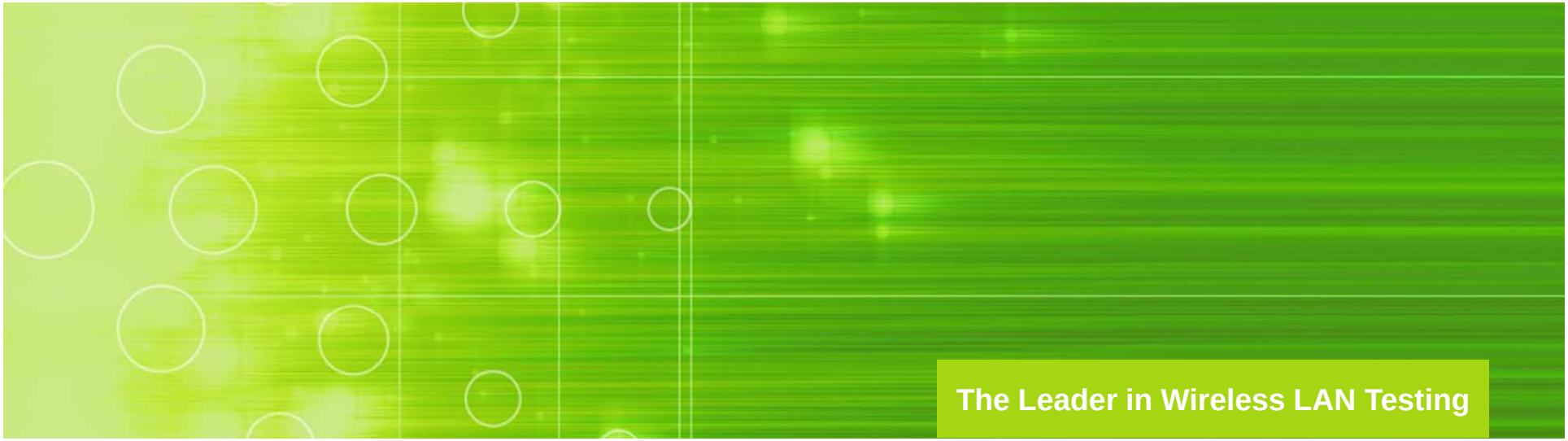
veriwave™

802.11 WLAN Systems – a tutorial



Agenda

- Introduction
- WLAN network basics
- Physical layer (radio) technologies
- Protocol architecture
- 802.11 MAC protocol
- Security protocols in WLANs
- Advanced topics in WLANs
- Wireless LAN standards
- WLAN testing challenges and test metrics
- Conclusion

veriwave

What is a WLAN? What is 802.11?

- **Wireless LANs (WLANs) are LANs that use RF instead of cable or optical fiber**
  - Allows high-speed data transfer without wires or cables
  - Supports typical enterprise applications (e-mail, file transfer, audio/video conferencing, etc)
  - First introduced in 1999, evolved from legacy RF data technologies such as Hiperlan
  - 120 million ports of WLAN shipped worldwide last year (virtually all laptops have WLAN interfaces now)
- **IEEE 802.11-1999 is the basic standard governing wireless LANs**
  - Standardized by the IEEE 802.11 group, which is a working group in the IEEE 802 LAN/MAN Standards Committee (LMSC)
  - Formed in 1991 to standardize a 1 Mb/s RF-based data network technology
  - Completed its work in 1999 with the first 802.11 wireless LAN standard
  - Now driving almost all WLAN technology development worldwide

Pros and Cons of 802.11

Pros..

- Mobility
- Compatible with IP networks
- High speed data connectivity
- Unlicensed frequencies
- Highly secure
- Easy and fast installation
- Simplicity
- Scalability
- Very low cost

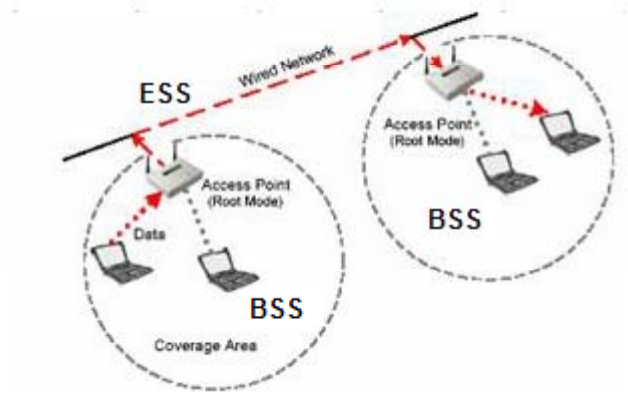
Cons..

- Shared-medium technology – bandwidth limited by RF spectrum
- Limited number of non-overlapping channels
- Multipath effects indoor
- Interference in the 2.4 GHz and 5 GHz bands
- Limited QoS
- Power control
- High overhead MAC protocol

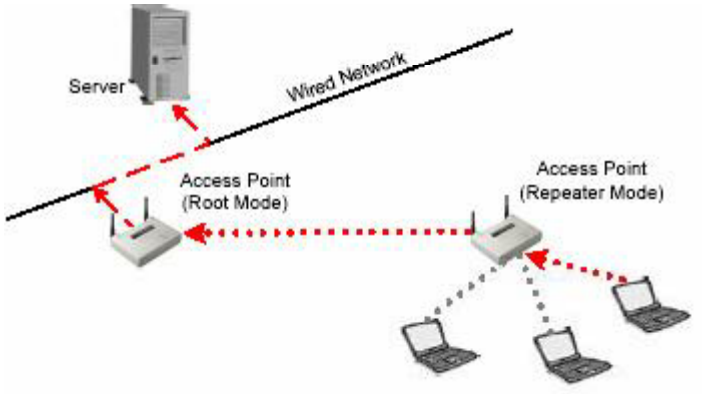
Basic 802.11 Operation

- WLAN network topology
- Channel scanning and synchronization
- Authentication and association
- Data transfer mechanism

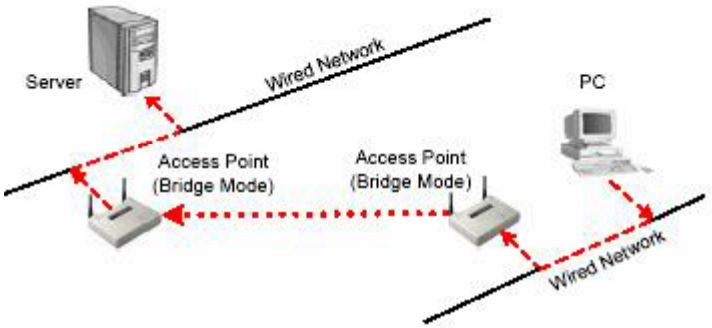
WLAN Network Topologies



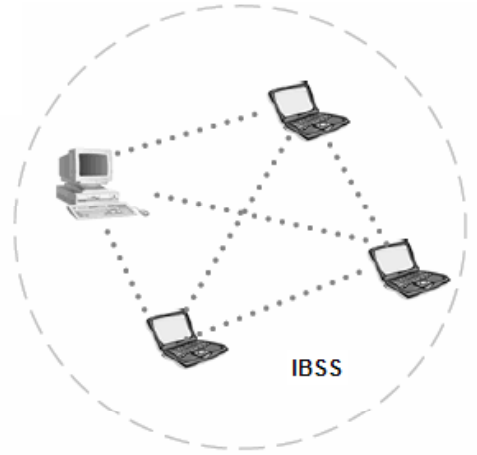
Infrastructure Mode



Repeater Mode



Bridge Mode

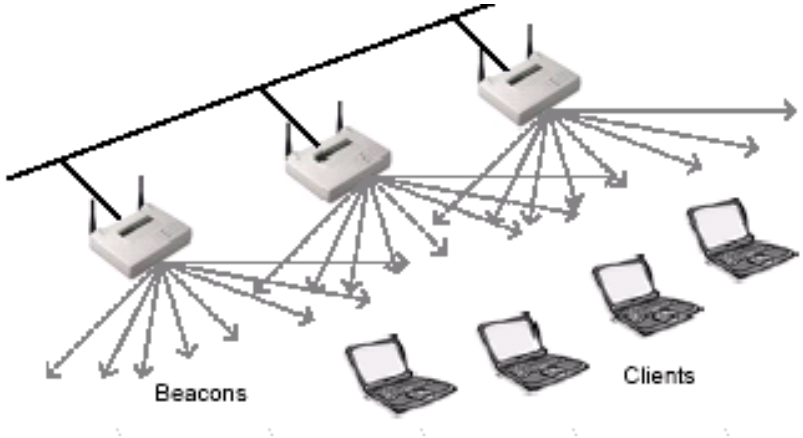


Ad-hoc Mode

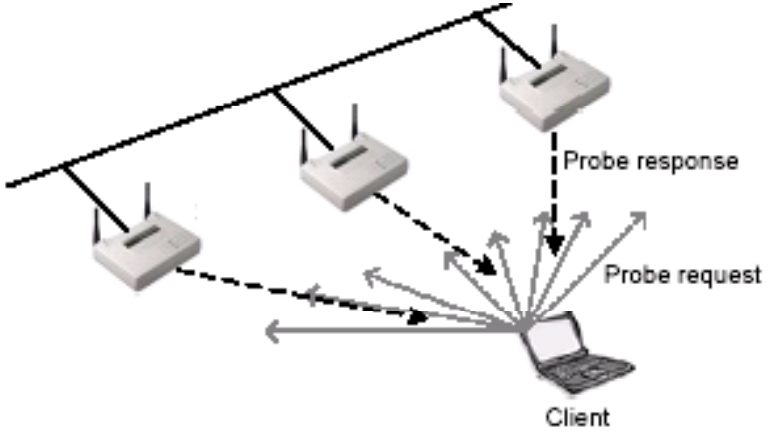
veriwave

Scanning

1. Scanning is the first step for the MC (Mobile Clients) to join an APs network.
2. In the case of passive scanning the client just waits to receive a Beacon Frame from the AP
3. MC (Mobile Clients) searching for a network by just listens for beacons until it finds a suitable network to join.



Passive Scan



Active Scan

1. The MC (Mobile Clients) tries to locate an AP by transmitting Probe Request Frames, and waits for Probe Response from the AP.
2. The probe request frame can be a directed or a broadcast probe request.
3. The probe response frame from the AP is similar to the beacon frame.
4. Based on the response from the AP, the client makes a decision about connecting to the AP

veriwave

Synchronization

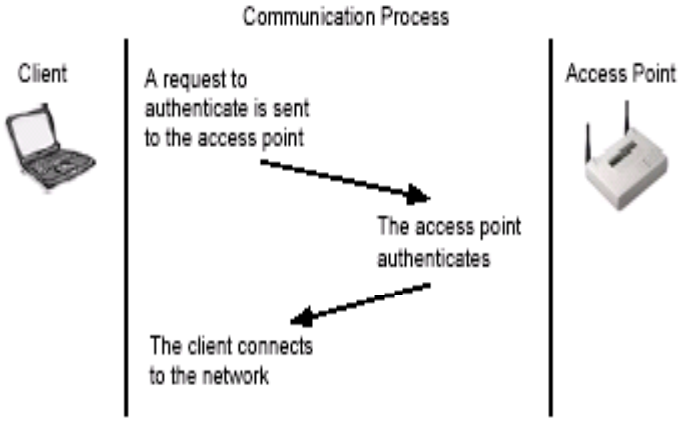
- Necessary for keep all the clients synchronized with the AP in order for the clients to perform functions like power save.
- AP periodically transmits special type of frames called Beacon Frames
- The beacons contain the timestamp of the AP. The clients synchronize their clocks with the APs clock using this timestamp.
- The AP also uses the beacon to advertise its capabilities and this information is used by the passively scanning clients to make a decision to connect to the AP.
- The AP advertises its capabilities in the form of Information Elements (IEs) in beacon frames
- Some of the IEs are: SSID, channel, Supported Rates, WPA IE, EDCA IE

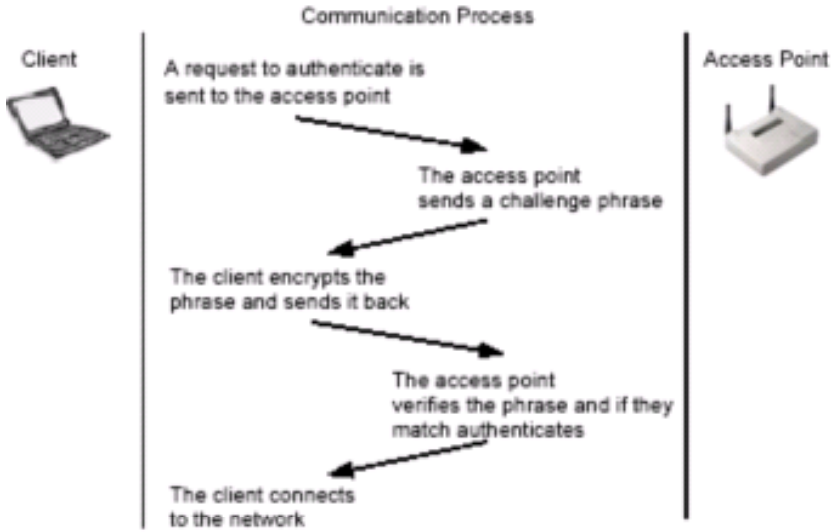
Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

veriwave

802.11 Authentication

- The station first needs to be authenticated by the AP in order to join the APs network.
- 802.11 defines two authentication subtypes: Open system and shared key





Open Authentication

A sends an authentication request to B.
B sends the result back to A

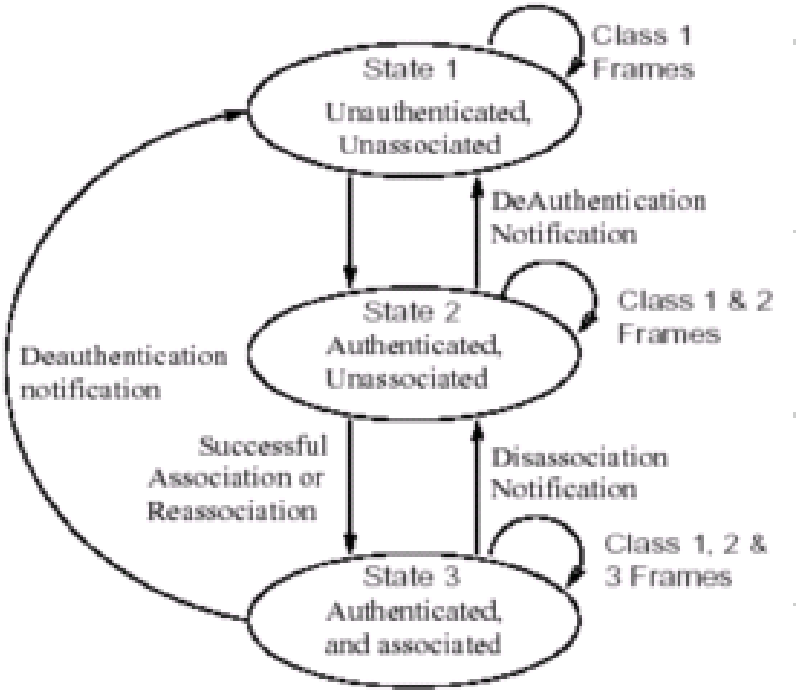
Shared Key Authentication

Uses WEP Keys
Considered more insecure than open system

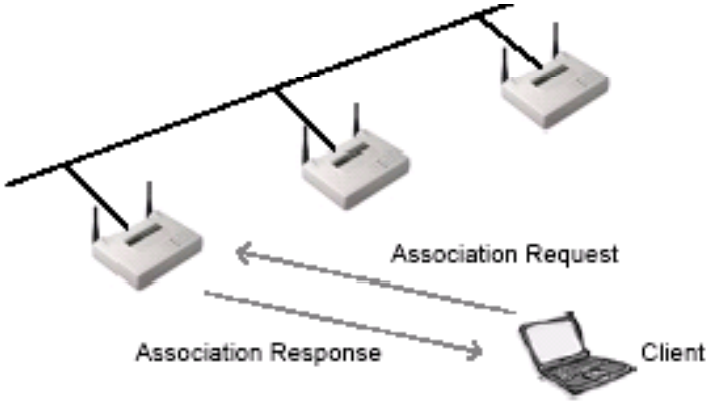
veriwave

802.11 Association

- Next Step after authentication
- Association enables data transfer between MC (Mobile Clients) and AP.
- The MC (Mobile Clients) sends an association request frame to the AP who replies to the client with an association response frame either allowing are disallowing the association.
- Once the association is successful, the AP issues an Association ID to the client and adds the client to its database of connected clients.



State Machine



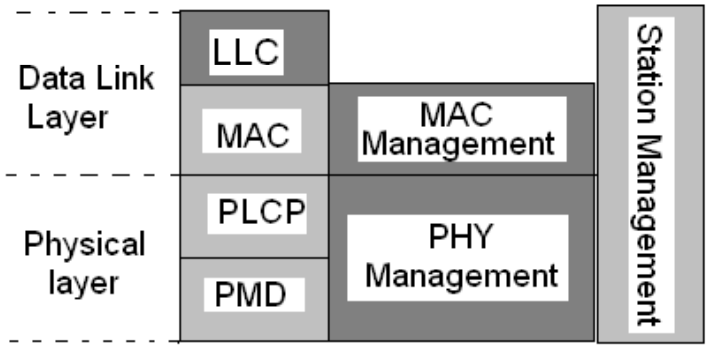
veriwave

Data Transfer

- Data transfer allowed only after authentication and association.
- Attempting to send data to an AP without proper authentication and association causes AP to respond with a de-authentication frame.
- Data frames are always acknowledged. If a client sends a data frame to an AP, the AP must send an acknowledgement. If the AP sends a data frame to a client, the client must send an acknowledgement
- The AP will forward data frames received from the client to the required destination on the wired network. It will also forward data directed to the client from the wired network. APs can also forward traffic between two clients, but this is not common.

IEEE 802.11 Protocol Architecture

- **MAC Layer:**
  - Provides access to contention based and contention-free traffic on different kinds of physical layers.
  - MAC layer responsibilities are divided into MAC sub layer and MAC management sub-layer.
  - MAC sub layer defines access mechanisms and packet formats.
  - MAC management sub-layer defines power management, security and roaming services.

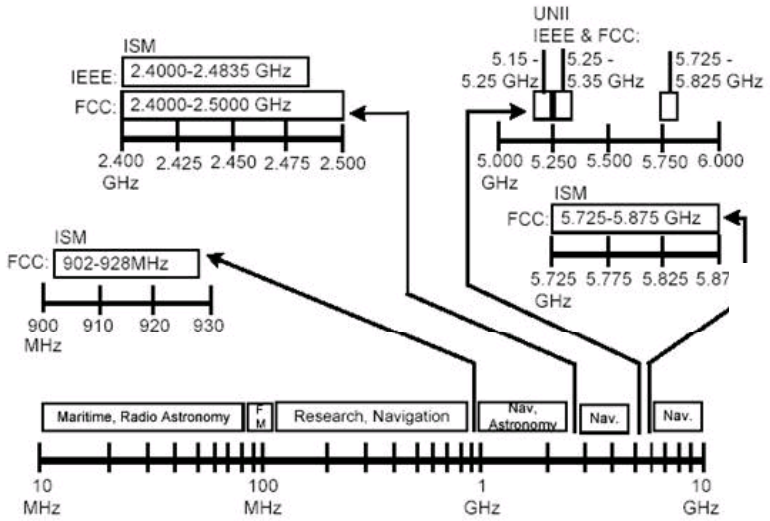


- **PHY Layer:**
  - The Physical layer is divided into three sub layers
  - The PLCP acts as an adaption layer The PLCP is responsible for CCA and building packets for different physical layer technologies
  - The PMD layer specifies modulation and coding techniques
  - The PHY management layer takes care of the management issues like channel tuning.
  - Station management sub layer is responsible for co-ordination of interactions between the MAC and PHY layers

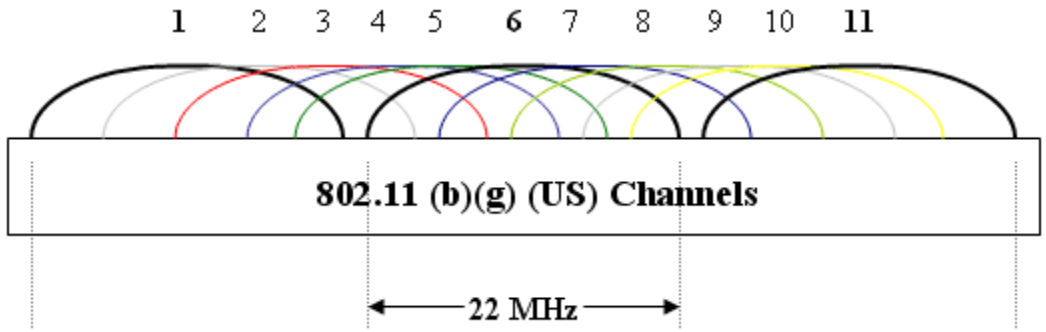
The 802.11 PHY (RF) Layer

- Radio channels and frequencies
- Modulation technologies
- PHY data rates used
- Improving data transfer: diversity and polarization

Frequency Channel Allocation for 802.11a/b/g



802.11 b/g



2.401 GHz

2.473 GHz

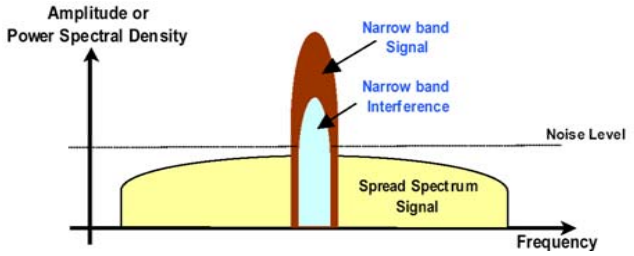
802.11a

Band	Channels	Use
5.15 GHz to 5.35 GHz	8 channels (36, 40, 44, 48, 52, 56, 60, 64)	Band is common between Europe and the US. It's used in almost every European country.
5.47 GHz to 5.725 GHZ	11 channels (100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140)	Band is currently available throughout all European countries. The band is expected to become widely available throughout the United States sometime in 2006.
5.725 GHz to 5.85 GHz	5 channels (149, 153, 157, 161, 165)	Band is available in U.S., Canada, and China but is not permitted in the EU.

veriwave

Physical Layer Technologies

Direct Sequence Spread Spectrum



- Spreads a signal power over a wider band of frequencies
- Frequency spectrum of a data-signal is spread using a code uncorrelated with that signal
- Codes used for spreading have low cross-correlation values and are unique to every user
- Sacrifices bandwidth to gain signal-to-noise performance
- Both the transmitting and receiving are done on a 22 MHz wide set of frequencies
- 1, 2, 5.5 and 11 Mbps data rates supported for 802.11b
- channels 1,6 and 11 are non overlapping channels and can be used for co-location

Orthogonal Frequency Division Multiplexing (OFDM)

- A special form of multicarrier modulation. Used for 802.11a and 802.11g
- Transmit broadband, high data rate information by dividing the data into several interleaved, parallel bit streams modulated on a separate sub-carrier
- Robust against the adverse effects of multipath propagation and ISI
- Provides several modulation and coding alternatives to adapt to the channel quality
- Using adequate channel coding and interleaving we can recover symbols lost due to the frequency selectivity of the channel.

PHY Data rates for 802.11a/b/g

802.11b

- Supports 1, 2, 5.5 and 11 Mbps data rates in the 2.4 GHz ISM band
- Backward compatible with the original 802.11 DSSS systems.
- Uses Complementary Code Keying (CCK) modulation for 5.5 and 11Mbps rates

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

802.11a

- Incompatible with devices operating in 2.4GHz
- Uses OFDM technique and supports Data rates up to 54 Mbps.
- Uses combinations of various modulation and coding rates to achieve the different PHY rates

Mode	Modulation	Code rate	PHY bit rate	bytes/OFDM symb.
1	BPSK	½	6 Mbps	3.0
2	BPSK	¾	9 Mbps	4.5
3	QPSK	½	12 Mbps	6.0
4	QPSK	¾	18 Mbps	9.0
5	16QAM	9/16	27 Mbps	13.5
6	16QAM	¾	36 Mbps	18.0
7	64QAM	¾	54 Mbps	27.0

Antenna Diversity and Polarization

Antenna Diversity

- Scheme devised to compensate multipath effects by using multiple antennas
- The incoming RF signal is received through one antenna at a time.
- The receiving radio constantly samples the incoming signals from both the antennas to determine the higher quality signal.
- The receiver radio then chooses to accept the higher quality signal.
- The receiver transmits its next outgoing signal out of the antenna that was last used to receive an incoming signal because the received signal was a higher quality signal than from the other antenna.

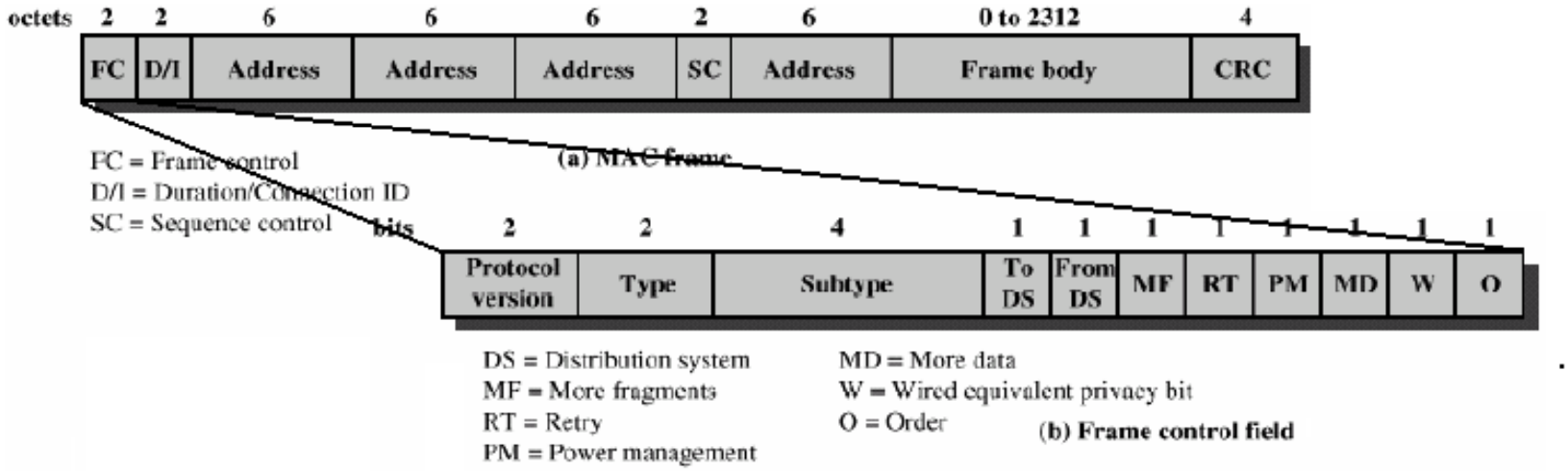
Polarization

- Radio wave made up of electric and magnetic fields which are in perpendicular planes to each other
- **Horizontal polarization** when electric field is parallel to ground
- **Vertical polarization** when electric field is perpendicular to ground
- Antennas that are not polarized in the same way may not be able to communicate with each other effectively.

The 802.11 MAC (Frame) Layer

- Framing data to be transmitted
- Spacing between frames
- Avoiding collisions: carrier sensing
- Avoiding collisions: the backoff algorithm

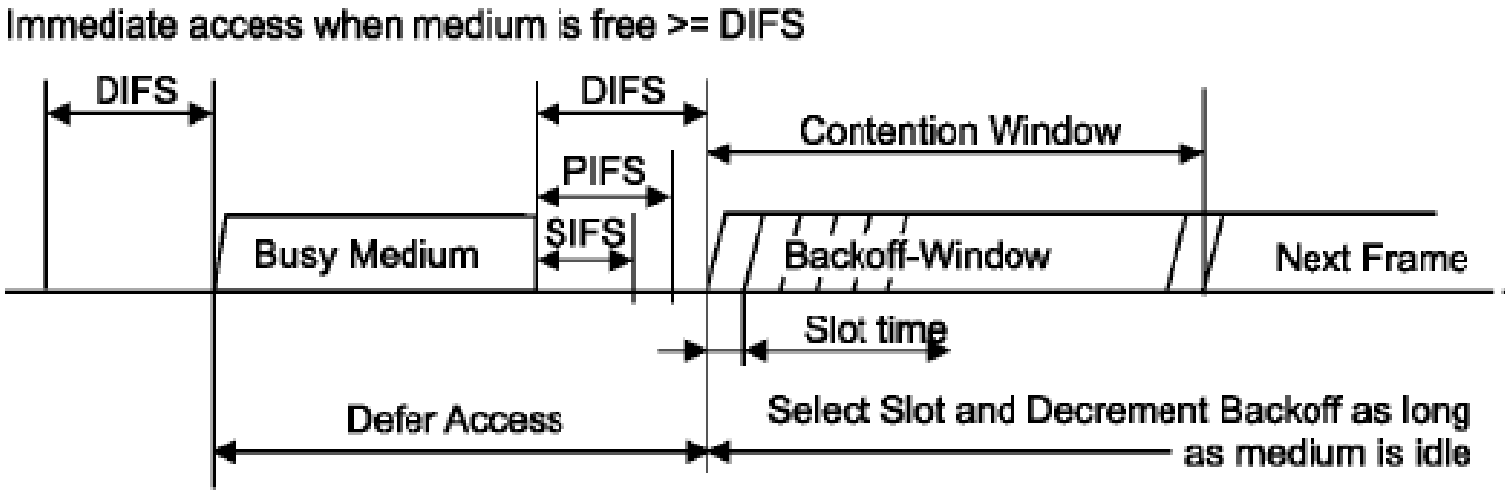
802.11 Frame Format



- **Management Frames**
  - Beacon, Probe request, Probe Response, Authentication, Association Request, Association Response, Deauthenticate, Disassociate, Reassociation request, Reassociation response,
- **Control Frames:**
  - RTS, CTS, Acknowledgment, PS-Poll
- **Data Frames:**
  - Data, Null frame

Inter Frame Spaces (IFS)

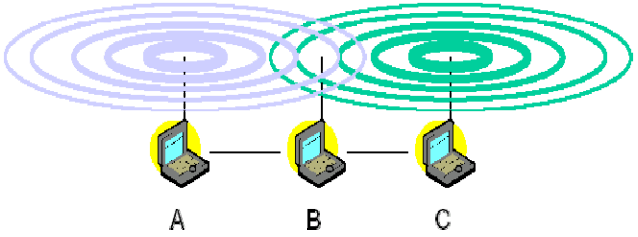
- The Inter Frame Spaces define the minimum time that a station needs to wait after it senses the medium free.
- The concept of IFS was introduced to enable different priority levels for transmission.
- The smaller the IFS, the higher the priority
- Various Inter Frame Spaces are defined to assign different priorities (SIFS, PIFS, DIFS)



Carrier Sensing

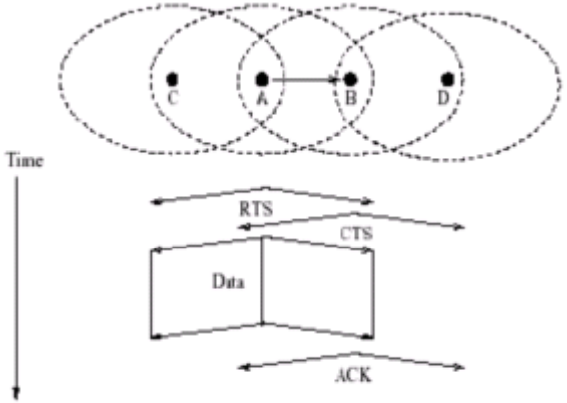
Physical Carrier Sensing

- Uses CSMA/CA scheme
- Each station detects activity on the channel by analyzing the signal from other clients in the network.
- All the clients connected to the same AP are considered to be in a common contention zone.
- If a station is not able to detect any signal then it assumes that none of the other stations are transmitting and hence starts transmitting.
- This scheme faces hidden terminal problem.



Virtual Carrier Sensing

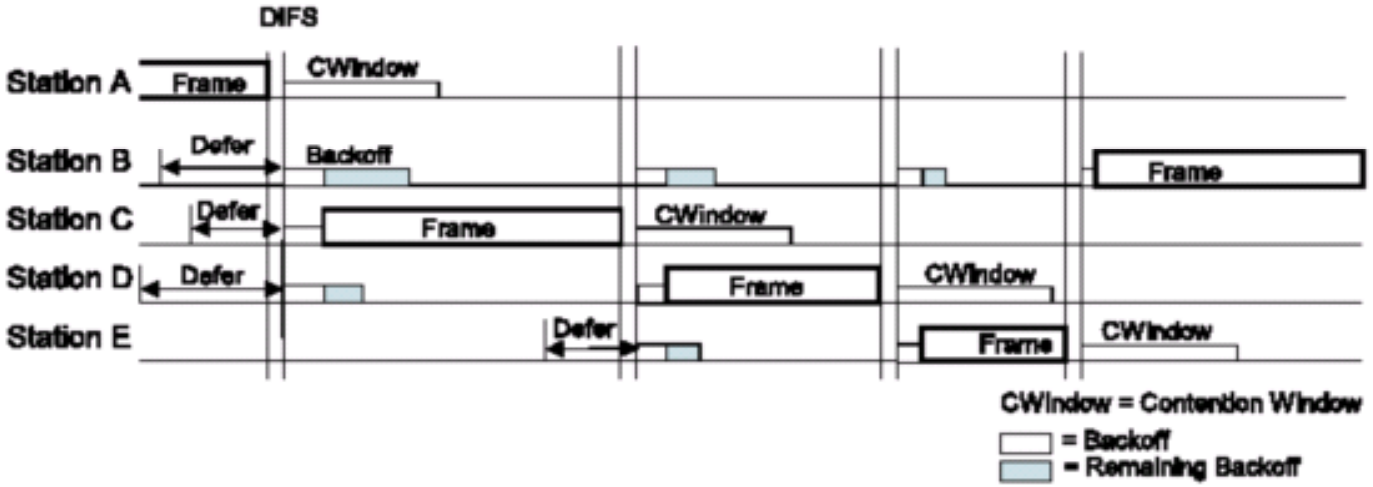
- This scheme uses CTS and RTS
- When a MC (Mobile Client) wants to transmit data, it sends an RTS packet which includes the source, destination and the duration of the following transaction
- Destination responds with CTS which includes the same duration information
- All stations receiving either CTS or RTS set their NAV for the given duration and don't try to transmit for that time



veriwave

Backoff Algorithm

- Each station senses the channel for an additional random time after detecting the channel as being idle for a minimum duration of DIFS.
- Only if the channel remains idle for this additional random time period, the station is allowed to initiate the transmission.
- Each station maintains a *CW*, which is used to determine the number of slot times a station has to wait before transmission.
- A backoff counter is maintained which counts the slots from the random time chosen to zero downwards.
- The Backoff Counter is decreased as long as a slot time is sensed as idle and it is frozen when a transmission is detected.
- As soon as the Backoff Counter reaches the value Zero the station transmits its own frame
- After any unsuccessful transmission attempt, another backoff is performed with a doubled size of the CW.
- This reduces the collision probability in case there are multiple stations attempting to access the channel



veriwave

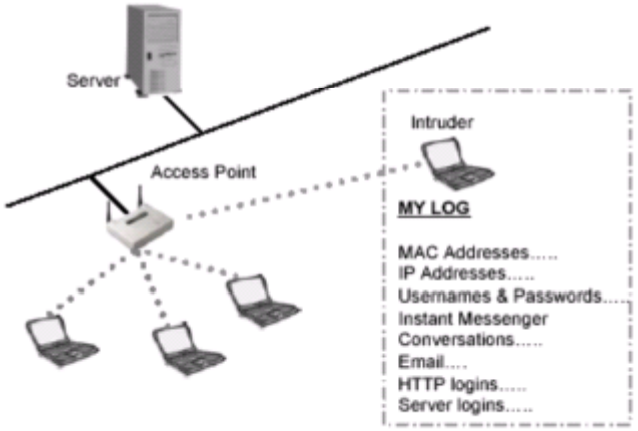
Security in 802.11 WLANs

- Framing data to be transmitted
- Spacing between frames
- Avoiding collisions: carrier sensing
- Avoiding collisions: the backoff algorithm

Common WLAN Attacks

Passive Attacks: eavesdropping

- Wireless LAN sniffers can be used to gather information about the wireless network from a distance with a directional antenna.
- These applications are capable of gathering the passwords from the HTTP sites and the telnet sessions sent in plain text.
- These attacks do not leave any trace of the hacker's presence on the network



PHY Layer attacks: RF Jamming

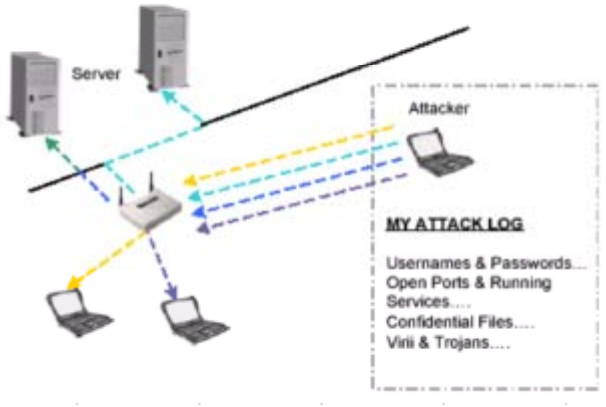
- The hacker can use a high power RF signal generator to interfere with the ongoing wireless connection, making it useless.
- Can be avoided only by physically finding the jamming source

veriwave

WLAN Attacks, Contd…

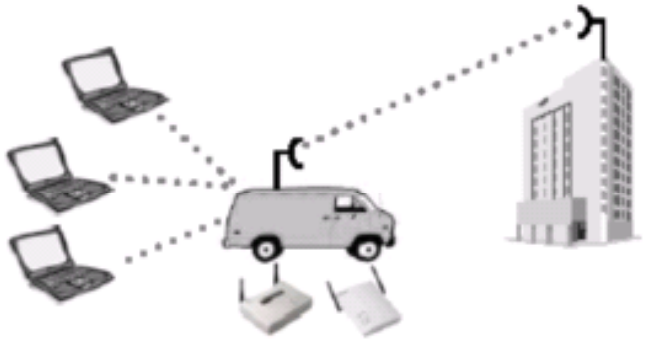
Active Attacks: hacking

- Hacker can connect to the network through the wireless LAN and obtain an IP address form the DHCP server.
- A business competitor can use this kind of attack to get the customer information which is confidential to an organization



Man-in-the-Middle Attack

- A hacker may use an rogue AP to hijack mobile nodes by sending a stronger signal than the actual AP is sending to those nodes.
- The MC (Mobile Client) then associates with the rogue AP, sending its data into the wrong hands.



An access point and sometimes a workgroup bridge are used to hijack users

veriwave

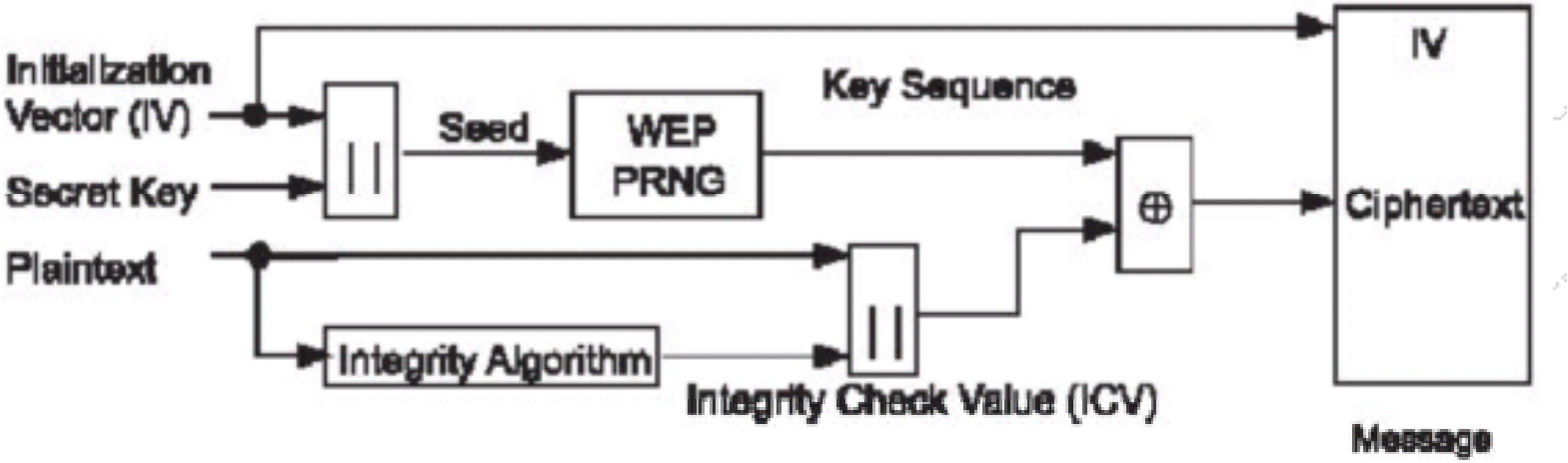
WLAN Security Solutions

- The two mains aspects of security are privacy and confidentiality
- In 802.11 the privacy problem is solved by robust mutual authentication mechanisms and the confidentiality problem is solved by encryption methods.
- Some of the existing and the newly introduced (by 802.11i) authentication and encryption methods are listed below:

- WEP-Open
- WEP-SharedKey
- WPA-PSK
- WPA-EAP/TLS
- WPA-EAP/TTLS-GTC
- WPA-PEAP/MSCHAPv2
- WPA-EAP/FAST
- WPA2-PSK
- WPA2-EAP/TLS
- WPA2-EAP/TTLS-GTC
- WPA2-PEAP/MSCHAPv2
- WPA2-EAP/FAST
- DWEP-EAP/TLS
- DWEP-PEAP/MSCHAPv2
- LEAP
- WPA-LEAP
- WPA2-LEAP
- WPA-PSK-AES
- WPA-EAP/TLS-AES
- WPA-PEAP/MSCHAPv2-AES
- WPA2-PSK-TKIP
- WPA2-EAP/TLS-AES
- WPA2-PEAP/MSCHAPv2-TKIP

WEP Encryption and Drawbacks

- 64 and 128 bit keys are used for authentication and encryption of data
- WEP protocol is fundamentally weak because it uses a static encryption key.
- Motivated attackers can easily crack WEP encryption by using freely available hacking tools.
- The determination and distribution of WEP keys are not defined
- No defined mechanism to change the WEP key either per authentication or periodically for an authenticated connection
- No mechanism for central authentication, authorization, and accounting

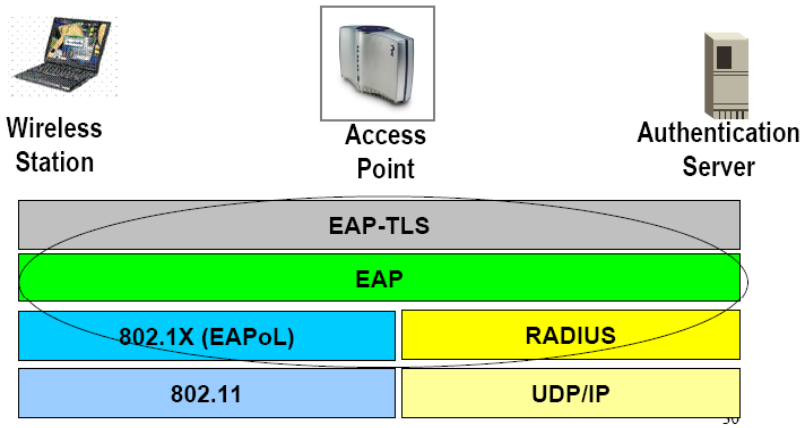


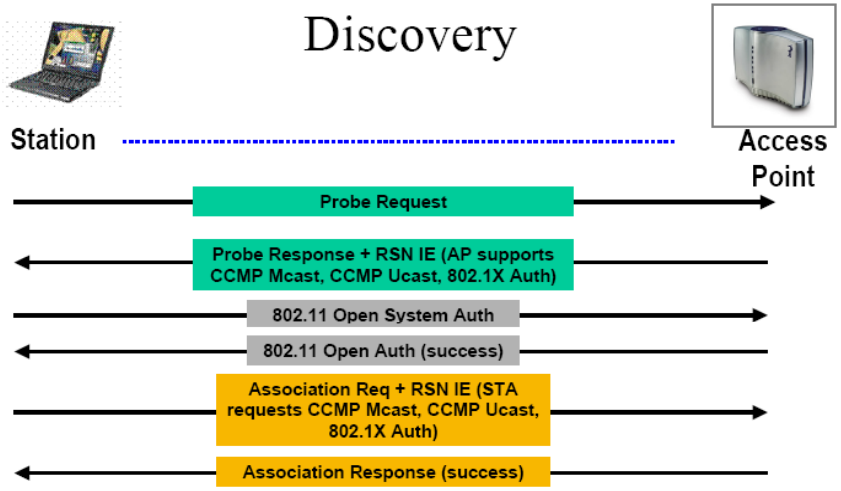
veriwave

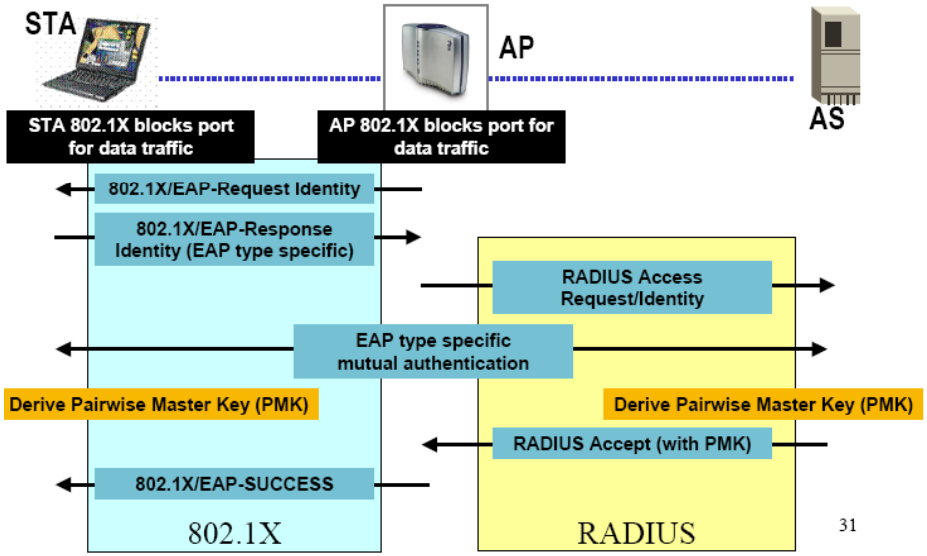
Server Based Authentication

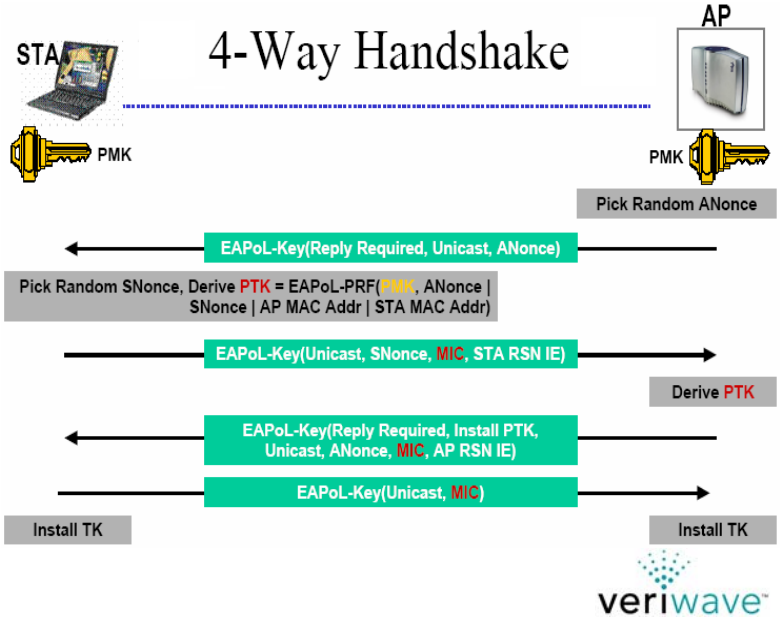
- A possible solution for the security problem is maintaining centralized key servers like a RADIUS server for centralized key generation and distribution.
- This would reduce the overhead of maintaining the key information of all the clients at the AP.
- With RADIUS, authentication is user-based rather than device-based, so, for example, a stolen laptop does not necessarily imply a serious security breach.
- RADIUS eliminates the need to store and manage authentication data on every AP on the WLAN, making security considerably easier to manage and scale.
- Steps for Authenticating with RADIUS server
  - The WLAN Client (the “Supplicant”) tries to access network. [EAPoL]
  - The AP (the “Authenticator”) responds to requests, and will ask client for identity. [EAPoL]
  - Client responds with identity to AP [EAPoL]
  - AP will forward Access-Request to RADIUS server with the user's identity. [RADIUS]
  - RADIUS server will respond with a challenge to AP. The Challenge will indicate the EAP authentication-type requested by the server [RADIUS]
  - AP forwards challenge to client [EAPoL]
  - If Client agrees to EAP-type, then negotiation will continue; if not, client will NAK request and suggest an alternative method. [EAPoL]
  - AP forwards response to RADIUS server. [RADIUS]
  - If these credentials are correct, the RADIUS server accepts the user. If not, the user is rejected. An Access-Accept or Reject is sent. [RADIUS]
  - If authentication succeeds, AP connects client to the network.

Server-based security: 802.1x / 802.11i









veriwave

Advanced Topics

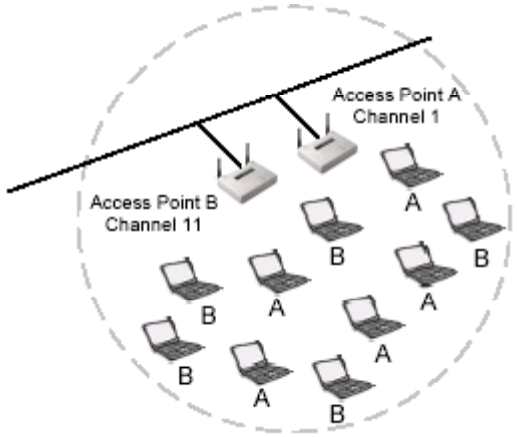
- Load Balancing and Rate Adaptation
- Power Management
- Roaming
- Quality of Service
- The next-generation WLAN: IEEE 802.11n

veriwave

Load Balancing and DRS

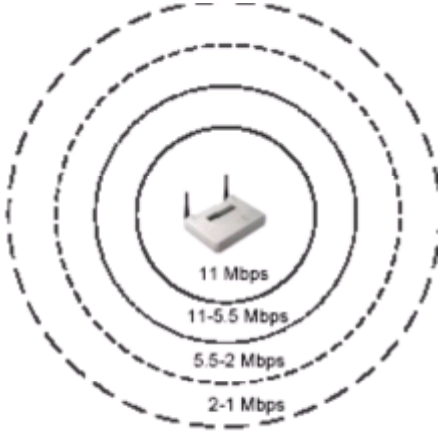
Load Balancing

- Important issue in areas of heavy traffic
- In multicell structure having heavy traffic, several co-located APs can cover the same region to increase the throughput.
- The clients having load balancing functionality configured can automatically associate with the AP that is less loaded and provides the best quality of service.



Rate Adaptation (dynamic rate shifting)

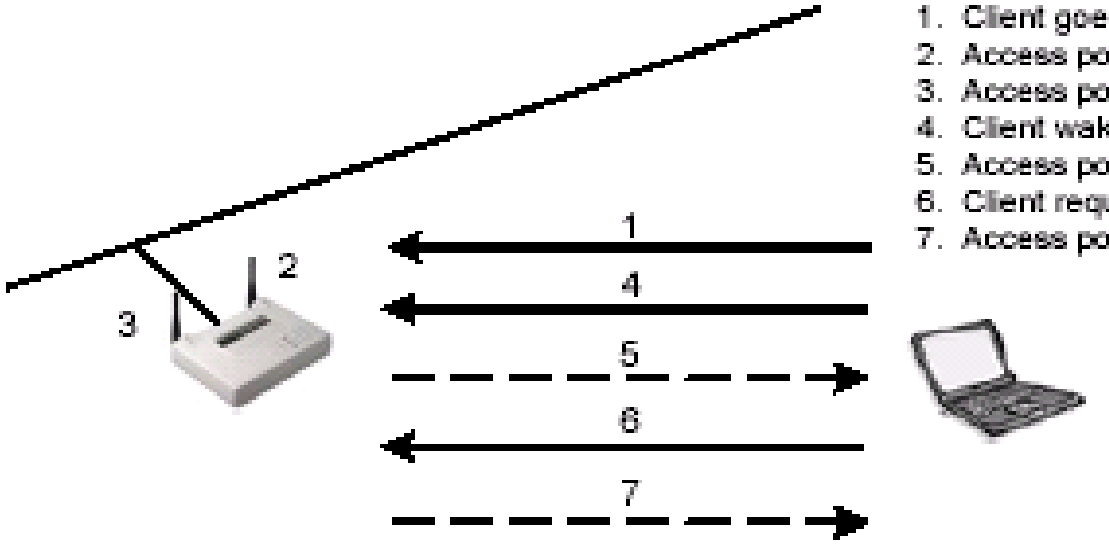
- Speed adjusted dynamically depending on the distance and the signal strength
- As the distance between the AP and the MC (Mobile Client) increases, the signal strength will decrease to a point where the current data rate cannot be maintained .
- when the signal strength decreases the transmitting unit will drop its data rate to the next lower data rate in order to maintain a reasonable SNR.



veriwave

Power Management

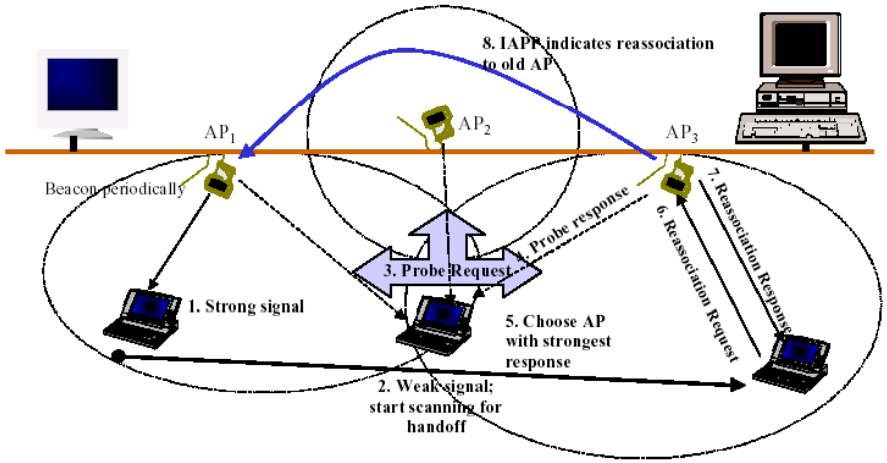
- Power save very important on battery operated 802.11 devices.
- Power-management schemes place a client in sleep mode when no activity occurs
- The MC (Mobile Client) can be configured to be in continuous aware mode (CAM) or Power Save Polling (PSP) mode.
- In the PSP mode, the client can go to sleep by informing the AP when there is no activity.
- The APs buffers any data directed to the client when the client is asleep.



1. Client goes to sleep
2. Access point marks client asleep
3. Access point buffers client packets
4. Client wakes up, notifies access point
5. Access point tells client data is waiting
6. Client requests data
7. Access point sends data

WLAN Roaming

- Roaming can be defined as the client moving between APs advertising the same or similar wireless network.
- Since the WLAN clients are mobile and coverage range of a single AP is limited, roaming happens whenever the client passes the boundaries of a WLAN cell.
- The roaming protocol should be implemented effectively in order to cause very minimal delays during the handoff.
- The clients usually make the roaming decisions by scanning the various available wireless networks at all times and trying to connect to the best available network.
- Decision to roam can be made on various factors such as RSSI, Number of missed beacons, SNR, frame errors etc..
- When a decision is made to roam the client can authenticate and associate with the new AP and continue its data communication through the new AP.
- Roaming when security is enabled would involve setting up a new security session with the new AP



veriwave

Fat AP Vs Thin AP

Fat AP Model

- Standalone APs which perform all 802.11 MAC and PHY functionalities.
- The APs pretty much work independent of each other except for limited inter-access point communication through IAPP and WDS.
- Fat APs are costly.

Thin AP Model

- The AP only performs the PHY and lower MAC layer functions like ACKing and MAC retries.
- All thin APs connect to a centralized switch and the switch performs all the upper MAC functions like client connections, security states, encryption keys, QoS policies, bandwidth management etc..
- **Advantages**
  - Manage and configure all the APs centrally through a WLAN switch/controller.
  - The AP hardware is cheaper and in large deployments this can cut a lot of cost.
  - The wireless switches can enforce network policies, network security and Quality of Service rules for applications such as IP telephony in a centralized fashion.
  - Since client connection and security state is maintained by the AP and not the switch, the clients can seamlessly roam between all the APs connected to the same switch without re-authenticating with the new AP.
  - Thin AP model allows implementation of radio resource management, load balancing, rogue AP detection etc…

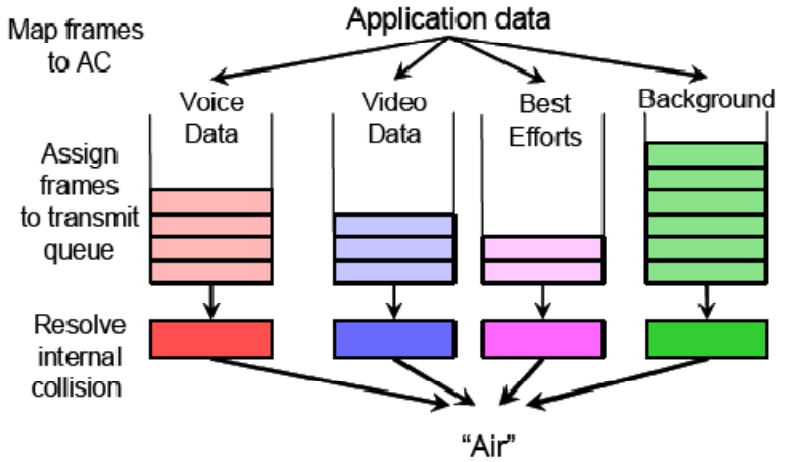
Quality of Service (802.11e)

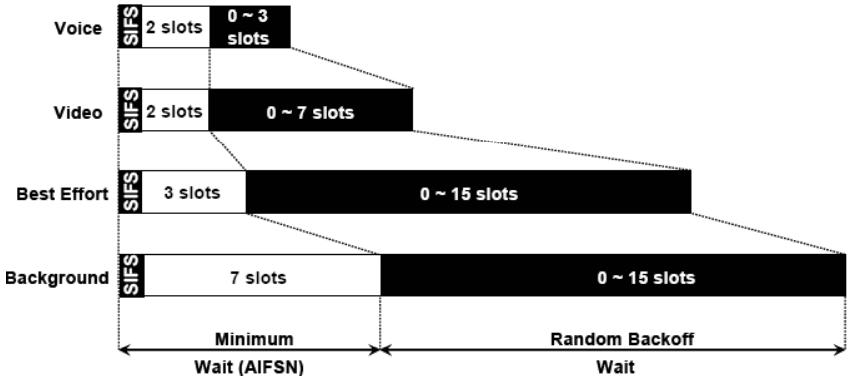
- QoS needed to support triple play traffic
- The IEEE 802.11e standard defines enhancements to support quality of service for the traditional 802.11 MAC protocol
- Introduces Enhanced Distribution Coordination Channel Access (EDCA) and Hybrid Coordination Channel Access (HCCA)

- QoS is supported with the introduction of Traffic Categories (TCs).
- In order to introduce priorities the CW sizes and IFS values are set differently for each TC.
- Each Traffic Queue within the stations contends for a transmission opportunity (TXOP) and independently starts a backoff after detecting the channel is idle for an Arbitration Inter frame Space (AIFS)

802.11e Contd…

- Each client station has 4 queues for different traffic types: Voice, Video, Best Effort and Background.
- The higher the AC, the higher the probability to transmit.
- The ACs were designed to correspond to 802.1d priorities
- The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit. Opportunity to Transmit (TXOP).
- Most AP vendors today implement the WMM spec which is EDCA only

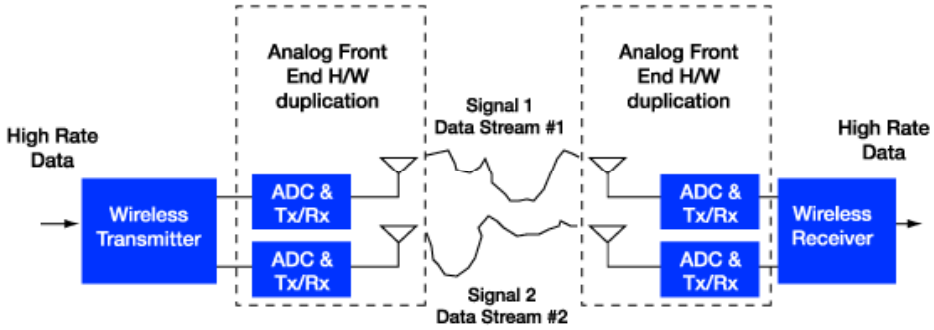




veriwave

802.11n

- The scope of TGn's objective is to define modifications to the Physical Layer and Medium Access Control layer (PHY/MAC) that deliver a minimum of 100 Mbps throughput at the MAC SAP.
- Increasing the physical transfer rate of wireless systems by using multiple antenna systems for both the transmitter and the receiver. This technology is referred to as multiple-input multiple-output (MIMO), or smart antenna systems.
- MIMO technology offers the ability to coherently resolve information from multiple signal paths using spatially separated receive antennas.
- Possible use of wider (40MHz) channels to achieve higher data rates.



- Use more complex modulation and coding techniques to improve spectral efficiency and hence increase the data rates.
- MAC layer improvements such as aggregating multiple MAC Protocol Data Units (MPDUs) into single PHY Protocol Data Units (PPDUs).
- Acknowledging multiple MPDUs with a single block acknowledgement (Block ACK) in response to a block acknowledgement request (BAR)

veriwave

A Rapidly Evolving Technology

- Fast Roaming (less than 50 msec => no call drops)
- Advanced Security
- Automatic Radio Resource Management
- Mesh Networks
- Wireless Network Management
- Wireless Access In a Vehicular Environment (WAVE)
- Roaming Across Heterogeneous Networks (802.11, 802.16, 3G, etc)
- etc.

veriwave

802.11 Standards and TGs

- 802.11a - 54 Mbps standard, 5 GHz signaling (ratified 1999)
- 802.11b - 11 Mbps standard, 2.4 GHz signaling (1999)
- 802.11c - operation of bridge connections (moved to 802.1)
- 802.11d - worldwide compliance with regulations for use of wireless signal spectrum (2001)
- 802.11e - Quality of Service (QoS) support (2005)
- 802.11f – Inter access point protocol to support roaming clients (2003)
- 802.11g - 54 Mbps standard, 2.4 GHz signaling (2003)
- 802.11h - Enhanced version of 802.11a to support European regulatory requirements (2003)
- 802.11i - Security improvements for the 802.11 family (2004)
- 802.11j - Enhancements to 5 GHz signaling to support Japan regulatory requirements (2004)
- 802.11k - WLAN system management (in progress)
- 802.11l - Skipped to avoid confusion with 802.11i
- 802.11m - Maintenance of 802.11 family documentation
- 802.11n - Future 100+ Mbps standard (in progress)

Contd..

- 802.11o – Voice over WLAN, faster handoff, prioritize voice traffic over data (in progress)
- 802.11p – Using 5.9GHz band for ITS (long range) (in progress)
- 802.11q – Support for VLAN (in progress)
- 802.11r – Handling fast handoff when roaming between APs (in progress)
- 802.11s – Self-healing/self-configuring mesh networks (in progress)
- 802.11t - Wireless Performance Prediction (in progress)
- 802.11u - Interworking with External Networks
- 802.11v - Wireless Network Management standard (in progress)
- 802.11w - Protected Management Frames standard (in progress)
- 802.11x – Summarize all 802.11 standards, but it is not a standard.
- 802.11y - Contention Based Protocol Study Group (in progress)

WLAN testing

- RF level testing
- Protocol Conformance Testing
- Performance Testing
- Interoperability Testing
- Functional Testing
- Management/Data plane testing
- Stress/Load Testing
- Scalability Testing
- Testing QoS support
- Testing security protocols
- VoIP over WLAN testing
- Testing Roaming
- Testing Rate Adaptation
- Testing mixed mode networks
- Testing for protection against security attacks
- Deployment Testing, site survey

veriwave

WLAN Performance Metrics

- **Primary Metrics**
  - Primary metrics are defined as the performance metrics that directly affect the quality of the application layer traffic.
  - R-values/MOS score, Jitter, packet loss, number of dropped calls in the case of voice
  - Connection setup time, Layer 4 through 7 throughput, latencies, frames loss etc…in the case of other application layer data traffic.
- **Secondary metrics**
  - Secondary metrics are defined as the performance metrics at layer 2 that indirectly affect the performance of any application running on the top of the layer 2 WLAN protocol.
  - Secondary metrics include, Throughput, Frame loss, latency and forwarding rate at the 802.11 layer
  - It can be argued that an AP performing well at layer 2 will perform well at all the layer above.
- **Both primary and secondary metrics are considered to be important for performance testing.**

WLAN testing today

- Mainly interoperability (Wi-Fi certification)
- Wi-Fi certification only tests for interoperability of the APs and NIC cards, which means if an AP interoperates with most of the common NIC cards with a reasonable throughput, the AP passes the certification
- No real performance testing being done, because of lack of proper performance test equipment.
- Performance Testing done using racks of real laptops running Chariot or similar traffic generators.
- No real way of synchronizing the traffic from all the laptops and hence the tests are never repeatable.
- Because of use of off the shelf equipment and protocol stacks of PCs, the test results are affected by a number of variables.
- Off the shelf equipment cannot generate traffic at full rate and hence cannot stress the DUT.
- Roaming testing done by placing laptops on carts or turn tables and moving them around which requires a lot of man hours.
- VoIP testing is being done by having real phones connect to the APs and having multiple people talk on the phones for long periods of time and providing a subjective analysis of the voice quality.
- Controlled RF environment for testing is a requirement.

VeriWave Application Classification

- **WaveTest system applications are broadly classified into five categories:**
  - Data Plane
  - Control Plane / Security
  - QoS and VoIP
  - Muni WiFi Mesh
  - Hybrid

Data Plane Applications

- Unicast Throughput
- Unicast Forwarding Rate
- Unicast Packet Loss
- Unicast Latency
- Multicast Forwarding Rate *
- Multicast Roaming *
- TCP Goodput
- Power Save Throughput

* available as script

veriwave

Control Plane / Security Applications

- Roaming Benchmark
- Roaming Stress
- Client Association Database Capacity
- AP Load Balancing *
- Connection Stress Test *
- Concurrent Connections Test *
- Thin AP Failover Test *
- 802.11 Frame Generator / Attack Generator
- AAA Server / RADIUS Authentication capacity *

* available as script

veriwave

QoS Applications

- VoIP Call Capacity
- VoIP Service Assurance
- QoS Service Differentiation *
- VoIP Roaming

* available as script

veriwave

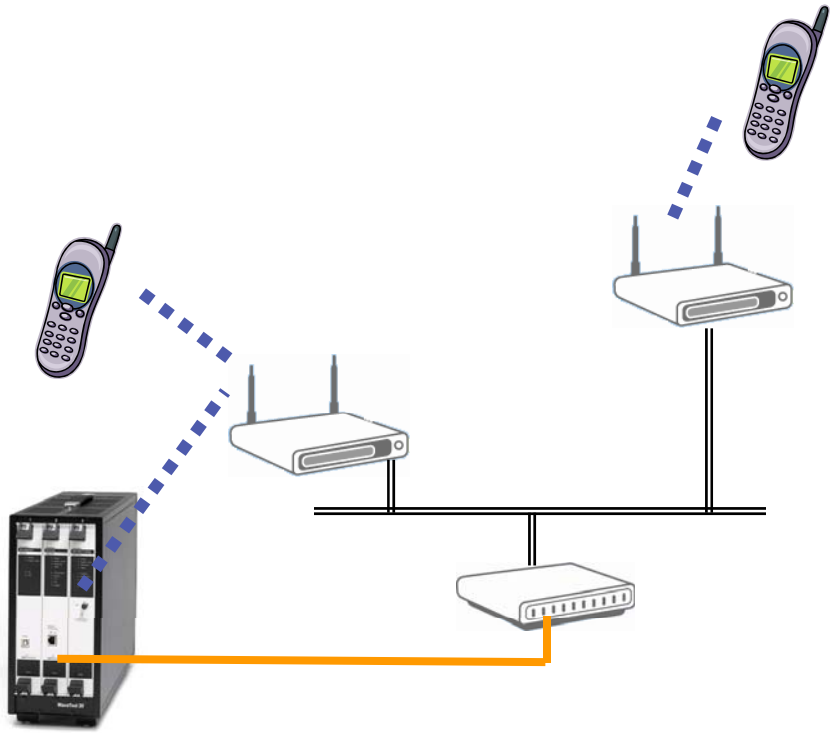
Muni WiFi Mesh Applications

- Mesh client capacity
- Mesh VoIP call capacity
- Mesh Throughput per hop
- Mesh Forwarding Rate per hop
- Mesh Latency per hop
- Mesh Backhaul Failover (self-healing)
- Mesh Backhaul Impairment Performance: Throughput
- Mesh Backhaul Impairment Performance: Latency

veriwave

802.11 Hybrid testing

- **Hybrid testing facilitates interoperability testing with WLAN 802.11 client devices**
- **Hybrid testing provides a controlled environment that allows the user to define a traffic model**
- **Key Focus Areas**
  - VoWLAN handsets
  - RFID tags
  - Laptop / PC clients
  - Mixed residential scenarios
  - Healthcare environments



veriwave

Conclusions

- WLAN technology is one of the faster growing networking technologies.
- Wireless LAN technology provides a very good business model as it uses free unlicensed frequencies and provides a wireless last hop to IP networking which is free too.
- Though WLAN protocol was initially designed for high bandwidth delay insensitive data applications, WLANs today are being used for a wide variety of traffic types and applications .
- Some of the applications of WLANs include, corporate wireless data networks, hotspots, medical facilities using VoIP over WLAN phones and badges, department stores using wireless barcode scanners, consumer electronics using wireless communications like wireless TVs, wireless cameras.
- The wide variety of applications and the sheer volume of deployments creates huge performance , scalability and QoS testing needs for the NEMS and the service providers

VeriWave's Mission

- **Enable the creation of high performance WLAN systems for mission critical enterprise and municipal wireless applications:**

  - Providing WLAN equipment manufacturers with the tools necessary to accurately analyze their products thus improving performance, interoperability, and profitability

  - Supplying service providers and enterprise users with the tools necessary to make the right choice when selecting WLAN equipment for deployment in their networks

veriwave

VeriWave's Technological Focus

- **Client Experts - stateful behavior, real 802.11 clients**
- **Loading and scalability of infrastructure devices**
- **Mobility - large scale and repeatable roaming test**
- **Technology & apps convergence**
  - Wireless and wired
  - Voice
  - QoS – prioritization, admission control, bandwidth utilization
  - Muni WiFi Mesh networks
  - Security

veriwave

VeriWave – efficiency gains & cost reductions

- **Reduce test time from days to minutes**
- **Increase test coverage**
- **Decrease time to market**
- **Reveal bugs early in QA cycle**

Minimize cost of ownership

- **Get to root cause & solve problems faster**
- **Avoid pitfalls when testing with off-the shelf clients**

Repeatability = confidence

- **Run hundreds of tests unattended**
- **Uninterrupted operation for extended periods of time**
- **Complete control over large scale deployment scenarios**

Automation – 10x more efficient

veriwave