NOKIA

Wi-Fi Training

Tianqi Nan

2018-3-5

Agenda

1. Overview of Wi-Fi, IEEE Standards, Organization
2. Radio frequency fundamentals
3. 802.11n
4. 802.11ac
5. WLAN topography and architecture
6. 802.11 Protocol analysis
7. 802.11 media contention
8. 802.11 Security
9. Performance analysis
10. ACS/DCS/DFS
11. Calibration and power management
12. FCU issue experience

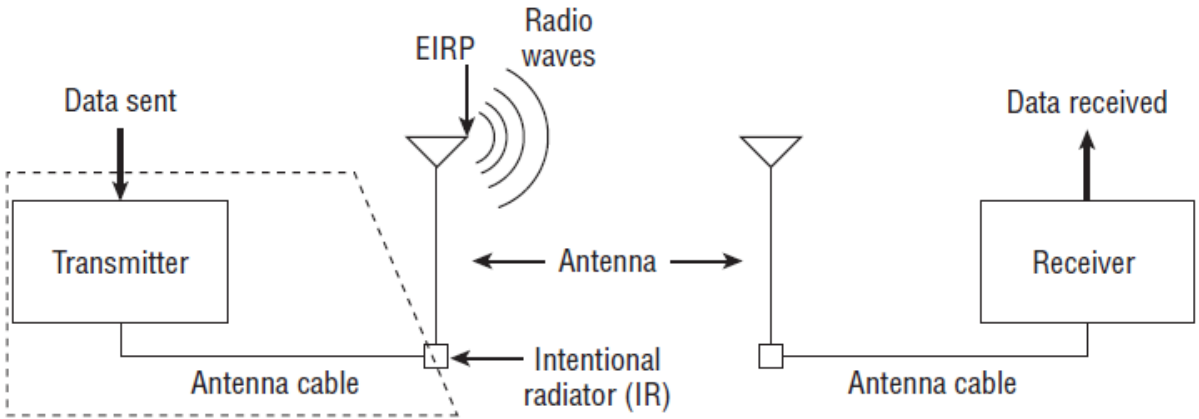
1.Overview of Wi-Fi, IEEE Standards, Organization

1.Overview of Wi-Fi, IEEE Standards, Organization

What's Wi-Fi?

- Wi-Fi is one technology of WLAN, most scenario Wi-Fi same as WLAN now.
- Wi-Fi is an acronym for the phrase wireless fidelity, but Wi-Fi is simply a brand name used to market 802.11 WLAN technology.
- Wi-Fi radios are used for numerous enterprise applications and can also be found in laptops, smartphones, cameras, televisions, printers, and many other consumer devices.
- The 2.4 GHz ISM band is 100 MHz wide and spans from 2.4 GHz to 2.5 GHz.
- The 5.8 GHz ISM band is 150 MHz wide and spans from 5.725 GHz to 5.875 GHz.
- Many Wi-Fi chip vendors in market.

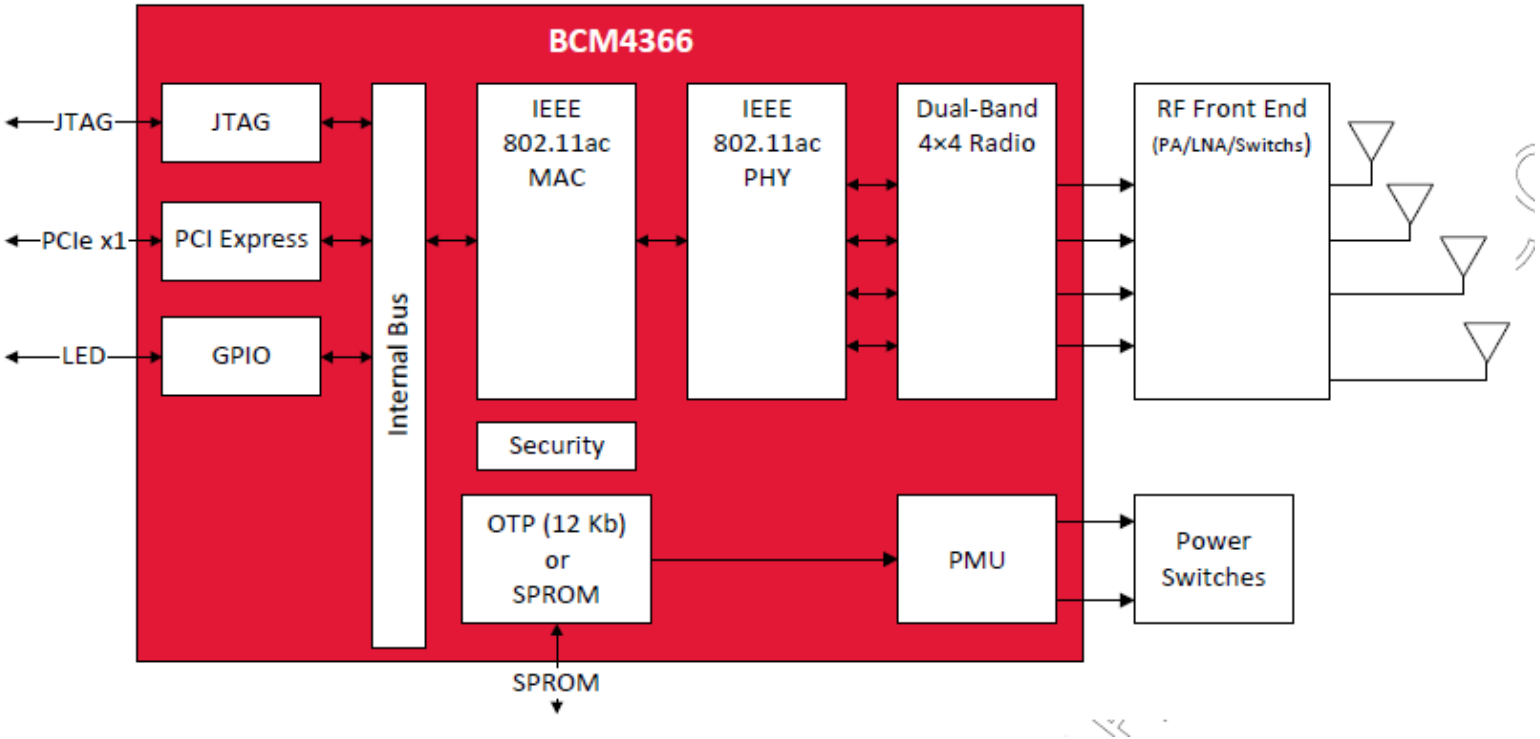
RF Components



- EIRP: The highest RF signal strength that is transmitted from a particular antenna

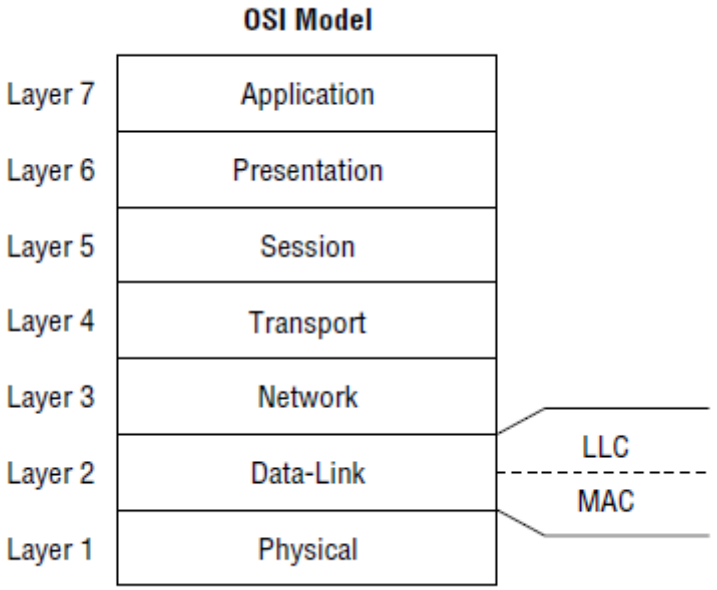
- Transmitter : Encode the data into the modulated AC signal .
- Receiver: Translate the modulated signals into 1s and 0s
- Antenna: 1) Direct or radiate the AC signal from the transmitter in a pattern;
  2) Receive through the air and directs the AC signal to the receiver.
- IR:1) Specifically designed to generate RF
  2) Consists of all the components from the transmitter to the antenna but not including antenna.
  3) Conducive power

BCM4366 Block Diagram for example

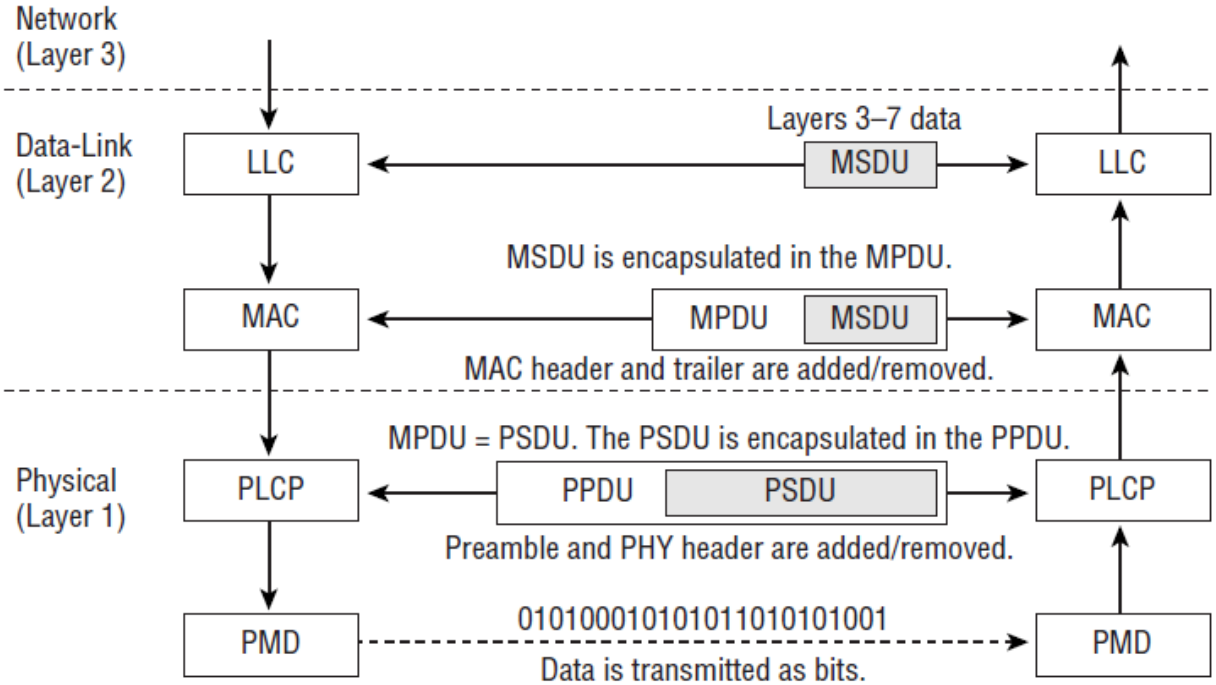


802.11 focus on Layer1 and Layer2 in OSI

- 802.11 Data-Link layer is divided into two sublayers:
  - *Logical Link Control (LLC)* sublayer,
    --identical for all 802-based networks.
  - *Media Access Control (MAC)* sublayer,
    --defined operations by 802.11 standards.
- 802.11 Physical layer is also divided into two sublayers:
  - *Physical Layer Convergence Procedure (PLCP)* sublayer,
    --prepare the frame for transmission .
  - *Physical Medium Dependent (PMD) sublayer,*
    --modulates and transmits the data as bits



Data-Link and Physical layers



- MSDU
  --MAC Service Data Unit
- MPDU
  --MAC Protocol Data Unit
- PSDU
  --PLCP Service Data Unit
- PPDU
  --PLCP Protocol Data Unit
- A-MSDU
  --Aggregate MSDU
- A-MPDU
  --Aggregate MPDU

IEEE802.11 standards

✓ **IEEE 802.11-2007 ratified amendments**

- IEEE Std802.11-1999 (R2003)
- 802.11b-1999
- 802.11a-1999
- 802.11d-2001
- 802.11g-2003
- 802.11h-2003
- 802.11i-2004
- 802.11j-2004
- 802.11e-2005

✓ **IEEE 802.11-2012 ratified amendments**

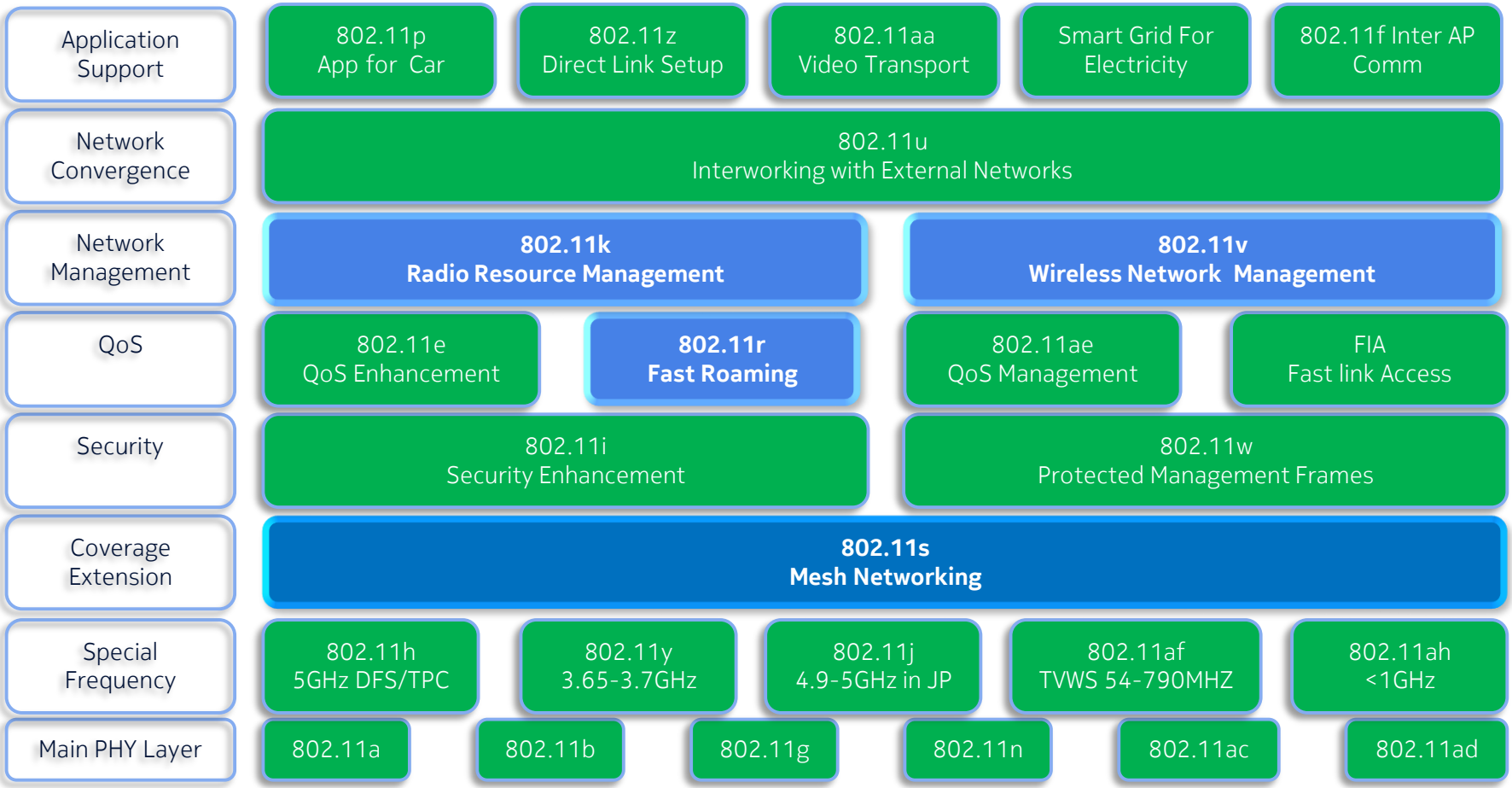
- 802.11r-2008
- 802.11k-2008
- 802.11y-2008
- 802.11w-2009
- 802.11n-2009
- 802.11p-2010
- 802.11z-2010
- 802.11u-2011
- 802.11v-2011
- 802.11s-2011

✓ **Post-2012 ratified amendments**

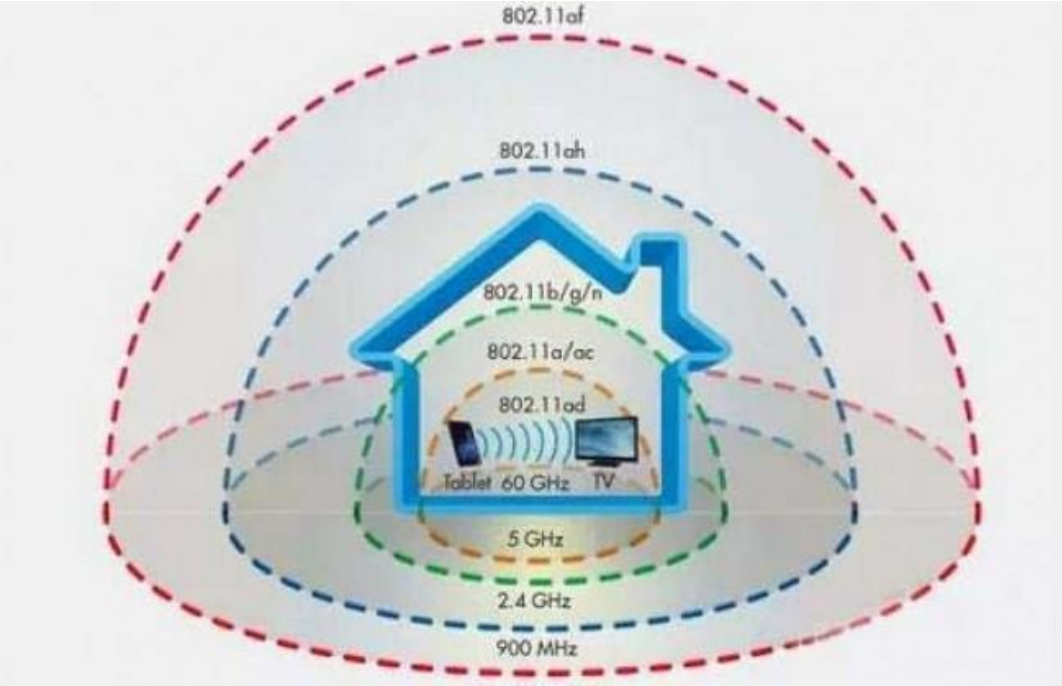
- 802.11ae-2012
- 802.11aa-2012
- 802.11ad-2012
- 802.11ac-2013
- 802.11af-2014

✓ **IEEE-2011 draft amendments**

- 802.11ah
- 802.11ai
- 802.11aj
- 802.11ak
- 802.11aq



Home Wi-Fi Spectral distribution



- ✓ 802.11ad
  - VHT with 60GHz;
  - Max 7Gbps
  - Used for high performance data transfer
  - Seamless transition between 60GHz and legacy 2.4GHz or 5GHz
  - New encryption mechanism: GCMP+AES
  - Less effective range than 5GHz
  - Still have debate if fallback to 5GHz in high-density deployment
  - Wireless Gigabit Alliance (WiGig) for unlicensed 60GHz,already consolidate into Wi-Fi Alliance

WiGig™ CERTIFIED by Wi-Fi Alliance

Standards organizations(1)

✓ **Standards organizations**

- Federal Communications Commission (FCC)
- International Telecommunication Union Radio communication Sector(ITU-R)
- Institute of Electrical and Electronics Engineers(IEEE)
- Internet Engineering Task Force(IETF)
- Wi-Fi Alliance(WFA)
- International Organization for Standardization(IOS)

  NOKIA

Standards organizations(2)

- ✓ Federal Communications Commission(FCC)

  Both licensed and unlicensed communications are typically regulated in the following five areas:

  - Maximum power of the intentional radiator (IR)
  - Maximum equivalent isotropically radiated power (EIRP)
  - Use (indoor and/or outdoor)
  - Spectrum sharing rules
  - Frequency
  - Bandwidth

Frequency Range (MHz)	5150-5250	5250-5350	5470-5725	5725-5850
Condition of Operation	Indoor/Outdoor, Master/Client, mobile/portable, and fixed Device, unless otherwise noted			
Max Conducted TX Power	30 dBm (1 W) for master device 24 dBm (250 mW) for mobile/portable client device	24dBm (250 mW) or 11 dBm + 10 log B, whichever is lower (B= 26-dB emission BW)		30 dBm (1 W)
Max_EIRP	4 W (36 dBm) with 6 dBi antenna 200 W (53 dBm) for fixed P-t-P application with 23 dBi antenna Additional rule for outdoor operation: Max_EIRP < 125 mW (21 dBm) at any elevation angle > 30° from horizon	1 W (30 dBm) with 6 dBi antenna		4 W (36 dBm) with 6 dBi antenna No EIRP limit for fixed P-t-P application (i.e. no antenna gain limit)
TX Power Reduction (dBm-by-dBi) required when antenna exceeds…	> 6dBi >23 dBi for fixed P-t-P application	> 6 dBi		> 6dBi Not required for fixed P-t-P application with any antenna gain
Out of Band e.i.r.p. Emission	≤-27 dBm/MHz outside 5150-5350 MHz		≤-27 dBm/MHz outside 5470-5725 MHz	≤-17 dBm/MHz within 5715-5725 MHz **and** 5850-5860 MHz ≤-27 dBm/MHz outside 5715-5860 MHz
Max Conducted Power Spectral Density (PSD)	17 dBm/MHz for master device 11 dBm/MHz for mobile/portable client device	11 dBm/MHz		30 dBm/500kHz
Dynamic Frequency Selection (DFS) required?	NO	YES, for master device with Detection Threshold of -64 dBm for 200 mW (23 dBm) ≤ Operating_EIRP ≤ 1W (30 dBm); -62dBm for Operating_EIRP < 200 mW (23 dBm) **and** PSD must be < 10 dBm/MHz. **Device must sense for radar signals at 100% of its emission BW** NO, for client device		NO
Transmit Power Control (TPC) required?	NO	YES, if Max_EIRP ≥ 500 mW (27 dBm) and able to lower EIRP below 24dBm NO, if Max_EIRP < 500mW (27dBm)		NO
Minimum BW requirement	N/A			6-dB BW ≥ 500 kHz

Standards organizations(3)

- ✓ International Telecommunication Union Radio communication Sector(ITU-R)
  - Communications are regulated differently in many regions and countries.
  - The United Nations has tasked the (ITU-R) with global spectrum management
  - The five administrative regions

    Region A: The Americas Inter-American Telecommunication Commission (CITEL)

    Region B: Western Europe European Conference of Postal and Telecommunications Administrations (CEPT)

    Region C: Eastern Europe and Northern Asia Regional Commonwealth in the field of Communications (RCC)

    Region D: Africa African Telecommunications Union (ATU)

    Region E: Asia and Australasia Asia-Pacific Telecommunity(APT)
  - The three radio regulatory regions

    Region 1: Europe, Middle East, and Africa

    Region 2: Americas

    Region 3: Asia and Oceania
  - More information refer www.itu.int/ITU-R

Within each region, some local government RF regulatory manage the RF spectrum for their respective countries:
Australia Australian Communications and Media Authority (ACMA)
Japan Association of Radio Industries and Businesses (ARIB)
New Zealand Ministry of Economic Development
United States Federal Communications Commission (FCC)

Standards organizations(4)

- ✓ Wi-Fi Alliance(WFA)
  - The Wi-Fi Alliance is a global, nonprofit industry association of more than 550 member companies devoted to promoting the growth of WLANs.
  - The Wi-Fi Alliance's main task is to ensure the interoperability of WLAN products by providing certification testing.
  - IEEE and the Wi-Fi Alliance are two separate organizations:

    The IEEE 802.11 task group defines the WLAN standards

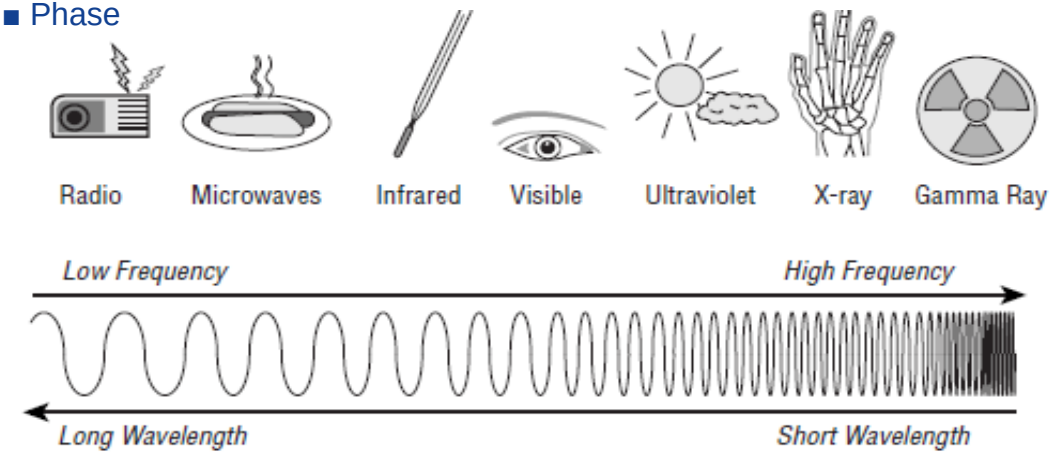
    The Wi-Fi Alliance defines interoperability certification programs
  - Learn more about the Wi-Fi Alliance at www.wi-fi.org,which contains many articles FAQs, and white papers

2.Radio frequency fundamentals

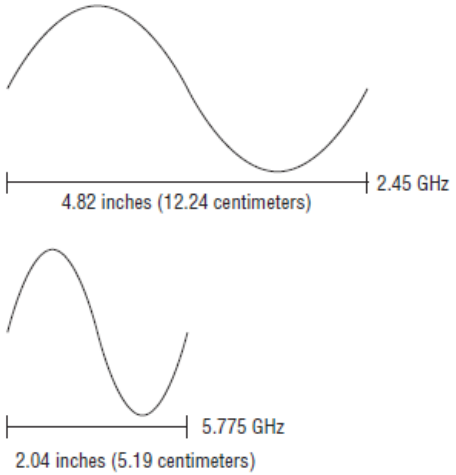
2.Radio frequency fundamentals
Radio Frequency Characteristics(1)

These characteristics exist in every RF signal

- Wavelength
- Frequency
- Amplitude
- Phase



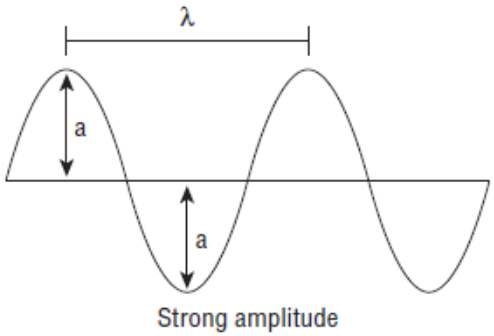
2.45 GHz wavelength and 5.775 GHz wavelength

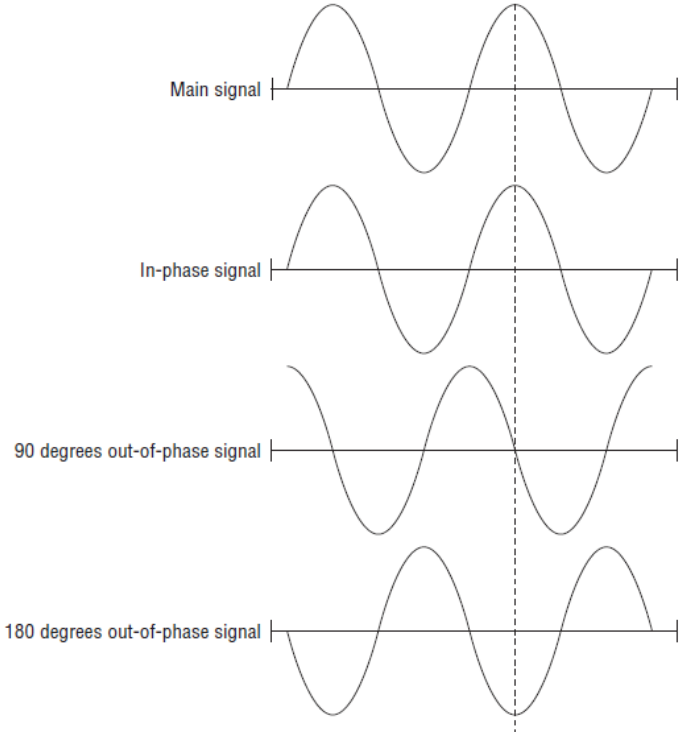


- Higher frequency signals will generally attenuate faster than lower frequency signals.
- 2.4 GHz signal will pass through objects with greater amplitude than 5GHz signal.

Radio Frequency Characteristics(2)

Amplitude :
Characterized simply as the signal's strength, or power.



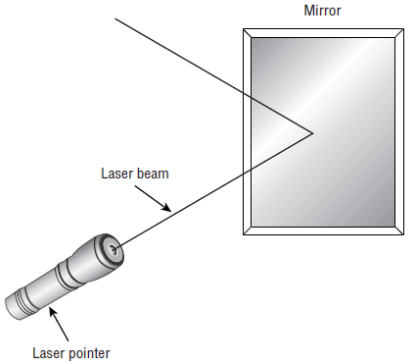


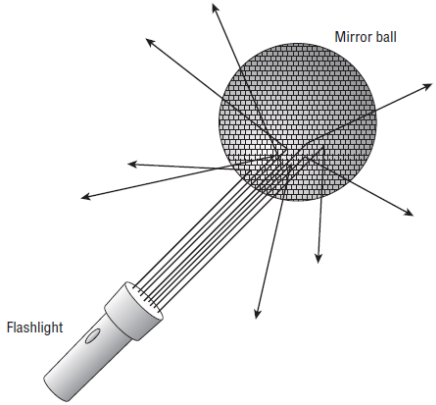
Phase:

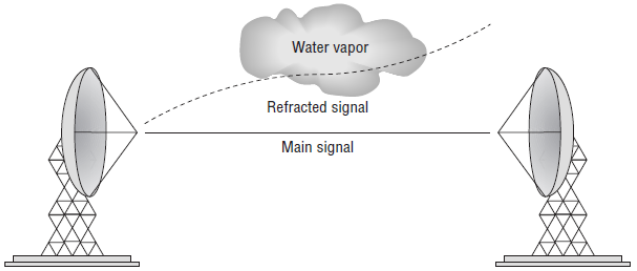
- Involves the relationship between two or more signals that share the same frequency.
- Cumulative effect will impact the effective received signal strength.

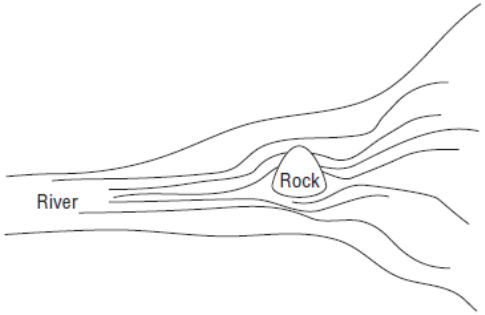
Radio Frequency Behaviors(1)

- ✓ RF propagation behaviors include **absorption, reflection, scattering, refraction, diffraction, free space path loss, multipath, attenuation, and gain**.









Radio Frequency Behaviors(2)

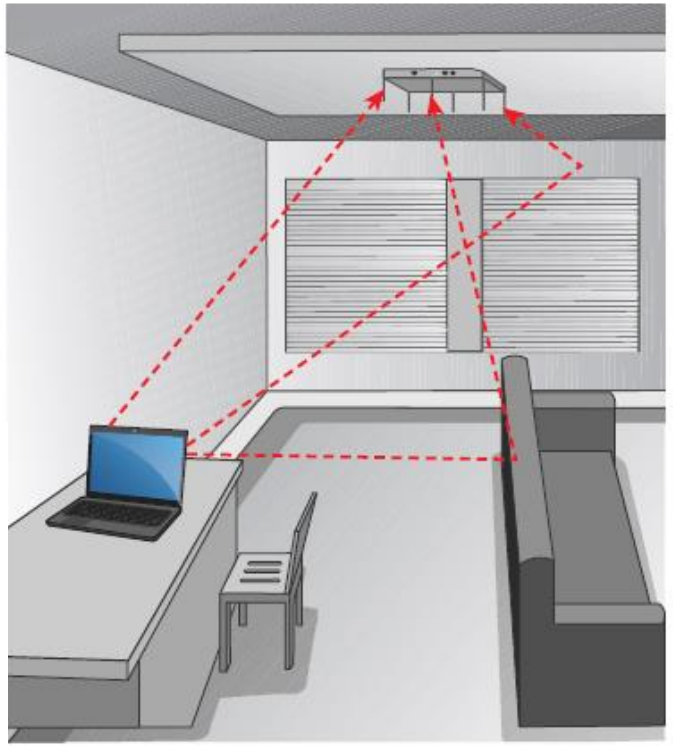
TABLE 2.2 Attenuation due to free space path loss

Distance (km)	Attenuation (dB)	
	2.4 GHz	5 GHz
1	100.0	106.4
2	106.1	112.4
4	112.1	118.5
8	118.1	124.5

TABLE 2.1 Attenuation comparison of materials

Material	2.4 GHz
Foundation wall	–15 dB
Brick, concrete, concrete blocks	–12 dB
Elevator or metal obstacle	–10 dB
Metal rack	–6 dB
Drywall or sheetrock	–3 dB
Nontinted glass windows	–3 dB
Wood door	–3 dB
Cubicle wall	–2 dB

Multipath



Units of Power and Comparison

✓ **Units of power (absolute)**

- watt (W)
- milliwatt (mW)
- decibels relative to 1 milliwatt (dBm)

- dBm = 10 × log10(PmW)
- 0 dBm is equal to 1 milliwatt

✓ **Units of comparison (relative)**

- decibel (dB)
- decibels relative to an isotropic radiator (dBi)
- decibels relative to a half-wave dipole antenna (dBd)

- An isotropic radiator can radiate an equal signal in all directions.
- The dBi value is measured at the strongest point of the antenna signal.
- dBi value of an antenna is always a positive gain.
- Any time you see *dBi,* think *antenna gain*.

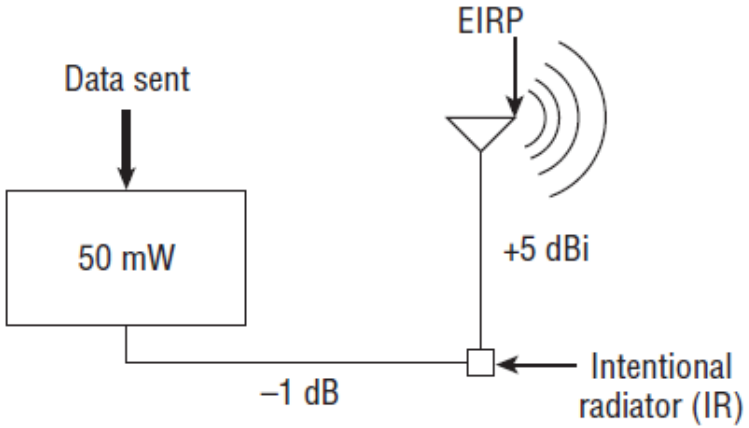
- The antenna industry uses two dB scales to describe the gain of antennas
- Higher the dBi or dBd value of an antenna,the more focused the signal

- Dipole antenna is the classic example of an omnidirectional antenna.
- The default antenna of many access points.
- The closest thing to an isotropic radiator is the omnidirectional dipole antenna.
- A dipole antenna is 2.14 dBi, so a 3 dBd antenna is equal to a 5.14 dBi antenna
- 802.11 antennas typically are measured using dBi, not often use dBd

RF Mathematics(1)

- ✓ **Rule of 10s and 3s :**
  - For every 3 dB of gain (relative), double the absolute power (mW).
  - For every 3 dB of loss (relative), halve the absolute power (mW).
  - For every 10 dB of gain (relative), multiply the absolute power (mW) by a factor of 10.
  - For every 10 dB of loss (relative), divide the absolute power (mW) by a factor of 10.

- ✓ **Math:**
  - 3 dB gain = mW × 2
  - 3 dB loss = mW ÷ 2
  - 10 dB gain = mW × 10
  - 10 dB loss = mW ÷ 10



3 + / 10 −	dBm	mW	× 2 / ÷ 10	
	0	1		
+ 10	10	10	× 10	
+ 10	20	100	× 10	Transmitter
− 3	17	50	÷ 2	
− 10	7	5	÷ 10	
+ 3	10	10	× 2	Connector
+ 3	13	20	× 2	
+ 3	16	40	× 2	
+ 10	26	400	× 10	
+ 10	36	4000	× 10	Antenna
− 3	33	2000	÷ 2	
− 3	30	1000	÷ 2	
− 3	27	500	÷ 2	
− 3	24	250	÷ 2	
− 3	21	125	÷ 2	

NOKIA

RF Mathematics(2)

✓ Noise Floor

- The noise floor is the ambient or background level of radio energy on a specific channel.
- The amplitude of the noise floor, which is sometimes simply referred to as “background noise,” varies in different environments.

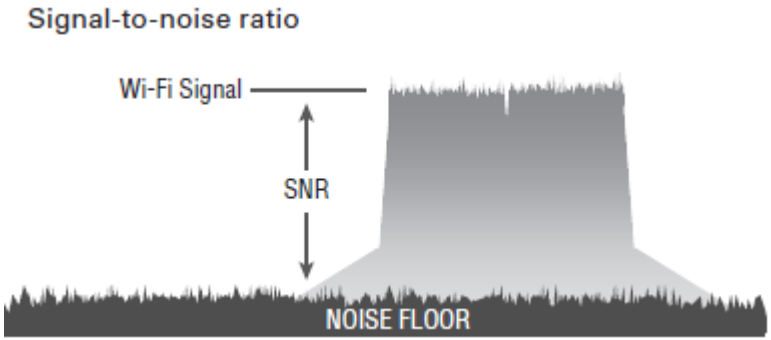
✓ Signal-to-Noise Ratio (SNR)

- Many Wi-Fi vendors define **signal quality** as the signal-to-noise ratio (SNR), not actually a ratio.
- SNR is the difference in decibels between the received signal and the background noise level (noise floor)
- Data transmissions can become corrupted with a very low SNR and result in layer 2 retransmissions
- An SNR of 25 dB or greater is considered good signal quality, and an SNR of 10 dB or lower is considered very poor signal quality.

For example :

Wi-Fi signal is -85dBm, Noise Floor is -100dBm

SNR is 15dB



RF Mathematics(3)

✓ Received Signal Strength Indicator(RSSI)

- RSSI refers to the power level of an RF signal required to be successfully received by the receiver radio.
- The lower the power level that the receiver can successfully process, the better the receive sensitivity.
- Wi-Fi vendors will usually specify their receive sensitivity thresholds at various data rates.
- More power is required by the receiver radio to support the higher data rates.
- The higher data rates use encoding methods that are more susceptible to corruption.
- The lower data rates use modulation-encoding methods that are less susceptible to corruption.
- The 802.11 RSSI measurement parameter can have a value from 0 to 255.
- The RSSI value is designed to be used as a relative measurement of the **RF signal strength**
- RSSI metrics are typically mapped to receive sensitivity thresholds expressed in absolute dBm values.
- Some chip vendor use RSSI as the important base for channel selection or data rate adaption .

RF Mathematics(4)

TABLE 3.4 Received signal strength indicator (RSSI) metrics (vendor example)

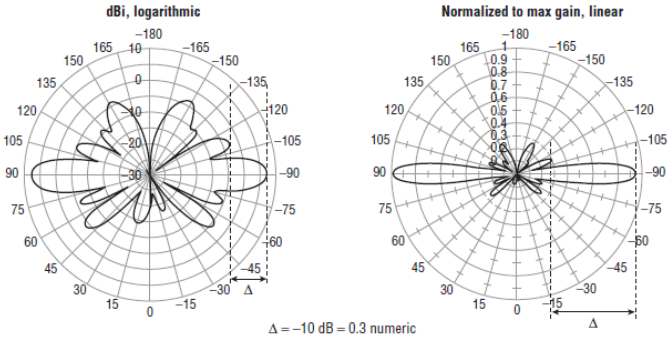
RSSI	Receive sensitivity threshold	Signal strength (%)	Signal-to-noise ratio	Signal quality (%)
30	–30 dBm	100%	70 dB	100%
25	–41 dBm	90%	60 dB	100%
20	–52 dBm	80%	43 dB	90%
21	–52 dBm	80%	40 dB	80%
15	–63 dBm	60%	33 dB	50%
10	–75 dBm	40%	25 dB	35%
5	–89 dBm	10%	10 dB	5%
0	–110 dBm	0%	0 dB	0%

NOKIA

Antenna

- ✓ **Four types of antennas are used with 802.11 networks:**
  - Omnidirectional Antennas(dipole, collinear)
  - Semidirectional Antennas (patch, panel, Yagi)
  - Highly directional Antennas (parabolic dish, grid)
  - Sector Antennas
- ✓ **The antenna types produce different signal patterns**
  - Azimuth charts
  - Elevation charts
- ✓ **Antenna Accessories**
  - Cables
  - Connectors
  - Splitters
  - Amplifiers
  - Attenuators

FIGURE 4.3 Omnidirectional polar chart (E-plane)



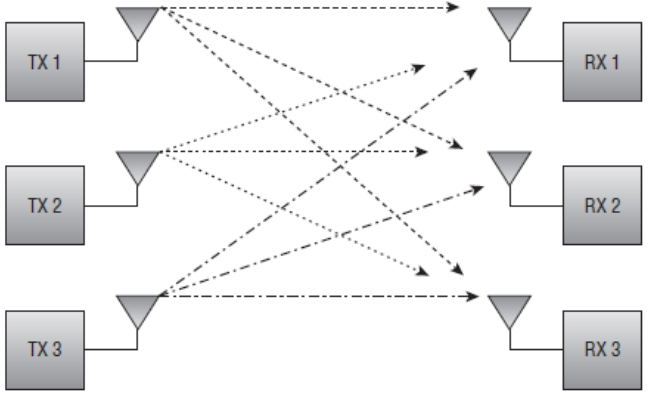
- ✓ **Antenna Connection and Installation**
  - Voltage Standing Wave Ratio(VSWR)
  - Signal Loss
  - Antenna Mounting
    - Placement
    - Mounting
    - Appropriate use and environment
    - Orientation and alignment
    - Safety
    - Maintenance

3.802.11N introduction

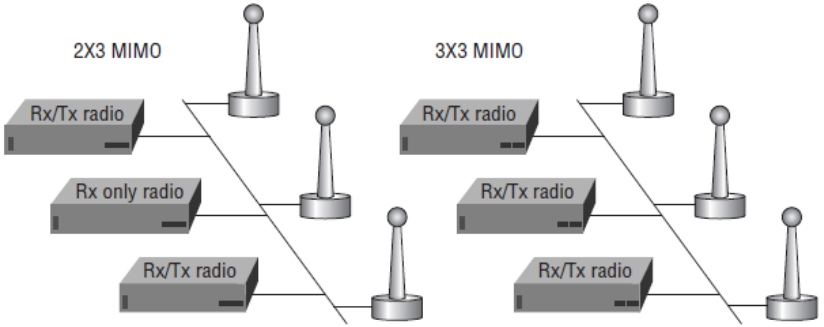
802.11N introduction

- ✓ **Wi-Fi CERTIFIED n baseline requirements**
- ✓ **MIMO**
  - Radio Chains
  - Spatial Multiplexing (SM)
  - MIMO Diversity
  - Space-Time Block Coding (STBC)
  - Cyclic Shift Diversity (CSD)
  - Transmit Beamforming (TxBF)

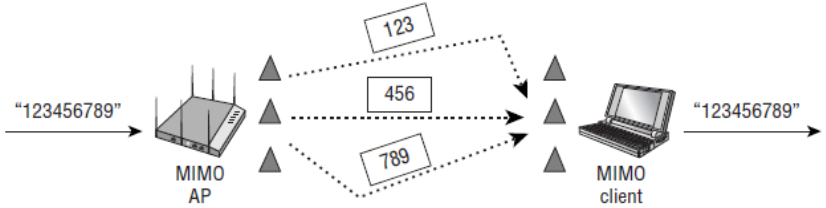
18.1 MIMO operation and multipath



URE 18.2 2×3 and 3×3 MIMO



URE 18.3 Multiple spatial streams



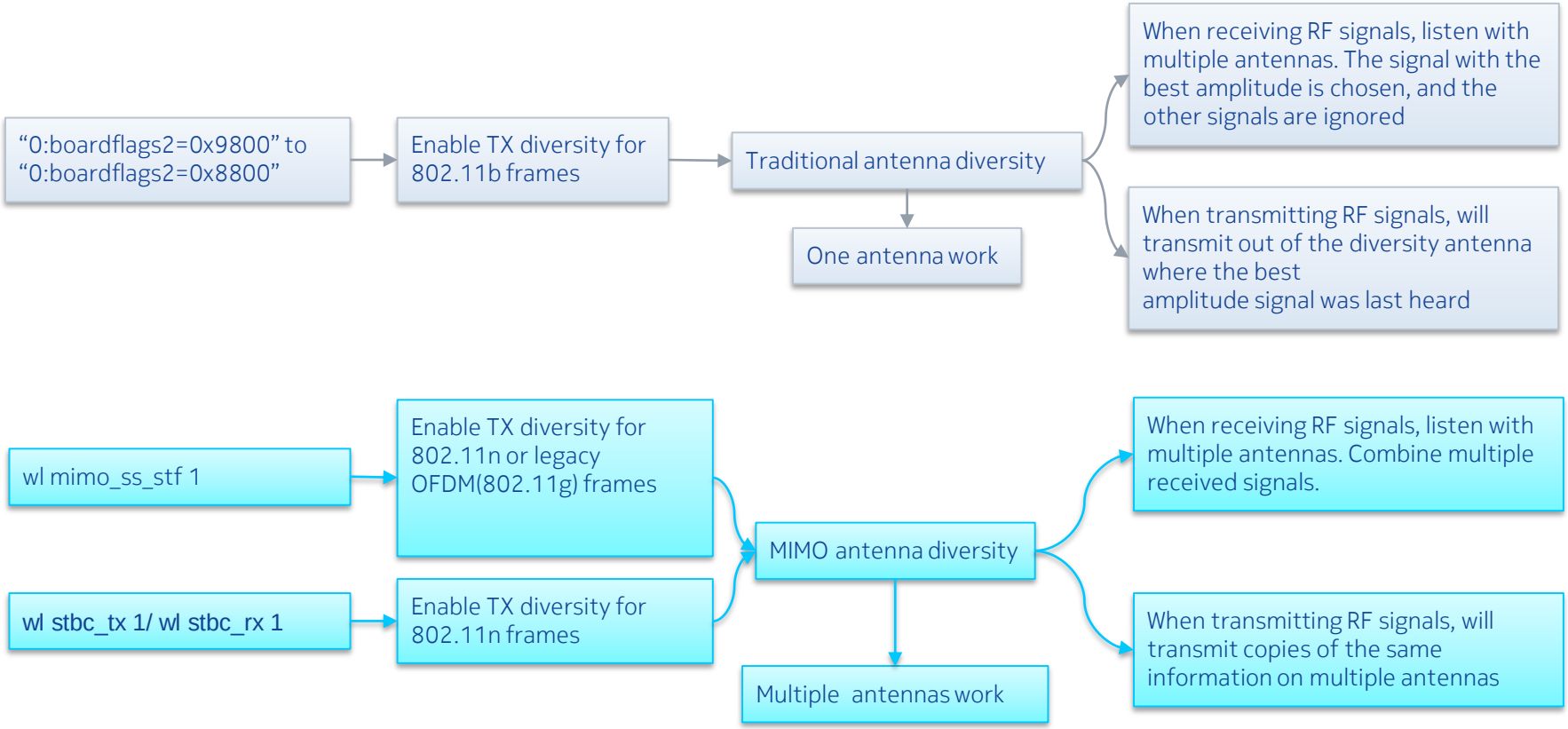
802.11N introduction (2)—MIMO diversity and SM

Difference between MIMO diversity and spatial multiplexing

- ✓ **MIMO diversity**
  - Antenna diversity (both receive and transmit) is a method of using multiple antennas to survive the negative effects of multipath.
  - Send multiple copies of the same signal , resulting in greater range, get some receive gain
  - STBC/CSD
- ✓ **Spatial multiplexing**
  - Each unique stream can contain data that is different from the other streams transmitted by one or more of the other radio chains.
  - Sending multiple ind al multiplexing (SM)

NOKIA

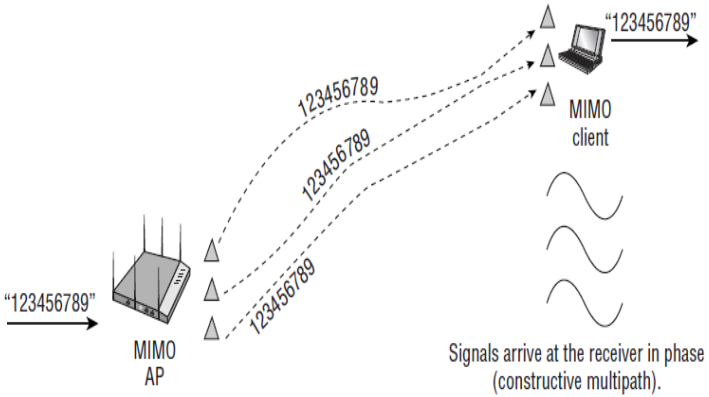
Summary above three modification about antenna diversity



802.11N introduction (3) --TXBF

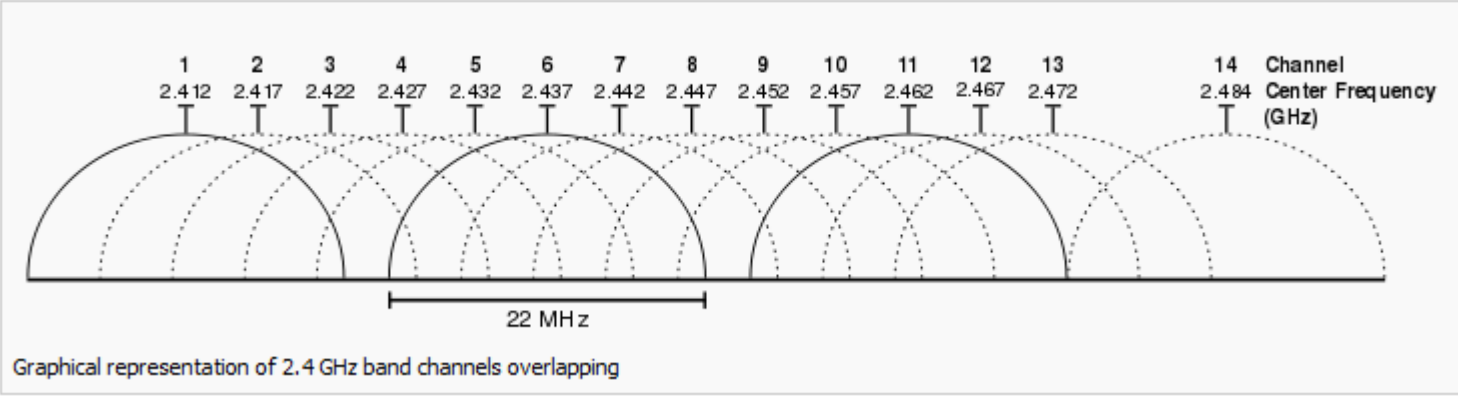
✓ Transmit Beamforming (TxBF)

- Transmit beamforming is a method that allows a MIMO transmitter using multiple antennas to adjust the phase and amplitude of the outgoing transmissions in a coordinated method.
- Transmit beamforming could be used together with spatial multiplexing (SM);
- Transmitters that use beamforming will try to adjust the phase of the signals based on feedback from the receiver by using *sounding frames(* any frames, o null function data frames)
- Transmitter is beamformer, the receiver is beamformee , beamformer and beamformee work together to create the steering matrix
- implicit feedback: there is no direct feedback from the beamformee and thus the beamformer creates the steering matrix
- explicit feedback: the beamformee creates the steering matrix
- It should be noted that explicit beamforming has never really been used with 802.11n radios. However, the 802.11ac amendment defines only explicit beamforming.
- 802.11n transmit beamforming has not been utilized due to the lack of client-side support for the technology



802.11N introduction (4) –HT channels

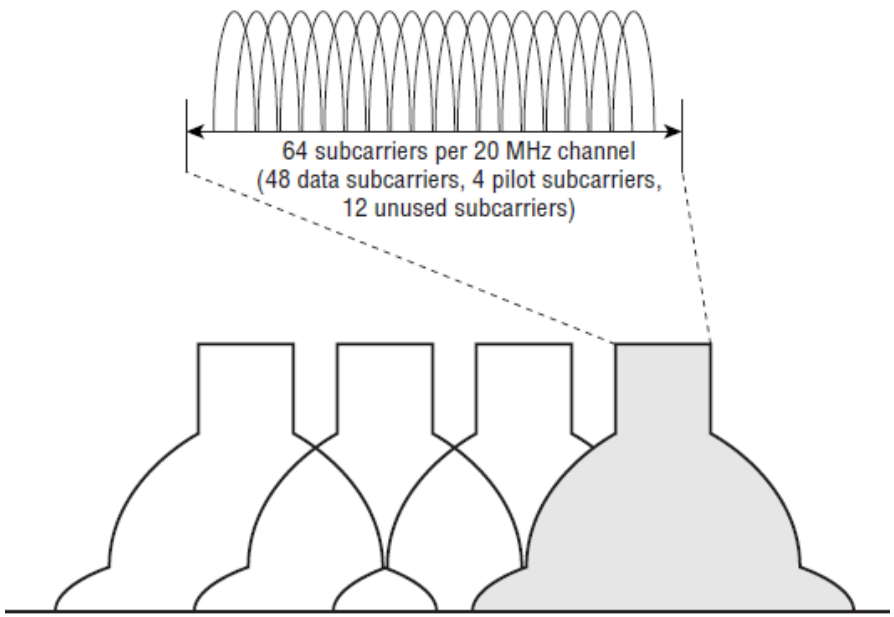
- ✓ **20MHZ Non-HT and HT channels**
  - 802.11b(HR-DSSS), ---center frequencies were 25 MHz apart，22MHZ channel width
  - 802.11g/n (ERP/OFDM)—backward require 25 MHz apart,20MHZ channel width
- ✓ **Nonoverlapping channel**
  - 1/6/11 for legacy mix mode deployment
  - 1/5/9/13 for g/n deployment



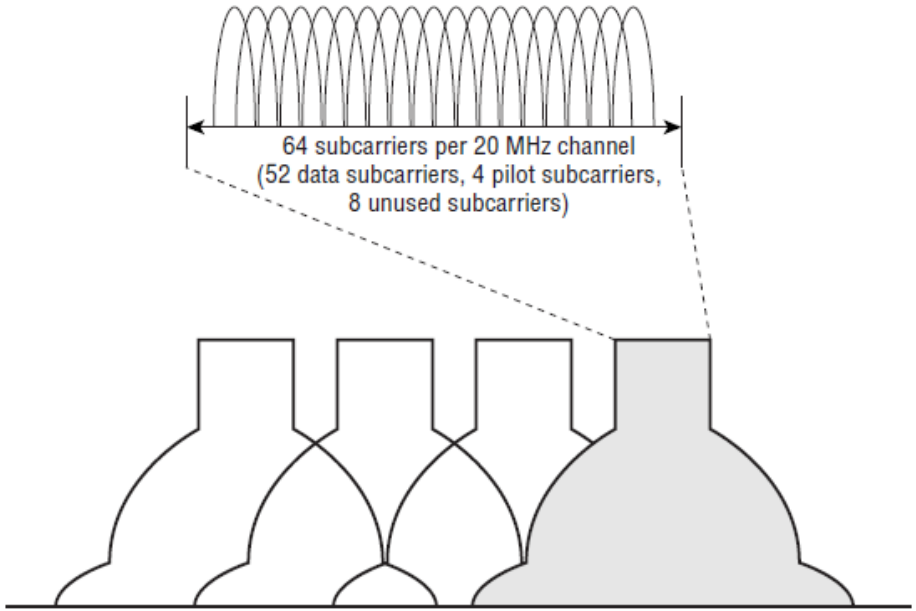
Graphical representation of 2.4 GHz band channels overlapping

802.11N introduction (5) –HT channels

18.6 20MHz non-HT (802.11a/g) channel



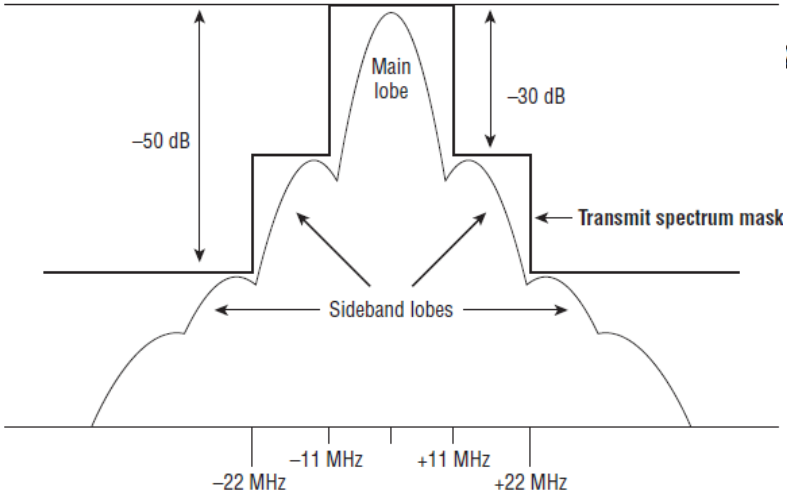
E 18.7 20MHz HT (802.11n) channel



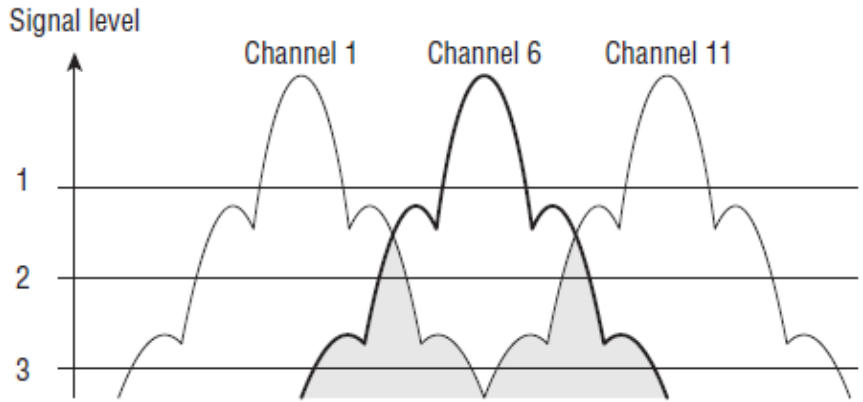
Why 802.11n can get high throughput than 802.11b/g

802.11N introduction (6) –HT channels

RE 2.9 IEEE 802.11b transmit spectrum mask



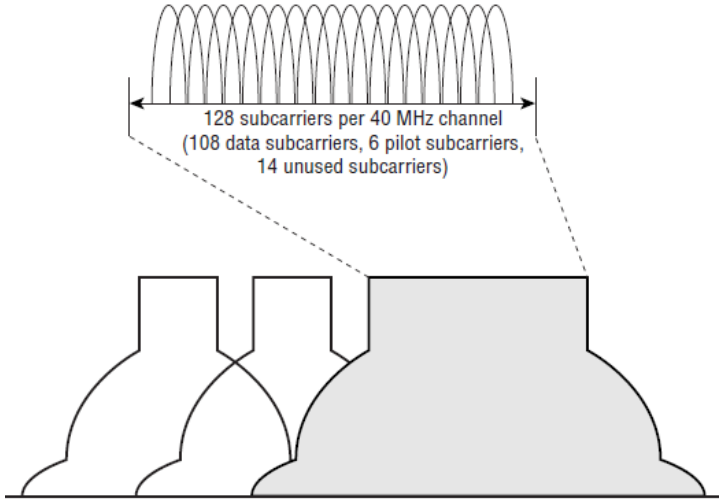
2.10 Sideband carrier frequency interference

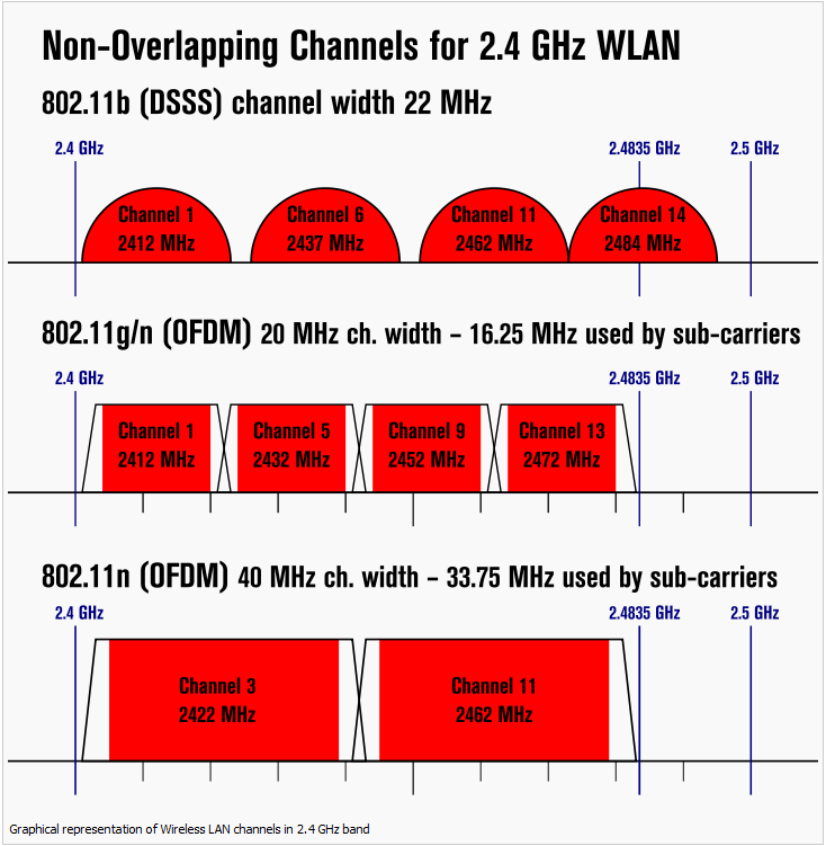


Adjacent channel interference

802.11N introduction (7)—HT channels

- ✓ **40MHz channels**
  - two nonoverlapping channel as adjacent channel
  - Two adjacent channel bond to one 40MHz channel
  - any two 40 MHz channels will overlap in 2.4GHz ISM band
  - Allow to fall back to 20MHz,easy to be interference





Graphical representation of Wireless LAN channels in 2.4 GHz band

802.11N introduction (8)—HT channels

✓ Forty MHz Intolerant

- 802.11n clients and APs can also advertise that they are Forty MHz Intolerant using various 802.11n management frames.
- Any 802.11n AP using a 40 MHz channel will be forced to switch back to using only 20 MHz channels if they receive the frames from nearby 802.11n 2.4 GHz stations that are intolerant.
- Effectively, Forty MHz Intolerant operations are a protection against your next-door neighbor who might deploy a 40 MHz channel and interfere with your 2.4 GHz 20 MHz channels.

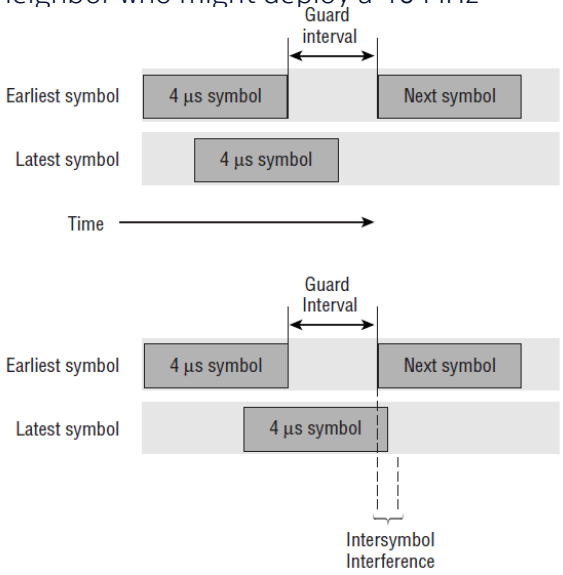
✓ Guard Interval (GI)

- 400-nanosecond guard interval, increase performance in clean environment
- 800-nanosecond guard interval, default guard interval setting

✓ Modulation and Coding Scheme (MCS)

- 802.11n data rates are defined with a modulation and coding scheme (MCS) matrix
- data rates based on numerous factors, including modulation, coding method,

the number of spatial streams, channel size, and guard interval.



802.11N introduction (9)—HT channels

TABLE 18.2 Mandatory modulation and coding schemes—20 MHz channel

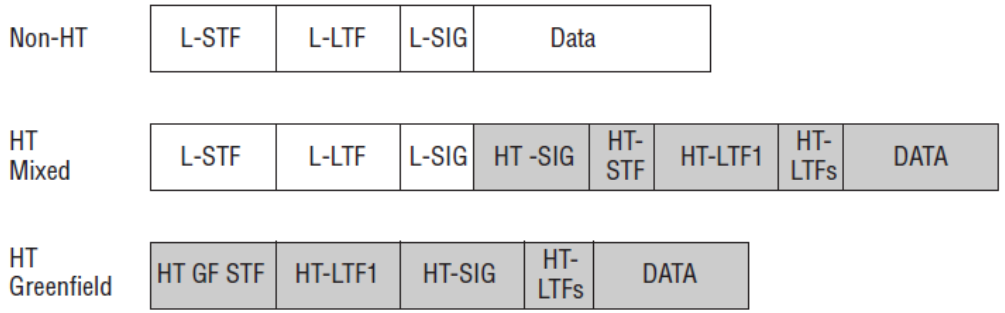
MCS index	Modulation	Spatial streams	Data rates	
			800 ns GI	400 ns GI
0	BPSK	1	6.5 Mbps	7.2 Mbps
1	QPSK	1	13.0 Mbps	14.4 Mbps
2	QPSK	1	19.5 Mbps	21.7 Mbps
3	16-QAM	1	26.0 Mbps	28.9 Mbps
4	16-QAM	1	39.0 Mbps	43.3 Mbps
5	64-QAM	1	52.0 Mbps	57.8 Mbps
6	64-QAM	1	58.5 Mbps	65.0 Mbps
7	64-QAM	1	65.0 Mbps	72.2 Mbps

NOKIA

802.11N introduction (10)—HT PHY

- ✓ **Three PPDU structures use three different preamble**
  - Non-HT Legacy
  - HT Mixed
  - HT Greenfield

RE 18.13 802.11n PPDU formats



L=Legacy (non-HT)
STF=Short Training Field
LTF=Long Training Field
SIG=Signal Field
HT=High Throughput
GF=Greenfield

The preamble is used for synchronization between transmitting and receiving 802.11 radios.

802.11N introduction (11)—HT MAC

- ✓ **A-MSDU/A-MPDU**
- ✓ **Block Acknowledgment**
- ✓ **Reduced Inter-frame Space(RIFS)**
  - WMM-compliant radios allotted period of time is called a transmit opportunity (TXOP)
  - During this TXOP, an 802.11 radio may send multiple frames in what is called a frame burst
  - During the frame burst, a short interframe space(SIFS) is used
- ✓ **HT Power Management**
  - 802.11e QoS amendment introduced unscheduled automatic power save delivery (U-APSD),WMM Power Save(WMM-PS)
  - The 802.11n amendment introduces two new power-management mechanisms:

    (1)spatial multiplexing power save (SM power save)

    (2)Power Save Multi Poll (PSMP),similar with U-APSD

802.11N introduction (12)—HT Operation

✓ 20/40 Channel Operation

- The 802.11n access point must declare 20-only or 20/40 support in the beacon management frame.
- 802.11n client stations must declare 20-only or 20/40 in the association or reassociation frames.
- Client stations must reassociate when switching between 20-only and 20/40 modes.
- If 20/40-capable stations transmit by using a single 20 MHz channel, they must transmit on the primary channel and not the secondary channel.

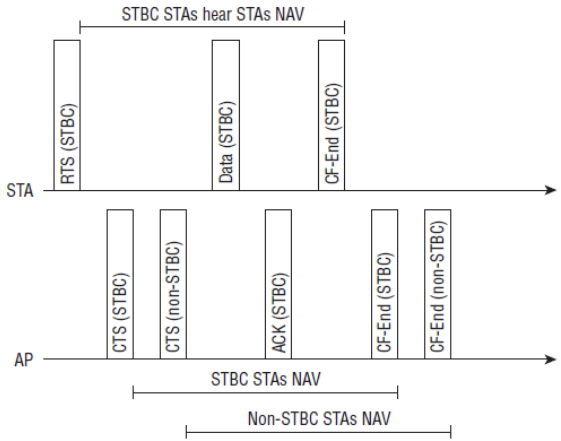
✓ HT Protection Modes (0–3)

- To ensure backward compatibility with older 802.11a/b/g radios
- Mode 0—Greenfield (No Protection) Mode :only HT radios are in use
- Mode 1—HT Nonmember Protection Mode
  - Protection mechanisms kick in when a non-HT client station or non-HT access point is heard that is not a member of the BSS
- Mode 2—HT 20 MHz Protection Mode
  - If a 20 MHz–only HT station associates to the 20/40 MHz AP, protection must be used
- Mode 3—Non-HT Mixed Mode : mostly commonly used
  - This protection mode is used when one or more non-HT stations are associated to the HT access point

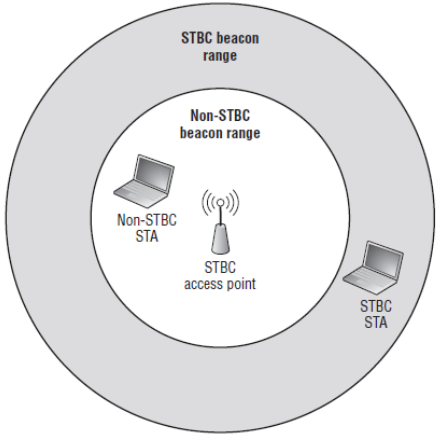
802.11N introduction (13)—HT Operation

- ✓ **HT Protection mechanisms**
  - RTS/CTS and CTS-to-Self
    - used in an ERP (802.11g) network protection to prevent 802.11b HR-DSSS collision.
    - Also used when HT protection is enabled within an HT BSS
  - Dual CTS :
    - STBC CTS and non-STBC CTS
  - L-SIG TXOP
    - optional Physical layer protection mechanism
    - Used in HT mixed PPDU header
  - phased coexistence operation (PCO)
    - operational mechanism
    - not in 802.11n standard

10.58 Dual CTS, initiating STA is STBC capable



7 STBC increased range



4.802.11AC introduction

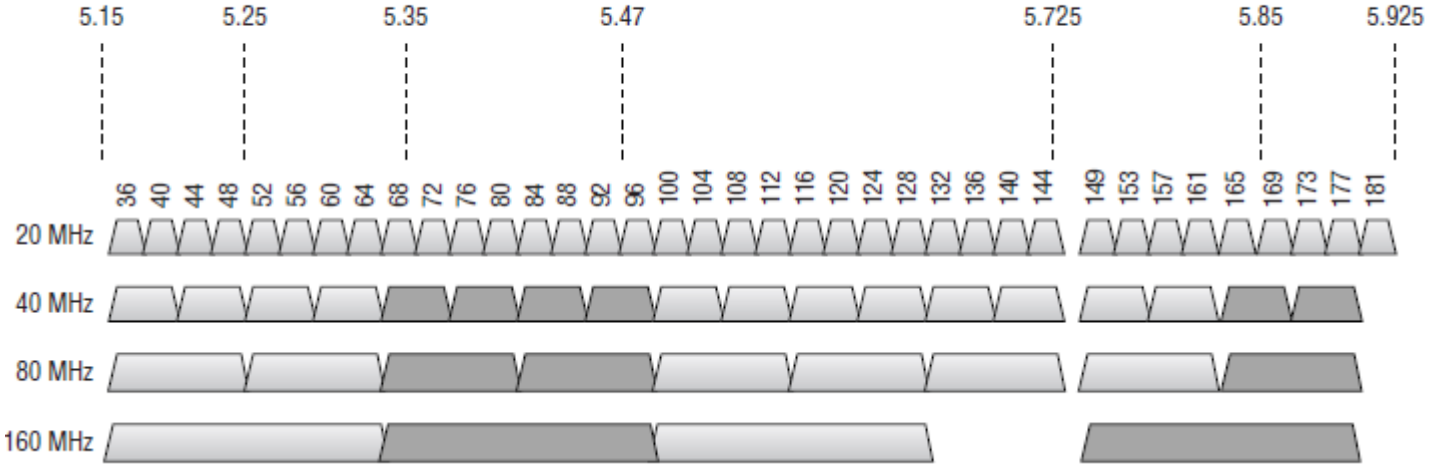
802.11AC introduction(1) --Comparison of 802.11n and 802.11ac

Technology	802.11n	802.11ac
Frequency	2.4 GHz and 5 GHz	5 GHz only
Modulation	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Channel widths	20 MHz, 40 MHz	20 MHz, 40 MHz, 80 MHz, 160 MHz
Spatial streams	Up to four	Up to eight on APs, up to four on clients
Short Guard Interval Support	Yes	Yes
Beamforming	Multiple types, both implicit and explicit, not typically implemented	Explicit beamforming with null data packets (NDPs)
Number of modulation and coding schemes (MCSs)	77	10
Support for A-MSDU and A-MPDU	Yes	Yes, all frames transmitted as A-MPDU
MIMO support	Single-user MIMO	Single-user MIMO and multiuser MIMO (MU-MIMO)
Maximum # of simultaneous user transmissions	One	Four
Maximum data rate	600 Mbps	6.933 Gbps

NOKIA

802.11AC introduction(2) -- 20, 40, 80, and 160 MHz Channels

FIGURE 19.6 20, 40, 80, and 160 MHz channels



For 802.11n:

When an AP was configured for a 40 MHz channel, it could not transmit until both the primary and secondary 20 MHz channels were available, reducing the 40MHz performance capabilities

For 802.11ac:

Support dynamic bandwidth operation

802.11AC introduction(3) -- dynamic bandwidth operation

FIGURE 19.7 Single AP 160 MHz channel plan

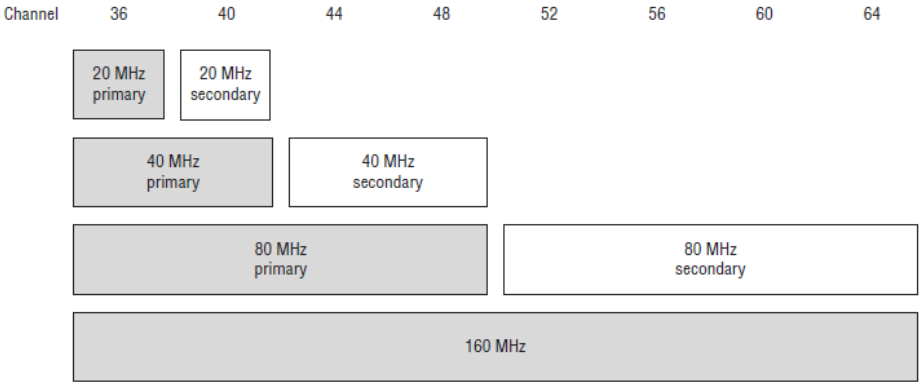
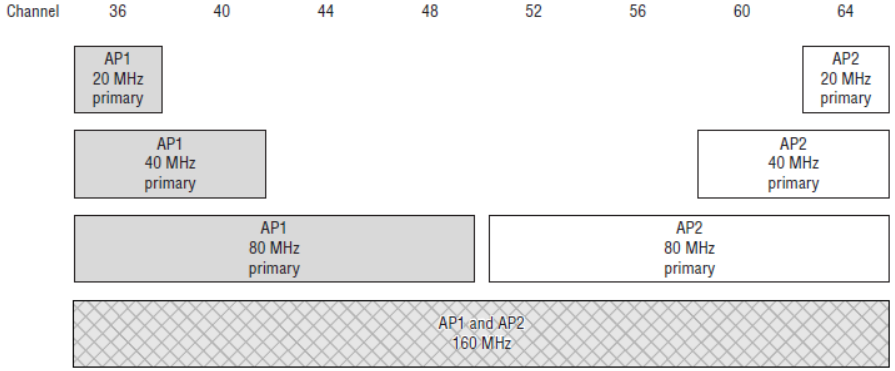


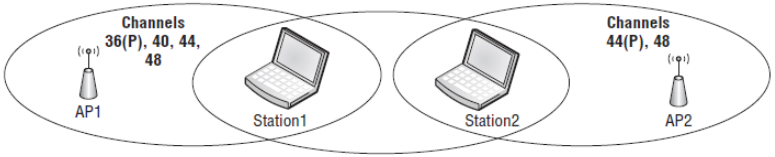
FIGURE 19.8 Two APs, 160 MHz channel plan



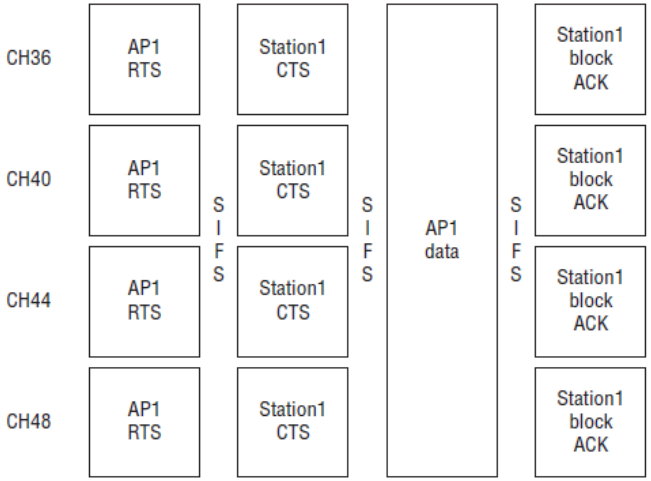
- The ability to switch bandwidth dynamically adds complexity to the channel selection.
- Primary channel selection becomes more complex as more APs join the network
- Different vendors have their own 802.11ac channel selection .
- Each of the APs uses its primary channel to transmit beacon frames and to perform media access control tasks.

802.11AC introduction(4) -- dynamic bandwidth operation using RTS/CTS

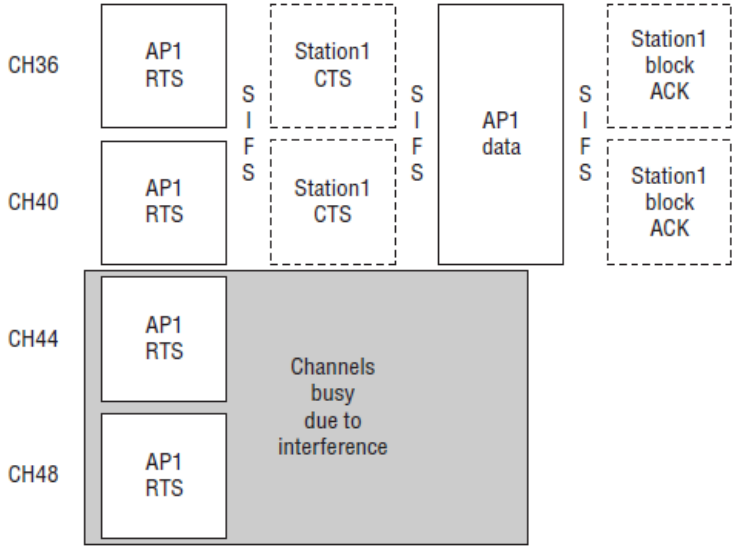
FIGURE 19.12 Interfering laptops



.13 Dynamic bandwidth operation using RTS/CTS



9.14 Dynamic bandwidth operation using RTS/CTS



802.11AC introduction(3) –Multiuser MIMO

- ✓ The most revolutionary part of 802.11ac, known as multiuser MIMO.
- ✓ The goal of MU-MIMO is to use as many spatial streams as possible.
- ✓ MU-MIMO is only performed from the AP to the client, so the acknowledgments must be single-user transmissions

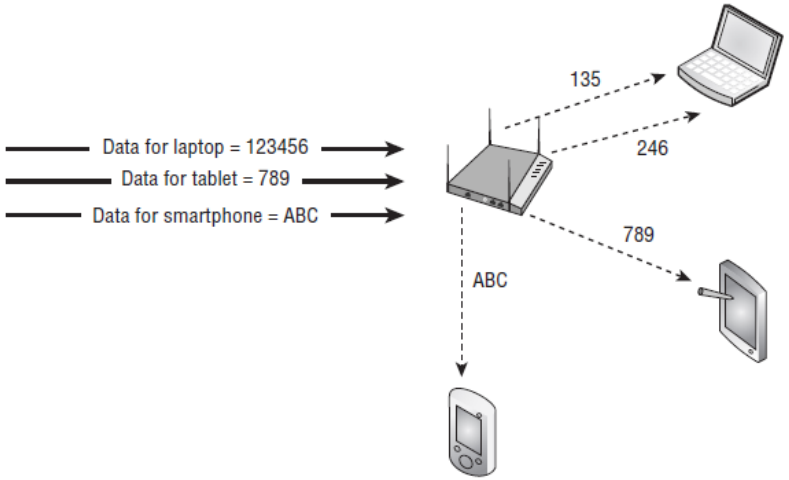
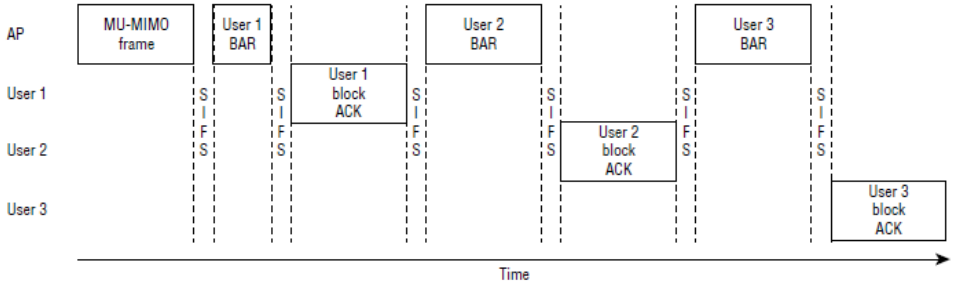


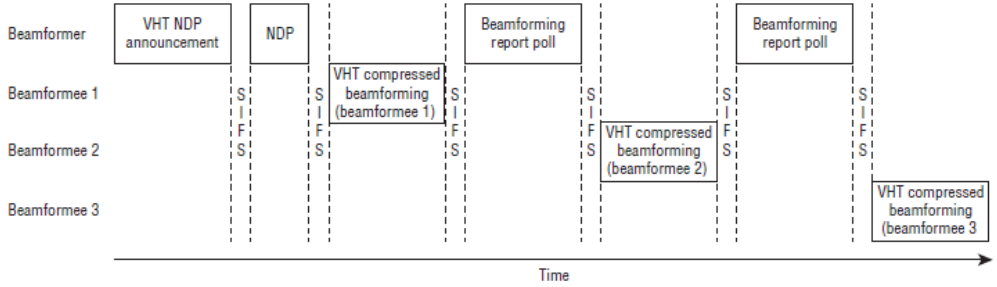
FIGURE 19.19 MU-MIMO block acknowledgments



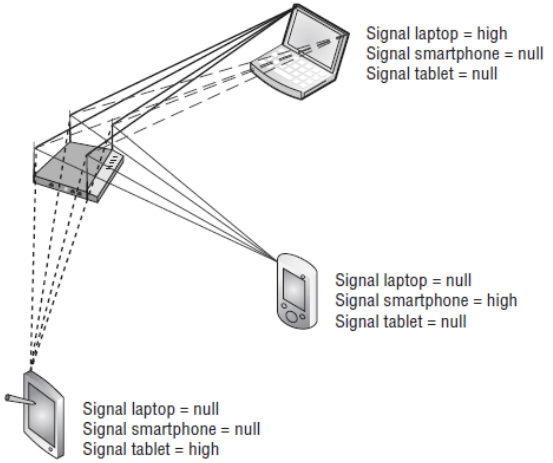
802.11AC introduction(4) –Multiuser Beamforming

- ✓ Each beamformee processes each OFDM subcarrier and creates feedback information, creating a compressed *feedback matrix.*
- ✓ Beamformees that are too close to each other could experience inter-user interference from signals directed toward other users.

FIGURE 19.17 Multiuser beamform sounding process



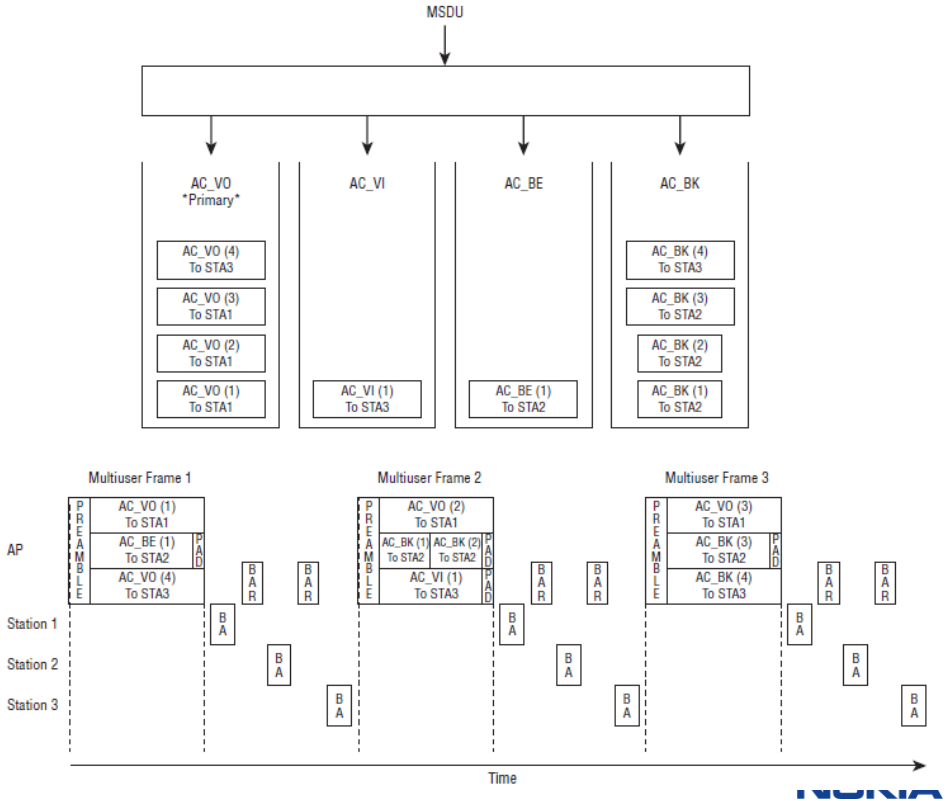
19.18 Beamformed transmissions in a MU-MIMO environment



802.11AC introduction(5) –MU-MIMO and QoS

With the implementation of MU-MIMO, the implementation of the queuing and transmission of QoS frames is handled differently than in single-user wireless environments

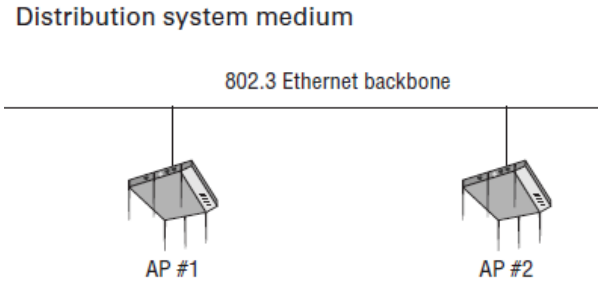
FIGURE 19.20 MU-MIMO and QoS



5.WLAN topography and architecture

WLAN topography(1)

- ✓ 802.11-2012 standard is defined as a *wireless local area network (WLAN)* technology.
- ✓ WLANs typically use multiple 802.11 access points connected by a wired network backbone.
- ✓ WLANs are used to provide end users with access to network resources and network services and a gateway to the Internet.
- ✓ IEEE802.11 wireless networks use half-duplex communications.
- ✓ Components to make up 802.11 service set:
  - **Access Point**: a half-duplex device with switch like intelligence(thin AP/fat AP)
  - **Client station**: layer 2 connection with an AP known as associated
  - **Integration Service** :frame format transfer method, transfer between 802.3 Ethernet frame and 802.11 frame
  - **Distribution System**: interconnect a set of basic service sets (BSSs) via integrated LANs to create an extended service



WLAN topography(2)

E 7.4 Repeater cell

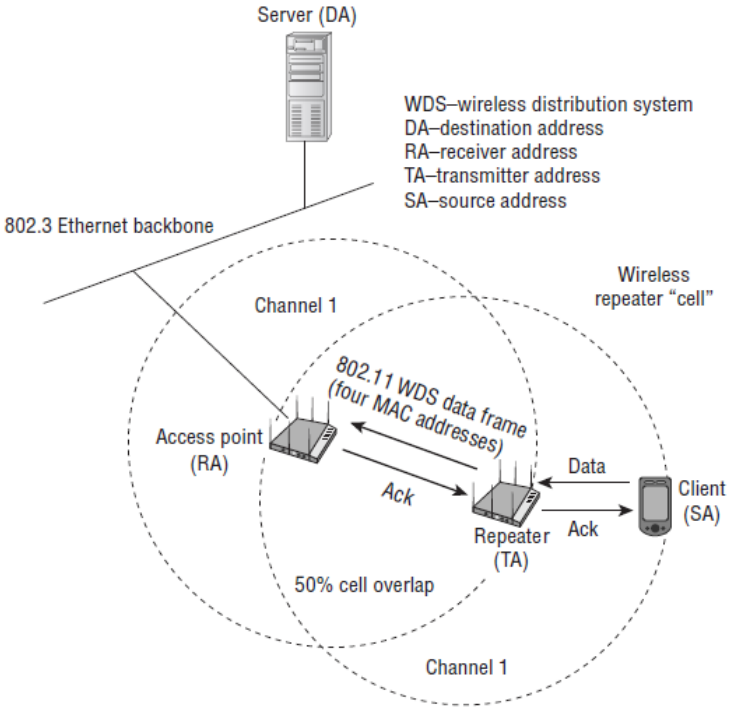


FIGURE 7.3 Wireless distribution system, dual radios

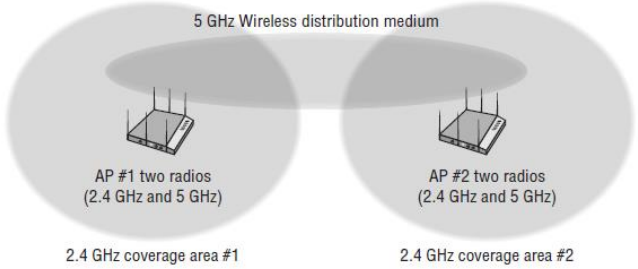
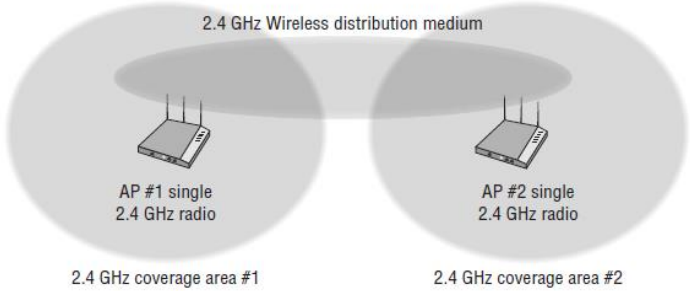
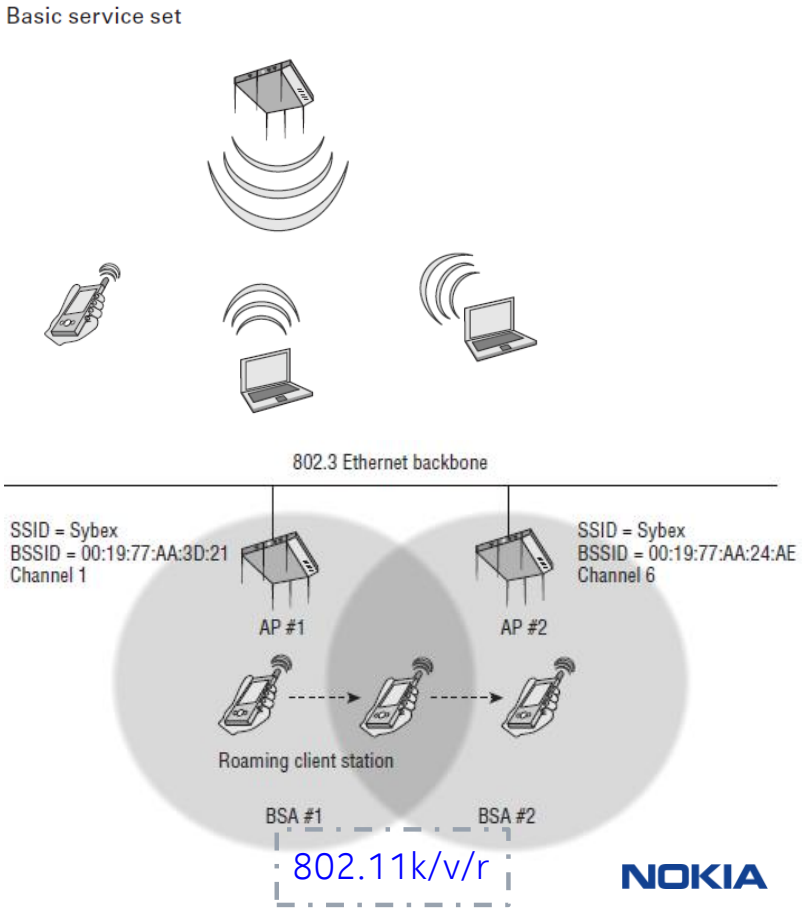


FIGURE 7.2 Wireless distribution system, single radio



WLAN topography(3)

- ✓ There are four 802.11 topologies:
  - basic service set (BSS)
    - ➢ Consist of one AP with one or more associated clients.
    - ➢ Cornerstone topology of an 802.11 network
  - extended service set (ESS)
    - ➢ Two or more BSS connected by DSM
  - independent basic service set (IBSS)
    - ➢ Consist solely of client stations no AP deployed
  - mesh basic service set (MBSS)
    - ➢ A set of APs that provide mesh distribution form a MBSS
- ✓ QoS Basic Service Set
  - ➢ QoS BSS can be implemented with in all of above 802.11 topologies
- ✓ Define SSID/BSSID/ESSID
  - ➢ SSID/ESSID: logic name of 802.11 network
  - ➢ BSSID: 48bit MAC address to identify the BSS.



WLAN topography(4)

Independent basic service set

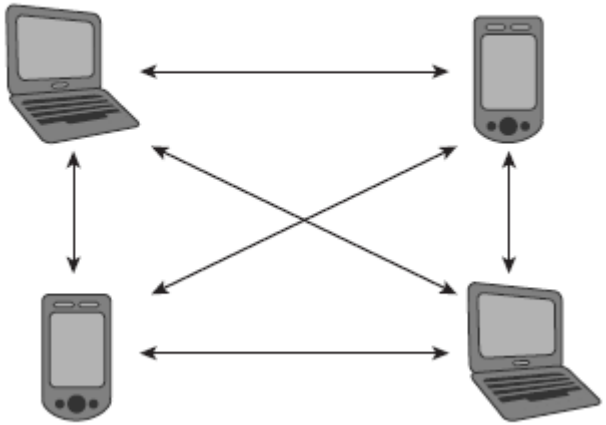
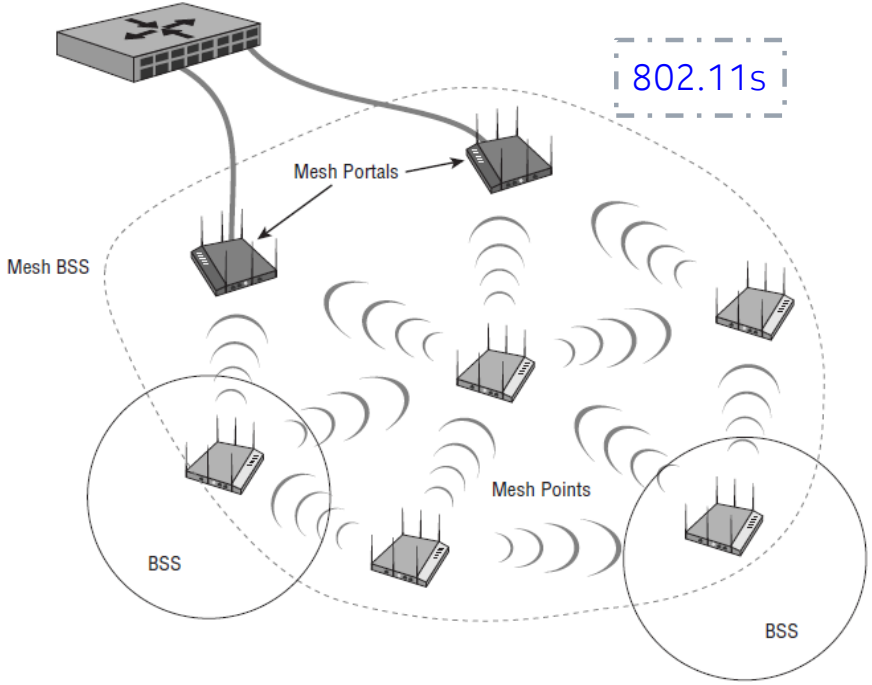


FIGURE 7.15 Mesh basic service set



WLAN architecture(1)

Three logical operation planes of 802.11 WLAN:

- ✓ **Management Plane**
  - WLAN Configuration
  - WLAN Monitoring and Reporting
  - WLAN Firmware Management
- ✓ **Control Plane:**

  The *control plane* is often defined by protocols that provide the intelligence and interaction between equipment in a network.
  - Dynamic RF
  - Roaming Mechanisms
  - Client Load Balancing
  - Mesh Protocols
- ✓ **Data Plane**

  The data plane is where user data is forwarded.

Three 802.11 WLAN architecture:

- ✓ Autonomous WLAN architecture
  - These AP often refer as *fat* AP or *standalone* AP, *autonomous* AP.
  - All setting exist in AP itself
- ✓ Centralized WLAN architecture
  - WLAN controller+ lightweight AP
  - All planes are moved to WLAN controller
- ✓ Distributed WLAN architecture
  - Cooperative APs share the control plane and data plane information using proprietary protocols.
  - The management plane remains centralized

WLAN architecture(2)

FIGURE 10.13 Simple wireless network using an autonomous architecture

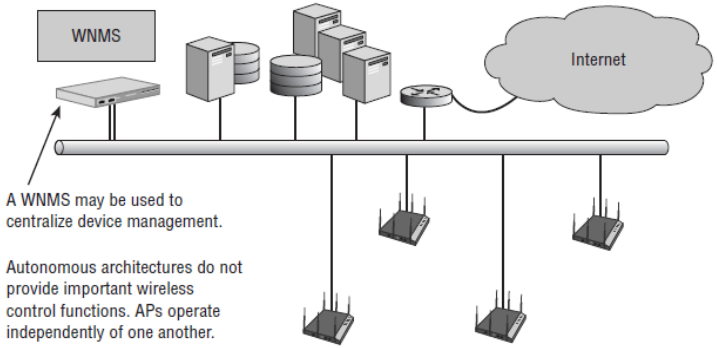


FIGURE 10.16 Centralized WLAN architecture: WLAN controller

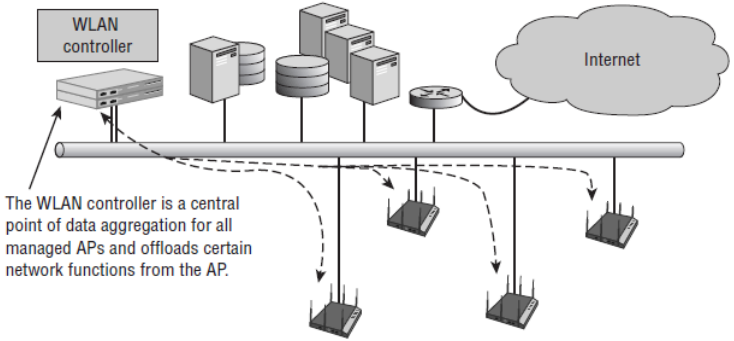
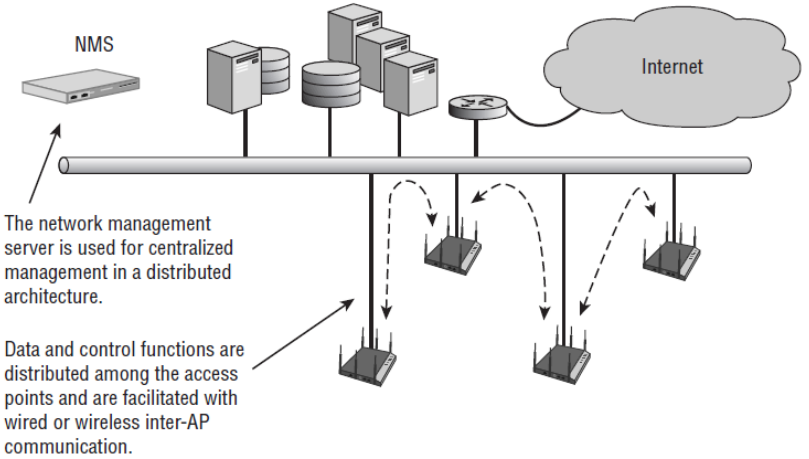


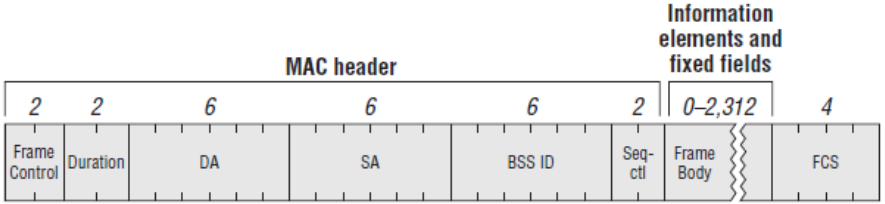
FIGURE 10.21 Distributed WLAN architecture

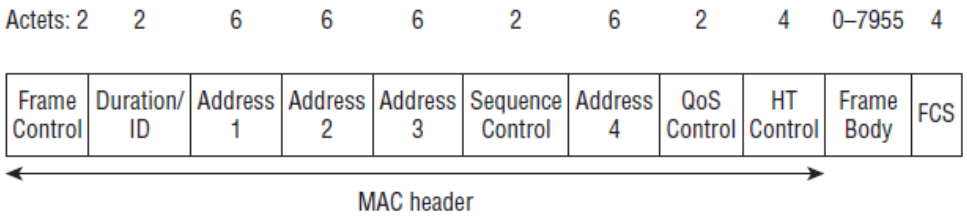


6.802.11 Protocol analysis

802.11 Protocol analysis
802.11 Frames overview(1)

- ✓ **Packets, Frames, and Bits**
- ✓ **MSDU,MPDU,PSDU,PPDU**
- ✓ **802.11 Frames**
  - Management Frames, 12 management frame subtypes (CWAP Chapter 4)
  - Control Frames, 8 control frame subtypes(CWAP Chapter 5)
  - Data Frames, 15 data frame subtypes(CWAP Chapter 6)





CWAP Chapter3 MAC sublayer Frame Format

802.11 Frames overview(2)

Wireshark Frame type and subtype list:

帧类型/子类型	过滤器语法
Management frame	wlan.fc.type == 0
Control frame	wlan.fc.type == 1
Data frame	wlan.fc.type == 2
Association request	wlan.fc.type_subtype == 0x00
Association response	wlan.fc.type_subtype == 0x01
Reassociation request	wlan.fc.type_subtype == 0x02
Reassociation response	wlan.fc.type_subtype == 0x03
Probe request	wlan.fc.type_subtype == 0x04
Probe response	wlan.fc.type_subtype == 0x05
Beacon	wlan.fc.type_subtype == 0x08
Disassociate	wlan.fc.type_subtype == 0x0A
Authentication	wlan.fc.type_subtype == 0x0B
Deauthentication	wlan.fc.type_subtype == 0x0C
Action frame	wlan.fc.type_subtype == 0x0D
Block ACK requests	wlan.fc.type_subtype == 0x18
Block ACK	wlan.fc.type_subtype == 0x19
Power save poll	wlan.fc.type_subtype == 0x1A
Request to send	wlan.fc.type_subtype == 0x1B
Clear to send	wlan.fc.type_subtype == 0x1C
ACK	wlan.fc.type_subtype == 0x1D
Contention free period end	wlan.fc.type_subtype == 0x1E
NULL data	wlan.fc.type_subtype == 0x24
QoS data	wlan.fc.type_subtype == 0x28
Null QoS data	wlan.fc.type_subtype == 0x2C

802.11 Management Frames(1)

✓ Beacon Frame

- Send periodically by AP(and stations in an IBSS),beacon interval
- Send in a specific data rate defined in AP MIB
- Contain time stamp as the time reference
- Contain many useful AP property info(mandatory or specific amendment)
- MBSS will send their own beacon info this is the one reason why impact performance.

✓ Probe Request Frame

- aimed at asking what network is available on this channel
- usually sent to the broadcast DA address
- may specify the SSID they are looking for
- Purpose is to discover APs and their supported network

✓ Probe Response Frame

- Response to the request frame

✓ Authentication Frame

- Purpose is to validate the device type if has proper 802.11 capabilities
- Open system: simple two dialogue
- WEP Share key authentication
- 802.1X/EAP authentication
- PSK authentication

AP will use beacons and probe request frames to inform STA of AP security capability

802.11 Management Frames(2)

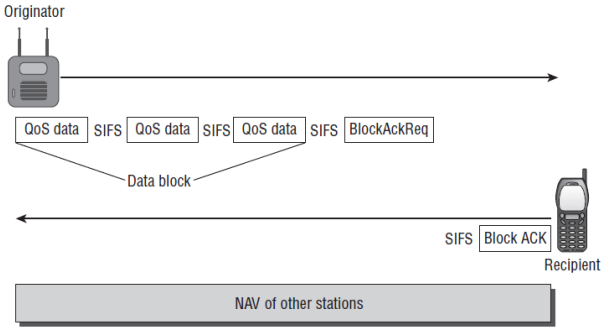
- ✓ **Association Request Frame**
  - Purpose is for the STA to join the AP and obtain the association ID(AID) .
- ✓ **Association Response Frame**
  - Response to the request frame
- ✓ **Disassociation Frame**
  - Once a station is associated to an AP, either side can terminate the association at any time by sending a disassociation frame
  - A disassociated station is still authenticated
  - In roaming scenario ,the kept authenticated status can accelerate the roaming process
  - Check the reason code
- ✓ **Deauthentication Frame**
  - This frame is used when all communications are terminated
  - AP has to reboot
  - STA stop the communication
  - Check the reason code

802.11 Management Frames(3)

- ✓ **Reassociation Request Frame**
  - sent only by a station to an AP
  - Already associated the ESS and want to associate another AP in the same ESS
  - The logic of the reassociation request was linked to roaming
- ✓ **Reassociation Response Frame**
  - Response to the request frame
- ✓ **ATIM Frame**
  - The ATIM frame is specific to IBSS networks
  - used for distribution of buffered frames to stations in sleep mode in the ad hoc network
  - Related to the 802.11 power management
- ✓ **Action Frame**
  - Trigger specific action
  - first appeared in 2003 with the 802.11h amendment
  - The number increased with each later amendment released
  - allow a form of added control
  - Action frame type: TPC request /report, channel switch announcement , block ack, link measurement .....

802.11 Control Frames(1)

- ✓ **RTS/CTS frames**
  - The purpose is to enhance the virtual carrier sense process
  - a mechanism that performs a NAV distribution and helps prevent collisions from occurring
  - dynamic bandwidth operations in 11ac
  - CTS-to-self is simply another method of performing NAV distribution that solely uses CTS control frames.
- ✓ **Power Save Poll (PS-Poll)**
  - STA is in power save mode
  - STA send PS-Poll frame to get the buffered unicast frame in AP
- ✓ **Acknowledgment (ACK)**
  - Response to the unicast frame to indicate if the frame is received or collision
  - a method of delivery verification
- ✓ **Contention Free-End (CF-End) CF-End + CF+ACK**
  - defined for use with an optional medium access methodknown as Point Coordination Function (PCF)
  - Less or even no Wi-Fi vendors support PCF
- ✓ **Block ACK Request (BlockAckReq)**
- ✓ **Block ACK (BlockAck)**
  - Transmit mechanism for QoS data
  - AP and STA both support Block ACK mechanism
  - Instead of acknowledging each unicast frame independently, the block of QoS data frames



802.11 Control Frames(2)

FIGURE 5.5 RTS/CTS Duration values

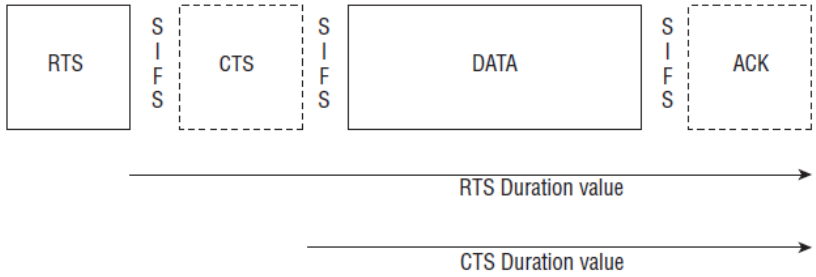
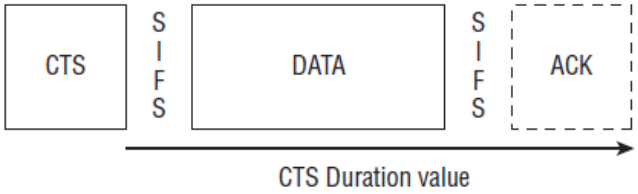
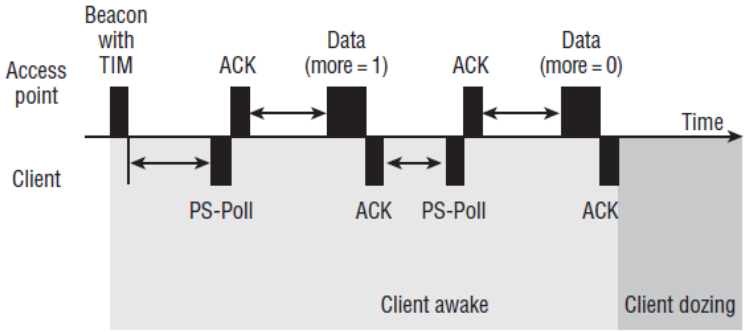
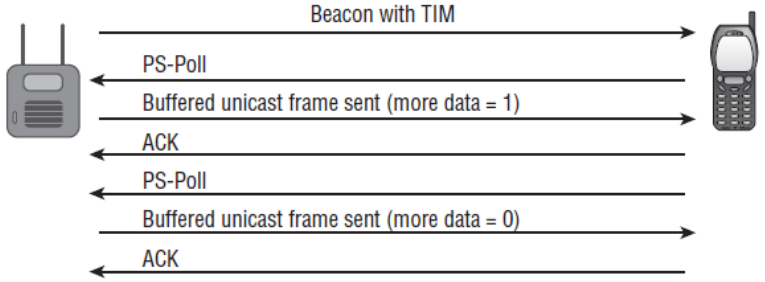


FIGURE 5.7 CTS-to-self frame Duration values



RE 5.15 Legacy power management





802.11 Data Frames(1)

✓ **Don't carry data frames**

- Null
- Qos Null
- CF-Ack
- CF-Poll
- CF-Ack + CF-Poll
- QoS CF-Poll
- QoS CF-Ack + CF-Poll

Purpose :

- transmit special control information
- enable or disable power save mode
- communicate with another device

✓ **Carry data frames**

- Data (simple data frame)
- QoS Data
- Data + CF-Ack
- Data+ CF-Poll
- Data + CF-Ack + CF-Poll
- QoS Data + CF-Ack
- QoS Data + CF-Poll
- QoS Data + CF-Ack + CF-Poll

CF: Contention free frames for PCF

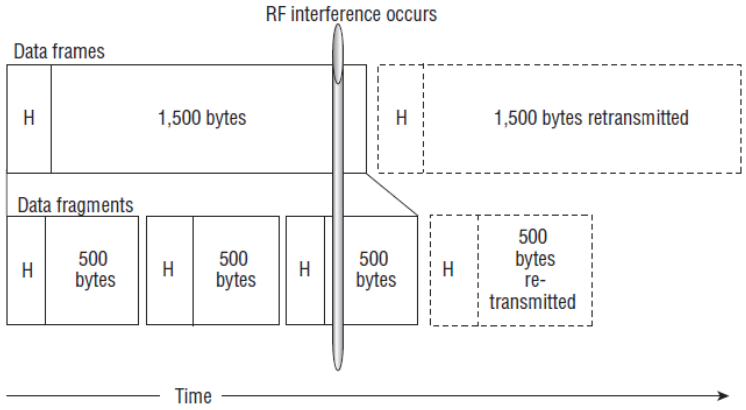
✓ **QoS and Non-QoS Data Frames**

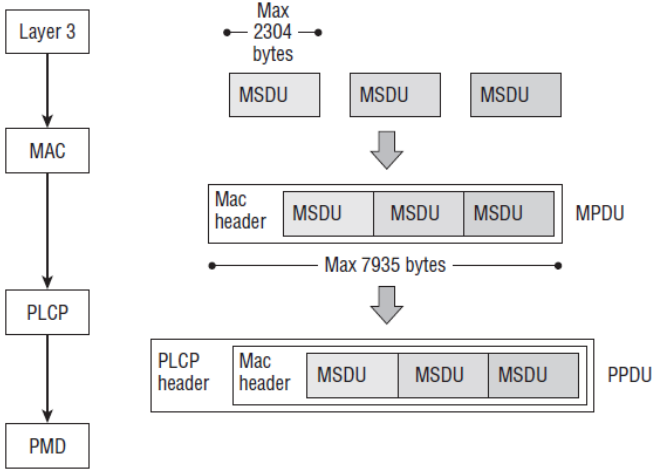
- QoS data frame is transmitted: QoS subfield =1 and include QoS Control field
- Non-QoS data frame is transmitted: QoS subfield =0 and not include QoS Control field

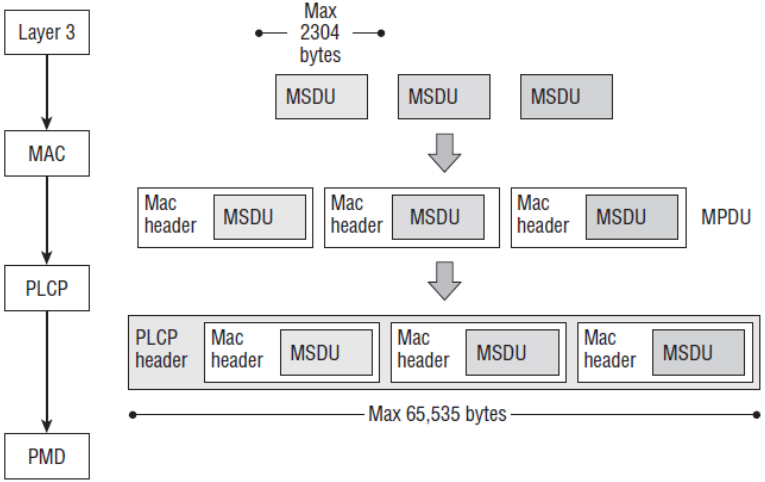
Transmitting station	Receiving station	Data frame subtype used
Non-QoS station	Non-QoS station	Non-QoS frame
Non-QoS station	QoS station	Non-QoS frame
QoS station	QoS station	QoS frame
QoS station	Non-QoS station	Non-QoS frame
All	Broadcast	Non-QoS frame, unless the transmitting station knows that all stations in the BSS are QoS capable, in which case a QoS frame would be used
All	Multicast	Non-QoS frame, unless the transmitting station knows that all stations in the BSS that are members of the multicast group are QoS capable, in which case a QoS frame would be used

802.11 Data Frames(2)

- ✓ **Data Frame fragmentation**
- ✓ **Data Frame Aggregation**
  - A-MSDU (in the standard)
  - A-MPDU (in the real world,CWAP chapter10)
  - Most chip vendor support A-MPDU not A-MSDU







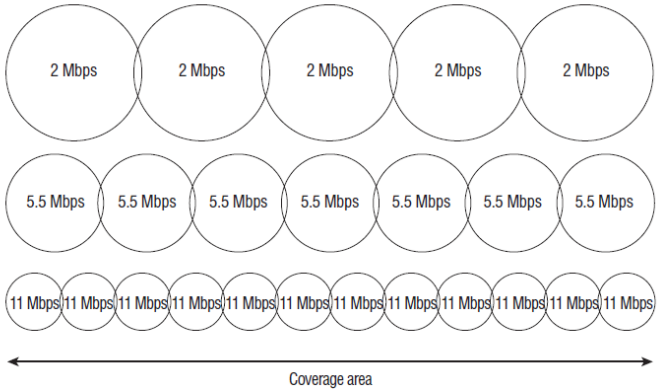
802.11 Data Frames(3)

- ✓ **Rate Selection**
  - Multirate Support
  - Basic and Supported Rates
  - Dynamic Rate Selection
    - The DRS algorithms are proprietary
    - Most vendors base DRS on RSSI thresholds, packet error rates, and retransmissions

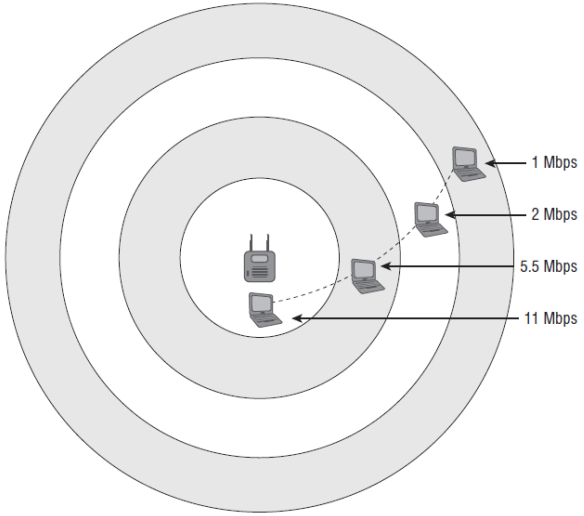
TABLE 6.4 WLAN data cell: vendor recommendations

Data rate	Minimum received signal	Minimum signal-to-noise ratio
54 Mbps	–71 dBm	25 dB
36 Mbps	–73 dBm	18 dB
24 Mbps	–77 dBm	12 dB
12/11 Mbps	–82 dBm	10 dB
6/5.5 Mbps	–89 dBm	8 dB
2 Mbps	–91 dBm	6 dB
1 Mbps	–94 dBm	4 dB

IGURE 6.11 Data rate coverage zones



RE 6.10 Dynamic rate switching



NOKIA

7.802.11 media contention

802.11 media contention(1)

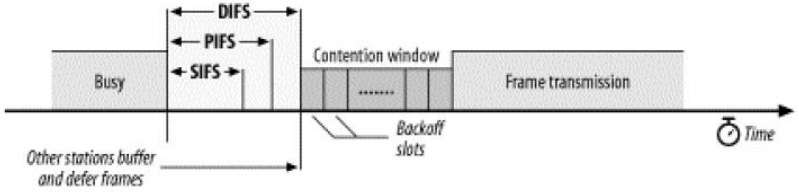
✓ CSMA/CA

- 802.11 stations, including both AP stations and non-AP stations, use carrier sense multiple access with collision avoidance (CSMA/CA) to contend for the wireless channel
- Collision avoidance means that collision handling has to happen before any data is transmitted.
- The end result is that CSMA/CA causes WLANs to have a much lower throughput-to-data rate ratio than wired LANs.
- The most basic goal of 802.11 medium contention to keep the channel clear so that collisions are avoided.
- Use the distributed coordination function (DCF) for non-QoS WLANs
- Use the the hybrid coordination function (HCF) using enhanced distributed channel access (EDCA) for QoS WLANs

✓ Carrier Sense

- Physical Carrier Sense :
  - CCA energy detection
- Virtual Carrier Sense : NAV, keeps APs and stations quiet even if the CCA cannot be used to clear the channel
  - RTS/CTS, CTS-to-self, Duration/ID

802.11 media contention(2)



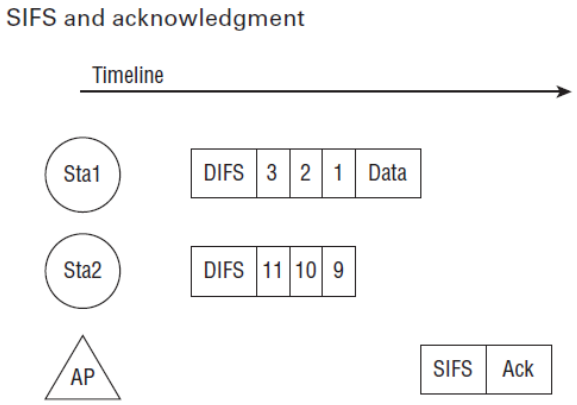
✓ Interframe Spaces

There are six different IFS values in 802.11 networks

- SIFS, If the arbitration has been completed ,SIFS will be used
- RIFS, If the arbitration has been completed ,RIFS will be used for consecutive frames transmission by same 802.11n
- DIFS, If arbitration has not been determined, DIFS will be used for WLAN not support 802.11e QoS
- AIFS, If arbitration has not been determined, AIFS will be used for WLAN support 802.11e QoS
- EIFS, If an AP or station has received a corrupted frame, EIFS will be used
- PIFS, part of PCF and therefore not used in the real world.

✓ Random Backoff

- The random backoff is a quiet period before a frame transmission
- the random backoff is not static



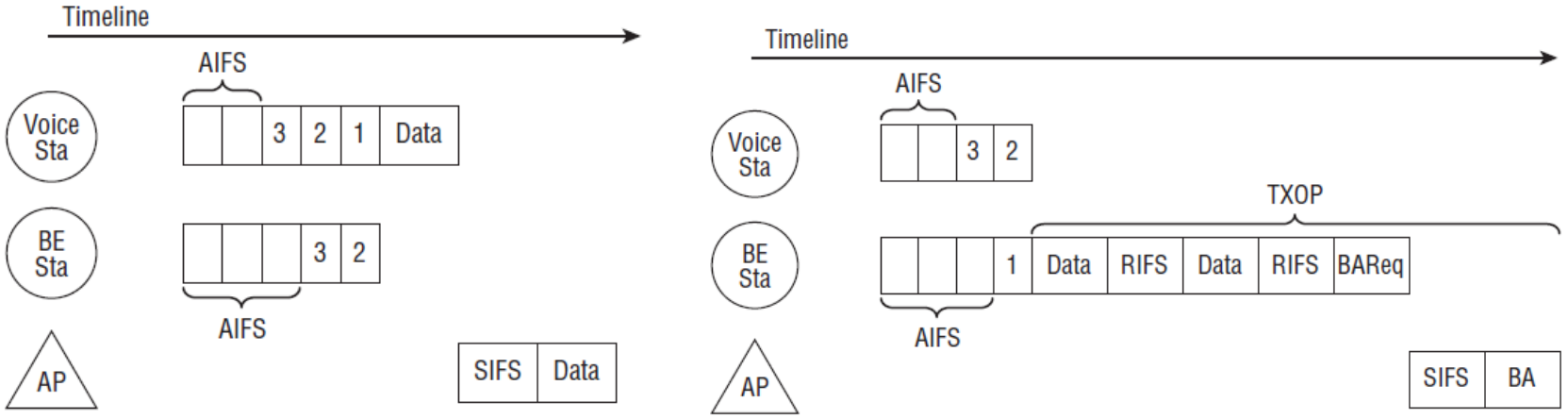
DCF media contention :CCA/NAV/IFS/Random Backoff

802.11 media contention(3)

Access category	Min *x*	CW Min	Max *x*	CW Max
Voice	2	3	3	7
Video	3	7	4	15
Best effort	4	15	10	1023
Background	4	15	10	1023

✓ EDCA for QoS WLAN

- prioritizes the four ACs: voice, video, best effort, and background
- **IFS** An AIFS is used instead of a DIFS.
- **CW** Different access categories are assigned different CW values.
- **Frame transmission A transmit opportunity (TXOP)** is allocated rather than allowing a single frame.

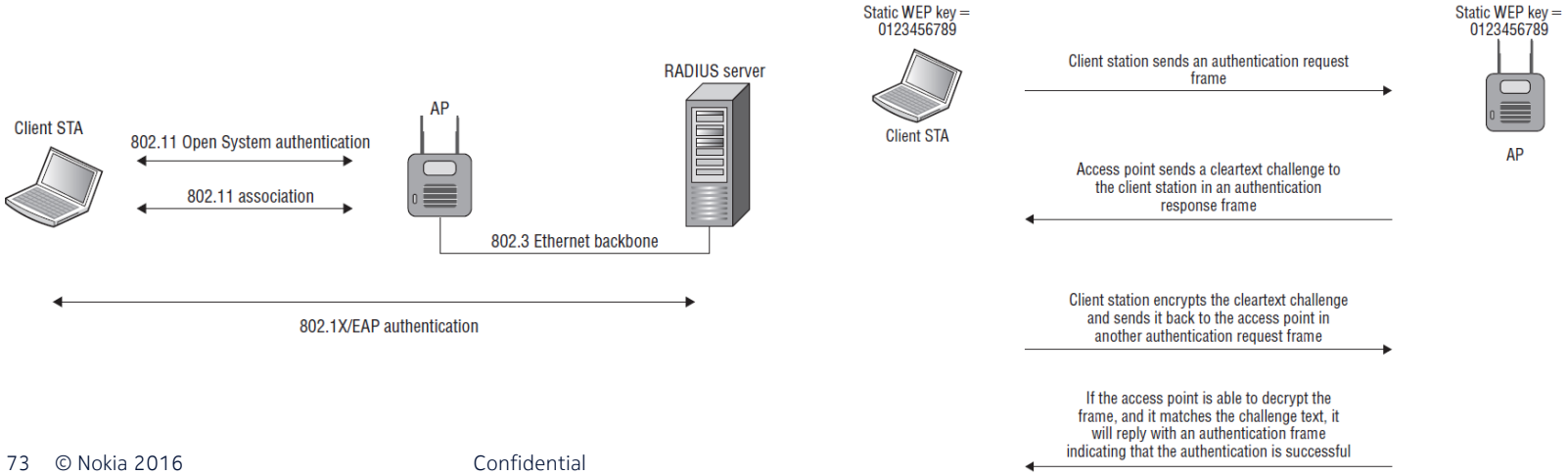


8.802.11 Security

802.11 Security (1)
Authentication

The 802.11 authentication merely establishes an initial connection between the client and the access point, basically validating or authenticating that the STA is a valid 802.11 device.

- Open System Authentication
- Shared Key Authentication (pre-RSNA security method)
  - four-way authentication frame exchange
  - If Shared Key authentication is successful, the same static WEP key that was used during the Shared Key authentication process will also be used to encrypt the 802.11 data frames.



802.11 Security (2)
WLAN Encryption Methods

Layer 2 encryption methods are used to provide data privacy for 802.11 data frames

- ✓ **Wired Equivalent Privacy (WEP)**
  - 64-bit WEP and 128-bit WEP as supported encryption methods,24-bit initialization vector(IV), RC4 algorithm
  - 64-bit WEP uses a secret 40-bit static key, 128-bit WEP encryption uses a 104-bit secret static key
  - WEP encryption adds 8 bytes of overhead to an 802.11 MPDU
- ✓ **Temporal Key Integrity Protocol (TKIP)**
  - TKIP is an enhancement of WEP
  - uses dynamically created encryption keys as opposed to the static keys, 4-Way Handshake
  - TKIP encryption adds 20 bytes of overhead to an 802.11 MPDU
- ✓ **CTR with CBC-MAC Protocol (CCMP)**
  - CCMP is based on the CCM of the AES encryption algorithm
  - CCMP encryption adds 16 bytes of overhead to an 802.11 MPDU

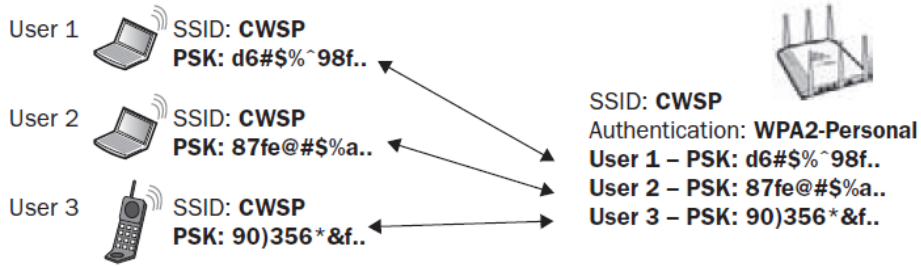
The RSN information element is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames.

802.11 Security (3)
WPA/WPA2 Certification

- ✓ **Wi-Fi Alliance introduced the Wi-Fi Protected Access (WPA) certification**
- ✓ **WPA, incorporating the TKIP/RC4 cipher.**
- ✓ **WPA2, incorporating the CCMP/AES cipher, backward compatible with WPA.**
- ✓ **WPA/WPA2-Personal use the PSK authentication.**
- ✓ **WPA/WPA2-enterprise use the 802.1X/EAP authentication.**
- ✓ **IEEE802.11n amendment stats that high throughput (HT) stations cannot use WEP or TKIP.**
- ✓ **The Wi-Fi Alliance also began requiring that all HT radios not use TKIP when using HT data rates.**
- ✓ **Most likely, the WLAN vendors will still offer support for TKIP and WEP with HT rates, but the use of TKIP and WEP will not be a default setting.**

802.11 Security (6)
SOHO 802.11 Security--WPA/WPA2-Personal

- ✓ WPA - Personal specifies TKIP/RC4 encryption and *WPA2 - Personal* specifies CCMP/AES.
- ✓ WLAN vendors have many names for PSK authentication, including WPA/WPA2 - Passphrase, WPA/WPA2 - PSK, and WPA/WPA2 - Preshared Key.
- ✓ A preshared key (PSK) used in a robust security network is 256 bits in length, or 64 characters when expressed in hex.
- ✓ user enters a *passphrase,* which is an 8 to 63 character string
- ✓ *passphrase - PSK mapping* formula: **PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)**
- ✓ The 256 - bit PSK is also used as the *pairwise master key (PMK)* , every client station uses the same PSK.
- ✓ Proprietary PSK for different clients.



802.11 Security (7)
SOHO 802.11 Security--WPS

- ✓ ***Wi - Fi Protected Setup (WPS)*** **defines simplified and automatic WPA and WPA2 security configurations for home and small - business users.**
- ✓ **WPS Architecture defines three primary and logical roles: AP/Enrollee/Register.**
- ✓ **Three easy setup solutions:**
  - ☐ personal identification number (PIN),mandatory, enter the PIN into the registrar or enrollee
  - ☐ push button configuration (PBC),optional , push button on both registrar and enrollee
    - WSC ease-of-use will be drastically degrade if long vs. short single vs. multiple button presses are required
    - PBC also use PIN code, value is '00000000'.
  - ☐ Near Field Communication (NFC),optional , tap two NFC-capable devices together
- ✓ **Provide visual indicator LED flashing frequencies, In-Progress/Error/Session Overlap/Success**
- ✓ **WFADevice**
  - ☐ with UPnP ™ Architecture
  - ☐ implements IP based transports provide an out-of-band mechanism to configure IEEE 802.11 (a,b,g,n) settings on the device.

802.11 Security (8)
SOHO 802.11 Security--WPS

- ✓ **Registration Protocol**
  - Discovery phase by beacon frame or probe request frame with WSC IE.
  - After discovery phase, client will find the target AP
  - After authentication phase, will start EAP-WSC process
  - Start with EAPPOL-Start, end with EAP-Fail, total 14 frame exchange
  - STA get all AP's security configuration by M1-M8, after the EAP-Fail, STA will disconnect with AP firstly
  - STA re-connect AP with already got security configuration
  - The core task of WSC is to finish the security info exchange between STA and AP, the left task is same as the STA connect AP's process.

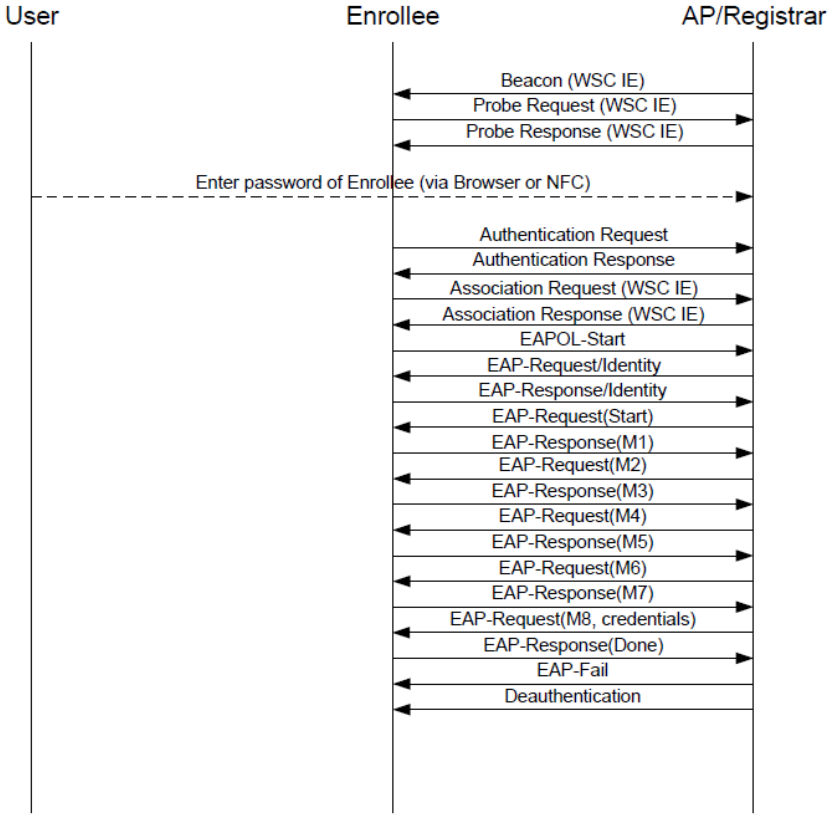


Figure 4 – In-band Setup Using a Standalone AP/Registrar

802.1X

- ✓ **The 802.1X standard is a port-based access control standard, provides an authorization framework.**
- ✓ **Extensible Authentication Protocol (EAP) is used as the layer 2 authentication protocol.**
- ✓ **The three major components of an 802.1X framework:**
  - ☐ Supplicant
    - use an EAP protocol to communicate with the authentication server at layer 2.
    - a software application that performs the 802.1X endpoint services
  - ☐ Authenticator
    - plays the role of the intermediary, passing messages between the supplicant and the authentication server
    - maintains two virtual ports: an uncontrolled port and a controlled port
    - need to be configured with the RADIUS server's IP address and UDP port along with a shared secret in order to communicate with the server
  - ☐ Authentication Server
    - validates the credentials of a supplicant that is requesting access and notifies the authenticator that the supplicant has been authorized
    - The 802.1X standard defines the authentication server as a RADIUS server.

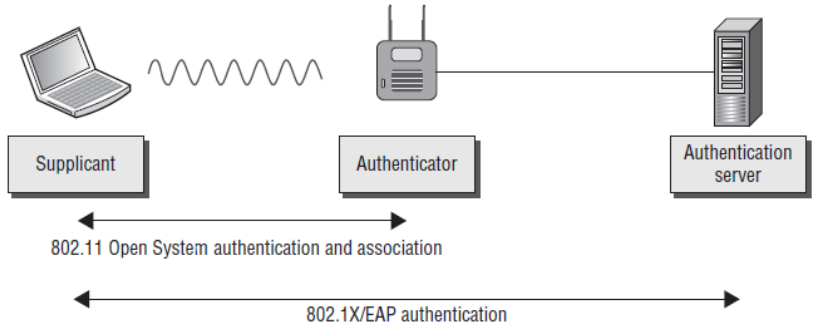
EAP(1)

- ✓ Extensible Authentication Protocol (EAP), as defined in IETF RFC 2284, provides support for many authentication methods.
- ✓ Most types of EAP that require mutual authentication use a server-side digital certificate to validate the authentication server.
- ✓ EAPOL is used between the supplicant and the authenticator.
- ✓ EAPOL is translated to EAP in RADIUS between the authenticator and the authentication server.

TABLE 9.1 EAPOL messages

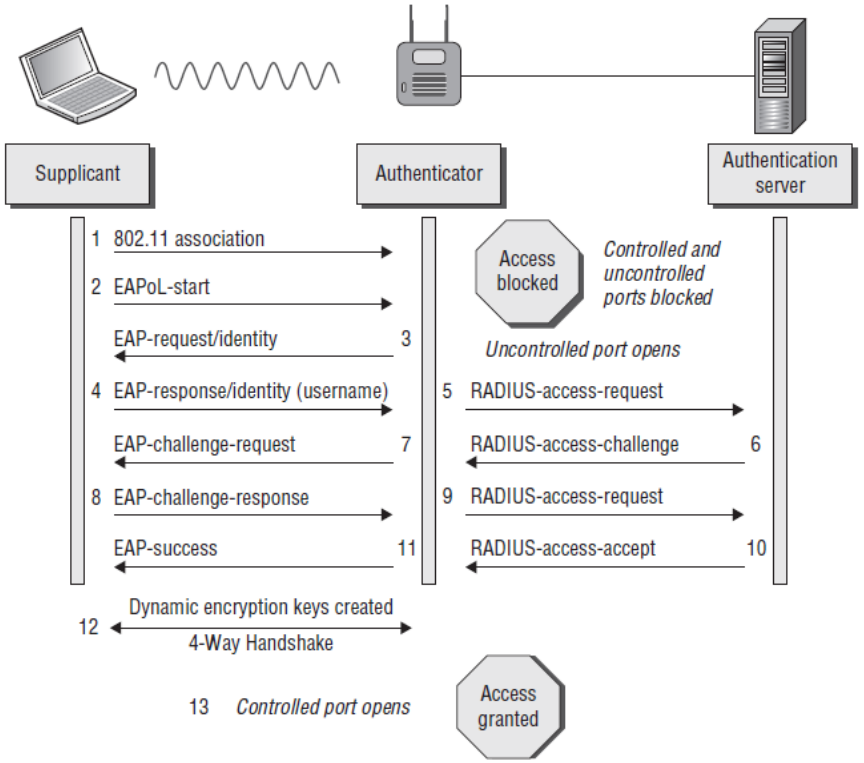
Packet type	Name	Description
0000 0000	EAP-Packet	This is an encapsulated EAP frame. The majority of EAP frames are EAP-Packet frames.
0000 0001	EAPOL-Start	This is an optional frame that the supplicant can use to start the EAP process.
0000 0010	EAPOL-Logoff	This frame terminates an EAP session and shuts down the virtual ports. Hackers sometimes use this frame for DoS attacks.
0000 0011	EAPOL-Key	This frame is used to exchange dynamic keying information. For example, it is used during the 4-Way Handshake.
0000 0100	EAPOL- Encapsulated - ASF-Alert	This frame is used to send alerts, such as SNMP traps to the virtual ports.

FIGURE 9.26 802.11 association and 802.1X/EAP



EAP(2)

- ✓ Generic EAP exchange
  - Step 4 : the supplicant's username is seen in clear text.
  - Steps 6-9： supplicant's password credentials are validated using a weak challenge/hash response.
  - The most secure EAP methods used today employ tunneled authentication to pass identity credentials



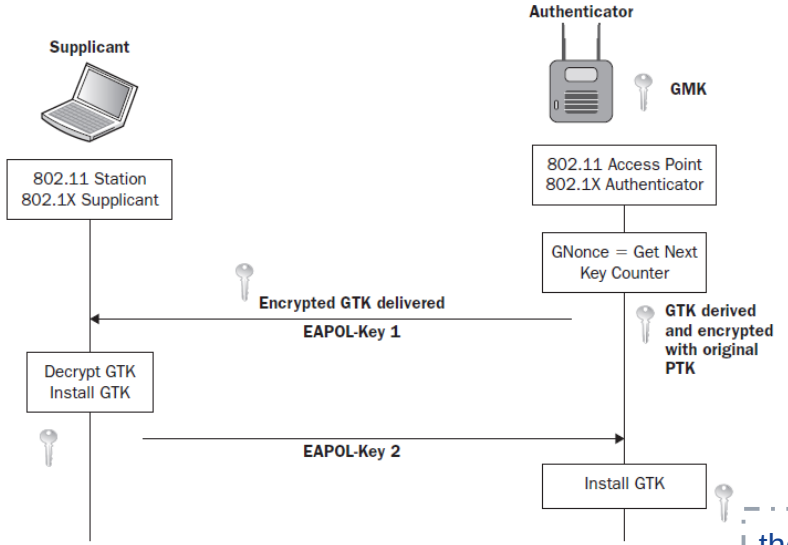
Strong EAP Protocols

- ✓ The stronger and more commonly deployed methods of EAP use *Transport Layer Security (TLS)*–based authentication and/or TLS-tunneled authentication.
- ✓ weaker EAP types, such as EAP-MD5 and EAP-LEAP, which have only one supplicant identity.
- ✓ tunneled authentication have two supplicant identities: *outer identity* and *inner identity*
- ✓ The whole purpose of tunneled authentication is to provide a secure channel to protect the user identity credentials.
- ✓ *EAP-Protected Extensible Authentication Protocol (EAP-PEAP)* (EAP inside EAP)
  - ◘ the supplicant's identity and credentials are always encrypted inside the TLS tunnel that is established
  - ◘ the most common and most widely supported EAP method used in WLAN security.
  - ◘ Three majority version: EAP-PEAPv0 (EAP-MSCHAPv2)/EAP-PEAPv0 (*EAP-TLS*)/EAP-PEAPv1 (EAP-GTC)

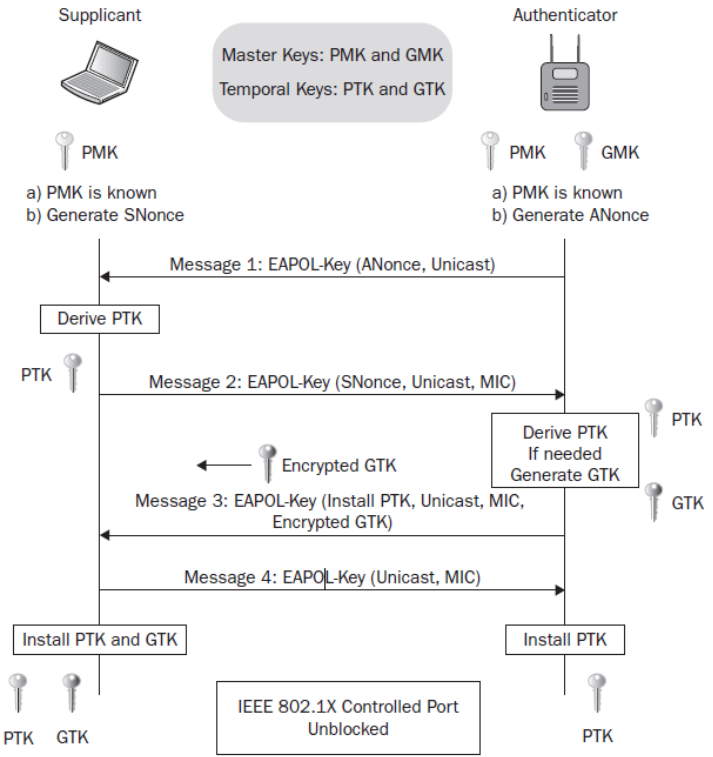
4 - Way Handshake+Group Key Handshake

The 4-Way Handshake is a final process used to generate pairwise transient keys for encryption of unicast transmissions and a group temporal key for encryption of broadcast/ multicast transmissions

IGURE 5.23 The Group Key Handshake



GURE 5.22 The 4-Way Handshake



the Group Key Handshake is identical to the last two frames of the 4 - Way Handshake.

802.11 Security (4)
Robust Security Network (RSN)

- ✓ **Robust security network associations(RSNAs)**
  - ☐ Two 802.11 stations should use 4-way handshake to create dynamic encryption key.
  - ☐ CCMP/AES encryption is the mandated encryption method, while TKIP/RC4 is an optional encryption method.
  - ☐ Each SSID can have their own encryption method separately.

FIGURE 9.15 Transition security network

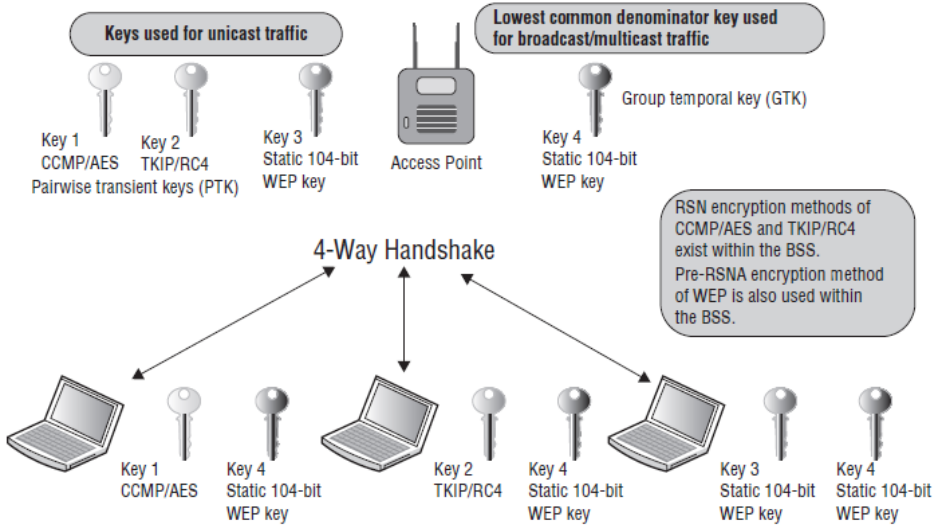
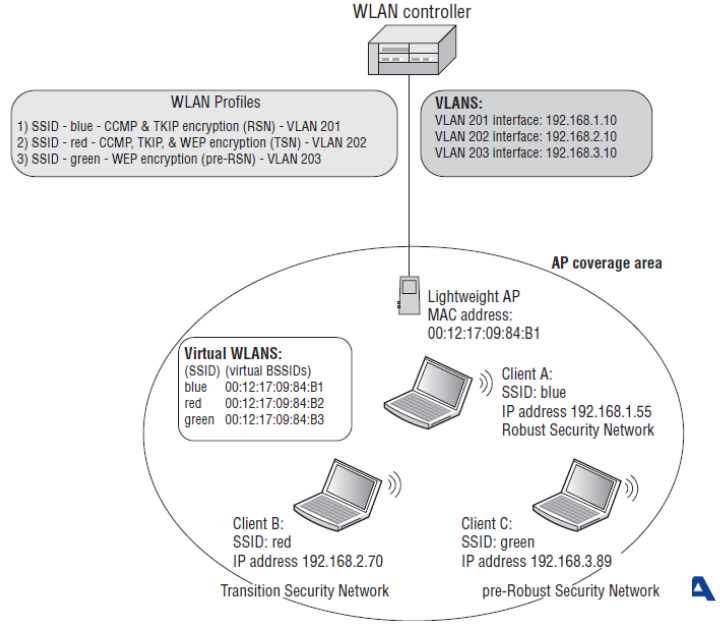


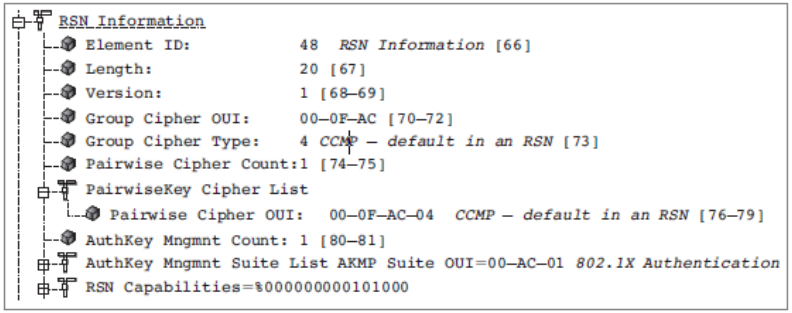
FIGURE 9.16 RSN, pre-RSN, and TSN within the same AP cell



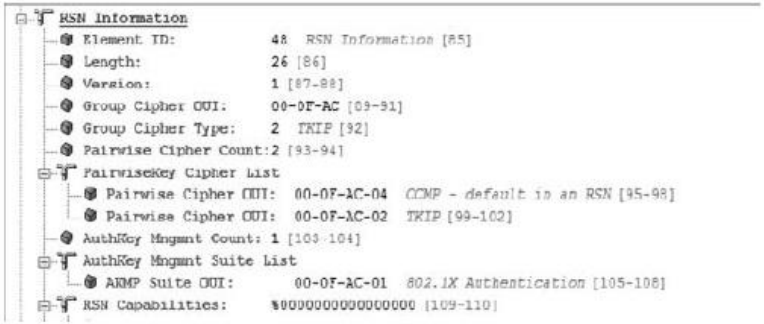
802.11 Security (5)
RSN Information Element

- ✓ Access points will use **beacons and probe response** frames to inform client stations of the AP security capabilities.
- ✓ Client stations use the **association request frame** to inform the access point of the client station security capabilities.
- ✓ The group cipher's encryption meth is the lowest common denominator.

JRE 9.19 RSN Information element—CCMP pairwise and CCMP group cipher



RE 9.20 RSN information element—CCMP pairwise and TKIP group cipher



9. Performance analysis

Performance Analysis(1)

- ✓ **Many different factors affect wireless network performance, some of which are listed here:**
  - High volumes of associated clients to a single access point
  - Clients communicating at low data rates because of physical distance from the access point
  - Mixed modulation types and protection mechanisms
  - Co-channel and adjacent channel 802.11 interfering devices
  - Non-802.11 RF interference
  - Inefficient roaming
  - Physical environment: multipath, obstructions, and absorption
  - Channel hops because of Dynamic Frequency Selection (DFS)

Performance Analysis(2)

- ✓ **Poor network performance manifests itself in wireless network analyzers as follows:**
  - High level of retransmissions
  - High level of corrupted packets
  - Weak signal
  - Excessive RTS/CTS packets
  - Excessive data rate changes
  - Too many clients associated to the same AP
  - High wireless utilization
  - Slow roaming times

Performance analysis(3)

- ✓ **The mortal enemy of Wi-Fi performance is layer 2 retransmissions that occur at the MAC sublayer.**
  - any good 802.11 protocol analyzer can track layer 2 retry statistics for the entire WLAN
  - RF Interference
    - 802.11 radios can sense the energy during the clear channel assessment (CCA) and defer transmission entirely
    - spectrum analyzer can see which channels are disrupted
  - Multipath
    - multipath can cause inter symbol interference (ISI), which causes data corruption.
    - Biggest problem for legacy 802.11 a/b/g,802.11n/ac use MIMO to take advantage of multipath
  - Adjacent Channel Interference
    - In reality, there will be some frequency overlap of the sidebands of each OFDM channel.
    - Overlapping channels
  - Co-channel interference

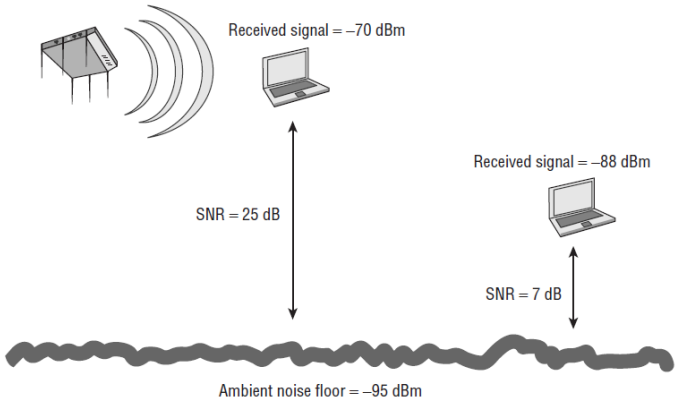
Low SNR

- The background noise is too close to the received signal or the received signal level is too low, data can be corrupted and retransmissions will increase.
- If the amplitude of the noise floor is too close to the amplitude of the received signal.

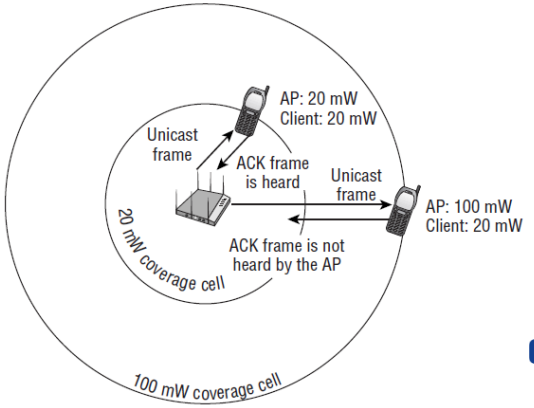
Mismatched Power Settings

- As a client moves to the outer edges of the coverage cell, the client can “hear” the AP; however, the AP cannot “hear” the client.
- Protocol analysis in AP side and client side, frame corruption and re-transmission in AP side but not in client side.
- Improve AP receive sensitivity can essentially fix this issue.
- Increasing the power of an access point is the wrong way to increase range, the best solution is to increase the antenna gain of the AP.

URE 12.9 High and low signal-to-noise ratio



12.10 Mismatched AP and client power

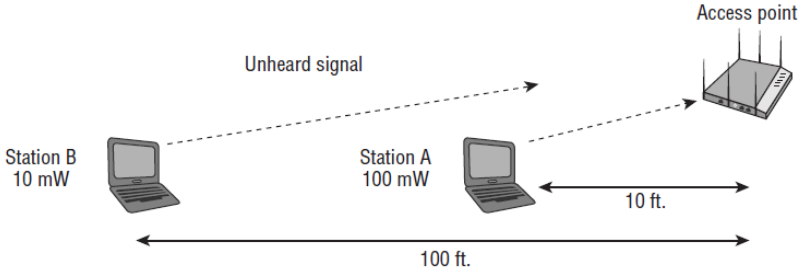


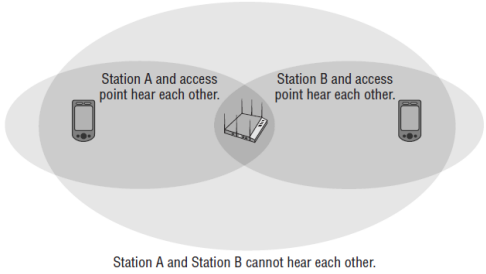
Near/Far

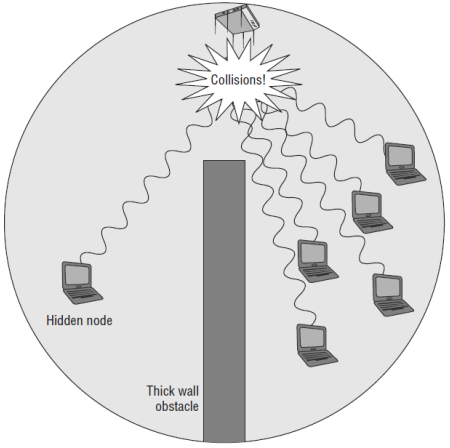
- A low-powered client station that is at a great distance from the access point could become an unheard client if other high-powered stations are very close to that access point.
- The far distance client occupied channel long time will impact the near client's performance.
- Troubleshoot with protocol analysis in AP and client side.

Hidden Node

- The hidden node problem occurs when one client station's transmissions are heard by the access point but are not heard by any or all of the other client stations in the basic service set (BSS).
- The hidden node problem may exist, poor WLAN design or obstructions such as a newly constructed wall or a newly installed bookcase, two client stations are at opposite ends of an RF coverage cell and they cannot hear each other.
- Troubleshoot with protocol analysis or enable RTS/CTS.







10. ACS/DCS/DFS

✓ ACS

The best channel is determined once at AP boot and won't change afterwards

✓ DCS

Monitor traffic and noise levels on the channel on which the AP is currently operating. Once exceed the configured DCS thresholds, will select an alternate channel

✓ DFS

avoid co-channel operation with radar systems in the 5GHz band.

✓ Channel Scanning

This is analysis that captures traffic on all selected channels, spending a short amount of time on each channel before moving to the next one.

✓ Channel Switch Announcement

This is used by the AP to inform the cell that all stations had to move to another channel. This is also related to 802.11h. When a radar blast is detected, all stations must leave the affected channel. The AP can be set to announce to the cell which is the next

channel.

Survey based algorithm of ACS/DCS

- ✓ The survey based algorithm to query the interface for channel active time, channel busy time, channel tx time and noise.
- ✓ Low-level noise: physical carrier sense
- ✓ High-level noise: RSSI/SNR
- ✓ Different chip vendors have their own algorithm.
- ✓ The survey algorithm relies on these values to build an *interference factor* to give a sense of how much interference was detected on the channel and then picks the channel with the lowest *interference factor*
- ✓ Refer URL: https://wireless.wiki.kernel.org/en/users/documentation/acs

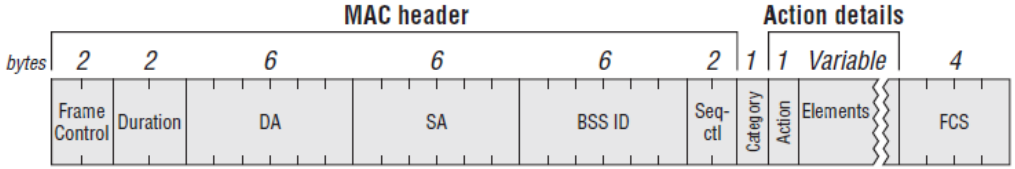
DFS

- ✓ Dynamic Frequency Selection allows 5 GHz capable 802.11 devices to share spectrum with radar devices.
- ✓ DFS is currently a requirement in the US, EU, and Japan, but it seems some other countries are starting to consider requiring DFS as well.
- ✓ Concepts
  - Non Occupancy List (NOL): channels which we know have recent radar pulses and we cannot use
  - Channel Availability Check (CAC) Time: amount of time we should sit idle on a channel checking for radar pulses before initiating 802.11 frames on
- ✓ Software then is needed for:
  - Management of which channels have seen radar pulses recently / timers to clean them
  - Management of informing connected clients of switching channels
  - Algorithms to help identify the next best channel - think the requirement is to actually choose one randomly

Channel Switch Announcement frame format

The Channel Switch Announcement frame uses the Action frame body format and is transmitted by an AP in a BSS, a STA in an IBSS, or a mesh STA in an MBSS to advertise a channel switch.

URE 4.34 Action frame structure



(1) 0 (spectrum management).
(2) 4(Channel Switch Announcement frame)
(3) described 8.4.2.21.

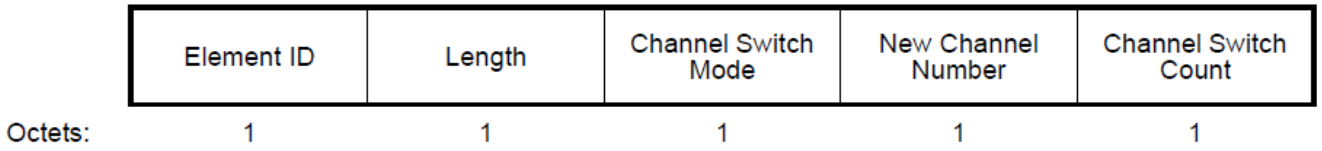
Category	Spectrum Management Action	Channel Switch Announcement element	Secondary Channel Offset element	Mesh Channel Switch Parameters element
Octets: 1	1	5	3	6

Figure 8-436—Channel Switch Announcement frame Action field format

802.11n-2012_8.5.2.6

Channel Switch Announcement element format

The Channel Switch Announcement element is used by an AP in a BSS, a STA in an IBSS, or a mesh STA in an MBSS to advertise when it is changing to a new channel and the channel number of the new channel. The format of the Channel Switch Announcement element is shown in Figure 8-102.



	Element ID	Length	Channel Switch Mode	New Channel Number	Channel Switch Count
Octets:	1	1	1	1	1

Figure 8-102—Channel Switch Announcement element format

802.11n-2012_8.4.2.21

Channel Switch Timing element

The Channel Switch Timing element contains information regarding the channel switch timing.

The STA sending the Channel Switch Timing element waits for the first data frame exchange on the off-channel for Switch Timeout microseconds before switching back to base channel.

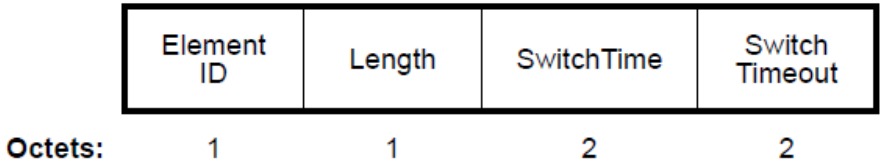


Figure 8-264—Channel Switch Timing element format

802.11n-2012_8.4.2.26

11. Calibration and power management

Document reference

- ✓ 3HH-03663-9034-DFZZA-01-G240WB F240WA Manufactory – WIFI Transmit Power Setting.pptx
- ✓ 3HH-10243-6018-DFZZA-01P04-AONTR34 - BCM43217 WiFi Calibrating Guide.doc
- ✓ 3HH-11109-0084-DFZZA-01P01-BRCM WiFi Calibration Strategy.pptx
- ✓ 3HH-11109-0086-DFZZA-01P01-BRCM WiFi power management introduction .pptx
- ✓ NSB XG-250XW-A 436024366 Wi-Fi calibration file update steps.docx

12. FCU issue experience

Function issue

- ✓ **Generally status check**
  - Test environment /scenario/steps
  - clean or interference environment
  - collect surround AP information
  - ……
- ✓ **Wi-Fi configuration**
  - Mode/channel/bandwidth/certification type
- ✓ **Collect logs**
  - SW info
  - Wi-Fi chip commands

- ✓ **Common Wi-Fi issue Q&A:**
- Check how many clients are connected to this ONT? If some clients are not authorized or the client number is more than 20, please change the password and reboot the ONT.
- What is wireless card, device model and type?
- If the clients and the ONT are not in same room, please move the clients closer to the ONT then check if the issue will disappear. Please measure the WIFI signal level at 1 meter and 5 meters distance separately.
- Connect your laptop to the WIFI and ping gateway IP to test the ping response time and packet loss. Also please run “speed test” and take snapshot of the test result.
- Connect your laptop to the ONT with LAN cable and check if the issue will disappear (internet speed, ping delay, packet loss etc).
- Measure the WIFI signal RSSI value.
- Please run inSSID list all of interference AP in the environment.

Catch Wi-Fi packets

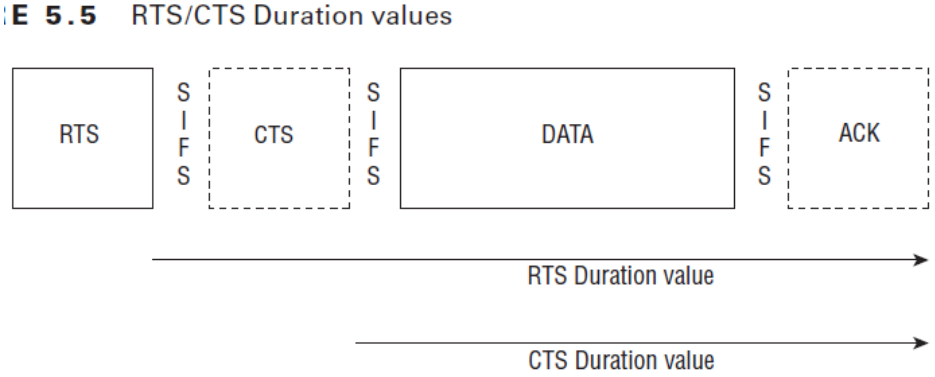
- ✓ **Mostly used tools:**
  - OmniPeek
  - Wireshark
- ✓ **How to catch Wi-Fi packets**
  - Catch wifi packet via Ubuntu+wireshark
  - Catch wifi packet via Microsoft_Network_Monitor_ver_3.4
  - Catch wifi packet via Windows+Omnipeek
  - Catch wifi packet via Macbook (capture 11AC packets)

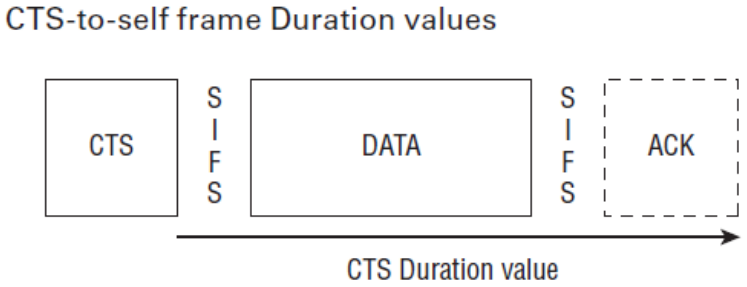
NOKIA

RTS/CTS summary

RTS/CTS summary(1)

- ✓ **RTS/CTS**
  - The purpose is to enhance the virtual carrier sense process
  - a mechanism that performs a NAV distribution and helps prevent collisions from occurring
  - dynamic bandwidth operations in 11ac
  - CTS-to-self is simply another method of performing NAV distribution that solely uses CTS control frames.
  - RTS threshold mechanism to support large frame transmission, work with fragmentation
  - Prevent hidden node issue

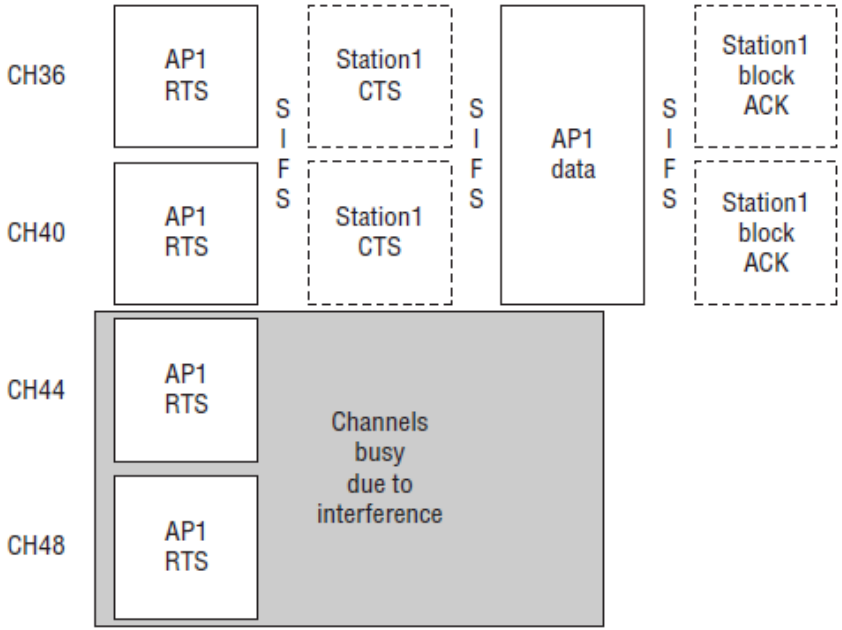




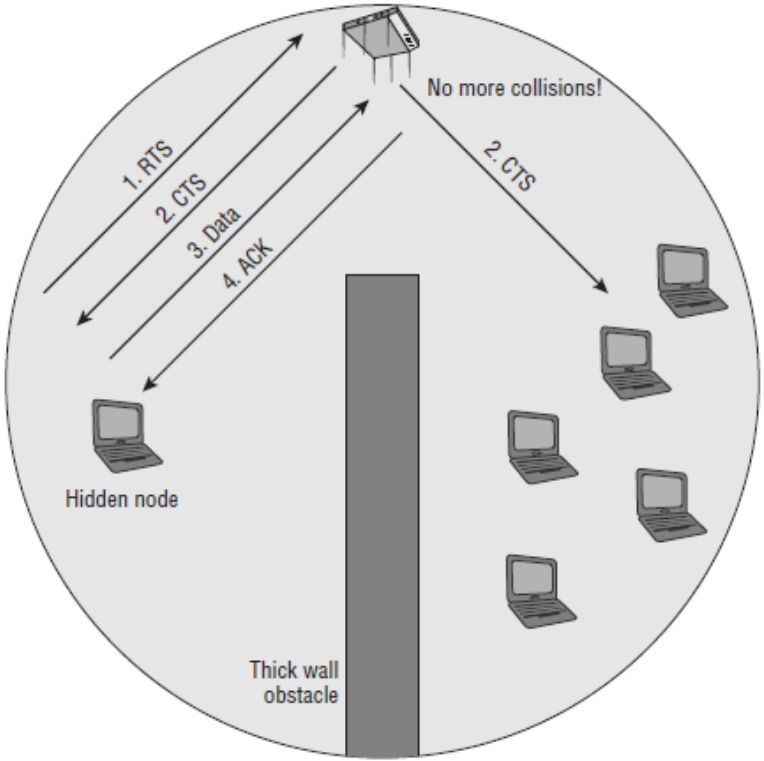
NOKIA

RTS/CTS summary(2)

9.14 Dynamic bandwidth operation using RTS/CTS



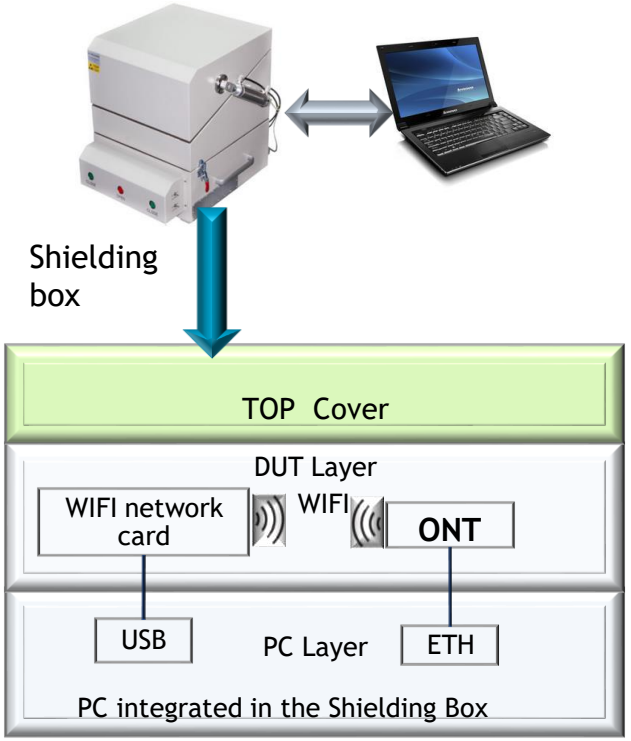
12.15 Hidden node and RTS/CTS



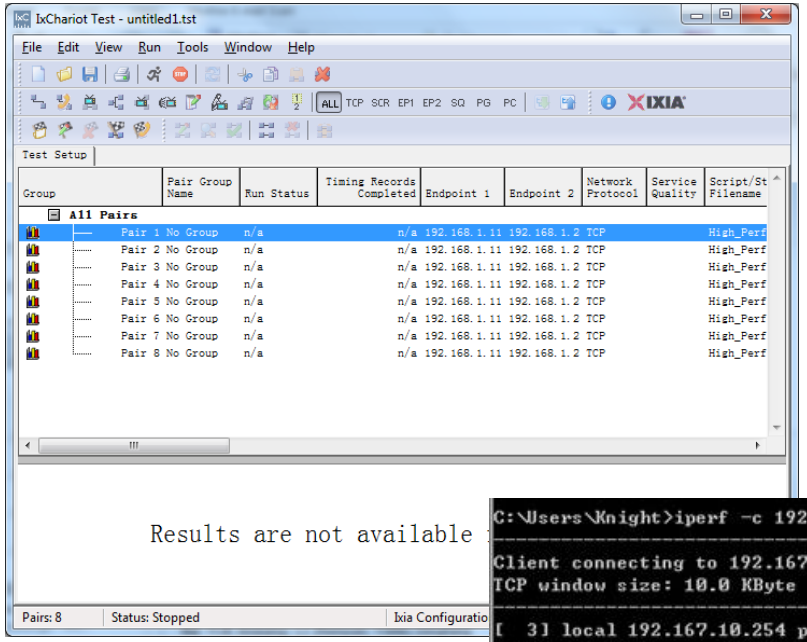
Misc/Backup

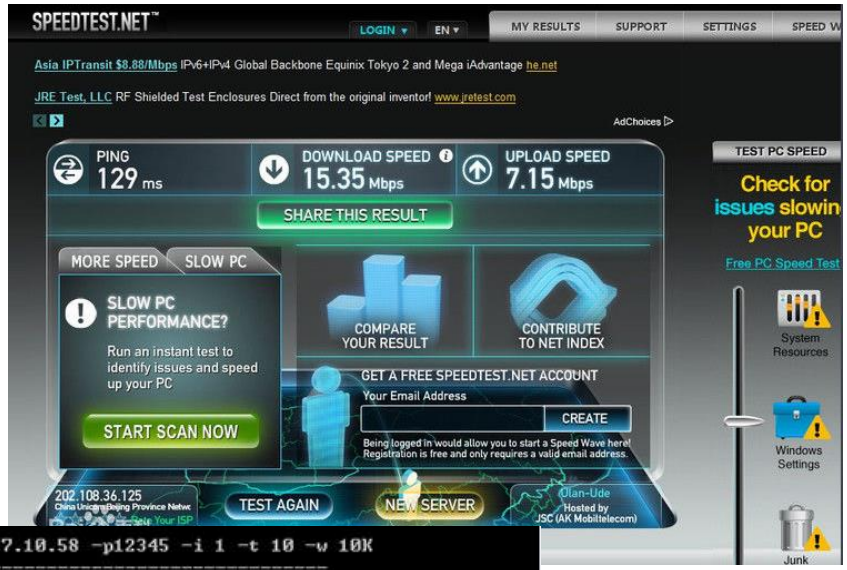
WLAN ATC test environment introduction

- **Ubuntu14.10+ robot1.5A2**
- **Focus on basic functionality and stability test**
- **Support BRCM/QTN/MTK test now**
- **150 automatic test cases has passed, target is total 205 which include the 2.4G and 5G**
- **Based on WebGUI now, many limitation as different WebGUI for different customer**
- **Will upgrade to command test and support cross platform test**



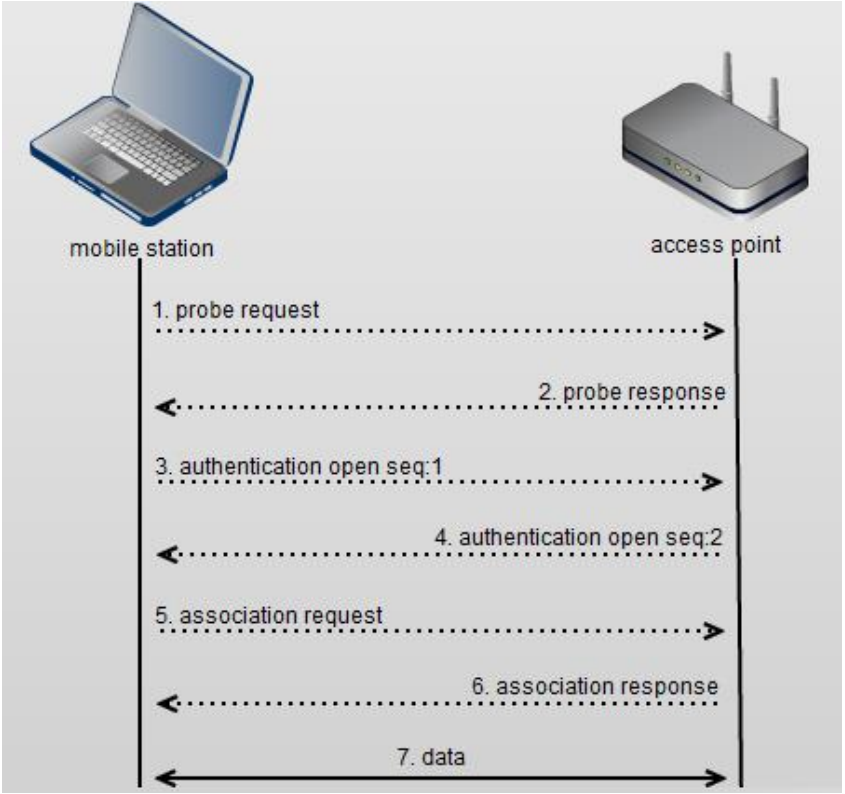
WIFI throughput test tools summary






```
C:\Users\Knight>iperf -c 192.167.10.58 -p12345 -i 1 -t 10 -w 10K
------------------------------------------------------------
Client connecting to 192.167.10.58, TCP port 12345
TCP window size: 10.0 KByte
------------------------------------------------------------
[  3] local 192.167.10.254 port 52876 connected with 192.167.10.58 port 12345
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec  10.6 MBytes  89.1 Mbits/sec
[  3]  1.0- 2.0 sec  10.8 MBytes  90.2 Mbits/sec
[  3]  2.0- 3.0 sec  10.8 MBytes  90.2 Mbits/sec
[  3]  3.0- 4.0 sec  10.9 MBytes  91.2 Mbits/sec
[  3]  4.0- 5.0 sec  10.6 MBytes  89.1 Mbits/sec
[  3]  5.0- 6.0 sec  10.8 MBytes  90.2 Mbits/sec
[  3]  6.0- 7.0 sec  10.8 MBytes  90.2 Mbits/sec
[  3]  7.0- 8.0 sec  10.8 MBytes  90.2 Mbits/sec
[  3]  8.0- 9.0 sec  10.6 MBytes  89.1 Mbits/sec
[  3]  0.0-10.0 sec   107 MBytes  90.1 Mbits/sec
```

Station connect AP



Improvement already DONE

- ✓ Wi-Fi new management architecture refactor
  - Independent progress, easily porting
  - Provide unified SAL_API for different Wi-Fi chip
  - Hardware wrapper for different vendor's different Wi-Fi chips
  - Already supported on G240WC/XGPON/MTK project from HDR5501
- ✓ Wi-Fi SDK independent management
  - Split Wi-Fi driver from PON SDK
  - Support upgrade Wi-Fi driver independently
  - Independent driver repo management
  - Same vendor's Wi-Fi chip share same driver and related modification
- ✓ Wi-Fi knowledge enhancement
  - Arrange discussion workshop with chip vendor periodically
  - Hold Wi-Fi basic knowledge training
  - Coach FCU issue process skill ,quickly/high quality response
- ✓ Domain FT ATC enhancement
  - Adding new test case based on FRs

Planning under GOING

- ☐ Migrate legacy BRCM/QTN/MTK Wi-Fi management to new architecture.
- ☐ Encourage engineers to pass the TOP-CODING training to improve coding ability.
- ☐ Encourage engineers to pass the CWNP certification to enhance Wi-Fi knowledge ability.
- ☐ Encourage engineers to follow-up and study new technology, like:WAVE2.0,Mesh,802.1D.
- ☐ Deeply understand and analysis Wi-Fi SDK and important features to reduce dependence on chip vendor.
- ☐ Enhance FT ATC capability, stability and coverage to reduce FT effort.
- ☐ Enhance code review.
- ☐ Enhance FR RCA summarize and improvement

Where to get useful Wi-Fi info?

- ✓ **Wi-Fi Alliance,** www.wi-fi.org, is an excellent resource.
- ✓ **CWNP** The website www.cwnp.com is also the best source of information about all the vendor-neutral CWNP wireless networking certifications.
- ✓ **WLAN Vendor Websites**
- ✓ **Useful document :**
  - Sybex.CWNA.Certified.Wireless.Network.Administrator.Official.Study.Guide.Exam.CWNA-106 4th (2014).pdf
  - Sybex.CWAP.Certified.Wireless.Analysis.Professional.Official.Study.Guide.Exam.PW0270.Mar.2011.ISBN.04707.pdf
  - Sybex.CWSP.Certified.Wireless.Security.Professional.Official.Study.Guide.Exam.PW0204.Feb.2010.ISBN.0470438916.pdf
  - 802.11 Wireless Networks - The Definitive Guide 2.pdf
  - 802.11ac_ A Survival Guide.pdf
  - 802.11n_A.Survival.Guide.Apr.2012.pdf
  - 802.11ac-2013.pdf
  - 802.11-2012.pdf
  - Wi-Fi Simple Configuration Protocol and Usability Best Practices for the Wi-Fi Protected Setup™ Program.pdf

- WFA_Device_1_0_Template_1_01.pdf
- Wi-Fi Simple Configuration Technical Specification v2.0.5.pdf
- Wi-Fi_WMM_Specification_v1.2.0.pdf
- Wi-Fi_Protected_Setup_Test_Plan_v2 0 16.pdf
- Wi-Fi_CERTIFIED_ac_Interoperability_Test_Plan_v2 0.pdf
- Wi-Fi_CERTIFIED_n_Interoperability_Test_Plan_TGnInteropTP_2.11.pdf

NOKIA