

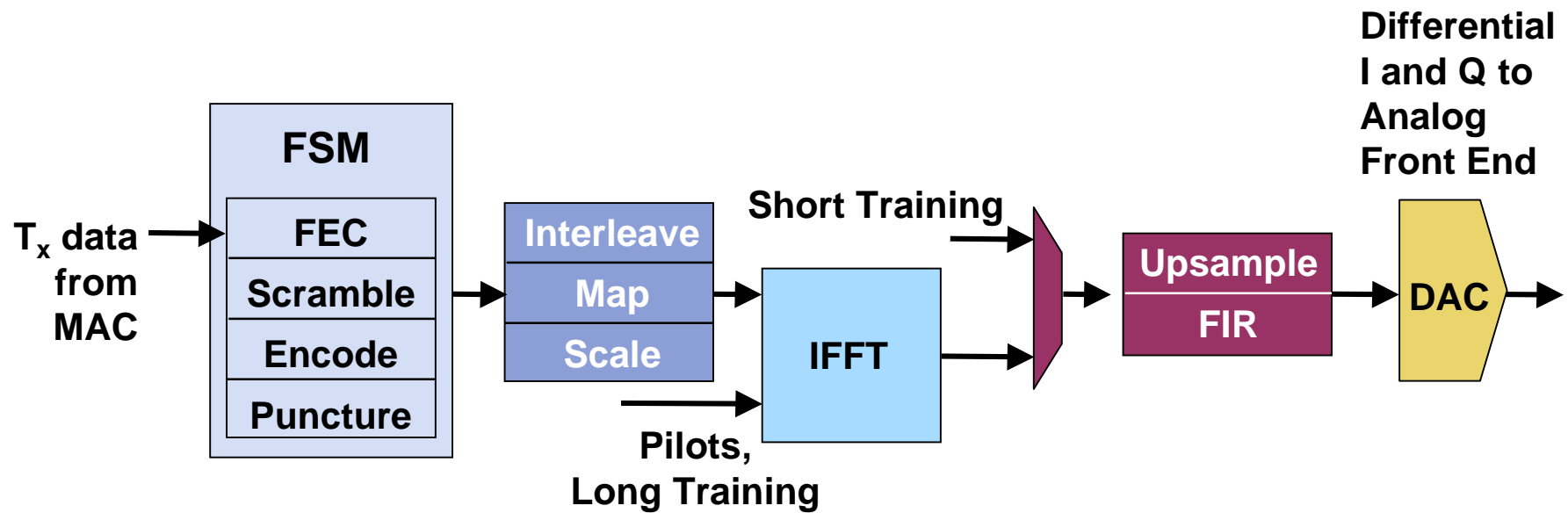DAC — 4
ADC — 4
REFCLK (32 MHz)
RF Data Out — 6

AR5211

- Two 80 Ms/s 9 bit ADCs
- Two 176Ms/s 9 bit DACs
- 196 pin PBGA
- ~7 M transistors
- 0.25um CMOS
- 175 GOPs equivalent
- WEP, AES encryption in hardware
- QoS support via EDCF with 12 priority queues
- <250 mW
- 802.11a data rates from 6 to 54Mb/s
- Turbo data rates from 12 to 108Mb/s
- 11b data rates from 1 to 11Mb/s
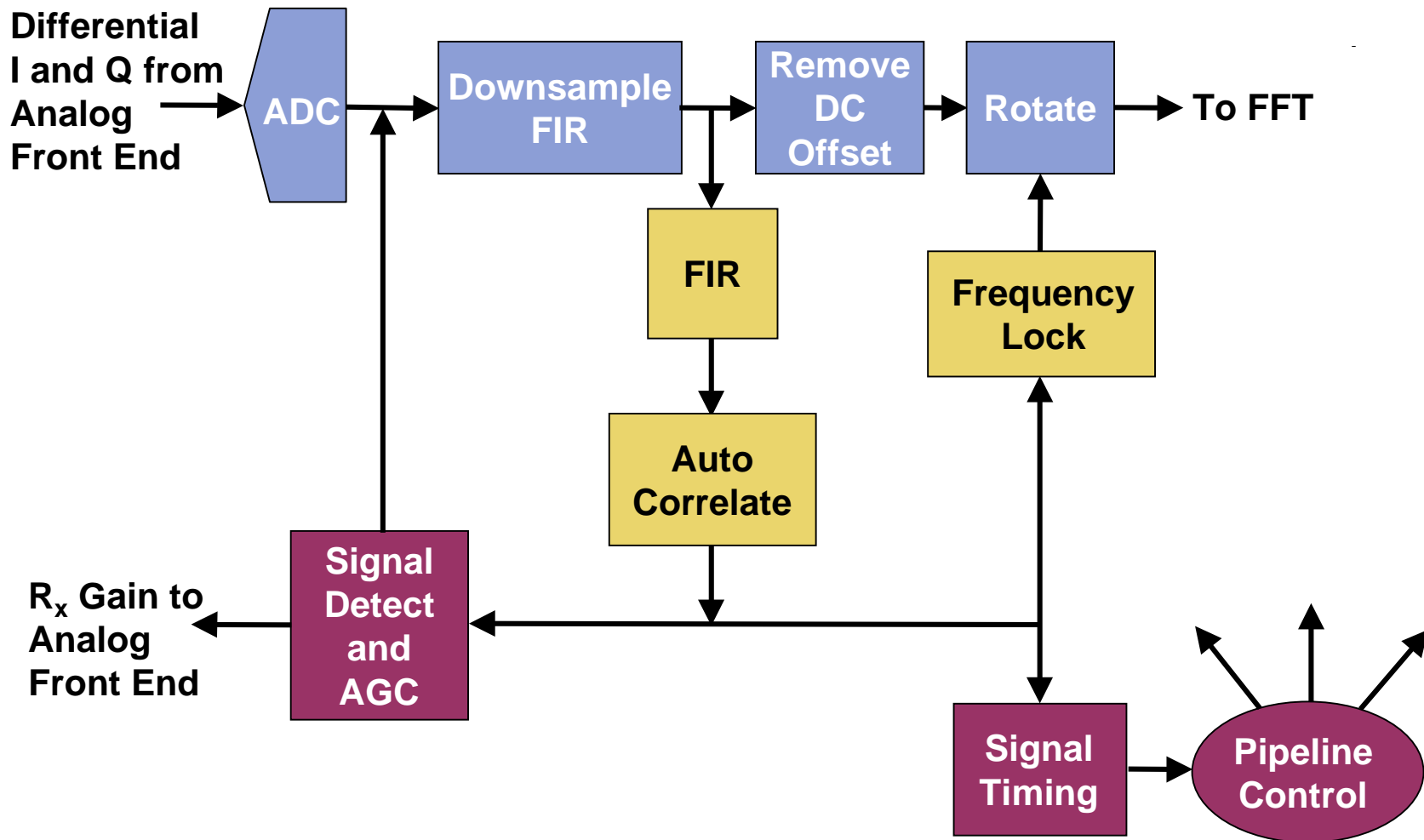
MAC Internals
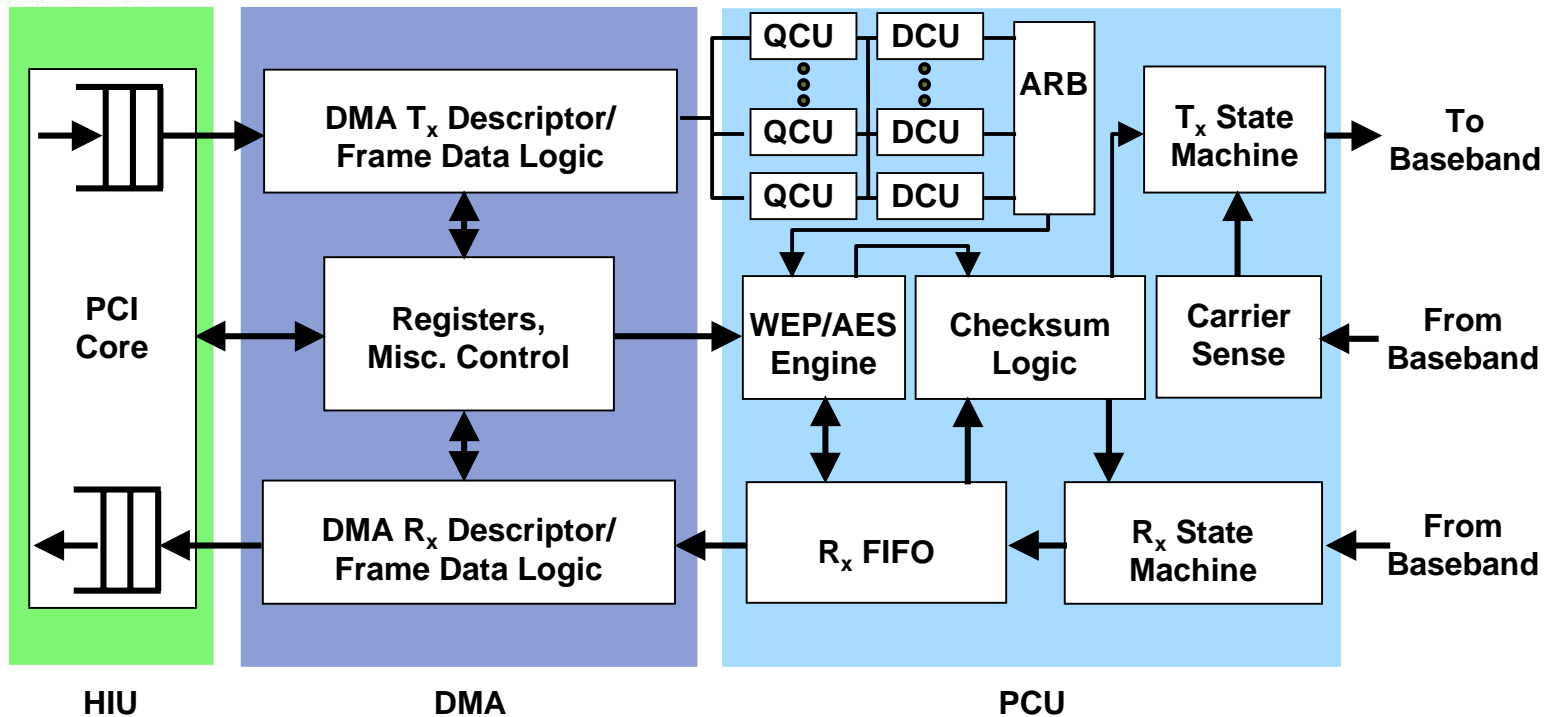
- Each QCU is associated with a individual stream of data
- Each DCU is associated with a QoS priority level
- The ARB chooses which packet goes next
- The MAC generates and sends packets that are time critical: ACKs, CTS, etc., and handles the automatic retransmission of failed packets (no ACK received)
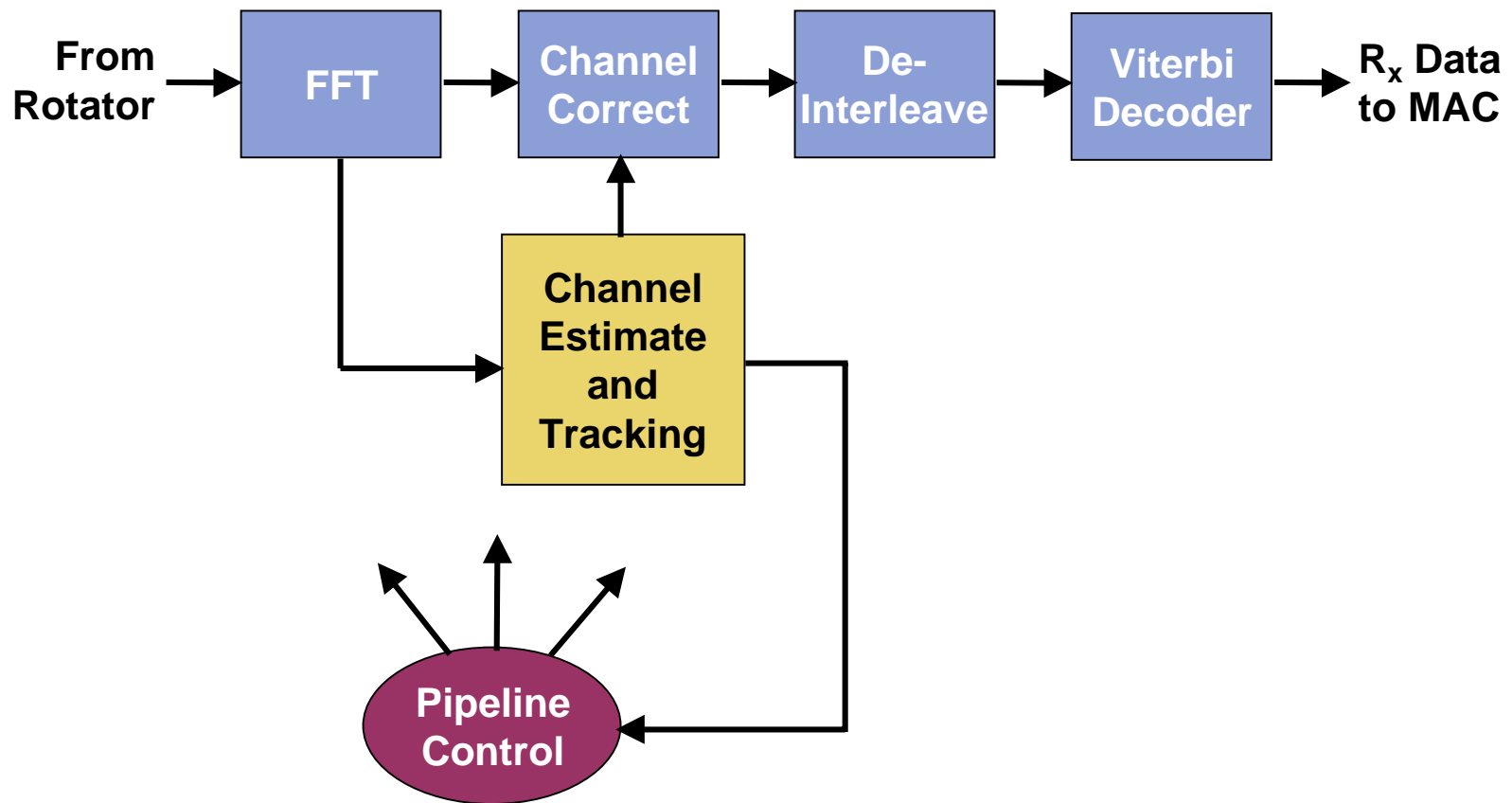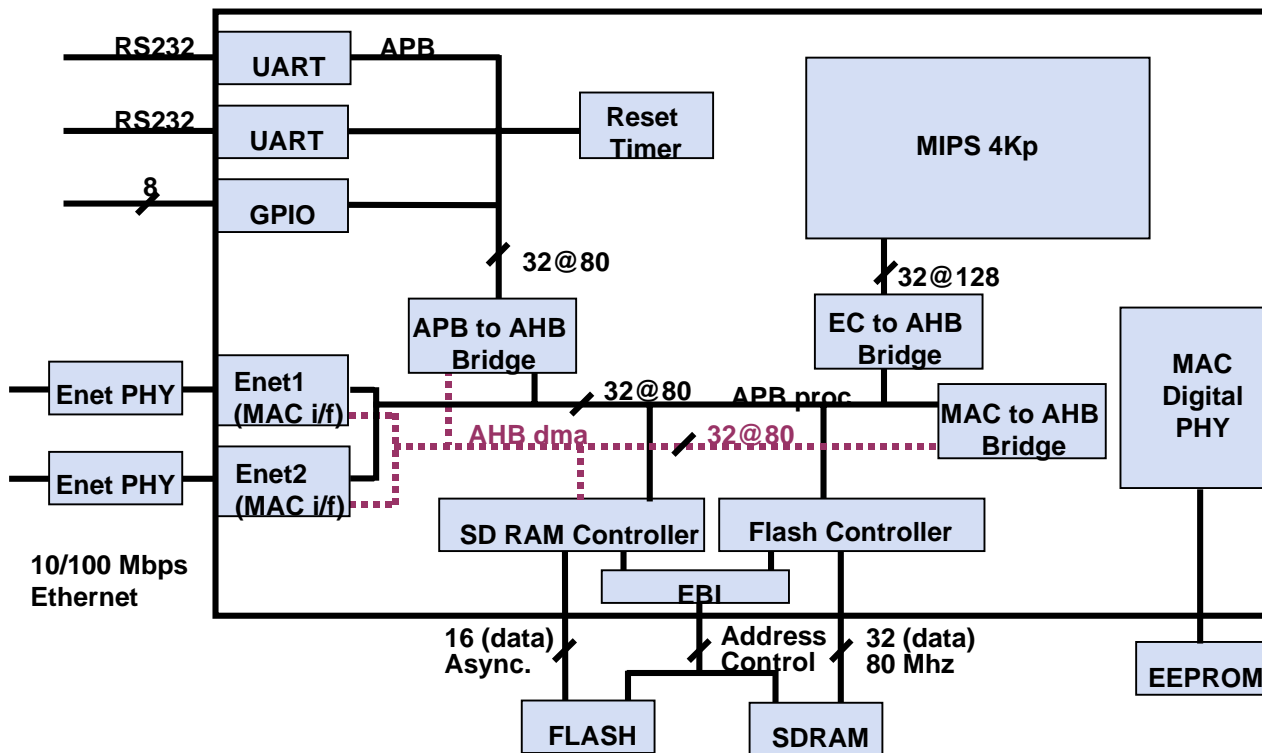
20

Digital PHY Tx internals

Digital PHY Rx Internals (2)

From Rotator → **FFT** → **Channel Correct** → **De-Interleave** → **Viterbi Decoder** → R$_x$ Data to MAC

**Channel Estimate and Tracking**

Pipeline Control

AR5311

- MAC and Digital PHY the same as AR5211
- 32-bit MIPS R4000 processor
- 16kB instruction cache
- 16kB data cache
- 1 Mb/s UART, can control Bluetooth radio
- Two Ethernet MACs for chaining with legacy AP or use as firewall device
- 32-bit SDRAM interface
- 16-bit FLASH interface
- Can support up to 4 memory devices
- Second FLASH interface can be used as local bus
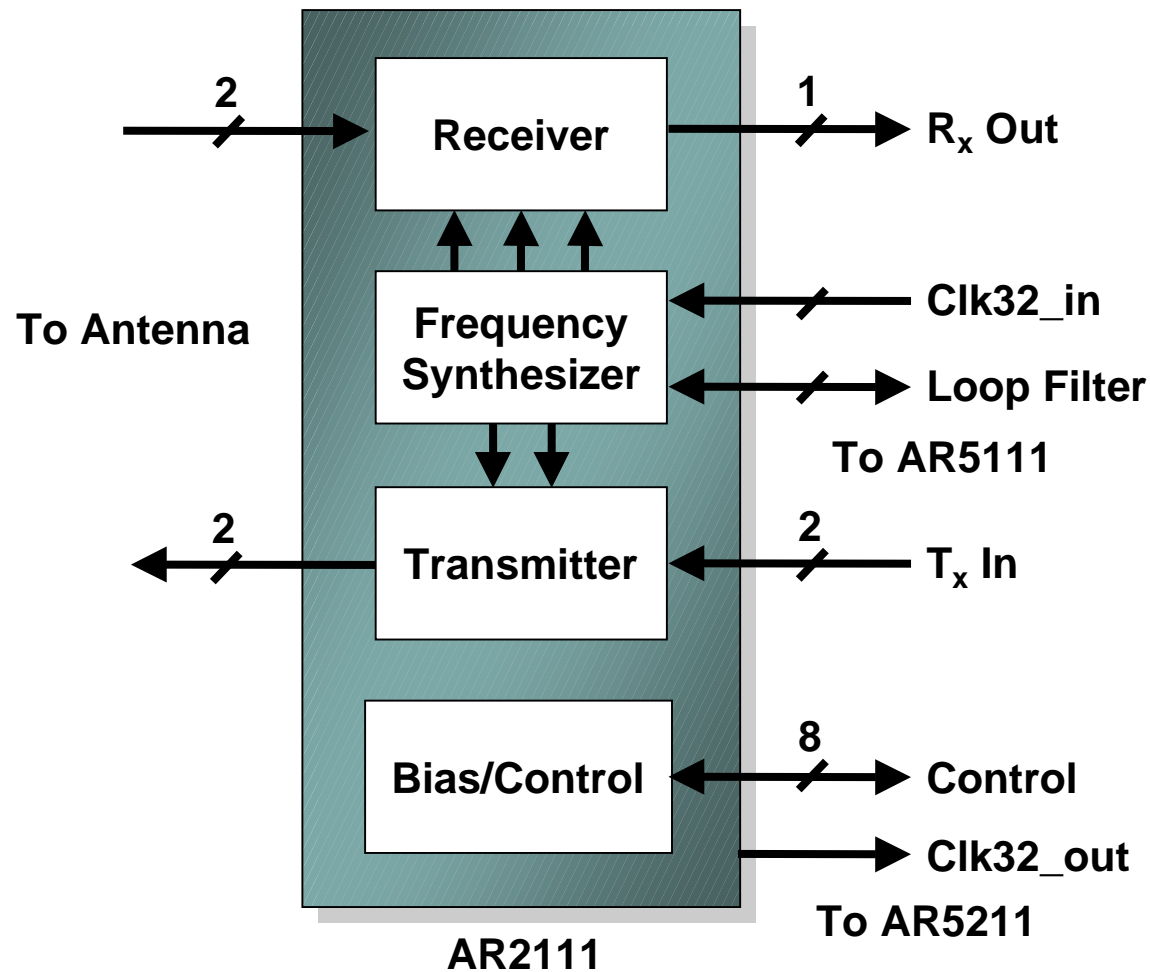- ~11M transistors, 0.25um CMOS
- 388 pin PBGA

AR5111 5 GHz Radio IC
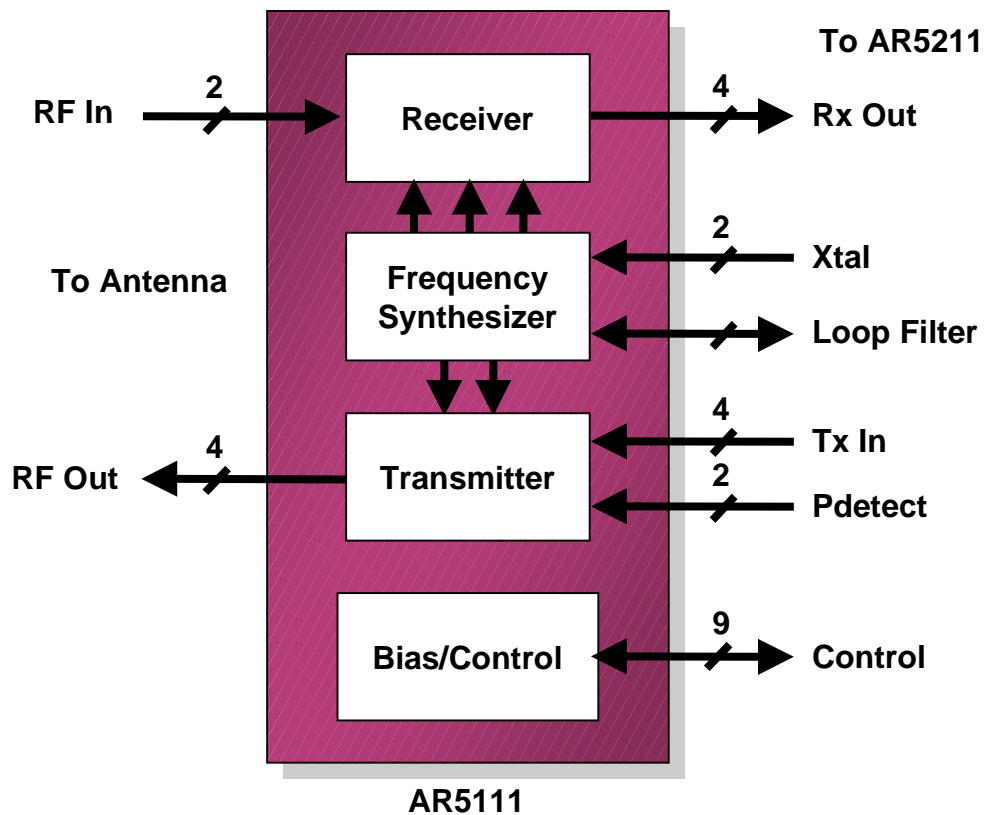
- On-chip transmit and receive filters
- Ultra-wide tuning range: 4.9-6 GHz
- On-chip Power Amplifier delivers 16dBm
- On-chip LNA with 5dB NF
- 64 pin QFN
- Standard 0.25um digital CMOS
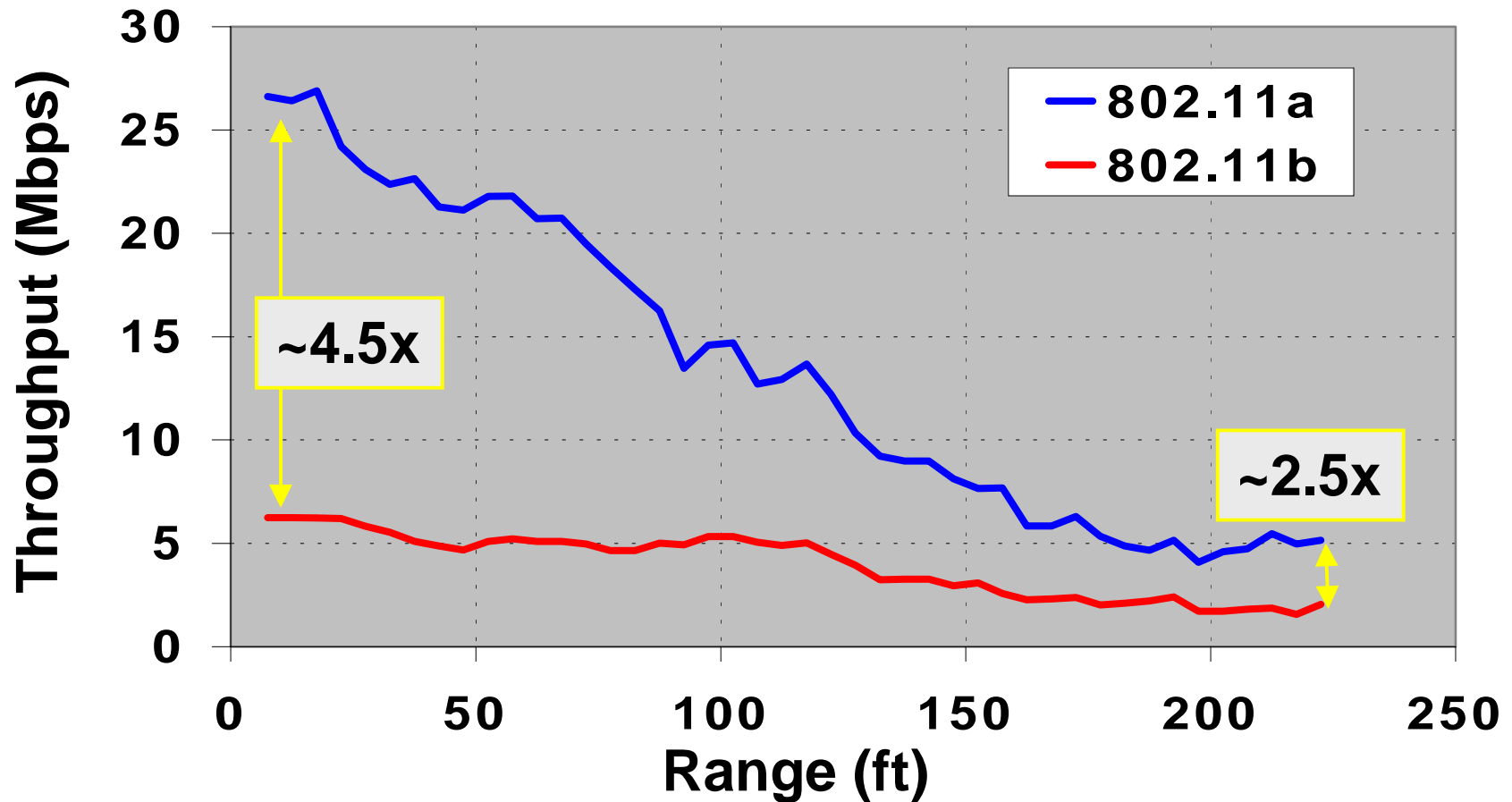
AR2111 Frequency Converter

- Converts signals between 5 GHz and 2.4 GHz
- Can support 802.11b or OFDM in the 2.4 GHz band (802.11g)
- 48 pin QFN
- Standard 0.25um digital CMOS

Measured Range and Data Rate

802.11a provides 2 to 4.5 times the throughput of 802.11b at the same distance when tested to 225 feet .

Summary

The Atheros 5001X chipset provides:

- Two chip 802.11a client solution, three chips for 802.11a/802.11b dual mode
- Two chip 802.11a Access Point solution
- Raw data rates from 1 to 108 Mb/s
- "Military strength" AES encryption and security
- Priority based Quality of Service

- More information about the 802.11 standard can be found in the book, "802.11 Handbook, A Designer's Companion", Bob O'Hara and Al Petrick, IEEE press, 1999

More information about the Atheros chipset can be found at

www.atheros.com