Wi-Fi Networks

Corso di Sistemi di Telecomunicazione

Università degli Studi di Parma

Nicola Iotti, CTO

(((Guglielmo)))

Wireless Internet Service Provider

www.guglielmo.biz

Wi-Fi : protocolli,implementazione e troubleshooting di WLAN

.Protocols
- . Layer 2
- . Standard 802.11
- . Access Point
- . Security

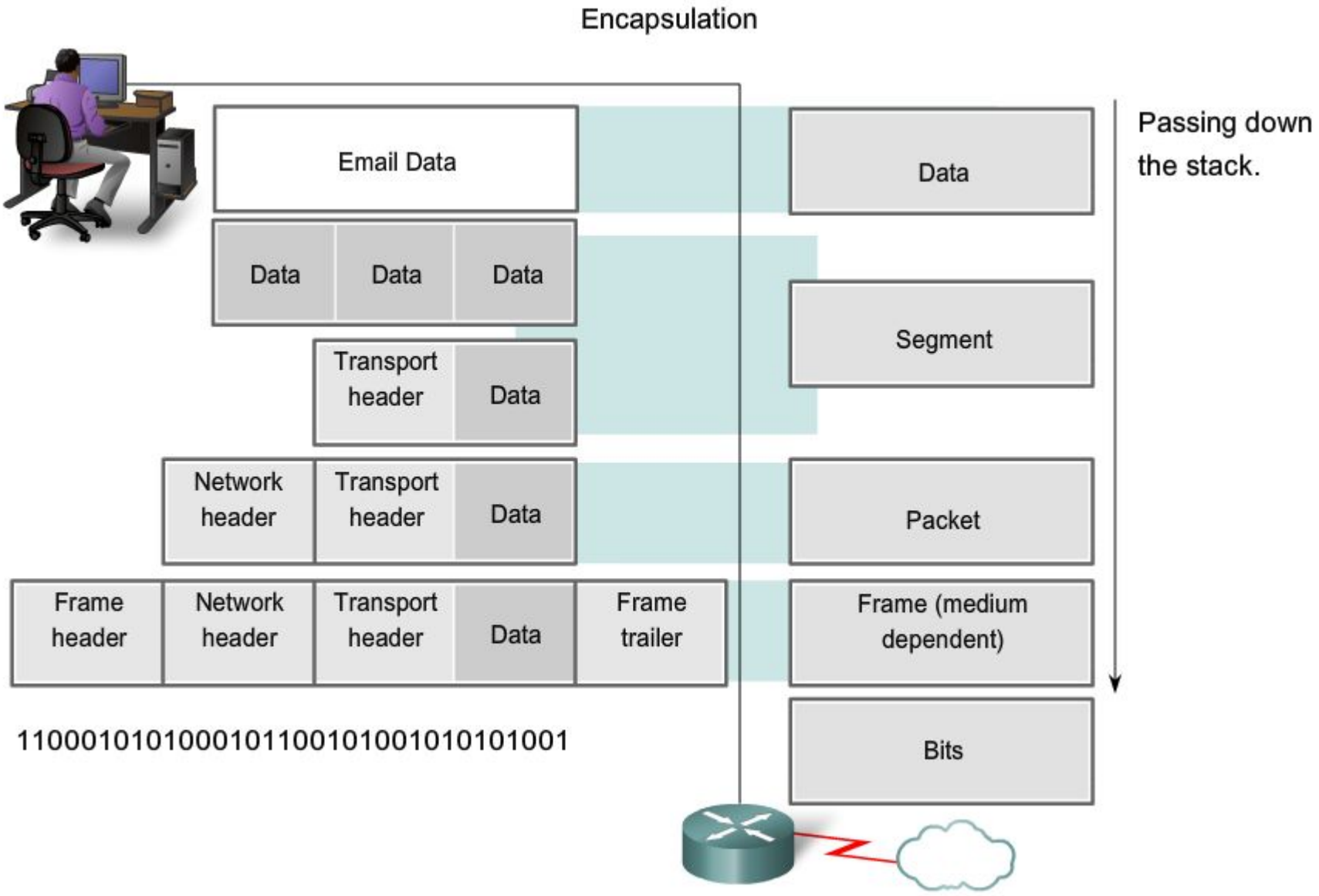
.WLAN Implementation
- . Planning
- . Configuration and Installation
- . Troubleshooting
- . Offloading
- . IoT Infrastructure

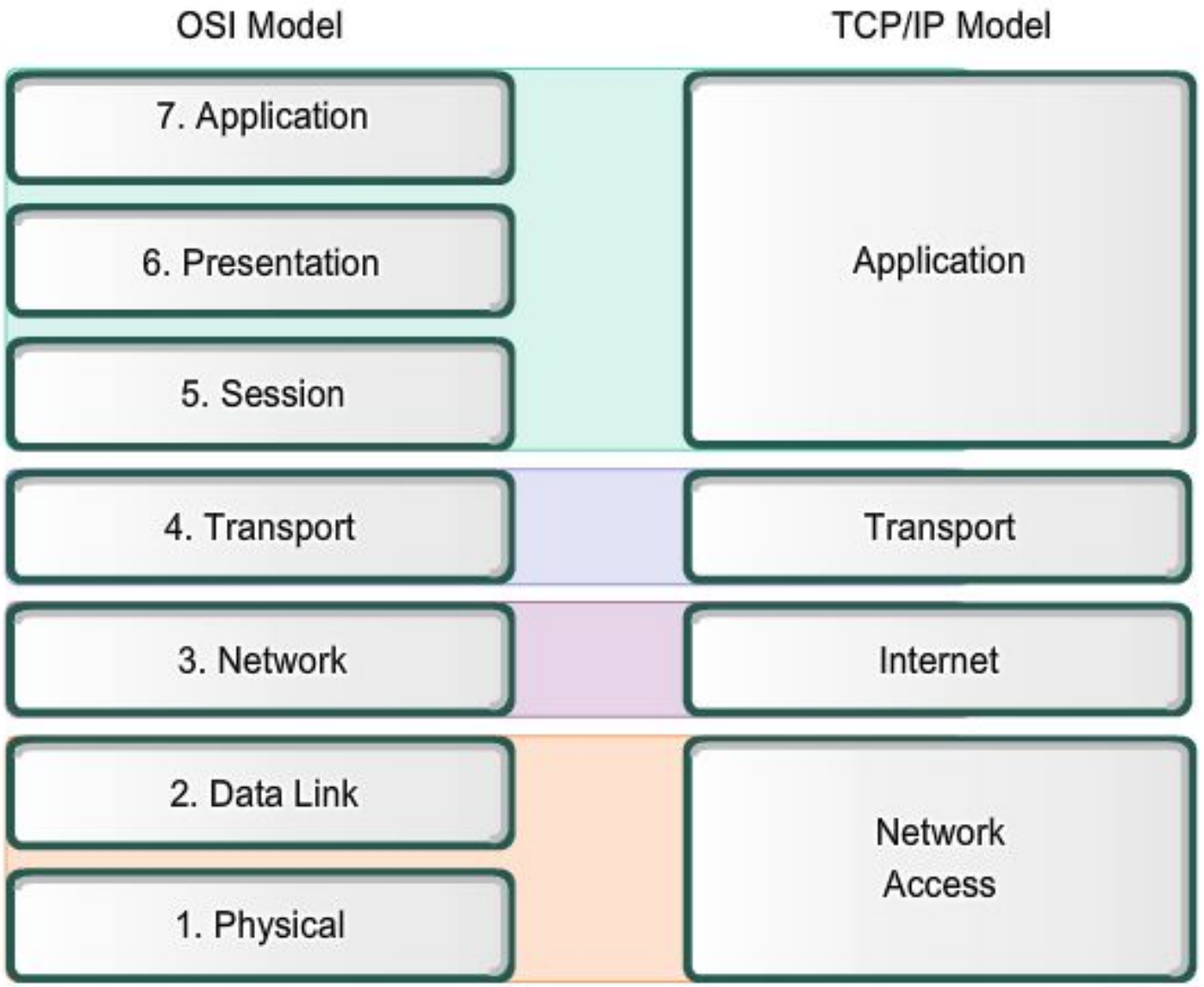
Nicola Iotti, CTO Guglielmo S.r.l.

Open Systems Interconnection (OSI) Model

ISO Standard

Layers	Short Description	Protocol Examples
7. APPLICATION	Interface with software application	HTTP, FTP, SNMP, SMTP POP
6. PRESENTATION	Negotiates syntaptic representation	SSL, ASCII, MPEG
5. SESSION	Coordinates connectkion and manages data flow	TCP, RTP
4. TRANSPORT	Data transfer integrity and multiple sessions	TCP, UDP
3. NETWORK	End-to-end routing	IPv4, IPv6, IPX
2. DATA LINK	Transfers data units on specific media and ensures integrity	Ethernet, PPP, **IEEE 802.11**
1. PHYSICAL	Bits encoding, electrical and mechanical formats definition	RS232, RJ45, DSL **IEEE 802.11**


Encapsulation
Email Data
Data
Data
Data
Data
Segment
Transport header
Data
Network header
Transport header
Data
Packet
Frame header
Network header
Transport header
Data
Frame trailer
Frame (medium dependent)
Bits
Passing down the stack.
1100010101000101100101001010101001

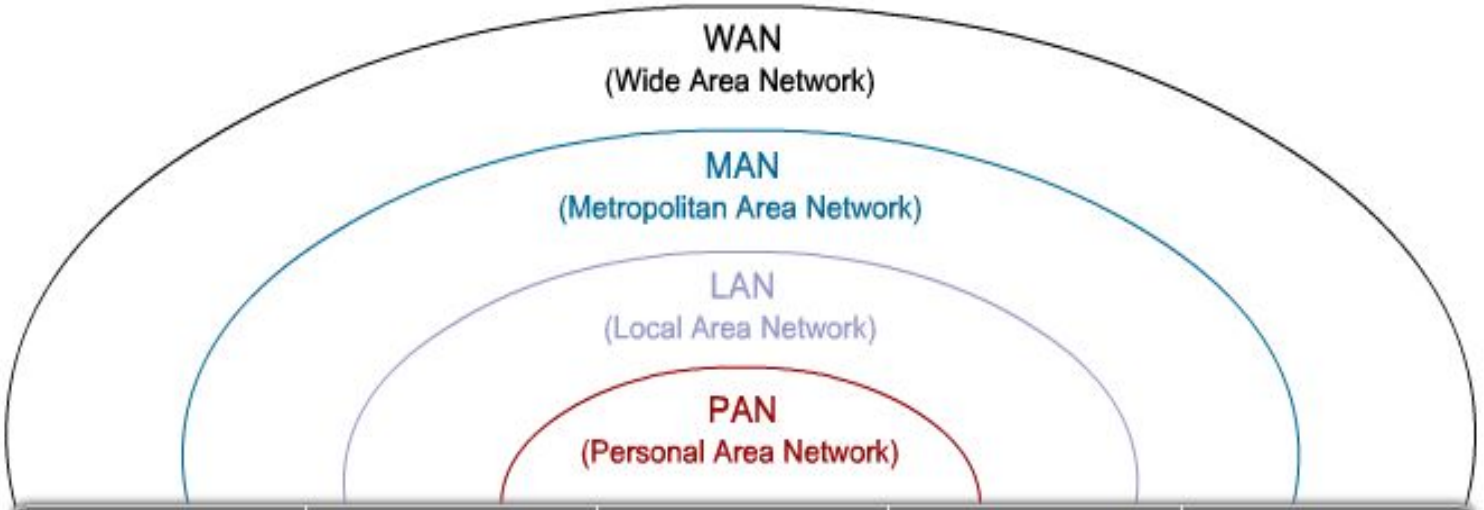

OSI Model
TCP/IP Model
7. Application
6. Presentation
5. Session
Application
4. Transport
Transport
3. Network
Internet
2. Data Link
1. Physical
Network Access

Layer 2

- L2 main problems
  - Media Access
  - Physical Addressing
  - L3 protocol
  - Error Detection
- Media Dependent: At each hop along the path, an intermediary device that receives frames from one medium and forwards it on a different one, decapsulates the frame and forwards the packet in a new frame with different header
- L3 devices decapsulate and build a new L2 frame

Generic L2 Frame Format

Wireless



	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

Tabella riassuntiva [modifica]

Standard	Frequenza	Velocità di trasferimento (Mbit/s)
802.11 legacy	FHSS, 2,4 GHz, IR	1, 2
802.11a	5,2, 5,4, 5,8 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11b	2,4 GHz	1, 2, 5.5, 11
802.11g	2,4 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11n	2,4 GHz, 5,4 GHz	1, 2, 5,5, 11; 6, 9, 12, 18, 24, 36, 48, 54, 125

IEEE 802.11ac provides Very High Throughput (VHT) - Max. Aggregate Capacity : 6.77 Gbps

IEEE 802.11AC SALIENT FEATURES	
PARAMETER	DETAILS
Frequency band	5.8 GHz ISM (unlicensed) band
Transmission bandwidth	20, 40, & 80 MHz 160 & 80 + 80 MHz optional
Modulation formats	BPSK, QPSK, 16-QAM, 64-QAM 256-QAM optional
FEC coding	Convolutional or LPDC (optional) with coding rates of 1/2, 2/3, 3/4, or 5/6
MIMO	Both single and multi-user MIMO with up to 8 spatial streams.
Beam-forming	Optional

- IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b: Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d: International (country-to-country) roaming extensions (2001)
- IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
- *IEEE 802.11F: Inter-Access Point Protocol (2003)* *Withdrawn February 2006*
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i: Enhanced security (2004)
- IEEE 802.11j: Extensions for Japan (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- IEEE 802.11k: Radio resource measurement enhancements (2008)
- IEEE 802.11n: Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- IEEE 802.11r: Fast BSS transition (FT) Working "Task Group r" (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (~ June 2011)
- IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled
- IEEE 802.11u: Interworking with non-802 networks (for example, cellular) (~ Dec 2010)
- IEEE 802.11v: Wireless network management (~ Dec 2010)
- IEEE 802.11w: Protected Management Frames (September 2009)
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)
- IEEE 802.11mb: Maintenance of the standard. Will become 802.11-2011. (~ Dec 2011)
- IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (~ Mar 2012)
- IEEE 802.11ac: Very High Throughput <6 GHz;[20] potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase); wider channels (80 or even 160 MHz), multi user MIMO;[21] (~ Dec 2012)
- IEEE 802.11ad: Very High Throughput 60 GHz (~ Dec 2012)
- IEEE 802.11ae: QoS Management (~ Dec 2011)
- IEEE 802.11af: TV Whitespace (~ Mar 2012)
- IEEE 802.11ah: Sub 1Ghz (~ July 2013)
- IEEE 802.11ai: Fast Initial Link Setup

IEEE 802.11 ac

MIMO and spatial stream axb:c

a = transmit antenna, b = receive antenna and c = spatial streams.

802.11n access points are labelled as 2x2:2, 2x3:2, 3x3:3, 3x4:3, 4x4:4 (or simply 2SS, 3SS, 4SS).600Mbps comes where both the access point and client support 4SS and achieve 4 x 150Mbps. 802.11ac up to 8SS (8 x 866.7 Mbps = 6.8 Gbps circa)

MU-MIMO: Multi User MIMO Wave 2 chipset

Theoretical throughput for single spatial stream (in Mbit/s)[8][a]										
MCS index[b]	Modulation type	Coding rate	20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			800 ns GI[c]	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7

MCS = Modulation and Coding Scheme

Mandatory features (from a/g)

800 ns regular guard interval
Binary convolutional coding (BCC)
Single spatial stream

New mandatory features

80 MHz channel bandwidths

Optional features (from /n)

two to four spatial streams
Low-density parity-check code (LDPC)
Space-Time Block Coding (STBC)
Transmit Beamforming (TxBF)
400 ns short guard interval (SGI)

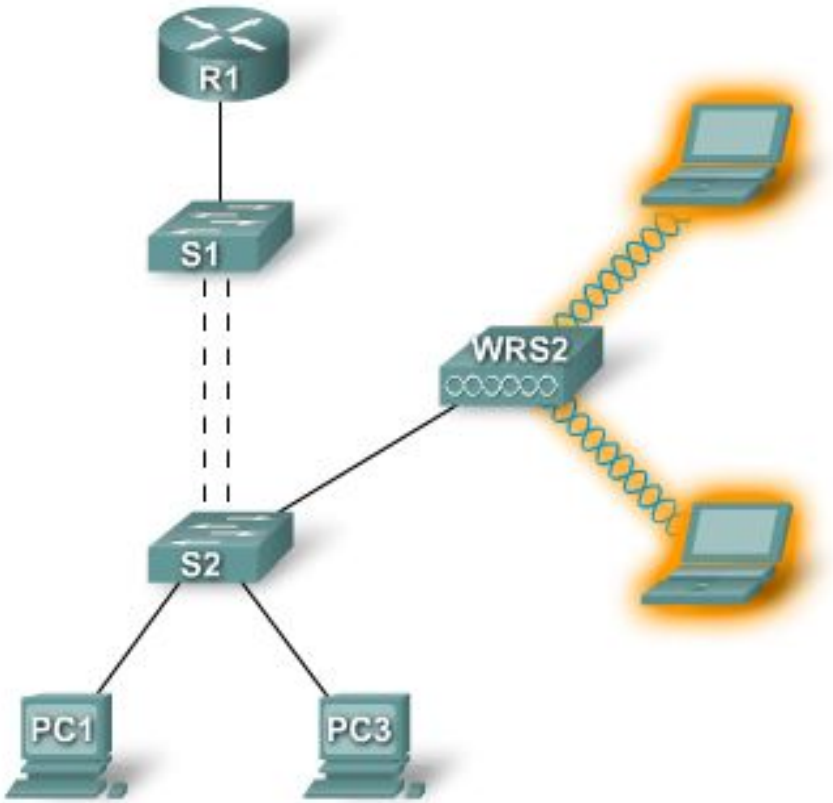
Optional features (newly introduced)

five to eight spatial streams
160 MHz channel bandwidths (contiguous 80+80)
80+80 MHz channel bonding (discontiguous 80+80)
MCS 8/9 (256-QAM)

Comparing a WLAN to a LAN

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

Wireless LAN Components



Wireless LAN Standards

	802.11a	802.11b	802.11g	
Band	5.7 GHz	2.4 GHz	2.4 GHz	
Channels*	Up to 23	3	3	
Modulation	OFDM	DSSS	DSSS	OFDM
Data Rates	Up to 54 Mbps	Up to 11 Mbps	Up to 11 Mbps	Up to 54 Mbps
Pros	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters	
Cons	October 1999	October 1999	June 2003	
Pros	Fast, less prone to interference	Low cost, good range	Fast, good range, not easily obstructed	
Cons	Higher cost, shorter range	Slow, prone to interference	Prone to interference from appliances operating on 2.4 GHz band	

* Non-overlapping channels.

- Half Duplex
- Shared Throughput

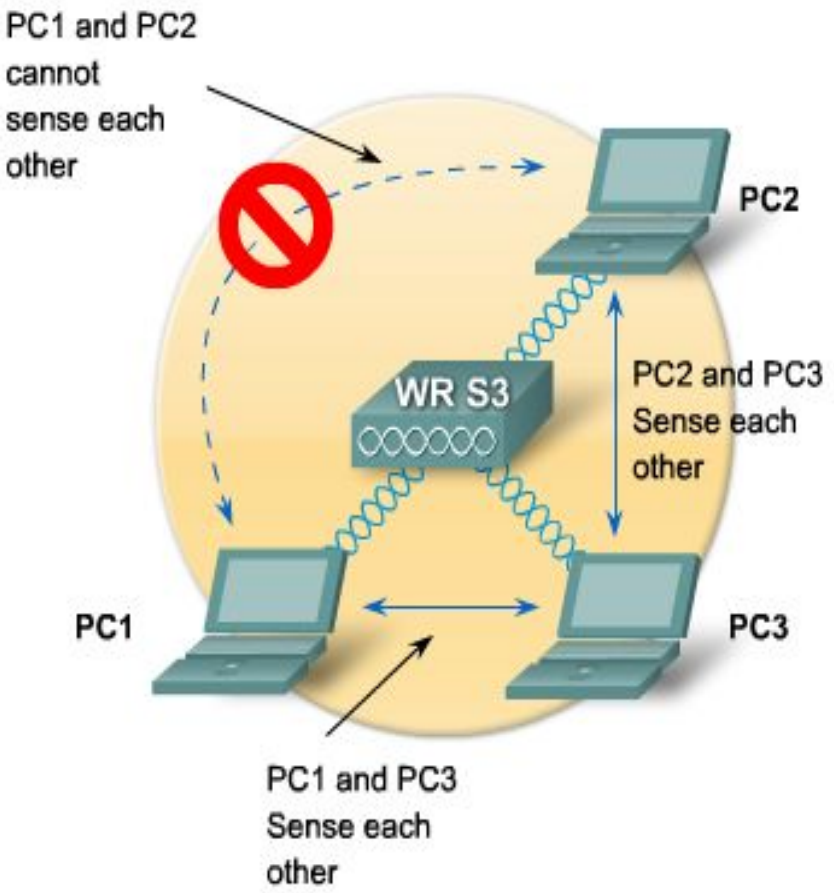
- 802.11 n : Higher throughput improvement using MIMO (Multiple Input, Multiple Output) Antennas.

Wireless Access Points

The Hidden Node Problem:

- PC1 and PC2 reach WRS3
- PC1 and PC2 cannot reach each other
- PC1 does not detect PC2 activity on the channel
- PC1 sends data while PC2 is transmitting
- A collision occurs

PC3 is sensed by both PC1 and PC2, so there are no collisions involving PC3.



IEEE 802.11 MAC Protocol

CSMA/CA with exponential backoff Algorithm

Operation Mode: DCF Distributed Coordination Function (PCF with polling-based priority not used)

Basic Timers:

- Slot Time: basic unit of backoff algorithm = time required for station to sense end of frame, start transmitting and propagate to others the beginning of frame (i.e. 20 u sec)
- SIFS: Short Inter-Frame Space = time required for station to sense end of frame and start transmitting (i.e. 10 u sec)
- DIFS: Distributed Inter-Frame Space = time to wait before transmitting (if medium is free) or starting backoff interval (if busy) = SIFS + 2 Slot Time (i.e. 50 u sec)
- CW: Contention Window, number (not time) in general chosen between min and max (i.e. 31 <= CW <= 1023)

CSMA/CA Operation

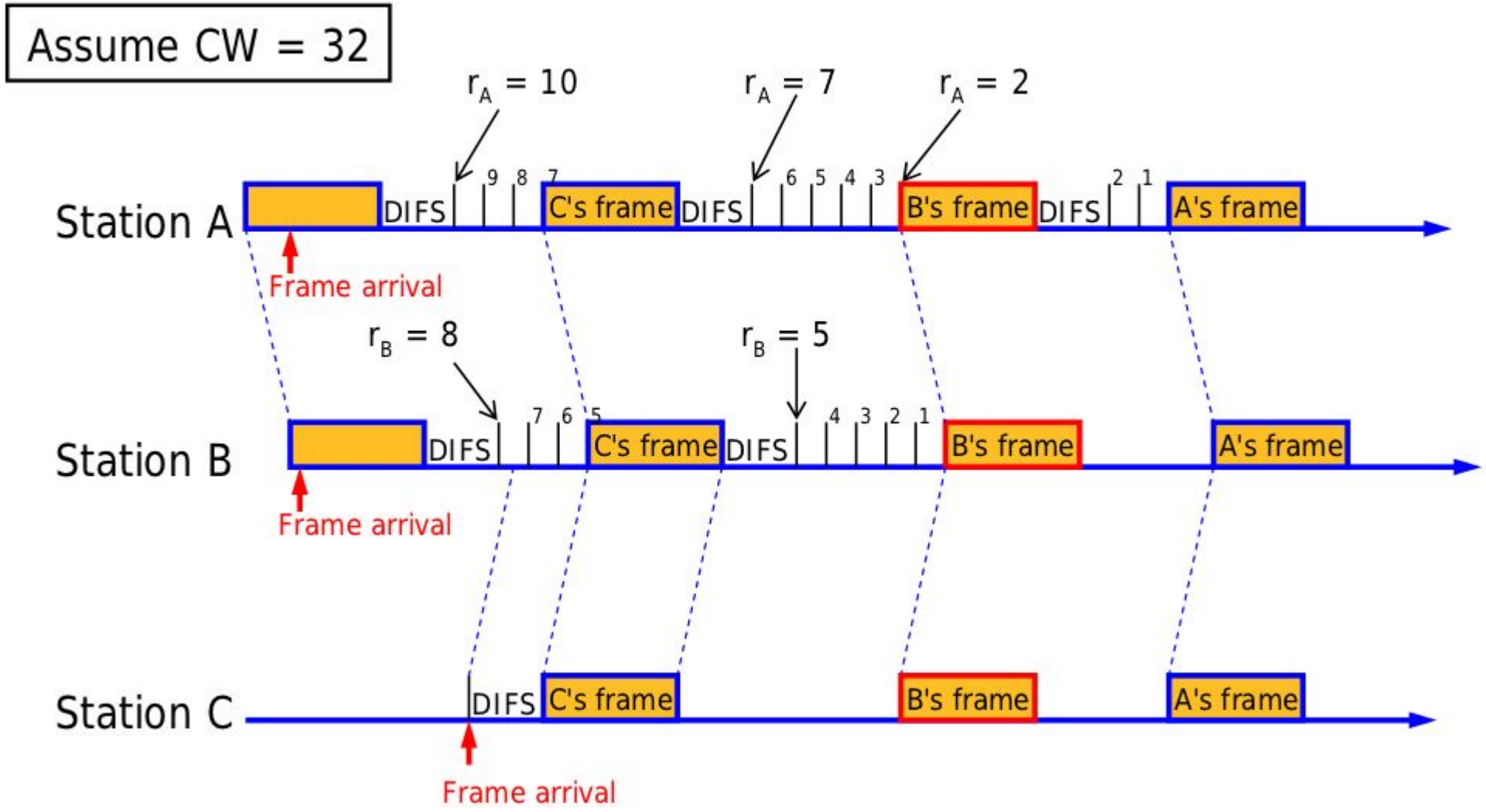
- *Sender*
  - MAC (firmware in NIC) receives frame from upper layer
  - If channel is free and stays free for DIFS : Transmit Frame
  - Else if channel is busy:
    - Backoff Procedure
    - Transmit the Frame
  - Waits for ACK
  - If received : end
  - Else if timeout :
    - Repeat
      - Backoff Procedure
      - Transmit the Frame
      - Waits for ACK or timeout
    - Until ACK is received or maximum retransmissions number is reached

CSMA/CA Operation

- *Receiver*
  - Interface receives a frame
  - Check if frame is OK
  - If frame is OK:
    - Waits for SIFS
    - Transmit ACK
- *Backoff Procedure*
  - If due to timeout: double CW
  - Else: wait until channel is free and stays free for DIFS
  - Choose random number: r between [1,CW]
  - Repeat
    - Sense medium for one Slot Time
    - If medium was free through slot: r = (r-1)
    - Else: wait until channel is free and stays free for DIFS
  - Until (r = 0)
  - Return

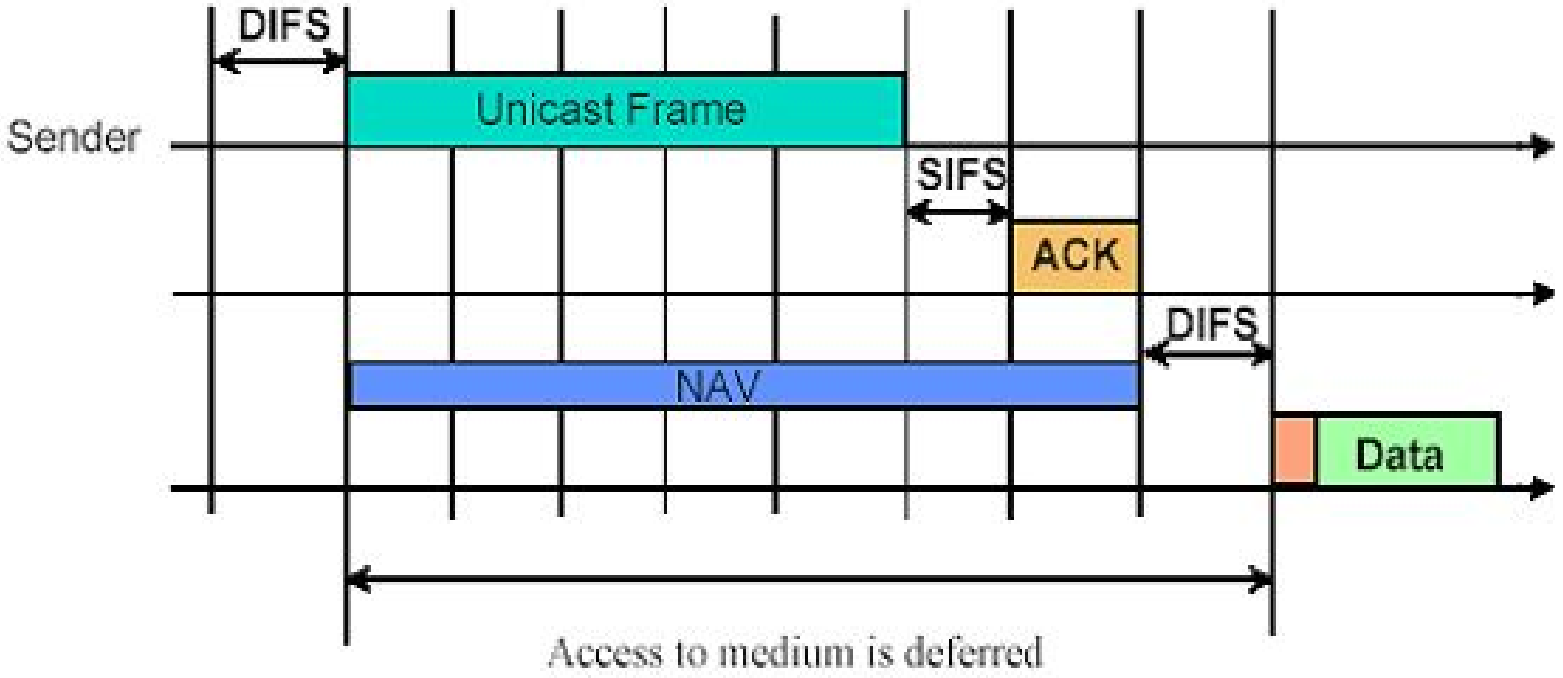
CSMA / CA

Backoff Operation



CSMA / CA

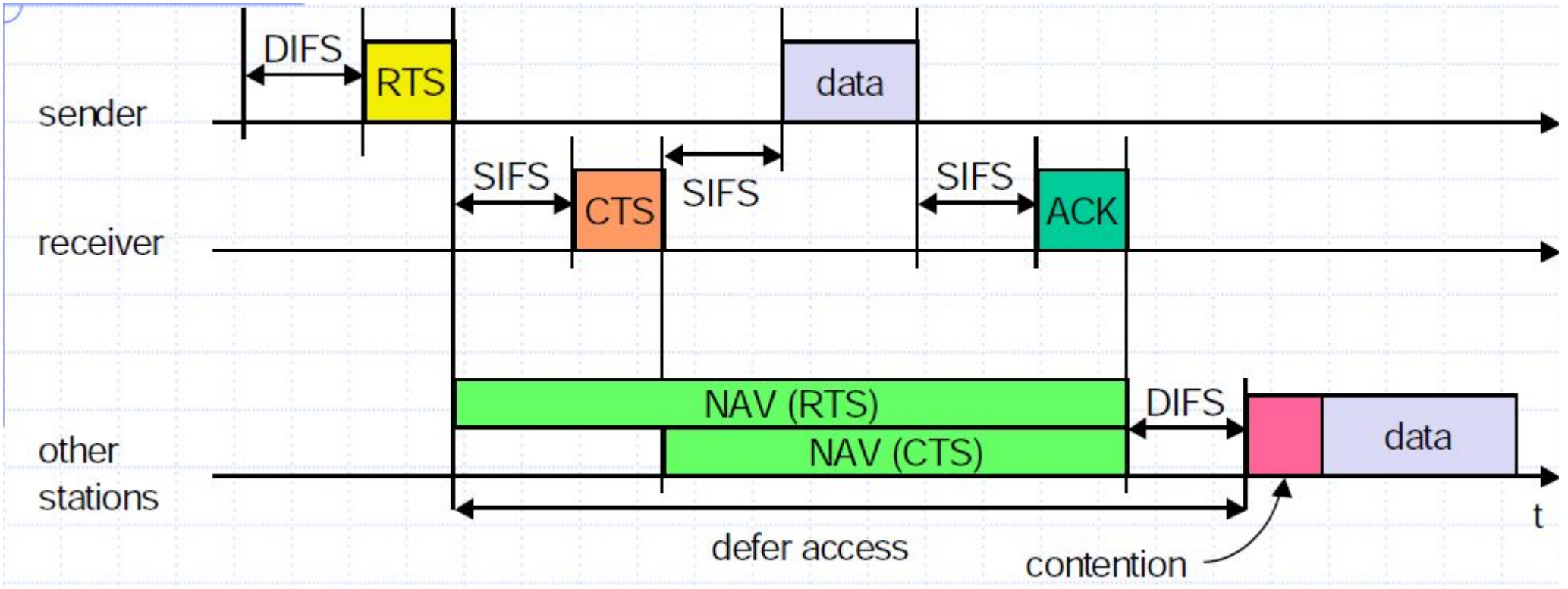
ACK

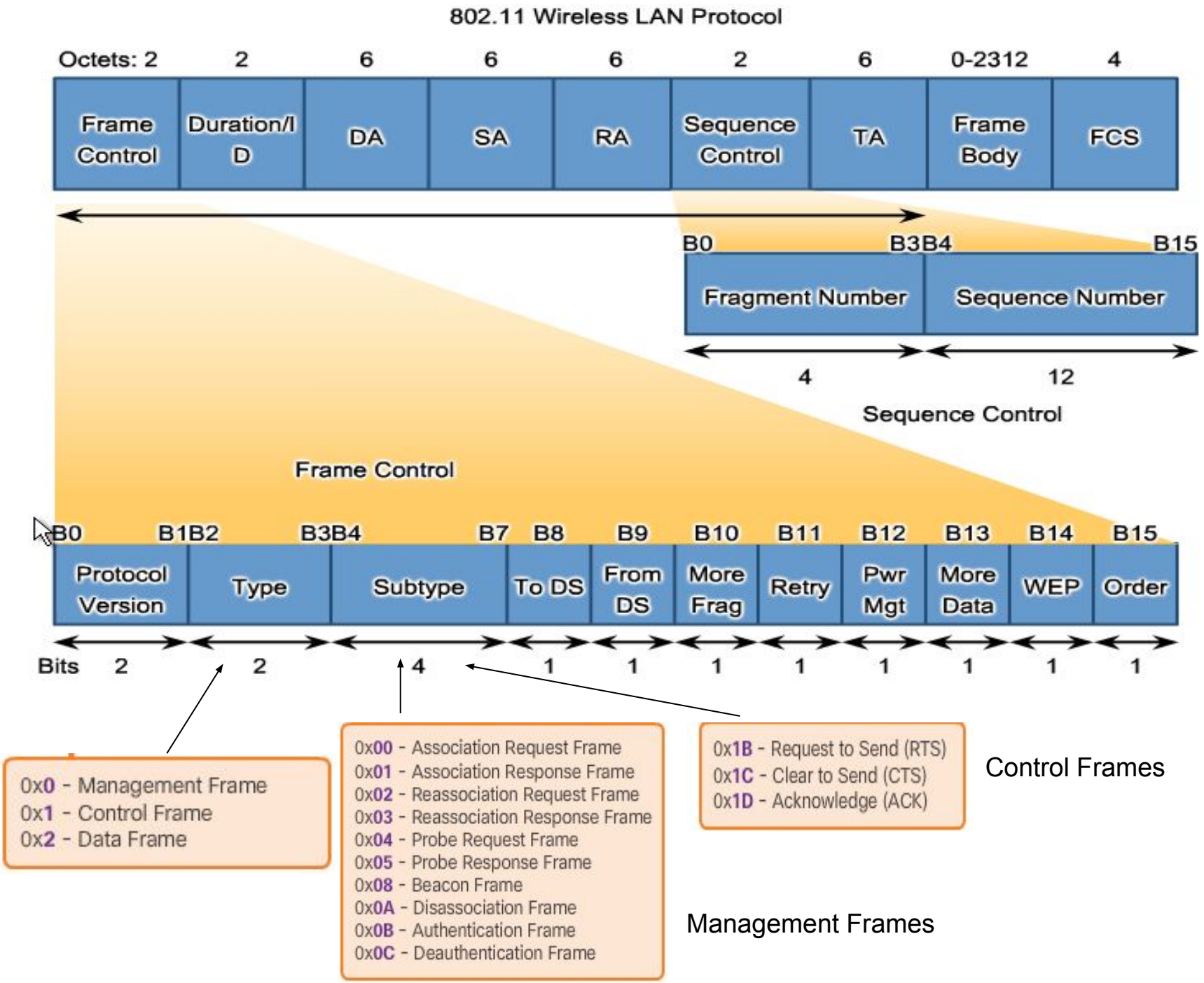


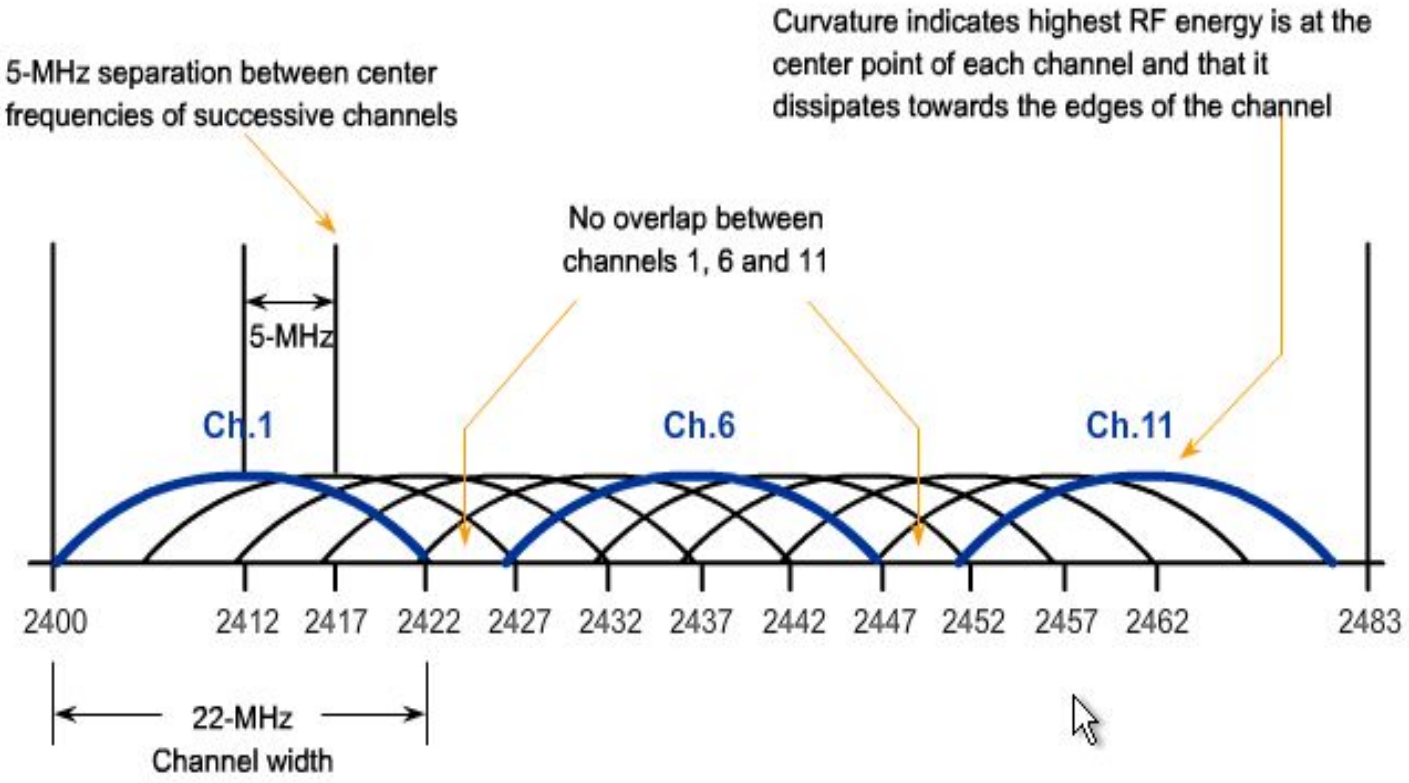
NAV = Network Allocation Vector

CSMA / CA

RTS / CTS




802.11 Wireless LAN Protocol
Octets: 2
2
6
6
6
2
6
0-2312
4
Frame Control
Duration/ID
DA
SA
RA
Sequence Control
TA
Frame Body
FCS
B0
B3B4
B15
Fragment Number
Sequence Number
4
12
Sequence Control
Frame Control
B0
B1B2
B3B4
B7
B8
B9
B10
B11
B12
B13
B14
B15
Protocol Version
Type
Subtype
To DS
From DS
More Frag
Retry
Pwr Mgt
More Data
WEP
Order
Bits
2
2
4
1
1
1
1
1
1
1
1
0x0 - Management Frame
0x1 - Control Frame
0x2 - Data Frame
0x00 - Association Request Frame
0x01 - Association Response Frame
0x02 - Reassociation Request Frame
0x03 - Reassociation Response Frame
0x04 - Probe Request Frame
0x05 - Probe Response Frame
0x08 - Beacon Frame
0x0A - Disassociation Frame
0x0B - Authentication Frame
0x0C - Deauthentication Frame
0x1B - Request to Send (RTS)
0x1C - Clear to Send (CTS)
0x1D - Acknowledge (ACK)
Control Frames
Management Frames



2.4-GHz RF Band

802.11 Topologies

Summary of WLAN Topologies

Wireless Devices	Topology Mode	Topology Building Block	Coverage Area
No access points	Ad Hoc	Independent Basic Service Set (IBSS)	Basic Service Area (BSA)
One access point	Infrastructure	Basic Service Set (BSS)	Basic Service Area (BSA)
More than one access point	Infrastructure	Extended Service Set (ESS)	Extended Service Area (ESA)

Discovering Access Points

Passive Mode

Beacon Frame (0x08)
SSID
Supported Standards
Security Settings

Beacon Frame (0x08)
SSID
Supported Standards
Security Settings

Beacon Frame (0x08)
SSID
Supported Standards
Security Settings

Active Mode

Probe Request Frame
(0x04)
SSID
Supported Standards

Probe Response Frame
(0x05)
SSID
Supported Standards
Security Settings

Authentication and Association

Authentication

Authentication Frame
(0x0B)
Type (open or shared key)
Key if shared

Authentication Frame
(0x0B)
Type
Key
Success or Unsuccess

Association

Association Request
Frame (0x00)
Client MAC address

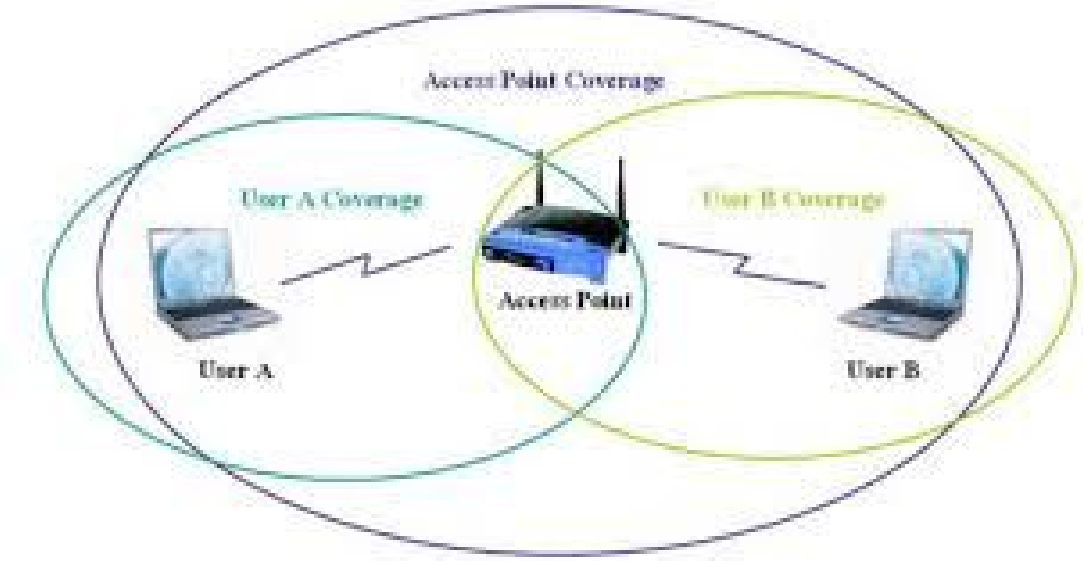
Association Response
Frame (0x01)
AP MAC address

Problems in Wireless MAC Layer

- Hidden Node
- Exposed Node
- Up/Down Anomaly
- Rate Anomaly

Hidden Node

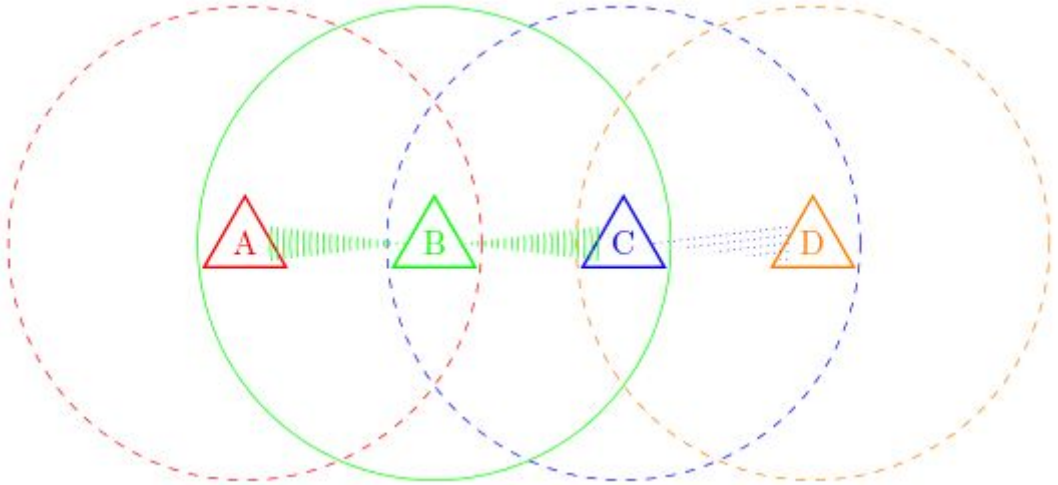
Not all clients are sensing each other



Basic reason for CSMA/CA

Exposed Node

Clients of different Access Points are sensing each other



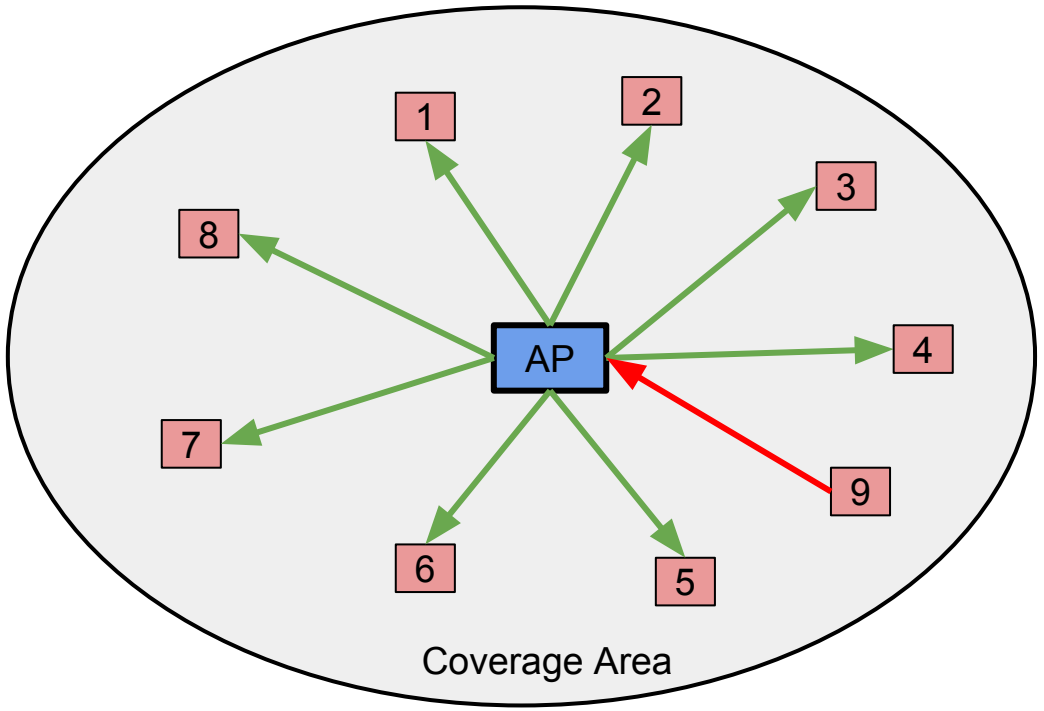
A,D : Access Points using the same channel
B,C : Clients sensing each other, they detect channel busy but actually they would not interfere

Careful channel and power planning

Experimental MAC

Up/Down Anomaly

Clients Uplink and Downlink activity is heavily unbalanced



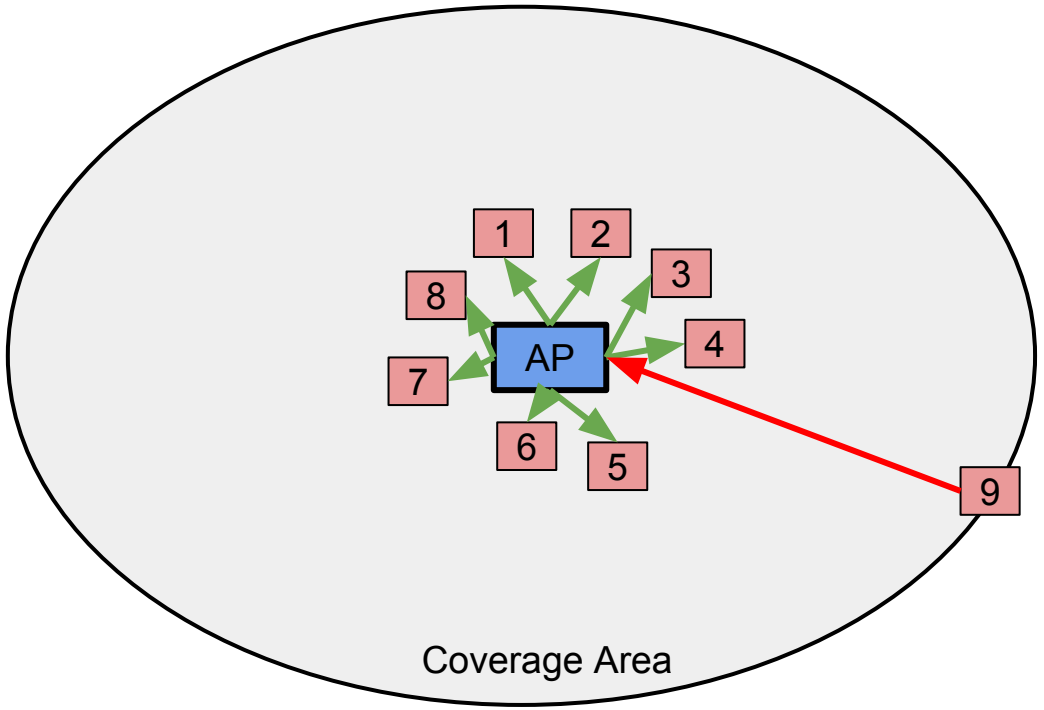
AP : Access Point
1,2,3,4,5,6,7,8 : Clients performing basically Download
9 : Client performing Upload

AP and client 9 share media access

Performance degradation

Rate Anomaly

Clients Bitrate is heavily unbalanced



AP : Access Point
1,2,3,4,5,6,7,8 : Clients working at the best possible bitrate
9 : Client with low signal/noise works at lowest possible bitrate

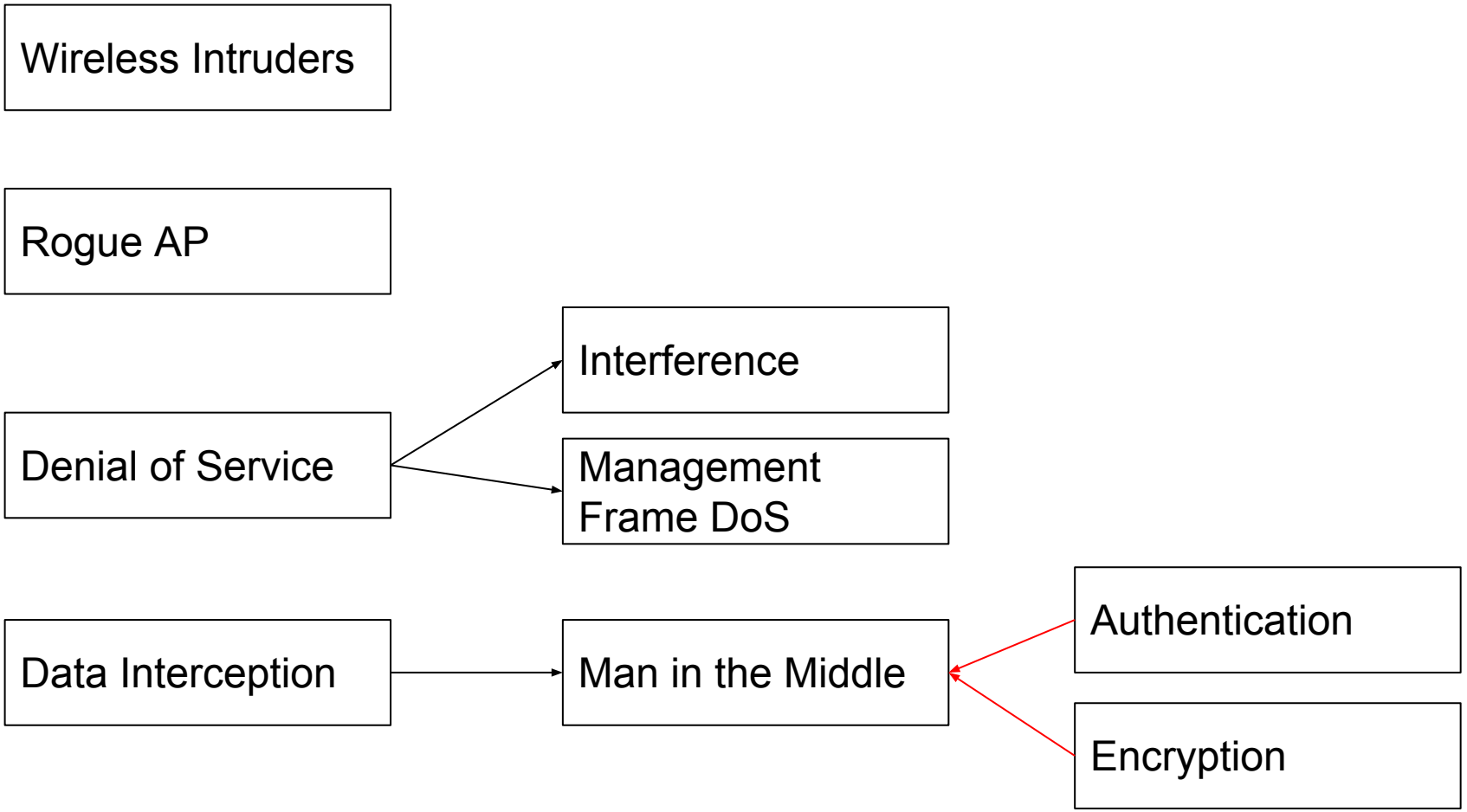
Client 9 introduces latency in other clients connections

Performance degradation

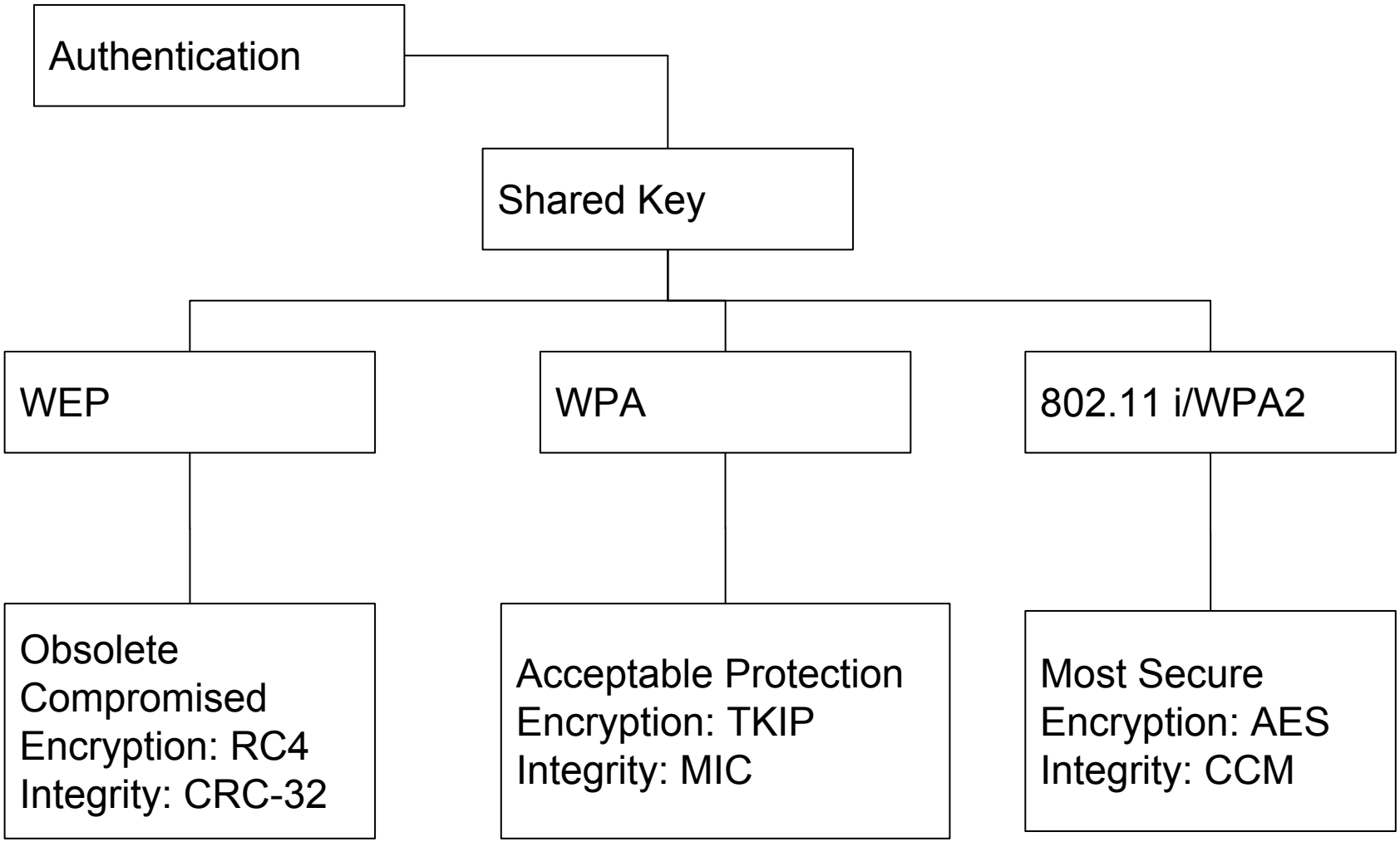
AP configuration not mixed (i.e. 802.11 g only) if possible (i.e. good coverage)

Security

Common Wireless Threats



Authentication and Encryption

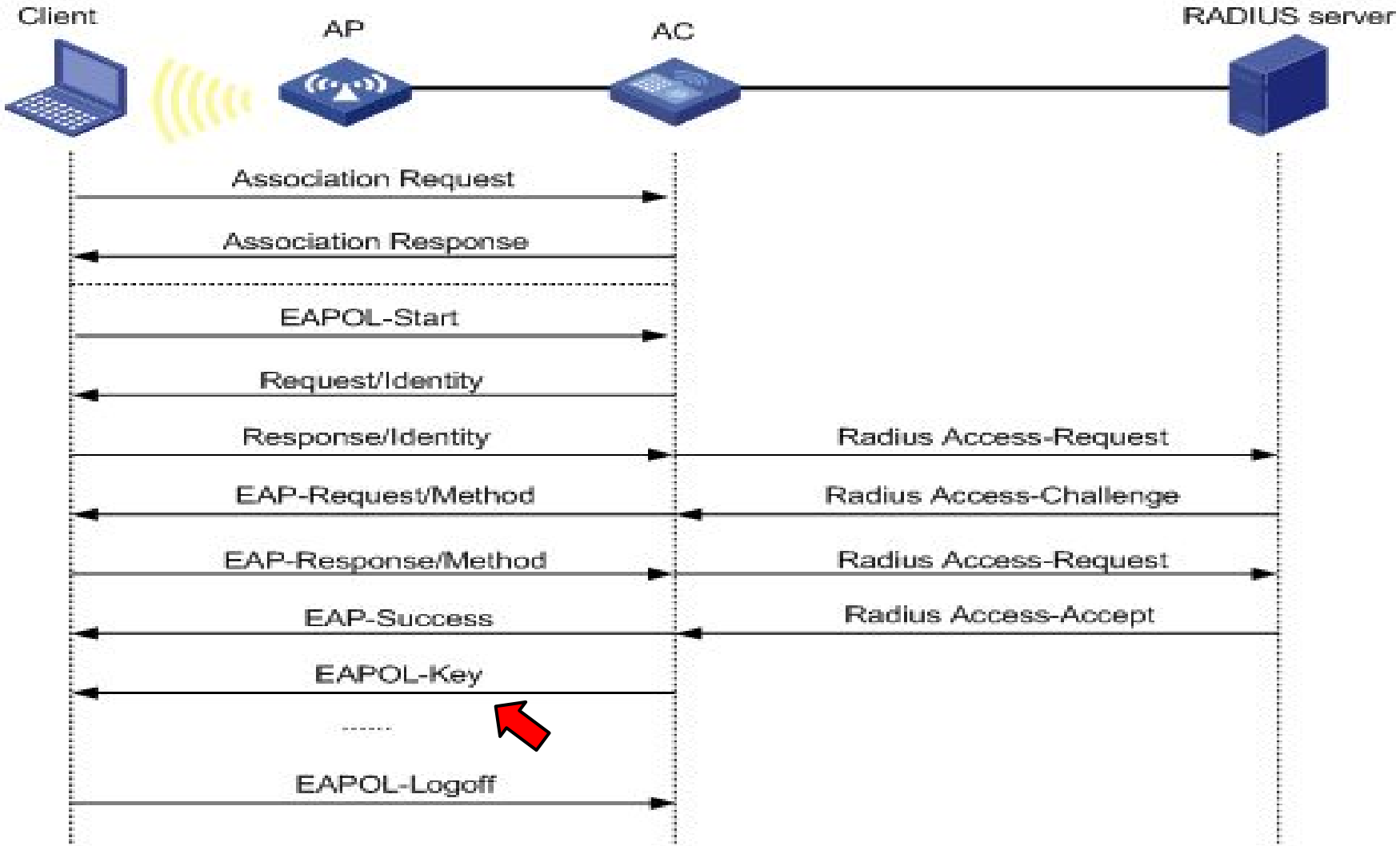


IEEE 802.1x

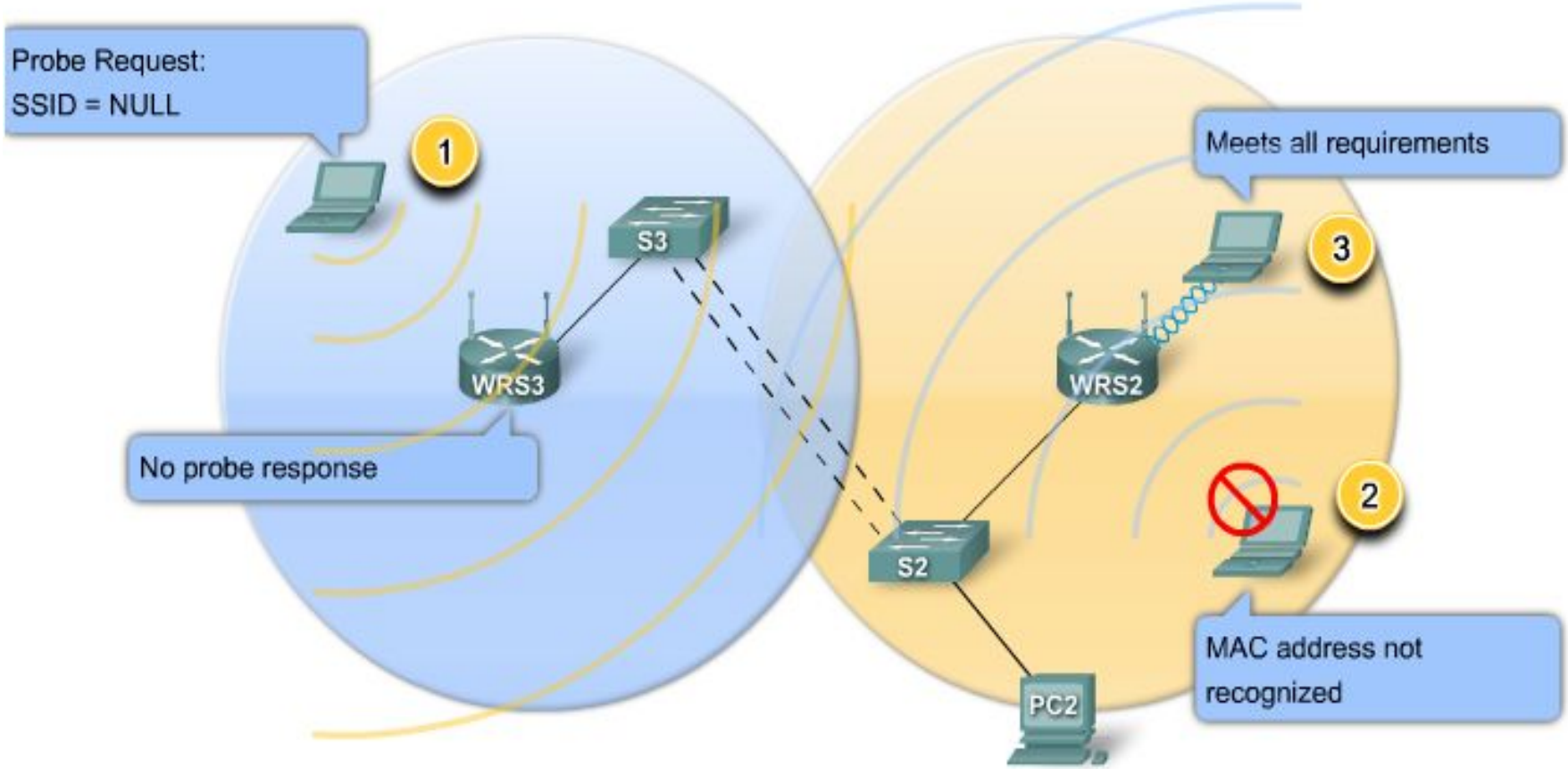
Supplicant

Authenticator

Authentication Server



Controlling Access to the Wireless LAN



Methods for controlling wireless LAN access:

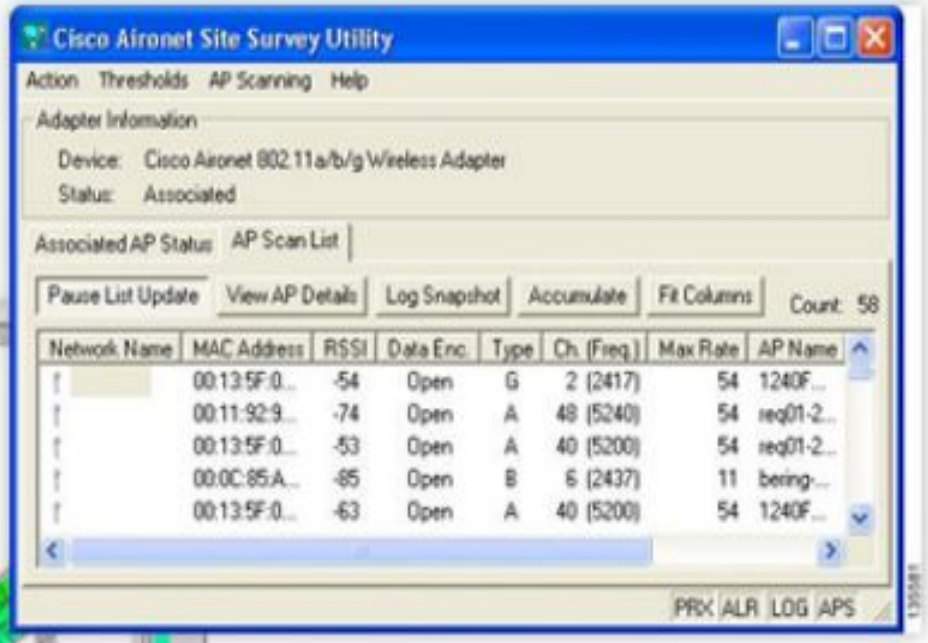
1. SSID broadcasts from access points are off
2. MAC Address filtering is enabled
3. WPA2 Security implemented

CAUTION: Neither items 1 or 2 are considered valid security measures

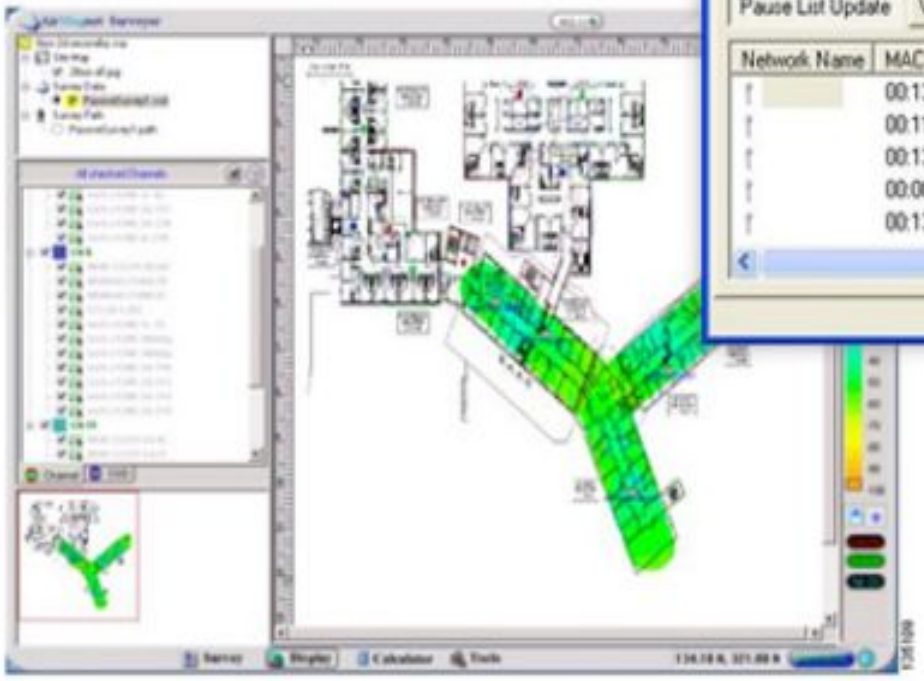
WLAN Implementation
- Site Survey

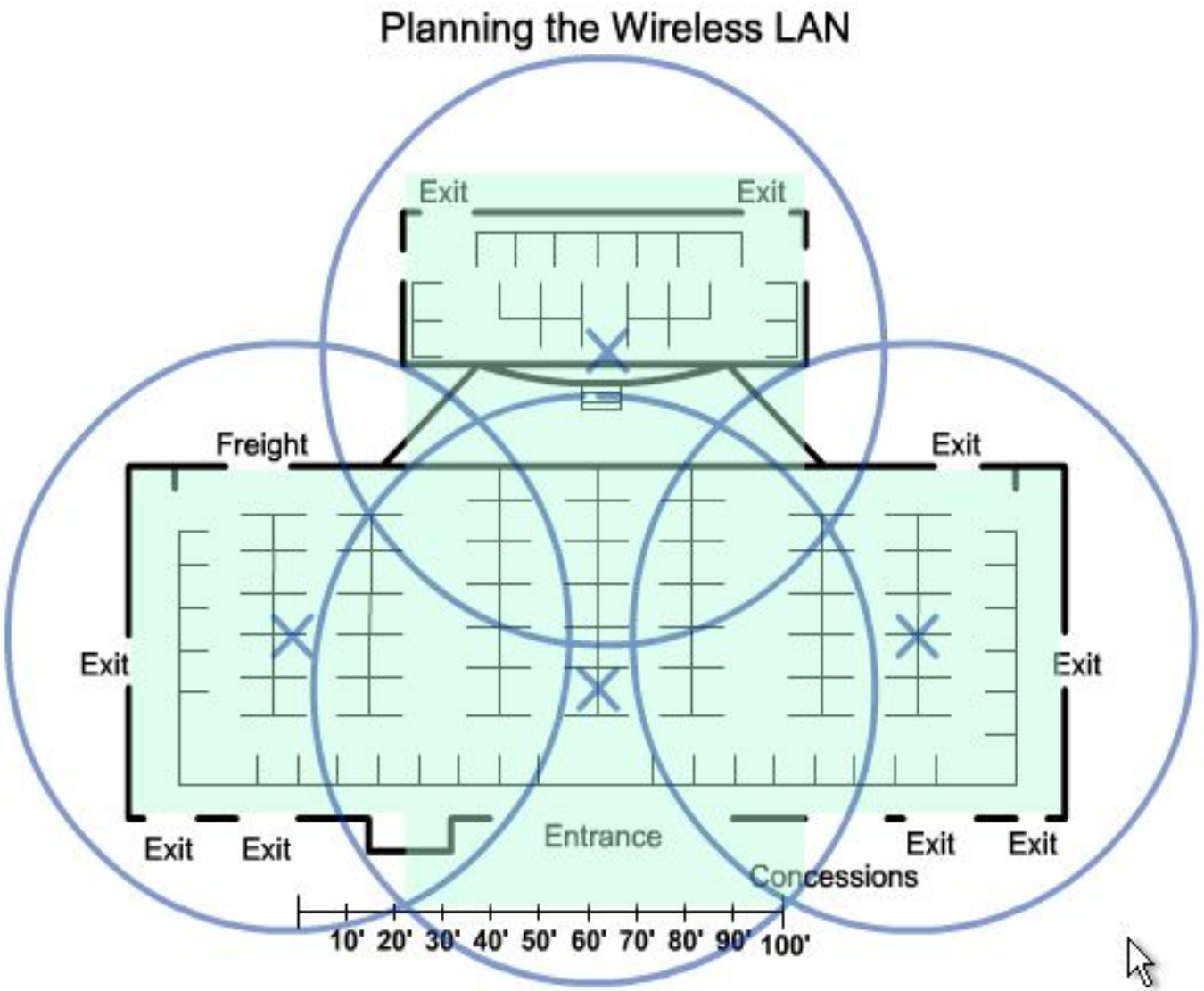
Correct RF Interference Issues

Screenshot 1



Screenshot 2




Planning the Wireless LAN
Exit
Exit
Freight
Exit
Exit
Exit
Exit
Exit
Entrance
Exit
Exit
Concessions
10' 20' 30' 40' 50' 60' 70' 80' 90' 100'

Configuring the Access Point

1. Verify wired LAN operation - DHCP, internet access ...
2. Access Point installation
3. Management IP Address, Subnet mask, Default gateway, DNS... configuration
4. Admin Password and policies configuration
5. Channel SSID, Mode (b, g, mixed ... no security) configuration
6. Turn on client and verify connection
7. Wireless security and filters configuration
8. Verify WLAN operation

Advanced Implementation

Controlled

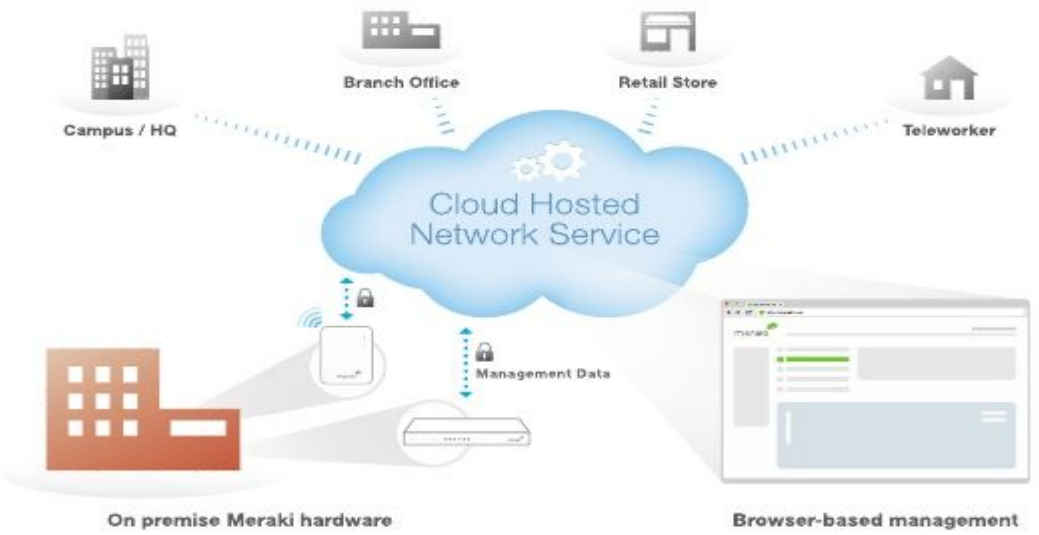
Layer 2 o Layer 3 Network

Controller

Traffic to the controller (CAPWAP)

Traffic Locally Routed

Cloud-based (Meraki)



Troubleshooting

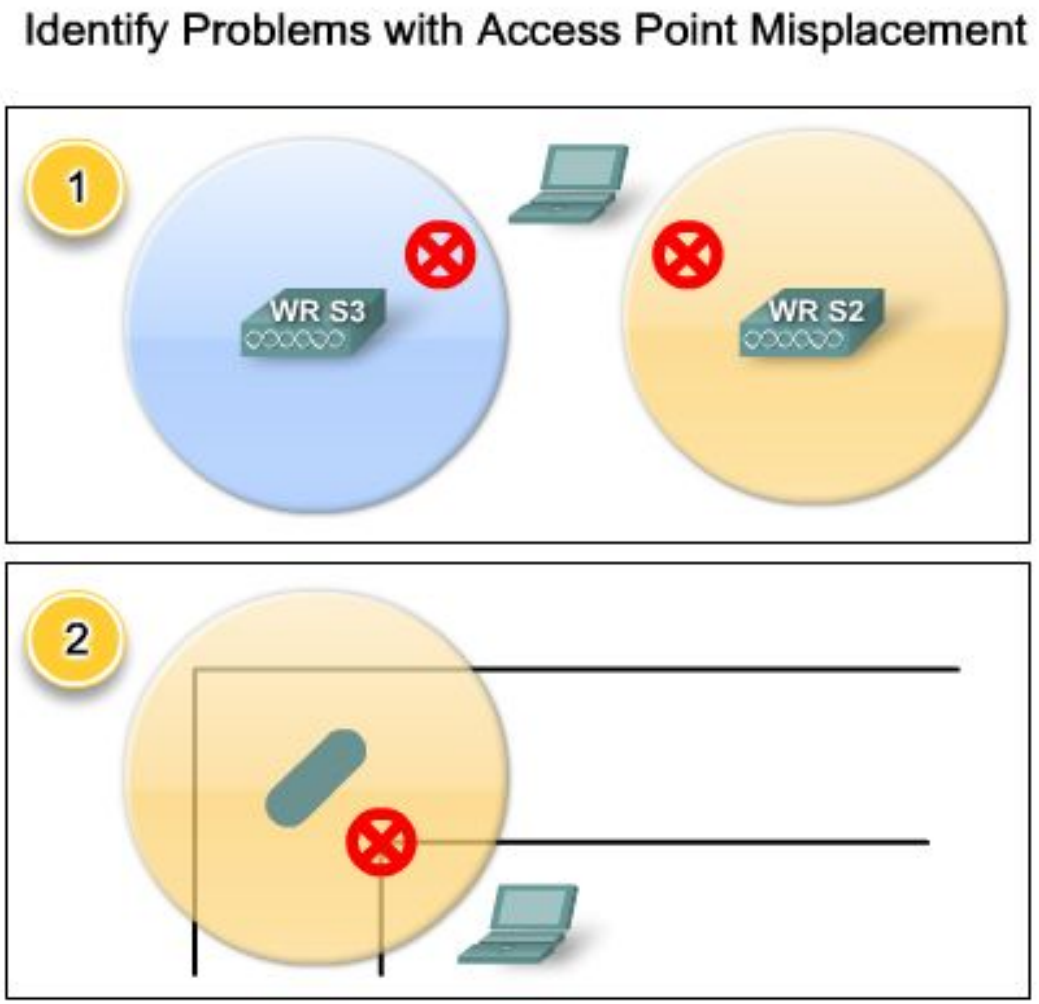
- General Approaches

- Top-Down : from layer 7 to layer 1
- Bottom-Up : from layer 1 to layer 7
- Divide-and-Conquer : starting from layer 3, up if OK, down if fails
- Following the Path : follow the traffic path
- Comparing Configuration
- Component Swapping

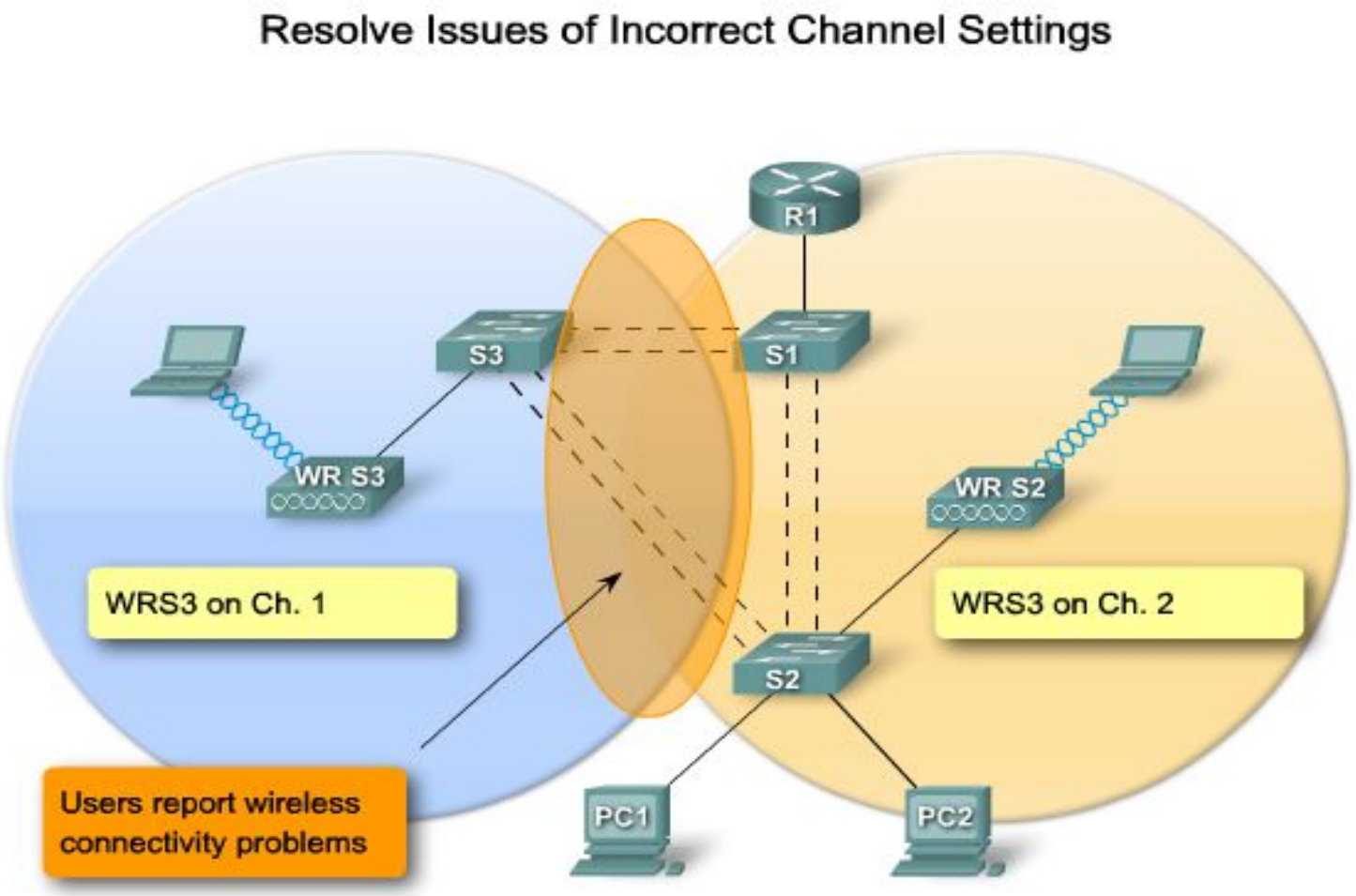
- WLAN Specific

- Remove Security (planned)
- Eliminate client device as possible problem source

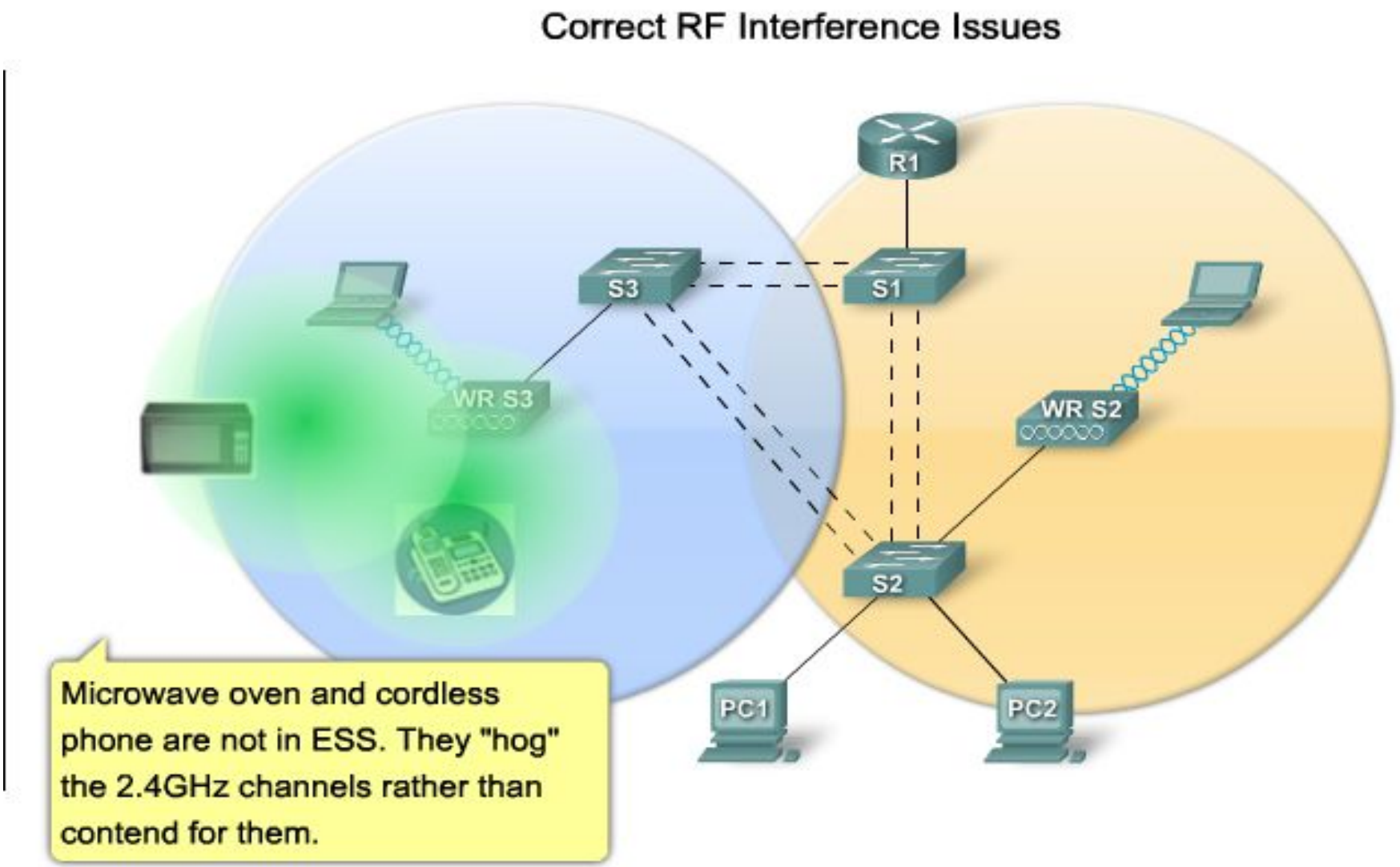
Troubleshooting - case 1



Troubleshooting - case 2

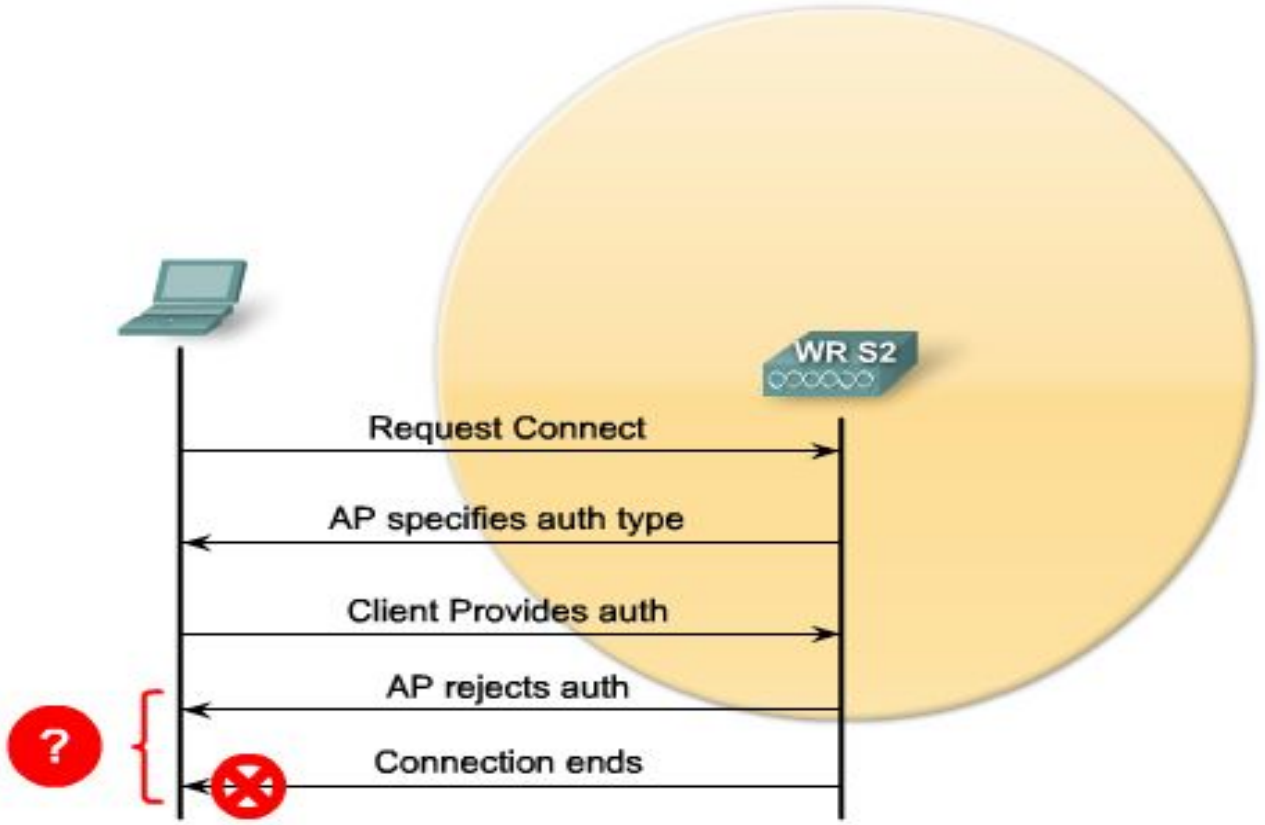


Troubleshooting - case 3



Troubleshooting - case 4

Resolve Problems with Wireless LAN Encryption and Authentication



WI-Fi Today
Internet Access

.Real Scenario : WISP
.Offload : key point of Mobile Internet Access

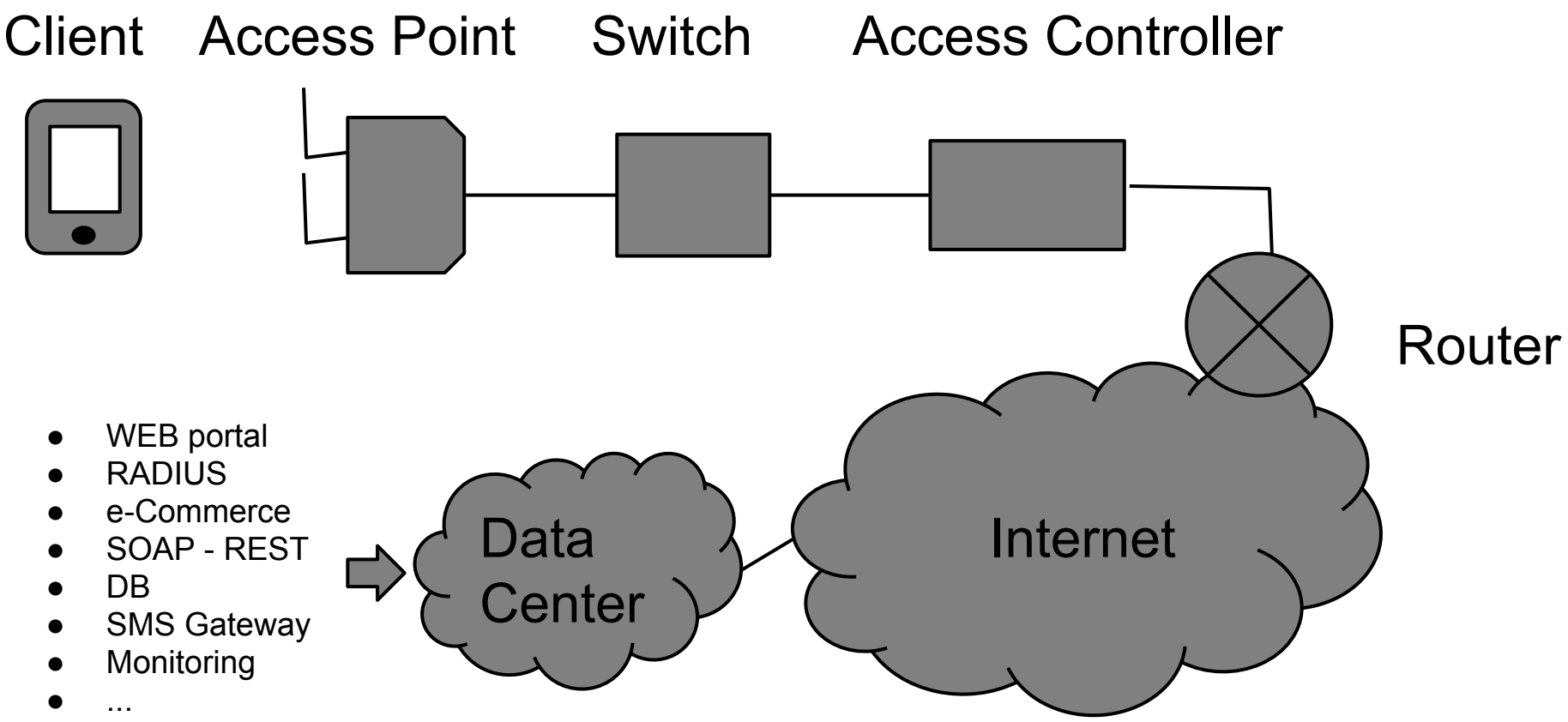
Nicola Iotti, CTO Guglielmo S.r.l.

Real Scenario: WISP

- General Scenario
- User Authentication
- Security
- Performance
- Typical Issues

Real Scenario WISPR

General Scenario



- WEB portal
- RADIUS
- e-Commerce
- SOAP - REST
- DB
- SMS Gateway
- Monitoring
- ...

Real Scenario WISPR

Authentication

.Legal Issues
.Billing

Security

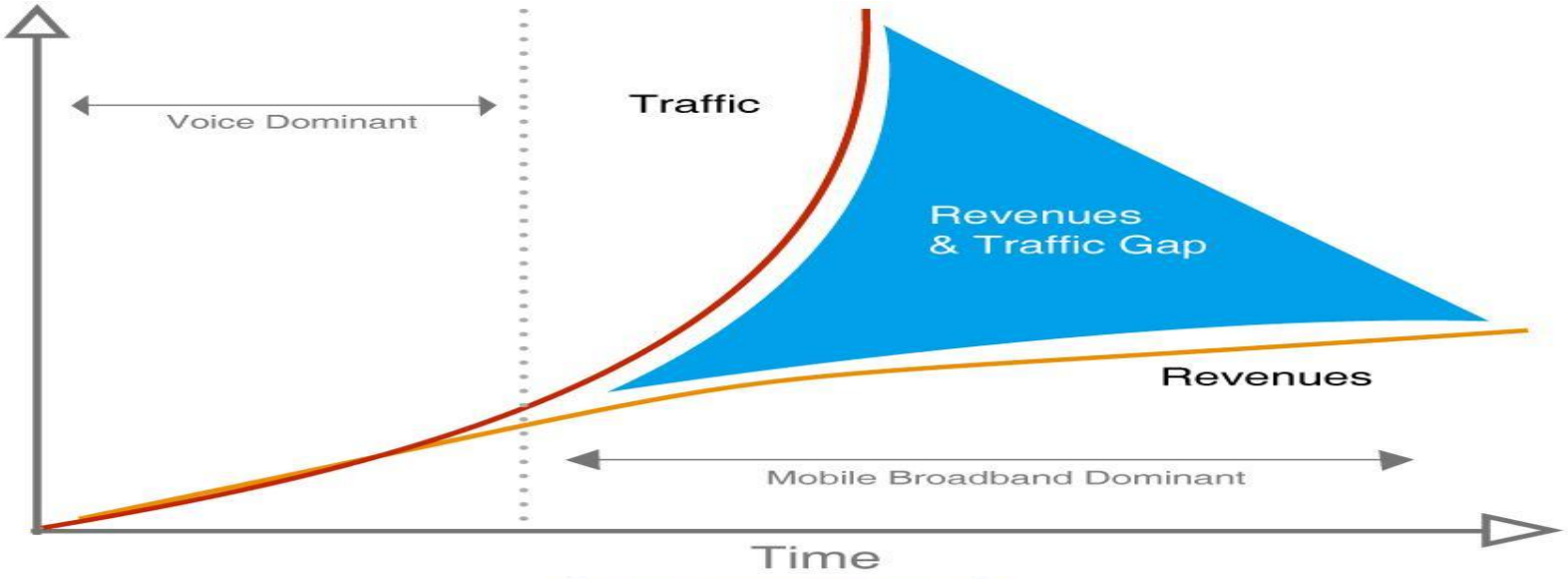
.Authentication → https
.Location LAN Security → Firewall
.Between Clients : critical → Client Isolation on AP

PVLAN on Switch

Real Scenario WISP

- Performance
  - Congestion
  - Internet access: possible bottleneck
  - Countermeasure
    - Session limit
    - Time limit
    - Bandwidth limit
- Typical issues
  - Coverage
  - Operating Systems Compatibility and Settings (PC and Mobile
  - Heterogeneous Applications → QoS
  - WAN Connection
  - Network Selection and Authentication

Offload – Basic Concept



Cisco forecasts video will account for 66 percent of global mobile data traffic by 2014.

Offload – Main Actors

	3G	Wi-Fi
Providers	3G Providers	3G Providers WISP
Vendors (Network)	Nokia Siemens, Qualcomm, Ericsson, Motorola, Huawei	Cisco
Vendors (Mobile Devices)	Apple, Google... Samsung, Microsoft,...	
Standard Organizations	3GPP	IEEE
Customers	Mobile Customers	

HOTSPOT 2.0 + 3GPP - THE MOST ENDORSED SOLUTION FOR WI-FI AND 3G/4G INTERACTION

LIST OF FEATURES, PROTOCOLS USED AND CHANGES NEEDED TO BE COMPLIANT

HS2.0 Release 1 :

- **Network Discovery and Selection** :
  - Information on Wi-Fi retrieved by the mobile devices using IEEE 802.11u from AP
  - *Not supported by Devices - replacement of not compliant Hotspot devices*
  - The device makes decision (no cloud nor centralized network selection)
- **Encryption** : WPA2- Enterprise - *Hotspot configuration changes needed*
- **Authentication** : IEEE 802.1x - *Manual Configuration - replacement of not compliant Gateway or Access Point* - provides base for several authentication methods. The most advanced methods are:
  - EAP-SIM (RFC-4186) : SIM based - *Not supported by most of Devices - infrastructure changes needed*
  - EAP-AKA (RFC-4187) : USIM based - *Not supported by most of Devices - infrastructure changes needed*

HOTSPOT 2.0 + 3GPP - THE MOST ENDORSED SOLUTION FOR WI-FI AND 3G/4G INTERACTION

LIST OF FEATURES, PROTOCOLS USED AND CHANGES NEEDED TO BE COMPLIANT

HS2.0 Release 2 :

- **Immediate account provisioning for SIM and non-SIM** - *infrastructure changes needed*
- **Centralized network discovery and selection based on operator specific policies** : ANDSF 3GPP - *Not supported by Devices*
- **Session Mobility, full IP-session continuity and IP-address preservation** between the cellular and the Wi-Fi network : I-WLAN 3GPP
  - Infrastructure integration - *infrastructure changes needed*
  - Tunnel from Device to core network- *Not supported by Devices*

New Challenge: IoT

Connected Objects: Big Number (32 billions by 2020)

- 802.15.4, BLE (Bluetooth Low Energy), but Wi-Fi probably

Infrastructure Issues → New Technologies

- SDN
- Fog Computing

IoT Infrastructure