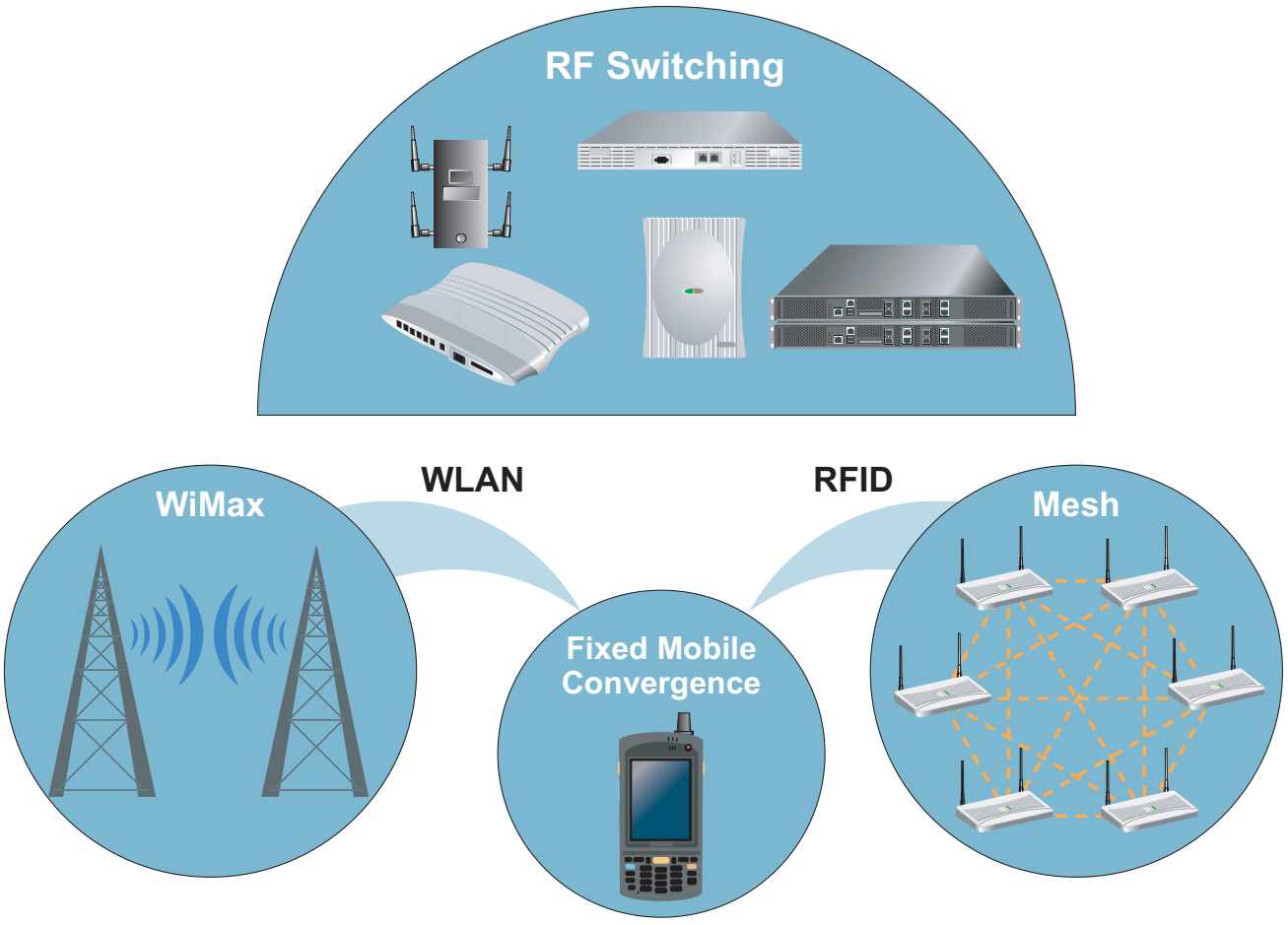
MOTOROLA

Enterprise WLAN Design Guide

Volume 1.2 March 2008



Contents

Chapter 1. Introduction

Chapter 2. WLAN Reference Architectures

Chapter 4. Understanding WLAN Connectivity

Chapter 5. Securing the Wireless Enterprise

Chapter 6. Wireless Switch Architecture

Chapter 7. Voice Over Wireless LAN

Chapter 8. Building Enterprise WLAN Solutions

Chapter 9. Canopy Systems

Chapter 10. Wireless Standards

Chapter 11. Motorola's Wireless LAN Products

Chapter 12. 802.11n

About This Guide

Preface

This guide was created to help you understand the philosophy behind Motorola's *Enterprise Wireless LAN* (EWLAN) products. This guide is intended for those interested in familiarizing themselves with the Enterprise wireless offerings available from Motorola. Additionally, once familiar with Motorola's solution set, this guide also explains how to plan and assist in the deployment of your wireless network in respect to emerging standards and technologies.

Once you have thoroughly reviewed the content of this *Enterprise WLAN Design Guide* and applied it theoretically to the new 802.11n standard (as described within *802.11n*), you will have all the pre-requisite knowledge required to plan the replacement of an existing wired network and deploy an Enterprise-class wireless network.

NOTE: Please keep in mind, successfully deploying a wireless network is directly related to successfully defining the user requirements, physical obstacles, growth expectations and emerging technologies both impacting your deployment now and in the future. The guidelines set forth within the guide will help prepare you to ask the right questions when faced with these decisions.

The graphical interfaces of Motorola's Enterprise WLAN products are designed intuitively. With just some basic knowledge of 802.11 wireless technology, you can plan, deploy and manage your infrastructure. All of Motorola's EWLAN products follow this philosophy of keeping things simple to optimize your deployment.

Motorola has observed that trying to push through your own *Command Line Interface* (CLI) is not really the best thing to do when you know there is a very strong CLI becoming a standard in the industry. Therefore, Motorola is moving its products to this type of CLI. To date, the WS5100, RFS6000 and RFS7000 are already using Motorola's proprietary *Wireless Next Generation* (Wi-NG) technology.

Document Conventions

The following conventions are used in this document to draw your attention to important information:

NOTE: Indicate tips or special requirements.

CAUTION: Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following additional notational conventions are used in this document:

- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen.
- **GUI** text is used to highlight the following:
  - Screen names
  - Menu items
  - Button names on a screen.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps not necessarily sequential
- Sequential lists (those that describe step-by-step procedures) appear as numbered lists.

1

Introduction

Installing a wireless network within an organization entails allot more then just performing a site survey. In fact, a site survey is just a small part of a wireless deployment. A better convention for the planning and deployment of wireless network is *wireless system design*.

NOTE: This guide was created to help you understand the philosophy behind Motorola's *Enterprise Wireless LAN* (EWLAN) products. This guide is intended for those interested in familiarizing themselves with the Enterprise wireless offerings available from Motorola. Additionally, once familiar with Motorola's solution set, this guide also explains how to plan and assist in the deployment of your wireless network in respect to emerging standards and technologies.

A good wireless system design entails the following:

- A site survey
  - Channel mapping
  - An understanding of the construction of the building
  - An understanding of where RF coverage is required
  - The esthetical position (corridors, isles and coverage area blockages)
- The number of users per AP
- The required throughput per user
- The distance from an AP to the LAN's entry point
- Power supply options
- Security options
- The location of the Radius Server (acceptable RTT yes/no)
- Understand if the applications are *wireless* ready

NOTE: Many protocols are designed for a wired environment where there is almost always a connection between the terminal and the server, whereas in a wireless environment the terminal can go in and out of RF coverage or go into sleep mode and loose its connection with the server.

A proper site survey is much more involved then just measuring RF coverage. That is why a more appropriate description might be *system design*. To add mobility in an Enterprise, conduct a complete wireless system design in is respect to the intended mobility features.

To design *mobility* within an Enterprise, conduct a complete wireless system design with respect to the mobility features planned.

NOTE: Please keep in mind, successfully deploying a wireless network is directly related to successfully defining the user requirements, physical obstacles, growth expectations and emerging technologies both impacting your deployment now and in the future. The guidelines set forth within the guide will help prepare you to ask the right questions when faced with these decisions.

1.1 Wireless LAN Specifications for Vertical Markets

Before anyone can design a good system, they must understand the wireless and mobility requirements for the target market. The following sections take a closer look at these requirements per vertical.

1.1.1 Mobility for the Enterprise

The advantages of Enterprise mobility include:

- Centralized management for easier deployment, management and upgrade at a lower cost
- VLAN architecture for multiple, secure entities for visitors, finance, HR etc.
- Enhanced mobility performance, *quality of service* (QoS), reliability and LAN integration
- Anytime, anywhere network access throughout a campus or facility
- Improved associate productivity and communication
- Network flexibility for workgroup and visiting associates within dynamic coverage areas
- Lower cost of deployment, and easier infrastructure scalability and maintenance

1.1.2 Mobility for Retail

The advantages of retail mobility include:

- Unique architecture enabling better wireless security
- Centralized management making it easier to upgrade and maintain networks per store
- Lower cost of deployment
- Support for new business applications, from self checkout and personalized interactive shopping assistants, to hotspot access for staff and customers
- Exceptional operating efficiencies, heightened productivity and enhanced customer service (at a lower cost of ownership)

1.1.3 Mobility for Manufacturing

The advantages of mobility in a manufacturing environment include:

- Reduced deployment, maintenance and expansion costs
- Enhanced mobility performance, quality of service (QoS), reliability and LAN integration
- Improved production efficiency, real-time data capture and transmission
- Procedures that efficiently pull materials and products through the supply chain

1.1.4 Mobility for Warehouse and Logistics

The advantages of mobility in a warehouse and logistics environment include:

- Low deployment costs, extensive network coverage and bandwidth
- Enhanced mobility performance, quality of service (QoS), reliability and LAN integration
- Better shipping efficiency, delivery and tracking, better control of materials in motion
- End-to-end management of an ever-increasing volume of goods, even when multiple vendors are involved
- Improved customer service via real-time status and faster response times to customer requests

1.1.5 Mobility for Education

The advantages of mobility for education include:

- Low deployment costs, extensive network coverage and bandwidth
- Enhanced mobility performance, quality of service (QoS), reliability and LAN integration
- Wireless access without compromising student records and other secure information
- Innovation by providing campus wide wireless access to information
- Quick, secure public access networks for conferences, alumni gatherings and other activities
- Enhanced administrative and operating efficiencies

1.1.6 Mobility for Health care

The advantages of mobility for health care include:

- Investment protection to expand the wireless network as standards and technologies evolve
- Secure voice and data application support within a centrally managed wireless network
- Protection for confidential patient information across the entire health care campus
- Improved patient care resulting from the accurate sharing of vital information among health care providers
- The most comprehensive wireless security available, including VLAN support

1.1.7 Mobility for Hospitality

The advantages of mobility for hospitality include:

- Enhanced mobility performance, quality of service (QoS), reliability and LAN integration
- Provide guests with greater convenience via faster, easier check-in/check-out including curb-side transactions
- The cutting-edge appeal of table-side ordering
- Greater accuracy, speed and efficiency for baggage tracking, housekeeping and room inspections
- Provide high-speed, secure Internet access anywhere on the property (for guests, conference attendees and staff)

1.1.8 Mobility for Government

The advantages of mobility for government include:

- Secure communications and data sharing to enhance processes, services and functions
- Military asset tracking down to the unit level
- Tactical wireless nets in theatres of operation
- Secure mobile communications in support of homeland defense
- Affordable cost of deployment and maintenance
- Data access for all military installations

1.1.9 Mobility for Airports

The advantages of mobility for airports include:

- Centralized management for easier deployment and upgrade
- VLAN architecture for multiple, secure entities (airlines, public, city etc.)
- Enhanced mobility performance, quality of service (QoS), reliability and LAN integration
- Secure, mobile communications
- Affordable cost of deployment and maintenance

1.1.10 Mobility for ISPs and Hotspots

The advantages of mobility for *Internet Service Providers* (ISPs) and hotspots include:

- Broadband services in areas lacking support or using DSL/Cable modems
- Common billing services
- Quick and cost effective scaling
- Wi-Fi standards-based for broad use
- User authentication and encryption for secure communications

2

WLAN Reference Architectures

2.1 History and Innovation

No entity has a stronger heritage in wireless than Motorola, and with the acquisition of Symbol Technologies, no one else can claim as much experience, innovation, or intellectual property in wireless communications. Motorola has been involved in RF for over 75 years, significantly longer than any of our competitors have been in business.

- Motorola's wireless communication systems were used by the Apollo astronauts when man first stepped on the Moon
- Motorola is chosen more often than any other vendor for large scale, secure mobile communications systems at international events like the Olympics, NFL games and NATO Summits
- Motorola was the 2006 winner of the National Medal of Technology - America's highest honor for innovations
- Motorola is a two time winner of Malcolm Baldrige Award - US Governments highest quality award
- Motorola is a leading provider of mobile data communications in the State & Local and Federal Markets

Symbol Technologies was the leader in WLAN innovation, with a long list of industry firsts and contributions:

- 1989: Brought to market the first commercial WLAN - the Spectrum 1
- 1993: founding members of the IEEE 802.11 committee
- 1998: Introduced the first wireless VoIP handset - the NetVision phone
- 1999: Founding member/chair of the Wi-Fi Alliance
- 2002: Invented the WLAN switch (controller) architecture
- 2007: Began shipping the industry's first RF switch (the RFS7000)

2.2 WLAN Market Leadership

Motorola is the best kept secret in WLAN infrastructure solutions. Many of our prospective customers are not aware of our position in the marketplace. If we have a weakness in our past, it certainly isn't technology, but rather our focus on marketing it.

Motorola's customer base includes many of the world's largest retailers, health care institutions, transportation companies, and manufacturers - to name a few - all of whom rely on a Motorola backbone for their mission-critical mobility needs. Billions of dollars in business is transacted across our networks every

year. If the stores or distribution centers of just one of our largest customers were to go down, there would be a very real material impact on the world economy.

A few facts:

- Over 100,000 WLAN switches sold - 2 times more than Cisco, the next closest competitor
- #1 or #2 in WLAN revenue in many key vertical markets: retail, health care, manufacturing, transportation and logistics. Bottom line: we win where we play.
- Largest WLAN deployment in the world with 100,000 APs and over 10,000 switches
- Largest wireless VoIP deployment with 40,000 Spectralink phones on our WLAN

2.3 End-to-End

Motorola provides the most comprehensive end-to-end Enterprise mobility solutions available in the market. Why is this important? CIO's increasingly like to buy from fewer and fewer manufacturers. They want fewer vendors in their account - thus, fewer necks to squeeze when there is a problem. Additionally, they want solutions that work well together, and thus are more easily managed and secured. Solutions sourced from a single vendor are far more likely to work together seamlessly.

Motorola offers solutions that span the entire range of Enterprise mobility. From where the network cable terminates, to the palm of the hand and beyond, from wireless infrastructure indoors and out, private networks and mesh technology, to mobile computing, advanced data capture, RFID, and management and security software, Motorola provides complete end-to-end Enterprise mobility solutions that no other single vendor can match.

Our competitors can easily be reduced to one-trick ponies or simply *blue wire* or *plumbing*. No one offers the industry expertise, or the breath of solutions and technology to provide true mobility.

Motorola is a leader in the various aspects of mobility: #1 in mobile computing, data capture, RFID, wireless broadband, two-way radios, and push email.

2.4 Edge Versus Core

Imagine for a minute the entire ecosystem of IT investments that one of your prospective customers will make to mobilize their business. The list is long, but it minimally includes:

> *IP Core Access Networks Clients*, *Switches*, *WLANs, Mobile Computers*, *Routers*, *Cellular, Rugged Laptops*, *Firewalls*, *WiMax and Wireless VoIP Handsets*

Motorola focuses on wireless networks and client devices. We have tremendous experience in mobility and our portfolio includes a strong set of solutions focused on the network edge. Our competitors, on the other hand, tend to focus on the core, or even worse, only a single element in the ecosystem.

To provide true mobility, a vendor must understand every piece of the mobile edge. How will your devices roam - between APs, indoors to outside, or from WLAN to WiMax? Can you manage your WLAN network and point-to-point broadband network seamlessly? How will you secure your mobile infrastructure and devices to ensure regulatory compliance and protect sensitive information?

Motorola coined the phrase *Enterprise mobility* by being the first to truly unwire the Enterprise and enhance productivity for the mobile worker. Doing so, required enormous amounts of innovation and expertise. A mobile environment requires a unique level of management, security, and control. Through a broad portfolio of wireless infrastructure solutions (not just WLAN), as well as market leadership in mobile devices, only Motorola truly understands mobility throughout the mobile edge.

2.5 Enterprise Class Versus SOHO Class Products

In terms of the differences between an Enterprise class and a typical SOHO class product:

a. Our infrastructure products are optimized to support mobile applications and devices. This includes functionality such as Pre-emptive Roaming/Load Balancing, Power Save Protocol, Virtual AP (Multi BSSID support for broadcast domain separation over the air), Proxy ARP, etc.

b. Enterprise class security including support for WPA2 (and fast roaming options such as PMK caching) and integrated AAA Server for local authentication - this precludes the need for an additional AAA / RADIUS server, lowering the cost of deploying Enterprise class Wi-Fi network in branch offices.

   We support Rogue AP detection (which none of the SOHO class product do). The AP-5131 and WS2000 also support integrated Stateful Packet Inspection Firewall and site-to-site IPSec VPN. Both products today support the provisioning and operation of secure guest access (hotspots).

c. Comprehensive remote monitoring and management capabilities including SNMP v3.

   Support for SNMP traps on various events RF health monitoring (very important for deployments in branch offices) Syslog with different log levels

d. Features that support auto update of configuration / Firmware files (again, very important for deployments and management in branch offices).

e. QoS support and support for evolving standards such as *Wi-Fi Multimedia* (WMM). Our infrastructure also supports packet prioritization and wireless bandwidth management. We have SpectraLink VIEW and Avaya DevConnect certification. The WS2000 supports SIP Call Admission Control. None of the SOHO products can lay claim to supporting voice with QoS.

f. The WS2000 supports up to 6 access ports; 200 MUs per switch. A WS5100 is capable of supporting up to 48 APs. Most SOHO class products pale in comparison in terms of performance.

g. Wired network integration (WLAN - VLAN mapping and auto assignment of VLAN IDs based on user authentication). We also map wired network prioritization as well (802.1p; DSCP).

h. Ruggedized design (of APs). Support for multiple antenna options.

i. Support for wireless bridging / mesh (AP-5131 currently supports it today)

j. High MTBF (>60,000 hours)

k. The backing of Motorola Services for extended product services/warranty, technical support, advanced exchange, etc

2.6 Inside Out

Motorola has the strongest and most-complete portfolio of wireless infrastructure solutions for inside and outside the *four walls*. Motorola has an advantage with customers that have outdoor wireless requirements (point-to-point connectivity, outdoor or campus-wide coverage, seamless connectivity indoors and out). Our outdoor broadband products and mesh capabilities are the best in the industry. The Canopy product line is a solid number one in the unlicensed broadband market. The ability for a customer to go with one vendor for both indoor and outdoor connectivity makes Motorola the clear leader in this space. For more information on Motorola's Canopy line, see *Canopy Systems on page 9-1*.

2.7 Differentiators

Differentiators for Motorola's WLANs include:

- *Lower Cost of Ownership*
- *Redundancy and Business Continuity*
- *RF Switching*
- *Wireless Intrusion Detection*
- *End-to-end Design and Management*
- *Voice Capabilities*
- *Ease of Use*

2.7.1 Lower Cost of Ownership

Motorola provides a reliable, scalable infrastructure and cost-effective infrastructure solution. Other vendors often hide costs, initially positioning features and functionality that is separately licensed. With Motorola, there are no hidden costs. Combine that with our smart licensing and zero-port licensed switches for competitive price points.

Included at no-extra cost:

- On-board firewall support
- VPN endpoints
- IDS / rogue detection
- A locationing engine
- *Adaptive AP* (AAP) support
- Hotspot / guest portal support

NOTE: Be sure your customers are comparing apples to apples when showing them the low cost of our products. Our competition has been known to *bait and switch,* effectively hiding the cost of additional features up front.

2.7.2 Redundancy and Business Continuity

Only Motorola offers wireless redundancy in a cost-effective manner. Support for multiple levels of redundancy and failover capabilities ensure an *always on* highly available network for superior performance.

- Zero port licensed switches, redundancy without the cost of a fully licensed switch
- Load balancing utilizes redundant switches in day-to-day operation to take advantage of the otherwise unused capacity
- Switch clustering combines two or more switches into a single management point to provide failover and unmatched capacity

2.7.3 RF Switching

Having strong investments in a wide variety of wireless technologies is a strong differentiator for Motorola. While our competitors offer only WLAN, Motorola can provide infrastructure solutions across a multitude of standards: Wi-Fi, RFID, WiMax, UWB, etc.

Motorola's RFS7000 (first launched in 2007), provides a scalable platform that supports multiple RF technologies, not just 802.11. This gives our customers the ability to manage multiple wireless networks with a single switch, thus providing investment protection as an alternative to rip and replace. The ability to easily upgrade the system to support new standards and features and to scale to meet capacity requirements as a company grows ensures the system you sell your customers today can continue to meet their needs tomorrow.

2.7.4 Wireless Intrusion Detection

AirDefense (recently acquired by Motorola) is the market leader in wireless security. They pioneered the *wireless IPS* (WIPS) market, own much of its intellectual property. The WIPS solution is the best-in-class wireless security product available, and provides a very strong differentiator for our infrastructure.

Highlights of the Wireless IPS product include:

- Proactive identification and correction of weaknesses - before a problem occurs
- Instant identification and notification of security breaches enables an immediate response, effectively minimizing the damage that can be caused by rogue devices to attacks
- Easy to scale, ensuring continued and uninterrupted monitoring regardless of company growth
- Easy to upgrade, ensuring protection against the latest viruses and other attacks
- Easy to manage, providing increased security without a significant increase in IT time or cost

WIPS should be strongly positioned when customers are concerned about wireless security - especially health care, retail, government, and financial customers

2.7.5 End-to-end Design and Management

One-stop shopping for all your wireless LAN requirements - from our planning and design tools, to hardware, management and security (including wireless intrusion protection). And we offer the ability to take the files created in LANPlanner and port them into the *RF Management Suite* (RFMS) application.

Only Motorola offers a package that allows a customer to plan, validate, manage and secure their wireless LAN from one vendor.

2.7.6 Voice Capabilities

Motorola's solutions are purposefully built from the ground up to handle voice as well as data. Some vendors claim to have great voice, but in the real-world, Motorola's WLAN solutions are handling voice very well for customer like Lowe's.

Motorola offers a complete fixed-mobile convergence solution (including the device) which allows seamless roaming across WLAN and cellular networks. No other vendor has such a complete solution.

2.7.7 Ease of Use

Certified Wireless Network Professionals (CWNP) rated Motorola the easiest to deploy and use. Our user interfaces are very user friendly, in numerous cases resembling Cisco's interface.

Motorola's wireless switch systems offer patented *Motorola-only* mobility features designed to manage the unique challenges mobility presents. For example, pre-emptive roaming and load balancing work hand-in-hand to ensure users roam before the wireless connection erodes. Virtual AP provides broadcast domain separation over the air improving security and manageability of wireless LAN traffic, and also works together with *Power Save Polling* (PSP) to optimize the battery life of client devices.

2.8 Motorola on Motorola Advantages

Motorola on Motorola is a term that describes the use of Motorola hand helds within a Motorola WLAN infrastructure. Since the creation of the standards body, many customers (even Motorola employees) feel equipment that is standards based can work perfectly with other standards based equipment. To a degree this is true, but much of the focus of the standards body is not at the level Motorola needs it to be. Many features have been enhanced to allow better performance within a complete end to end Motorola installation. They include:

2.8.1 Advanced Load Balancing

Motorola wireless clients maintain a table of APs in their vicinity and log their respective load information. The AP passes on the loading information to the clients. To keep this table up-to-date, Motorola wireless clients do periodic full scans. This table is then used to make roam decisions to better spread the load on one AP to other APs in the vicinity.

Motorola clients use a sophisticated load-balancing algorithm when too many clients attempt to connect to a particular access point. The clients use a beacon element to perform pre-emptive roaming and load balancing, thereby *moving* from a heavily loaded AP to one that is less loaded.

Motorola's wireless switch systems allow wireless devices to roam to a less busy access port when the existing connection quality deteriorates due to excessive network traffic. The switch sends load information to wireless devices so dynamic load-balancing decisions can be made when needed. The wireless switch facilitates fast roaming within a WLAN, to maintain real-time voice and data connections and application performance. The switch sends information used by wireless devices to make roaming decisions before the existing connection deteriorates.

Motorola's wireless switch products can be configured with maximum thresholds that govern the number of devices that can be connected to each AP; therefore ensuring no one AP is overloaded and any new devices will have to find a less busy access point connection.

Dynamic load balancing is accomplished by including load indicators in the beacons sent by APs (as directed by wireless switch). Two types of load indicators are sent: Symbol/Motorola proprietary as well as 802.11e standard specific.

Motorola wireless clients can use this load balancing information to auth/associate with the AP best suited based on load and RSSI.

The elements used in Symbol/Motorola Proprietary mechanism include 2 byte: Kbps (traffic load indicator) and 2 byte: MU Count.

The QBSS load element used in 802.11e includes 1 byte: air channel utilization % and 1 byte: MU count.

NOTE: The only restriction for load balancing is that it works only when clients make use of the fields for load balancing.

2.8.2 Pre-Emptive Roaming

Clients roam to the best available access port/point based on the information sent by the switch. Clients also attempt to automatically load balance across access points based on the load balance element in the frame sent by the AP.

The roaming mechanism implemented on Motorola wireless products (mostly on the client, with support on the AP) was designed to meet the mobile requirements of handheld wireless device users. The idea is that the choice of the new AP is made before the existing connection is lost or deteriorates too much. A typical 802.11 device, scans every channel (full scan) after it loses its existing connection to find new APs and blindly roams to a new AP irrespective of the quality of new connection. Motorola clients use the RSSI, percentage of missed beacons, and drop in RSSI as thresholds (hard-coded in firmware) to indicate deterioration of service. If at anytime, the existing connection deteriorates below any of these thresholds, the Motorola wireless clients supplant the roam by doing a full scan before it actually loses its connection. In fact, these thresholds are high enough so a minimum level of service is maintained at all times. During a full scan, Motorola wireless APs forward load information in the proprietary part of the 802.11 frame. Therefore, clients can make educated decision on which AP to initiate a roam with.

The benefits of pre-emptive roaming and secure fast roaming can also be extended to clients roaming across a campus (or IP domains). The overlay architecture of the wireless switch and AP300, allow for seamless roaming across each building in the campus. Since device traffic from each building (IP domain) is tunneled back over the access port to the wireless switch, devices moving from one building to another (or one IP domain to another) do not need to renew their IP addresses and continue to communicate with a disruption in service. Roam times of <50ms can be maintained even when roaming across IP domains.

2.8.3 Client Assisted Rogue AP Detection

Motorola clients provide information to the infrastructure on the APs they see as they roam across the network. This provides better visibility to any rogues devices that might jeopardizing security in the network.

2.8.4 Security Optimizations

Network Time Synchronization (NTP) allows Motorola clients to automatically synchronize system time with the network allowing for 802.1x authentication.

2.8.5 Hyper Fast Secure Roaming

Hyper Fast Secure Roaming (HFSR) is roaming on a switch that is faster than 802.11r and WPA2 for all security mechanisms (including non credential caching authentication). If a client is authenticated and remains on a current switch, no re-authentication is conducted between APs.

Key features (differentiators) of HFSR include:

- Motorola's Enterprise WLAN products support a patented proprietary extension to the current IEEE 802.11i specification known as HFSR.
- This mechanism off loads the key handshake mechanism used by 802.11i encryption standards resulting in *hyper-fast* seamless roaming

- Handshake messages are used to derive a new *Pairwise Transient Key* (PTK) and *Group Transient Key* (GTK)
- HFSR overloads 802.11 association messages between the mobile client and the AP to carry out the handshake mechanism
- The entire roam is carried out without doing *EAP over LANs* EAPOL key handshake messages. thereby improving roaming handoff times (making it ideal for voice applications)

The current 802.11i standard defines two ways to perform fast roaming; PMK key caching and pre-authentication. Most vendors support an extension to PMK key caching known as opportunistic PMK key caching. The drawbacks of these three standards include:

- No support for Pre-shared key Authentication
  - 802.1x supplicant is not available on all clients
  - 802.1x Radius is not a viable option always
  - 4-way or 6-way EAPOL key handshake still needs to be performed
  - Not desirable for VOIP Applications
  - Not power save friendly

2.8.5.1 Theory of Operation

Motorola Enterprise WLAN products support HFSR within their 802.11 management frames. Motorola clients add a proprietary HFSR *Information Element* (IE) in the 802.11 re-association request containing the current PTK hashed (HMAC-SHA1).

The wireless switch verifies the validity of the PTK and adds the proprietary HFSR IE in the 802.11 association response containing HFSR roam status and new GTK and *Receive Sequence Counters* (RSC).

Both GTK and RSC are encrypted using the underlying encryption method in the association request (RC4 or AES-CCMP). MUs decrypt the new GTK and RSC and continue to use the current PTK and the new GTK.

A user configurable PTK validity life time is provided to prevent PTK from being compromised

For 802.1x MUs, user configurable re-authentication intervals ensure the PTK cache lifetime is controlled. This 802.1x Re-Authentication option is already available on all Motorola WLAN Products.

Non HFSR compliant MUs are allowed to co-exist in Motorola's HFSR enabled infrastructure, since the wireless switch invokes the HFSR only if initiated by the MU.

2.8.5.2 Advantages of HFSR

Key advantages of HFSR include:

- Hyper fast roam times can be guaranteed, making HFSR an ideal choice for voice applications requiring WLAN infrastructure
- Fewer message exchanges make HFSR very less susceptible to roam failures
- HFSR is secure since it extends the existing 802.11i standard to a level higher
- HFSR has a user configurable key life time
- HFSR is an authentication independent solution - rendering 802.1x as not mandatory
- No configuration modifications are required on the client side, all control resides on a centrally managed wireless switch or wireless switch cluster

2.8.6 Voice Optimization

Smart scans reduce the amount of scanning time from the AP. Using voice load balancing, an AP supplies load information in the access category of the beacon. With optimized load balancing, abbreviated AP back-offs for voice devices are identified via a WNMP message.

2.8.7 Location Optimizations

Radios can be configured with custom messages. Any MU that associates with that radio is provided with that message.

- All Motorola WLAN Products shipping today support a legacy Motorola proprietary element in the 802.11 management frames
- The purpose of this proprietary element is to ensure MUs use the advertised information in the proprietary element to make intelligent roaming decisions
- The Motorola proprietary element ensures roam quality, not roam speed, as roam speed doesn't always guarantee an optimal user experience if the roaming decision is flawed
- The proprietary element facilitates load balancing based on:
  - Client capacity per AP
  - RF activity and bandwidth usage per AP
- MUs use advertised values in the proprietary element to perform pre-emptive roaming.

3

Wireless System Design Methodology

Motorola's development methodology is largely based on standards. The firmware is all Wifi and IEEE standards based. For a thorough review of the 802.11 standards supported by Motorola in the development of their wireless infrastructure offerings, refer to *Wireless Standards*.

Motorola also uses non-standard based mechanisms (when needed) to add mobility enhancements. However, Motorola only uses non-standard development strategies when a standard does not yet meet the needs of the mobile workforce.

Before you can dive into the philosophy behind the Motorola's wireless products, you need to understand the following:

3.1 Where to Start the Design?

Focus on determining the following key elements when qualifying a design:

3.1.0.1 Cover the Basics!

Review the current wireless environment:

- Is wireless deployed today?

  If wireless is already deployed, don't stop there. Many deployments require upgrades or refreshes of an existing network.
- Where is wireless deployed?
- How long ago was it deployed?
- What applications are currently being used?
- What vendor was used?
- Are there any issues with the current deployment (coverage, roaming, management)?
- Does the network require upgrade to support future applications (voice)?

3.1.0.2 What is Needed with Wireless in the Future?

Review the requirements of the wireless network in respect to scalability and the future goals.

- What will the future applications for wireless be?
- Is the customer looking at any of the following technologies on their wireless network?
  - Locationing
  - Voice
  - Guest access

  - RFID
  - Security and PCI
- Is there a requirement for outdoor coverage?

3.1.0.3 What are the Security Requirements?

Assess the data protection requirements of the wireless network.

- What are the wireless security policies?
- What regulatory compliance (PCI, HIPPA etc.) agencies are involved?

3.1.0.4 What is the Size of the Deployment?

Assess the physical size of the intended coverage area.

- How many facilities will be deployed?
- Approximately how many square feet require coverage?

3.1.0.5 What is the Business Problem?

Define the needs of the business to better gauge their network deployment considerations.

- What mobile business process and applications are they seeking to deploy, and why? Understand the customer business needs, and if mobile devices will be required

  Highlight Motorola's strong understanding of mobile applications, focus on end-to-end solutions that enable faster development and deployment of applications, and 30 years of Enterprise mobility experience.

  When deploying applications with mobile devices, have they considered the post deployment issues (such as battery life and day-to-day management?

- Remind the customer of Motorola's Enterprise mobility leadership!

  Emphasize Motorola's leadership position and 30 years of experience in Enterprise mobility as well as those mobility features that extend battery life, enhance device performance and enable fast roaming without using proprietary technology. Highlight how both the client devices and wireless infrastructure can be centrally managed using MSP to significantly reduce management costs and lower total cost of ownership (TCO).

- What are the customer's main security issues (examples include PCI, HIPAA, Sarbanes-Oxley and other regulatory compliance; rogue devices; data security; secure guest access)? Understand the customer's security needs in order to direct them towards the right solution

  Emphasize Motorola's end-to-end security, which allows data to travel securely from the end-user device all the way to application. Tout built-in IDS capability that does not impact performance as well as a dedicated centralized WIPS system providing comprehensive security and compliance reporting (VISA CISP, HIPAA, Sarbanes-Oxley).

- Is the customer facing significant cost pressures in terms of providing voice (cellular) services to employees? Direct the customer towards fixed/mobile convergence (FMC) and Motorola's strengths in this area

  FMC can provide significant cost savings to Enterprises by migrating cellular calls that typically cost 9 cents per minute to Voice over WLAN, which costs about 1 cent per minute.

3.1.0.6 Determine the Specifics of the Design!

Define the particulars of the customer's network.

- Is the customer planning to deploy *voice over WLAN* (VoWLAN)?

  Highlight Motorola's experience dating back to 1998 in VoWLAN including pioneering the technology, as well as one of the world's largest VoWLAN deployments at Lowes with 45,000 SpectraLink phones. Motorola has demonstrated higher voice capacity than competing solutions with a lower TCO. Highlight end-to-end QoS support with WMM and call admission control. Gain credibility by highlighting strong eco-system of telephony partners including Avaya, SpectraLink, Nortel and Siemens enabling the extension of desk phone features and functionality to mobile voice and data devices.

- Is the customer deploying or considering RFID applications in the future? Determine whether or not to position RF switching, and plant the seed for future expansion options.

  Position Motorola's long history of innovation leadership in wireless networking. Motorola has announced the industry's first RF switching architecture that allows customers to easily take advantage of emerging RF technologies such as RFID, WiMAX, mesh and fixed/mobile convergence - without having to rip and replace their infrastructure or purchase and manage disparate networks.

- How many locations will need wireless? Uncover the level of management complexity.

  *Highlight Motorola's experience, with the world's largest multi-location Enterprise wireless deployment with 10,000 switches and 100,000 access points at Wal-Mart, and the benefits Wal-Mart receives through our centralized management s*olution.

- How much time does the customer typically spend deploying and troubleshooting networks?

  Position Motorola's comprehensive management suite. Highlight Motorola's complete set of management solutions: RF Management Suite (RFMS) for planning, MSP for easy roll-out and ongoing management of large deployments, and WIPS for comprehensive security.

- Does the customer have plans to provide wireless coverage outside the four walls or in other hard to wire places?

  Direct the customer towards Motorola's bridging/meshing capabilities. Highlight mesh capabilities in AP-5131 and switch-assisted mesh. Share our mesh white paper with the customer.

- Does the customer have adequate IT staff to deal with all the complexities of remote network and device management?

  Emphasize the advantages of Motorola's management solutions and how they work together. Cover Motorola RFMS for planning, MSP for easy roll-out and ongoing management of large deployments, and WIPS for comprehensive security.

- What level of redundancy is required?

  Motorola provides 1-to-1 (Active-Standby or Active- Active) and cluster-based 1-to-many redundancy. Some competitors require a dedicated management server in a cluster, which increases the total cost of ownership.

- What are the specifics of the coverage environment - how many locations are there? How many employees will need service at each of the locations? In general, what is the size of the opportunity?

  Highlight Motorola's broad wireless LAN infrastructure, which can meet any need cost-effectively - from a large campus-style headquarters to a series of branch offices, a series of offices around the world, or a small retail shop.

3.1.0.7 What is the Technical Environment?

Define the existing infrastructure.

- What are the systems in place?

  Discuss partnerships and alliances with major ERP and hardware providers, such as IBM, Intel, Microsoft, Oracle, SAP and Zebra - and the benefits. Cover ease of integration with their existing applications, and flexibility to implement new leading applications as needed to support the business today and in the future.

3.2 Site Surveys

Motorola's LANPlanner enables you to:

- Create design plans
- Simulate network traffic
- Perform site surveys for 802.11a/b/g/n networks.

By accounting for the number of users, the deployment environment and the applications in use - including wireless voice over IP - LANPlanner recommends equipment placement and density for optimal performance and provides site survey tools for network validation and troubleshooting.

3.2.1 Creating Network Design Plans

Place access points and sensors and predict how RF will perform in the deployment environment.

Rapidly load AutoCAD, PDF, JPEG, and any common building or site map file format and create a reusable, extensible RF-intelligent model.

Graphically visualize the physical location and configuration of all installed network equipment activity.

Automatically generate bill-of-materials and maintenance records for use by deployment teams and in future network expansion

3.2.2 Customizing Equipment Parameters

LANPlanner comes pre-installed with access points and hundreds of antenna options.

Add, configure or change access points and antennas to meet the unique deployment requirements

3.2.3 Automated Placement Recommendations

Define application throughput requirements and LANPlanner will make recommendations for the placement and settings of access points or sensors.

NOTE: With LANPlanner's measurement module, users are able to collect RF information and client performance statistics to improve the quality of their wireless models.

3.2.4 Importing Site Survey Data

By integrating site survey data into the network plan, users can compare the actual RF loss values in their deployment with the planned values and automatically adjust the deployment model.

Verify post-deployment network performance and visualize heat maps of measured data

Review QoS critical information such as *Received Signal Strength Intensity* (RSSI), *Signal to Interference Ratio* (SIR), *Signal to Noise Ratio* (SNR) and data rates

Reduce the cost of ownership of wireless networks by eliminating costly rework that frequently occurs with measurement-based network design.

As part of the RF Management Suite, LANPlanner seamlessly integrates with network management software for visualizing, troubleshooting and maintaining the quality of service built into the design plan.

3.2.5 Management Software Integration

Open network design plans within Motorola RFMS. Verify ongoing network performance and visualize heat maps of live data. Identify areas with changes to user-defined parameters such as signal strength, noise or SIR.

4

Understanding WLAN Connectivity

4.1 How MUs Associate to an Access Point

Whether a MU is associating to an AP-5131 or an AP300 (connected to a wireless switch), the MU association process remains the same. In fact, to make the association process as transparent as possible, the association process is almost 100% standards based.

However, an MU's decision to choose an AP can be made using some additional proprietary mechanisms in the AP's beacons and the driver in the MU radio.

For security, extra functionality should be added to the wireless switch to control if an MU has WLAN access, based on a user's credentials, time, or other parameters in respect to business needs.

Lets take a closer look at how an MU associates to an access point (with or without security) and the additional Motorola advantages designed to optimize the association process.

4.1.1 The MU Association Process

The MU association process can be viewed (at a high level) as the following sequence of device interactions:

- MU -> probe request -> AP
- AP -> probe response -> MU
- MU -> authentication request -> AP
- AP -> authentication response ->MU
- MU -> association request -> AP
- AP -> association response -> MU

4.1.1.1 Probe Requests

A probe request is a broadcast message serving the following two functions:

- A probe for the ESSID needed for connection
- A probe for the supported data rates of the AP targeted for connection

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        63
  Timestamp:            12:46:22.134064000 04/21/2008
  Data Rate:            2   1.0 Mbps
  Channel:              11  2462MHz  802.11bg
  Signal Level:         77%
  Signal dBm:           -41
  Noise Level:          12%
  Noise dBm:            -88
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %0100  Probe Request
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:18:DE:07:71:75
  BSSID:                FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Seq Number:           442
  Frag Number:          0
802.11 Management - Probe Request
SSID
  Element ID:           0  SSID
  Length:               8
  SSID:                 Motorola

Supported Rates
  Element ID:           1  Supported Rates
  Length:               8
  Supported Rate:       1.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       2.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       5.5  Mbps  (Not BSS Basic Rate)
  Supported Rate:       11.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       6.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       9.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       12.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)

Extended Supported Rates
```

```
  Element ID:           50  Extended Supported Rates
  Length:               4
  Supported Rate:       24.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       36.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       48.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       54.0  Mbps  (Not BSS Basic Rate)

Vendor Specific
  Element ID:           221  Vendor Specific
  Length:               7
  Value:                0x00034701020101

FCS - Frame Check Sequence
  FCS:                  0xFA04739F
```

4.1.1.2 Probe Responses

A probe response has almost the same information as a beacon, the only difference is a beacon is a broadcast message and a probe response is a unicast message to the terminal initiating the probe request.

The following values should be considered in a probe response:

- Supported data rates form the AP point of view
- SSID
- Country ID this is the support of 802.11d
- QBSS load to support 802.11e
- ERP information to support 802.11b/g

NOTE: When WPA2/CCMP (802.11i) is enabled, there is an extra element in the probe request called *Robust Security Network* (RSN).

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        104
  Timestamp:            12:46:22.135419000 04/21/2008
  Data Rate:            2   1.0 Mbps
  Channel:              11  2462MHz  802.11bg
  Signal Level:         70%
  Signal dBm:           -46
  Noise Level:          12%
  Noise dBm:            -88
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %0101  Probe Response
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             320  Microseconds
  Destination:          00:18:DE:07:71:75
  Source:               00:15:70:65:A3:60
  BSSID:                00:15:70:65:A3:60
  Seq Number:           290
  Frag Number:          0
802.11 Management - Probe Response
  Timestamp:            202193454  Microseconds
  Beacon Interval:      100
  Capability Info:      %0000010000000001
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
                        .....1.. ........ G Mode Short Slot Time [9 microseconds]
                        ......0. ........ QoS is Not Supported
                        .......0 ........ Spectrum Mgmt Disabled
                        ........ 0....... Channel Agility Not Used
                        ........ .0...... PBCC Not Allowed
                        ........ ..0..... Short Preamble Not Allowed
                        ........ ...0.... Privacy Disabled
                        ........ ....0... CF Poll Not Requested
                        ........ .....0.. CF Not Pollable
                        ........ ......0. Not an IBSS Type Network
                        ........ .......1 ESS Type Network
```

```
SSID
  Element ID:           0  SSID
  Length:               8
  SSID:                 Motorola

Supported Rates
  Element ID:           1  Supported Rates
  Length:               8
  Supported Rate:       1.0  Mbps  (BSS Basic Rate)
  Supported Rate:       2.0  Mbps  (BSS Basic Rate)
  Supported Rate:       5.5  Mbps  (BSS Basic Rate)
  Supported Rate:       11.0  Mbps  (BSS Basic Rate)
  Supported Rate:       6.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       9.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       12.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)

Direct Sequence Parameter Set
  Element ID:           3  Direct Sequence Parameter Set
  Length:               1
  Channel:              11

Country
  Element ID:           7  Country
  Length:               6
  Country Code:         USI
  Starting Channel:     1
  Number of Channels:   11
  Max Tx Power (dBm):   30

QBSS Load
  Element ID:           11  QBSS Load
  Length:               5
  Station Count:        0
  Channel Utilization:  0x05  %
  Avail Admission Capacity:2365

ERP Information
  Element ID:           42  ERP Information
  Length:               1
  ERP Flags:            %00000000
                        x... .... Reserved
                        .x.. .... Reserved
                        ..x. .... Reserved
                        ...x .... Reserved
                        .... x... Reserved
                        .... .0.. Not Barker Preamble Mode
                        .... ..0. Disable Use of Protection
                        .... ...0 Non-ERP Not Present
```

```
Extended Supported Rates
  Element ID:           50  Extended Supported Rates
  Length:               4
  Supported Rate:       24.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       36.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       48.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       54.0  Mbps  (Not BSS Basic Rate)

Symbol Proprietary
  Element ID:           173  Symbol Proprietary
  Length:               15
  OUI:                  0x00-0xA0-0xF8
  Number of clients:    0
  Load (kbps):          256
  Load (kpps):          2560
  Tx power:             0
  ntp time:             0

FCS - Frame Check Sequence
  FCS:                  0x20CA42DB
```

The Symbol proprietary element is present to help Motorola MUs make a better decision as to which AP to roam to.

Symbol proprietary extensions define:

`Number of clients:  0`

Ensures an equal number of MUs are attached to APs as seen from the MU's point of view.

`Load (kbps):  256`

Indicates the throughput of the AP during the probe request. Very important metric for defining the QoS.

`Load (kpps):  2560`

Indicates the amount of packets per second the AP is processing during the probe request. Very important metric for defining the QoS.

`Tx power:  0`

This parameter is for advanced power control over the MU. It is not good when an AP is set to 1mW and all the MUs are still operating at 100mW. In this case, the MU will suppress the AP signal and there is instability in terms of associated users on respective APs.

`ntp time:  0`

This is a time field used to update MU time. This option is very important when the auto deployment of MUs is requested in combination with authentication. Authentication is always time based, and not all MUs are have the current time when deployed out-of-the-box. Therefore, this parameter ensures the MU can adopt to the WLAN's time.

4.1.1.3 Authentication

The authentication portion of the association process is not in parallel with 802.11i, as 802.11i process kicks in after association.

Authentication produces the following:

- *Authentication algorithm number* - When this is zero there is open authentication or no authentication at all. When this is one, there is shared authentication. This means that the MU and AP will follow a protocol of hashing a text with the shared WEP key to find out if they are who they say they are. Better Authentication methods are available today in the form of 802.11i.
- *Authentication Transaction Sequence Number*
- *Status Code* - Provides feedback on the progress of the selected authentication method.

NOTE: De-authentication is often used in IPS systems. De-authentication is a much more aggressive way to *kick* a rogue MU form the network then de-association.

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        34
  Timestamp:            12:46:22.164458000 04/21/2008
  Data Rate:            108 54.0 Mbps
  Channel:              11  2462MHz  802.11bg
  Signal Level:         77%
  Signal dBm:           -41
  Noise Level:          12%
  Noise dBm:            -88
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1011  Authentication
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             44  Microseconds
  Destination:          00:15:70:65:A3:60
  Source:               00:18:DE:07:71:75
  BSSID:                00:15:70:65:A3:60
  Seq Number:           442
  Frag Number:          0
802.11 Management - Authentication
  Auth Algorithm:       0  Open System
  Auth Seq Num:         1
```

```
  Status Code:          0  Reserved
FCS - Frame Check Sequence
  FCS:                  0x09F51EA5
```

4.1.1.4 Association Requests

An association request consists of four important elements:

- *Capability Information* - tells what the MU is capable of, e.g. roaming, short preamble, Privacy,...
- *Listen interval* - used in relation to power save management and DTIM
- *ESSID*
- *Supported Rates and Extended Supported Data Rates*

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        58
  Timestamp:            12:46:22.167495000 04/21/2008
  Data Rate:            108 54.0 Mbps
  Channel:              11  2462MHz  802.11bg
  Signal Level:         77%
  Signal dBm:           -41
  Noise Level:          12%
  Noise dBm:            -88
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %0000  Association Request
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             44  Microseconds
  Destination:          00:15:70:65:A3:60
  Source:               00:18:DE:07:71:75
  BSSID:                00:15:70:65:A3:60
  Seq Number:           443
  Frag Number:          0
802.11 Management - Association Request
  Capability Info:      %0000010000000001
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
```

```
                        .....1.. ........ G Mode Short Slot Time [9 microseconds]
                          ......0. ........ QoS is Not Supported
                          .......0 ........ Spectrum Mgmt Disabled
                          ........ 0....... Channel Agility Not Used
                          ........ .0...... PBCC Not Allowed
                          ........ ..0..... Short Preamble Not Allowed
                          ........ ...0.... Privacy Disabled
                          ........ ....0... CF Poll Not Requested
                          ........ .....0.. CF Not Pollable
                          ........ ......0. Not an IBSS Type Network
                          ........ .......1 ESS Type Network

    Listen Interval:      10
SSID
    Element ID:           0  SSID
    Length:               8
    SSID:                 Motorola

Supported Rates
    Element ID:           1  Supported Rates
    Length:               8
    Supported Rate:       1.0  Mbps  (BSS Basic Rate)
    Supported Rate:       2.0  Mbps  (BSS Basic Rate)
    Supported Rate:       5.5  Mbps  (BSS Basic Rate)
    Supported Rate:       11.0  Mbps  (BSS Basic Rate)
    Supported Rate:       6.0  Mbps  (Not BSS Basic Rate)
    Supported Rate:       9.0  Mbps  (Not BSS Basic Rate)
    Supported Rate:       12.0  Mbps  (Not BSS Basic Rate)
    Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)

Extended Supported Rates
    Element ID:           50  Extended Supported Rates
    Length:               4
    Supported Rate:       24.0  Mbps  (Not BSS Basic Rate)
    Supported Rate:       36.0  Mbps  (Not BSS Basic Rate)
    Supported Rate:       48.0  Mbps  (Not BSS Basic Rate)
    Supported Rate:       54.0  Mbps  (Not BSS Basic Rate)

FCS - Frame Check Sequence
    FCS:                  0x6FF31B0E
```

4.1.1.5 Association Response

An association response consists of 3 information elements:

- *Capability information* - Informs the MU the capabilities from the WLAN point of view; whether or not the WLAN can support roaming or if privacy is required.
- *Status code* - Tells the MU whether or not he was successful associated
- *AID* - Association ID

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        51
  Timestamp:            12:46:22.171177000 04/21/2008
  Data Rate:            2   1.0 Mbps
  Channel:              11  2462MHz  802.11bg
  Signal Level:         78%
  Signal dBm:           -40
  Noise Level:          12%
  Noise dBm:            -88
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %0001  Association Response
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             320  Microseconds
  Destination:          00:18:DE:07:71:75
  Source:               00:15:70:65:A3:60
  BSSID:                00:15:70:65:A3:60
  Seq Number:           292
  Frag Number:          0
802.11 Management - Association Response
  Capability Info:      %0000010000000001
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
                        .....1.. ........ G Mode Short Slot Time [9 microseconds]
                        ......0. ........ QoS is Not Supported
                        .......0 ........ Spectrum Mgmt Disabled
                        ........ 0....... Channel Agility Not Used
                        ........ .0...... PBCC Not Allowed
                        ........ ..0..... Short Preamble Not Allowed
                        ........ ...0.... Privacy Disabled
                        ........ ....0... CF Poll Not Requested
                        ........ .....0.. CF Not Pollable
                        ........ ......0. Not an IBSS Type Network
                        ........ .......1 ESS Type Network
```

```
  Status Code:          0  Successful
  Association ID:       1
Supported Rates
  Element ID:           1  Supported Rates
  Length:               8
  Supported Rate:       1.0  Mbps  (BSS Basic Rate)
  Supported Rate:       2.0  Mbps  (BSS Basic Rate)
  Supported Rate:       5.5  Mbps  (BSS Basic Rate)
  Supported Rate:       6.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       9.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       11.0  Mbps  (BSS Basic Rate)
  Supported Rate:       12.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)

Extended Supported Rates
  Element ID:           50  Extended Supported Rates
  Length:               5
  Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       24.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       36.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       48.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       54.0  Mbps  (Not BSS Basic Rate)

FCS - Frame Check Sequence
  FCS:                  0xBB04C748
```

4.2 BSSIDs versus ESSIDs

BSSID - Basic Service Set ID

ESSID - Extended Service Set ID

Compare an ESSID and BSSID with the MAC address of a PC and the DNS of the PC. It all comes down to the same principle. All devices connected to a network can only talk to each other when their respective MAC address is known. However, people are not good at remembering MAC addresses. Consequently, naming each *PC* and *User* is needed. These are often the same names as the ESSID and BSSID.

One BSSID is the radio MAC address of a single AP. In theory if you have one AP, you should be able to connect to this AP by configuring the MU with the BSSID of the AP.

The problem is when you have more then one AP, and you want to be *mobile*. How can you determine the MAC addresses of potentially 10 APs (available for association) in such a mobile environment? You will have to determine the BSSIDs of 10 APs!

An ESSID provides assistance. An ESSID (*Extended Service Set ID*) is a group of BSSIDs with the same common name. This name is most often the ESSID or SSID of the configuration software of the AP.

When the ESSID is configured in an MU, the radio driver of this MU will use this name to determine (via Probe Requests) if there is an AP in the area of this ESSID.

When the MU discovers an AP with this ESSID, it will associate to the BSSID of the AP.

NOTE: An MU only communicates to the BSSID, not to the ESSID. The ESSID is generally used to retrieve the BSSID of an AP belonging to the ESSID.

This is why there are three MAC addresses in the header of an 802.11 wireless trace instead of 2 MAC addresses like in an 802.3 wired trace.

- *Source address* - the address of the source device (mainly the MU, server or router)
- *Destination address* - the address of the Source Device mainly the MU or the Server or Router
- *ESSID* - the MAC address of the wireless distribution device, the device of which the Mobile Unit is communicating through to the wired network.

..	Source	Destination	BSSID	Channel	Signal	Data Rate	Relative Time	Protocol
1	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	70%	1.0	0.000000	802.11 Beacon
2	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	68%	1.0	0.102405	802.11 Beacon
3	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	68%	1.0	0.204803	802.11 Beacon
4	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	68%	1.0	0.307195	802.11 Beacon
5	IPv6-FE80::21E...	IPv6-FF02::FB	00:15:70:65:A3:60	11	65%	1.0	0.309790	DNS
6	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	68%	1.0	0.409601	802.11 Beacon
7	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	71%	1.0	0.511999	802.11 Beacon
8	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	71%	1.0	0.614398	802.11 Beacon
9	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	68%	1.0	0.716798	802.11 Beacon
0	VINCENT-1DEE516	IP-192.168.1.2	00:15:70:65:A3:60	11	71%	54.0	0.720605	PING Req
1	*00:15:70:65:A3:60*	00:18:DE:07:71:75		11	67%	24.0	0.720647	802.11 Ack
2	IP-192.168.1.2	VINCENT-1DEE516	00:15:70:65:A3:60	11	64%	54.0	0.722233	PING Reply
3	*00:18:DE:07:71:75*	00:15:70:65:A3:60		11	71%	24.0	0.722274	802.11 Ack
4	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	67%	1.0	0.819197	802.11 Beacon

Multiple ESSID support is available on the access point.

4.3 VLAN to ESSID Mapping

WLANs are becoming more and more popular. The concept of copying the functionality of a *wired* LAN to a *wireless* LAN is real.

Therefore, trunking (802.1q) technology is added to APs and switches. This enables AP to map VLANS to WLANS (in other words VLANS to ESSIDs).

This is done is differently depending on the manufacturer.

Imagine the following scenario:

You have 4 VLANS, and you want to map them to 4 ESSIDS. Remember a MU can only communicate with a BSSID. In this scenario you have 4 ESSIDS in the AP mapped to one single BSSID. This means the broadcast and multicast traffic coming from the 4 VLANS is sent (in the air) with the same BSSID.

Disadvantages of this scenario include:

- *Reduced battery capacity for MUs* - The MU has to listen to broadcast and multicast traffic coming from the 4 VLANS.
- *Reduced security options* - For example you have configured one VLAN for WEP security and one VLAN for WPA2/CCMP. The whole network is only as secure as the weakest security mechanism in use.
- *Reduced QoS* - Resulting from an overhead in a specific user's VLAN traffic in the user's respective WLAN. For example, when using one VLAN for VoWLAN (*Voice over WLAN*), the voice application has to

share the BSSID with 3 other VLANs, in worst case, the 3 other VLANS can occupy all the available bandwidth with the consequence there is not enough room for voice traffic.

NOTE: MUs in *Power Save Mode* (PSP) have to wake up to listen to a broadcast traffic. Since multicast is seen as broadcast, the MU must listen to the multicast traffic coming from that BSSID.

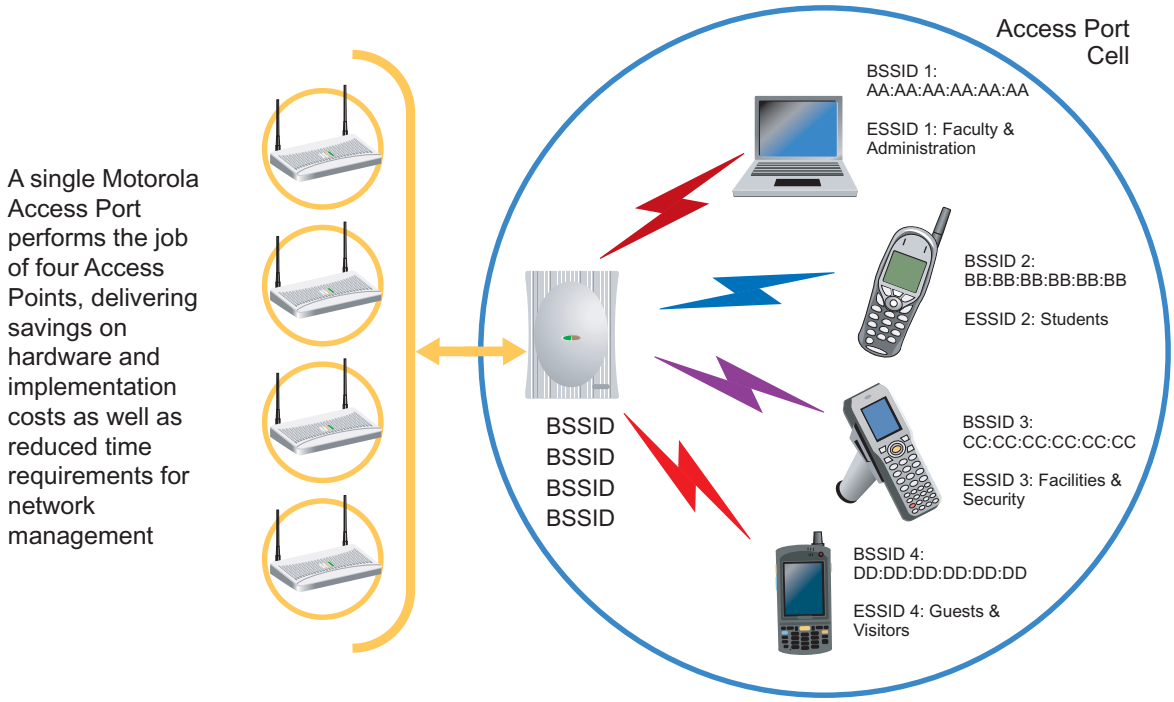
In respect to the switch wired LAN, the WLAN is a large collision domain where the VLAN traffic is broadcasted over the WLAN.

NOTE: A current trend is having one ESSID, and assigning the respective VLAN to the user through Radius authentication. This is tempting, and simple to do, but not suitable for a mobile environment. When integrating this type of service, you have 1 ESSID mapped to 1 BSSID. All the broadcast and multicast traffic of the available VLANS is sent in the air (with all the disadvantages that entails).

The solution to overcome this issue is called Multi BSSID (or as some manufactures call it, Virtual AP).

4.3.1 Multi BSSID

Multi BSSID coverts an AP into 4 virtual APs with 4 BSSIDS per radio. 4 BSSIDs for the 802.11b/g radio and 4 BSSIDs for the 802.11a radio.



Using a wireless trace, multi BSSID could appear as follows:

P...	Source	Destination	BSSID	Channel	Signal	Data Rate	Relative Time	Protocol
1	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	70%	1.0	0.000000	802.11 Beacon
2	00:15:70:65:A3:63	Ethernet Broadcast	00:15:70:65:A3:63	11	62%	1.0	0.025607	802.11 Beacon
3	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	71%	1.0	0.051200	802.11 Beacon
4	00:15:70:65:A3:61	Ethernet Broadcast	00:15:70:65:A3:61	11	61%	1.0	0.076807	802.11 Beacon
5	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	71%	1.0	0.102404	802.11 Beacon
6	00:15:70:65:A3:63	Ethernet Broadcast	00:15:70:65:A3:63	11	64%	1.0	0.128002	802.11 Beacon
7	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	64%	1.0	0.153607	802.11 Beacon
8	00:15:70:65:A3:61	Ethernet Broadcast	00:15:70:65:A3:61	11	70%	1.0	0.179205	802.11 Beacon
9	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	60%	1.0	0.204803	802.11 Beacon
10	00:15:70:65:A3:63	Ethernet Broadcast	00:15:70:65:A3:63	11	67%	1.0	0.230400	802.11 Beacon
11	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	60%	1.0	0.256003	802.11 Beacon
12	00:15:70:65:A3:61	Ethernet Broadcast	00:15:70:65:A3:61	11	68%	1.0	0.281601	802.11 Beacon
13	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	62%	1.0	0.307199	802.11 Beacon
14	00:15:70:65:A3:63	Ethernet Broadcast	00:15:70:65:A3:63	11	70%	1.0	0.332806	802.11 Beacon
15	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	64%	1.0	0.358402	802.11 Beacon
16	00:15:70:65:A3:61	Ethernet Broadcast	00:15:70:65:A3:61	11	70%	1.0	0.384000	802.11 Beacon
17	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	61%	1.0	0.409598	802.11 Beacon
18	00:15:70:65:A3:63	Ethernet Broadcast	00:15:70:65:A3:63	11	68%	1.0	0.435205	802.11 Beacon
19	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	61%	1.0	0.460799	802.11 Beacon
20	00:15:70:65:A3:61	Ethernet Broadcast	00:15:70:65:A3:61	11	71%	1.0	0.486397	802.11 Beacon
21	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	58%	1.0	0.512003	802.11 Beacon
22	00:15:70:65:A3:63	Ethernet Broadcast	00:15:70:65:A3:63	11	70%	1.0	0.537601	802.11 Beacon

In this trace you see that the same AP is sending on 4 BSSIDS namely 00:15:70:65:A3:60 - *:61 - *:62 - *:63

Using Multi BSSID, map up to 4 WLANs to 4 BSSIDs, granted you still share the same collision domain in respect to the RF channel used by that AP.

However, the user is seeing only the traffic coming from his VLAN and the traffic from the other VLAN(s). Consequently, you should:

- *Increase battery life* - The MU has to wake up for broadcast and multicast traffic coming from his WLAN.
- *Increase security* - Since you segment the traffic, you can also size the security. In other words, a WLAN/VLAN using WEP will not affect the security of a WLAN/VLAN using WPA2.
- *Increase QoS* - If deploying VoWLAN, the devices connected to this WLAN/VLAN will not have the annoying overhead broadcast and multicast traffic coming the other VLANs, and have room to make a voice conversation.

4.3.2 Multicast over WLAN

Audio and video are just two of techniques that blend multimedia and networks. Packets can be send at an uneven rate and order. Multimedia requires data packets arrive at the client on time and in the proper order.

We all know the differences between wired and wireless networking. One of these differences is the way multicast is handled by an access point. With the arrival of Motorola's wireless switch technology, new challenges arise from the integration of multicast streaming services in the wireless switched environment.

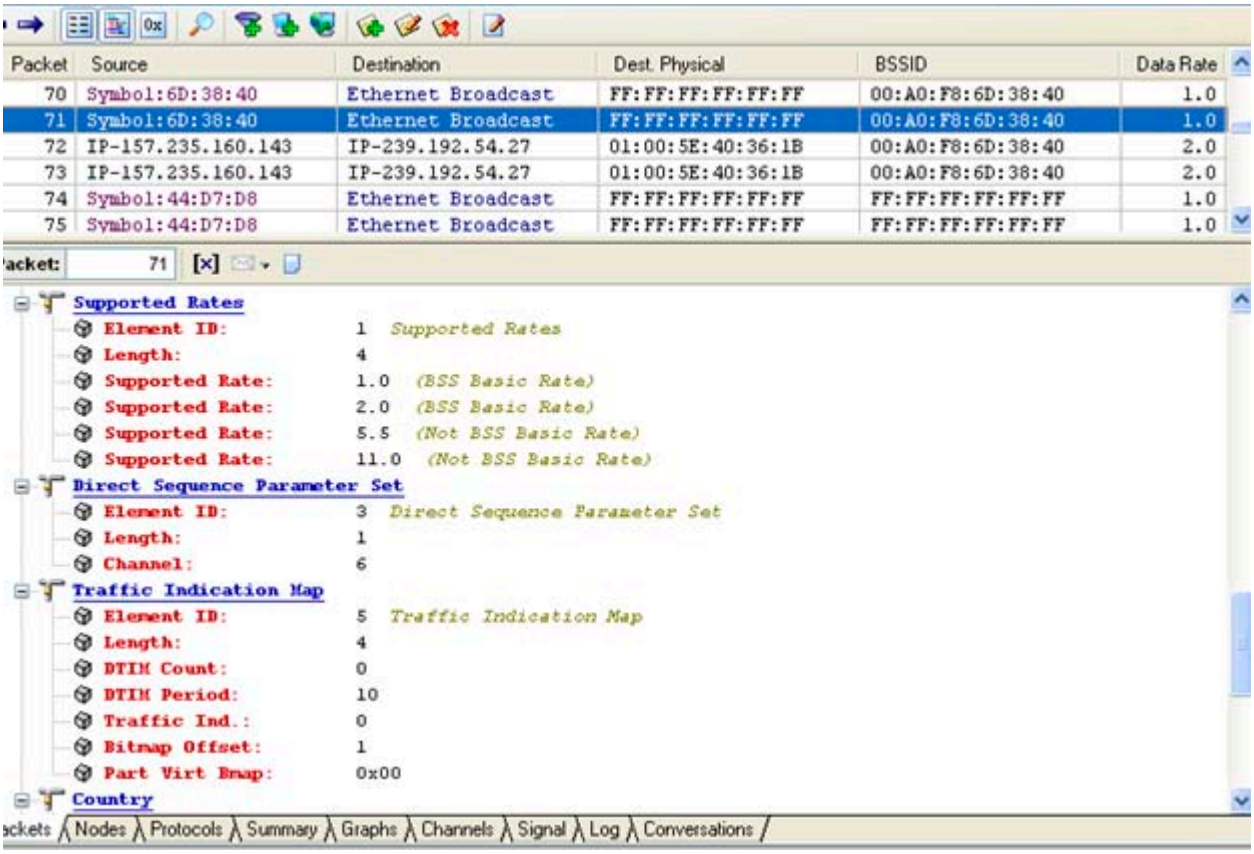
4.3.2.1 Why do You Need Multicast?

Multimedia requires data packets arrive at the client on time and in the proper order. The same is true for wireless environments. The sections that follow explain how to implement a wireless multicast mechanism.

The main reason for configuring the multicast mask is the *Delivery Traffic Indication Messages* (DTIM). The DTIM determines how often the MAC-layer forwards multicast traffic. Mobility requires the DTIM parameter to supply the battery life to a terminal. By default, the DTIM in within Motorola's switches is set to 10. This means an access port will save the multicast packet for this BSSID and send the respective packet/frames after every 10th beacon.

Having smaller DTIMs delivers multicast packets in a more timely matter. The disadvantage is MUs in PSP mode will wake up more often, with a negative battery drain being the consequence. With a large DTIM, the

multicast will have larger delays with a direct result of bad streaming video quality. Consequently, you need a multicast mask.



Within the wireless trace above, packet 71 is the beacon with the last DTIM count: 0 This message, in combination with Bitmap Offset: 1 (which is a bug in Airopeek, it should be Traffic Ind: 1), warns the MU there is/are message(s) waiting for it. As a result of the message, the MU will wake up and receive the two multicast packets. Why two packets? That's the buffer size of the AP100 used in this scenario.

The data rate for management packets (beacons) is different for the multicast packets. Management packets are sent at the lowest possible basic data rate. Multicast packets are sent at the highest possible basic data rate.

4.4 Securing WLANs using Motorola's EWLAN Products

As stated previously, the functionality and integration of Motorola's EWLAN products is more or less the same. Whether it is an AP-5131 or a RFS7000 deployment, the configuration and integration philosophy is identical. This is also true for integrating wireless security

The following table represents security possibilities per product:

°	AP5131	WS2000	WS5100	RFS6000	RFS7000
Access Control List	X	X	X	X	X
Per WLAN configurable Security	X	X	X	X	X
Pre-Shared Key	X	X	X	X	X
EAP - TLS	X	X	X	X	X
EAP - TTLS	X	X	X	X	X
PEAP with Username and Password	X	X	X	X	X
PEAP with CA certificate	X	X	X	X	X
External Radius Server	X	X	X	X	X
Intgrated Radius Server	X	X	X	X	X
LDAP	X	X	X	X	X
Native PEAP	X	X	X	X	X
Native EAP - TTLS	X	X	X	X	X
IPSEC VPN with DES, 3DES and AES	X	X	X	X	X
User Based VLAN (Standard)	°	°	X	X	X
MAC Based Authentication (Standard)	°	°	X	X	X
User Based QoS (VSA*)	°	°	X	X	X
Location Based Authentication (VSA*)	°	°	X	X	X
Allowed ESSID (VSA*)	X°	°X	X	X	X
NAC with Microsoft and Sygate	°	°	X	X	X
Rogue AP detection	X	X	X	X	X
IDS	X	X	X	X	X
WIPS**	X	X	X	X	X
* Vendor Specific Attribute					
** Wireless Intrusion Protection					

Motorola still supports WEP. However WEP is becoming less significant and we haven't included it into our list of supported security mechanisms.

4.4.1 Integrating Motorola EWLAN products with an External Radius server

Aside from PSK, an external Radius server is the simplest means of integrating security to protect WLAN data.

A Motorola WLAN device can operate as a Radius Proxy server and forward authentication traffic coming from an MU to the Radius server defined in the configuration of that specific WLAN.

You do not need to configure an EAP-type since it is provided to the Radius server by the MU. The Radius server then checks if it supports the EAP-type received from the MU.

It's this flexibility that makes Radius integration with Motorola infrastructure so easy. It doesn't matter if it is Microsoft Radius, Steel Belted or Cisco ACS you connect to them all via the Radius port.

Be careful with the Cisco ACS. Cisco is not using the default Radius port (1812) for authentication and1813 for accounting. Cisco uses ACS 1645 for authentication and 1646 for accounting.

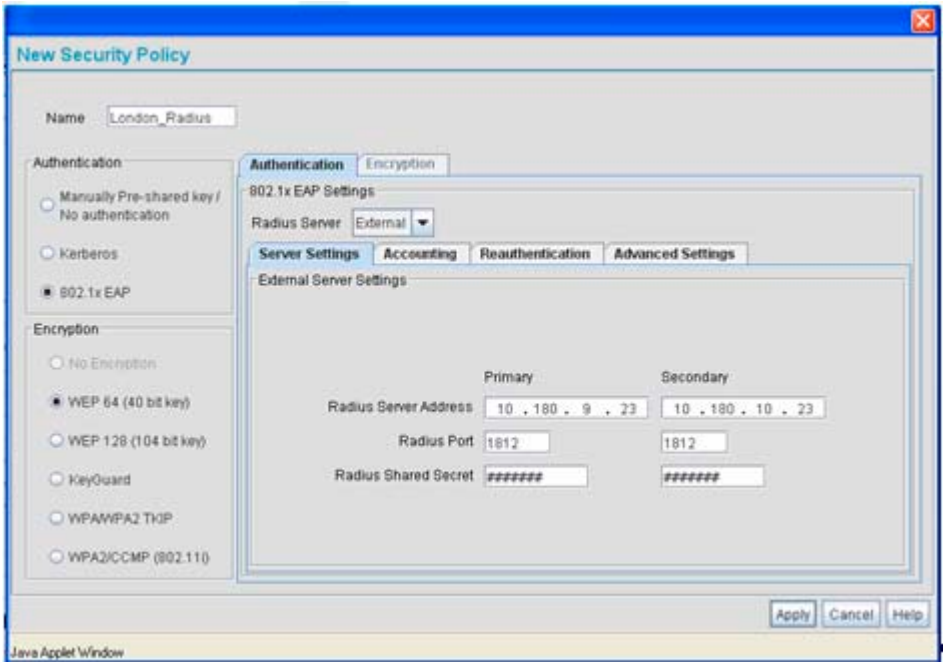
If configuring Radius parameters on Motorola's EWLAN products using Cisco port numbers, the integration should be somewhat seamless.

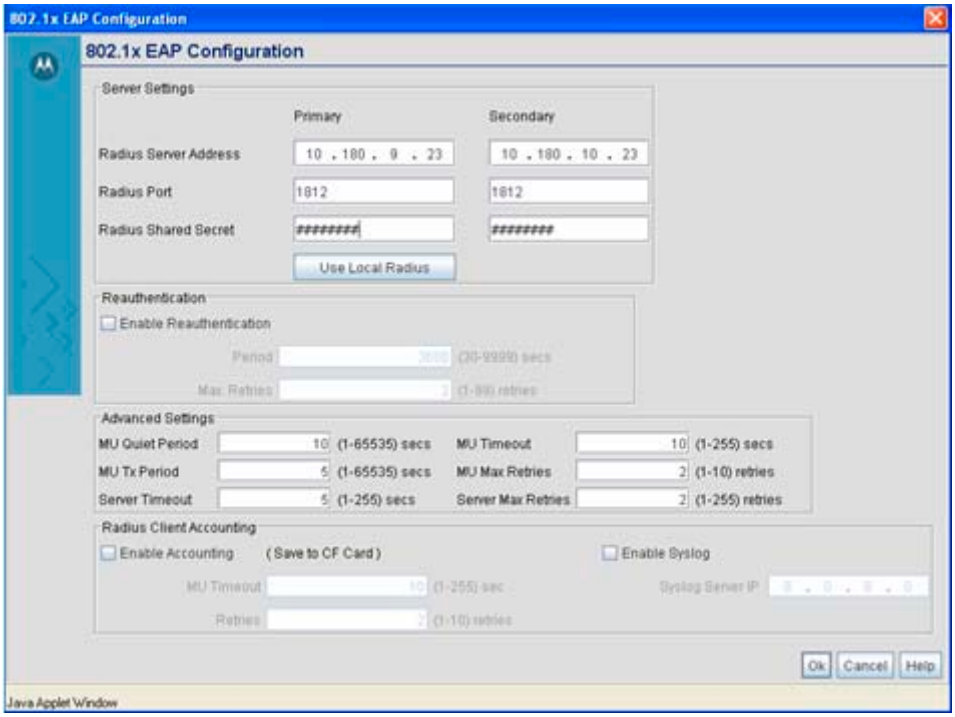
NOTE: It is possible (for security) a company is stepping away from ports 1812, 1813 or 1645 and1646. It is always good to ask an on site professional for these port settings.

P...	Source	Destination	BSSID	Channel	Signal	Data Rate	Relative Time	Protocol
:...	00:18:DE:07:71:75	00:15:70:65:A3:60		11	92%	1.0	54.292057	802.11 Ack
:...	00:18:DE:07:71:75	Ethernet Broadcast	Ethernet Broad...	11	70%	1.0	54.296085	802.11 Probe Req
:...	00:15:70:65:A3:60	Ethernet Broadcast	00:15:70:65:A3:60	11	68%	1.0	54.297611	802.11 Beacon
:...	00:15:70:65:A3:60	00:18:DE:07:71:75	00:15:70:65:A3:60	11	68%	1.0	54.299083	802.11 Probe Rsp
:...	00:18:DE:07:71:75	00:15:70:65:A3:60		11	71%	1.0	54.299397	802.11 Ack
:...	00:15:70:65:A3:61	Ethernet Broadcast	00:15:70:65:A3:61	11	67%	1.0	54.322823	802.11 Beacon
:...	00:18:DE:07:71:75	00:15:70:65:A3:60	00:15:70:65:A3:60	11	70%	54.0	54.325419	802.11 Auth
:...	00:15:70:65:A3:60	00:18:DE:07:71:75		11	65%	24.0	54.325459	802.11 Ack
:...	00:15:70:65:A3:60	00:18:DE:07:71:75	00:15:70:65:A3:60	11	67%	1.0	54.327220	802.11 Auth
:...	00:18:DE:07:71:75	00:15:70:65:A3:60		11	70%	1.0	54.327531	802.11 Ack
:...	00:18:DE:07:71:75	00:15:70:65:A3:60	00:15:70:65:A3:60	11	70%	54.0	54.327787	802.11 Assoc Req
:...	00:15:70:65:A3:60	00:18:DE:07:71:75		11	67%	24.0	54.327830	802.11 Ack
:...	00:15:70:65:A3:60	00:18:DE:07:71:75	00:15:70:65:A3:60	11	67%	1.0	54.331489	802.11 Assoc Rsp
:...	00:18:DE:07:71:75	00:15:70:65:A3:60		11	71%	1.0	54.331803	802.11 Ack
:...	00:18:DE:07:71:75	00:15:70:65:A3:60	00:15:70:65:A3:60	11	90%	54.0	54.339046	EAPOL-Start
:...	00:15:70:65:A3:60	00:18:DE:07:71:75		11	67%	24.0	54.339086	802.11 Ack
:...	00:15:70:65:A3:60	00:18:DE:07:71:75	00:15:70:65:A3:60	11	62%	54.0	54.340293	EAP Request
:...	00:18:DE:07:71:75	00:15:70:65:A3:60		11	81%	24.0	54.340335	802.11 Ack
:...	00:15:70:65:A3:62	Ethernet Broadcast	00:15:70:65:A3:62	11	70%	1.0	54.348427	802.11 Beacon
:...	00:15:70:04:BF:C1	Mcast 802.1d Br...	00:15:70:65:A3:62	11	70%	1.0	54.349293	802.1

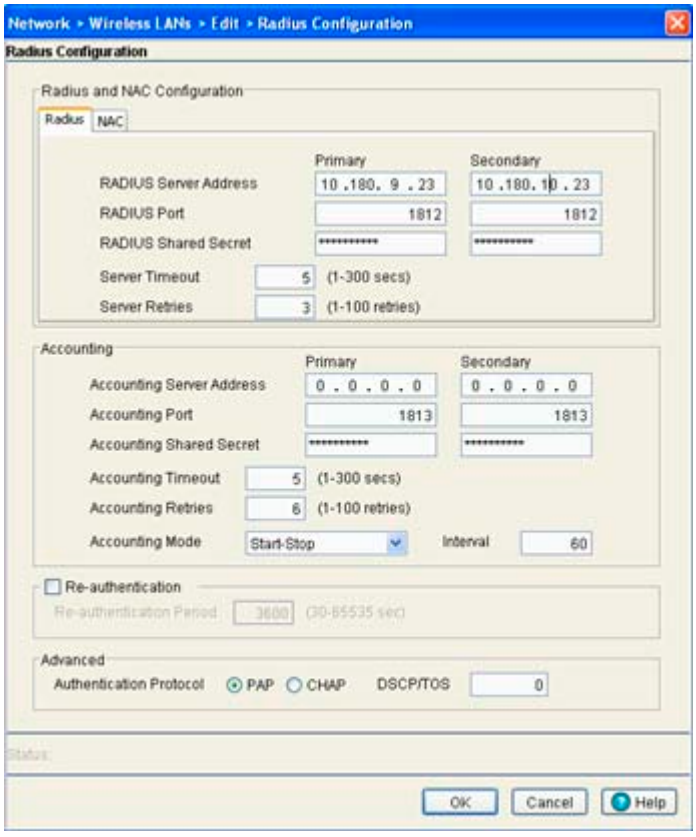
For redundancy, configure a secondary Radius server.

The following are examples of how to configure a Radius server on an AP-5131 and a WS2000.





Since the operating systems on the WS5100, RFS6000 and the RFS7000 are based on a common user interface, those platforms display as follows:


Network > Wireless LANs > Edit > Radius Configuration
Radius Configuration
Radius and NAC Configuration
Radius
NAC
Primary
Secondary
RADIUS Server Address
10 .180. 9 .23
10 .180. 10 . 23
RADIUS Port
1812
1812
RADIUS Shared Secret
Server Timeout
5
(1-300 secs)
Server Retries
3
(1-100 retries)
Accounting
Primary
Secondary
Accounting Server Address
0 . 0 . 0 . 0
0 . 0 . 0 . 0
Accounting Port
1813
1813
Accounting Shared Secret
Accounting Timeout
5
(1-300 secs)
Accounting Retries
6
(1-100 retries)
Accounting Mode
Start-Stop
Interval
60
Re-authentication
Re-authentication Period
3600
(30-85535 sec)
Advanced
Authentication Protocol
PAP
CHAP
DSCP/TOS
0
OK
Cancel
Help

5

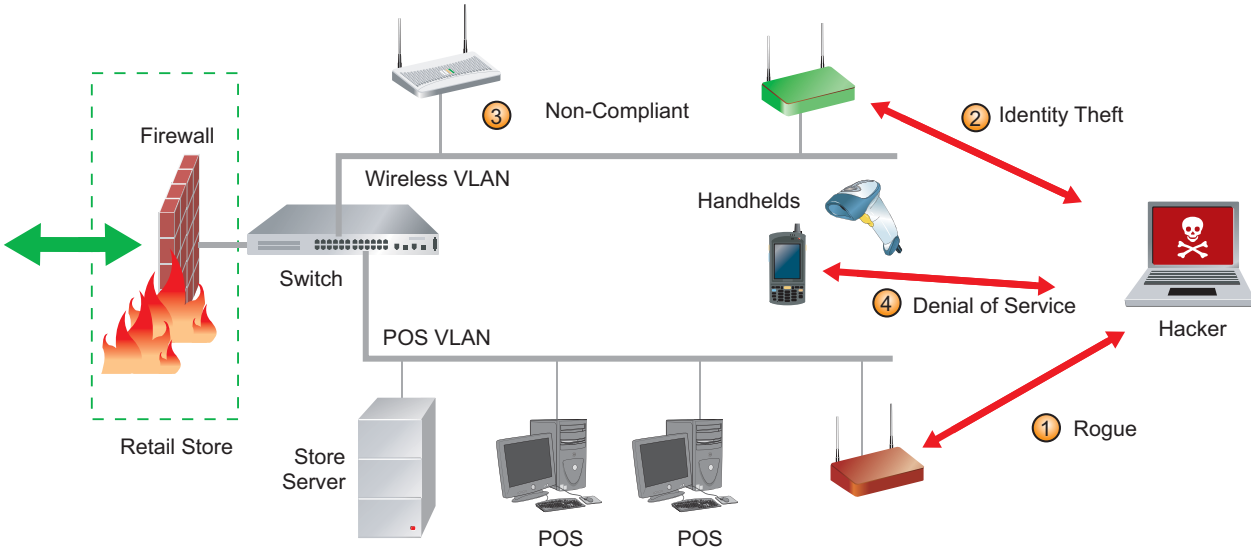
Securing the Wireless Enterprise

The ubiquity of WiFi has meant that increasing amounts of corporate and personal data is being accessed and transferred over the wireless medium. This leads to uninterrupted access to information whether at home, on the road or at the corporate office, and provides significant productivity gains. However, it also exposes valuable data to the unsolicited and malicious intent of hackers. The fact that sensitive information is available on air, and can be accessed from outside the confines of the office or home, makes tackling WLAN security very challenging. It is important the possibility of data theft is checked to prevent productivity and financial loss.

Security protocols, if implemented and used effectively, can prevent data theft (owing to strong encryption and authentication algorithms), but they still leave a lot to be desired. An attacker can still launch a *Denial of Service* (DoS) attack to deny resources to a valid user. Or, a valid user can access the resources beyond what they authorized. A malicious visitor or a careless employee can jeopardize corporate resources if their actions lead to a backdoor entry to the network by a rogue AP. An employee returning from vacation could jeopardize the network because their Virus resources may not be up-to-date. By the time they connect to the corporate WLAN and update their laptop, it could be too late.

Checks based on a user's IP or MAC address are no longer sufficient. It's more important to grant access to resources based on user identity, location and the posture of the device accessing the WLAN.

Wireless technologies are testing the physical boundaries, and any Enterprise relying on perimeter security can do so only at their own peril. A firewall at the perimeter was enough when you could ensure no malicious activity. Within wireless Enterprises, the corporate network sometimes extends beyond the corporate perimeter. The mobile workforce is no longer tied to their workplace, but can move and work from anywhere within the organization. Consequently, segregating network traffic using VLANs based on location is out of date.



The illustration above depicts how perimeter security is not enough to prevent wireless attacks.

It is important to tackle Enterprise WLAN security from multiple dimensions and not rely on perimeter defences and wired Enterprise mentalities.

In this guide, we identify some common security threats affect the WLAN. We'll discuss the options and strategies available to mitigate each of these threats and the challenges in order to deploy a secure WLAN environment.

This chapter is dedicated to the following Enterprise WLAN security concepts:

- *Securing an Enterprise WLAN*
- *Smart RF*
- *Network Integrity Checks*
- *Network Privacy*
- *Certifications and Legal Requirements*
- *WiFi Security Standards Overview*

5.1 Securing an Enterprise WLAN

There are multiple dimensions to be considered when addressing the security of an Enterprise WLAN. One has to evaluate each with the utmost care and make sure there are no weak links in the chain. It starts with ensuring only the right users access the right information, preventing information from falling into the wrong hands and removing threats to network integrity through continuous monitoring and control.

This section includes a discussion on the following Enterprise WLAN security measures:

- *Access Control*
- *802.1x Authentication with WPA/WPA2*
- *Access Control Lists (ACLs)*
- *VLAN Segregation*
- *Role Based Access Control*
- *Location Based Access Control*
- *Network Access Control (NAC)*

For an overview of the WiFi security standards impacting your Motorola Enterprise WLAN deployment, refer to *WiFi Security Standards Overview on page 5-30*.

5.1.1 Access Control

Access control ensures the right user accesses the right information. It starts with authenticating the user to ensure they are who they claim to be. While authentication ensures a network entity as a valid user, it's silent on the kind of access the entity is entitled to. For example, a sales executive may not be authorized to access HR records. Or an employee may be authorized to access the Internet only during certain times of the day. Once authenticated, it's important to determine the user's access control policy based on the networked device's MAC address, authentication type, user identity and current location.

5.1.2 802.1x Authentication with WPA/WPA2

Validating the identity of a network entity is the starting point on which any security policy is based. It can be based on the network device, like the MAC address of the device. Or user identity based, like user-id and password combination. The challenge of password based authentication is to find a secure way of sharing the password amongst credible users and ensure it satisfies cryptographic requirements. *Wired Equivalent Privacy* (WEP), was part of the initial 802.11 standard in 1999. In the interim, the Wi-fi alliance developed *WiFi Protected Access* (WPA).

WPA & WPA2 recommend port based authentication (IEEE 802.1x) using the *Extensible Authentication Protocol* (EAP). 802.1x provides many authentication protocols, some of which use digital certificates and are based on well known standards like SSL. Since 802.1x is widely used for Enterprise authentication on the

wired side, organizations are familiar with it and can make use of the same infrastructure. The following lists some of the authentication methods used within Motorola's wireless LAN security protocols.

Protocol	***Encryption***	***Authentication***	***Integrity***
WEP	WEP	Shared Key 802.1x (dynamic WEP)	CRC
WPA	TKIP	802.1x (EAP, PEAP, TTLS) PSK	MIC
WPA2	AES	802.1x (EAP, PEAP, TTLS) PSK	CBC-MAC

NOTE: If using WPA-PSK or WPA2-PSK, keep in mind weak passwords are prone to dictionary and brute force attacks. It's critical a password policy be in place which mandates passphrases that are truly random, at least 20 bytes long, include alphanumeric characters and special symbols and change frequently (every two weeks or so).

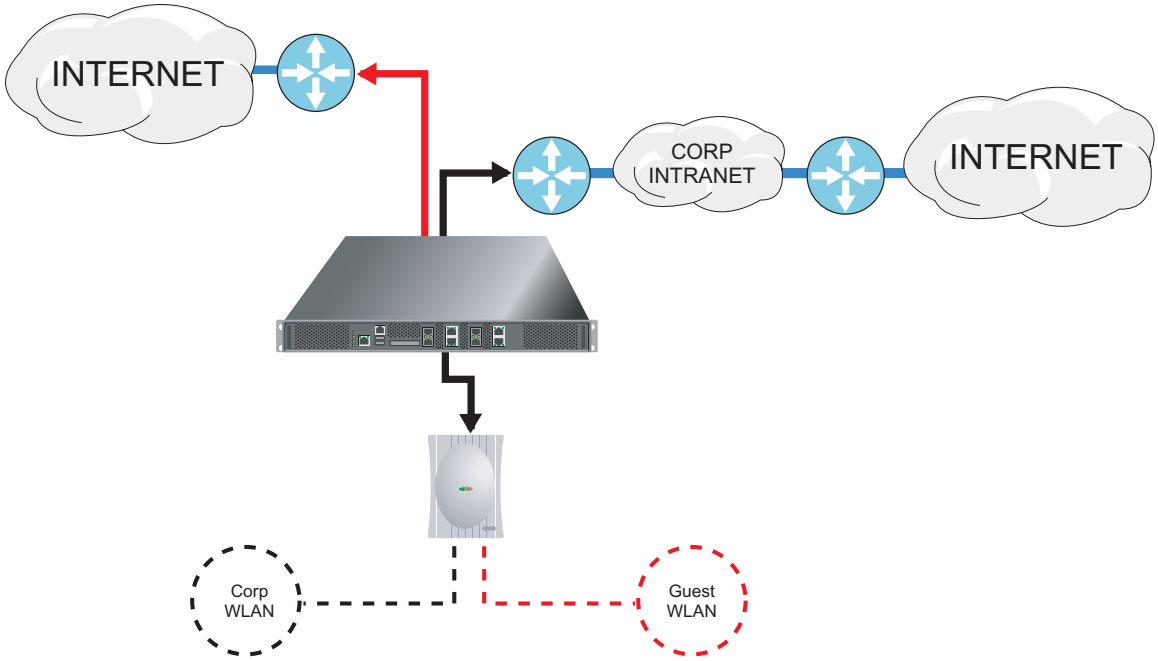
5.1.3 Access Control Lists (ACLs)

Traditionally, ACLs only supported MAC address based authentication. But increasing WLAN sophistication saw various enhancements in ACLs. ACLs now have enhanced packet filtering capabilities, which can be at layer 3 (IP address, port number, protocol) or at layer 2 (MAC address, ether type, VLAN id). Thus, access can be granted based on packets matching the defined criteria.

5.1.4 VLAN Segregation

Virtual LANs (VLANs) have long been used in wired deployments to create logical workgroups and apply access and traffic management policies. The same benefit can be extended to wireless LANs. In the wired world, VLANs were defined based on the port (physical location) to which the user is connected. A VLAN should be configured based on the identity of the user in the wireless world, irrespective of t location. Access policies are then applied based on the VLAN the user belongs to. For example, separate VLANs can be

created for employees and guest users. Guest users can then be prevented from accessing any other network resource apart from the Internet.



5.1.4.1 User Based VLANs

Traditionally, VLANs were assigned based on the WLAN. Users from a finance department would use WLAN-FINANCE, which in turn would map to VLAN 100. HR employees would access the wireless network WLAN-HR mapped to VLAN 200. With user based VLANs, all the employees in the organization would use the same WLAN, yet be mapped to different VLANs based on their identity. This is used in conjunction with 802.1x authentication, such that VLAN information is provided to the controller by the Radius server once the user is authenticated. The access policies are then applied to the employees specific to the VLAN they are mapped to.

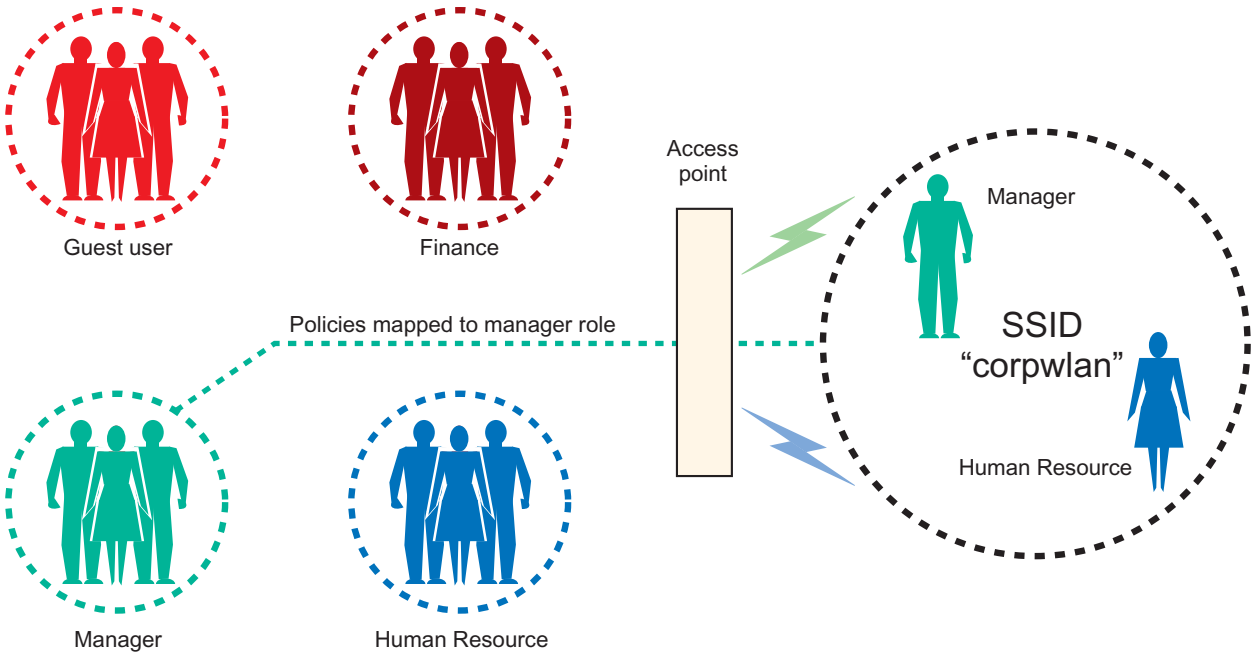
5.1.5 Role Based Access Control

Wired clients access the network through a fixed port and location, usually protected by a physical boundary. This is not true for wireless networks. There is a need to find the identity of a wireless user and apply access policies based on their role within the organization, irrespective of the location from where they are accessing the wireless network. Even though Finance and Human Resource employees access the wireless network from a common cafeteria using a common ESSID, their access policies depend on their identities.

Defining access policies for each user may be inconvenient and unnecessary. Users can be grouped according to their role, and access policies can be applied to the group based on their role. The user role can be identified based on parameters like device MAC address, authentication type, encryption type or ESSID. The group can be identified during authentication, by querying the group from the authentication server.

Other wireless parameters also get identified during the authentication process, and the role of the user is determined before association.

Each role in the system can have its definition in the organization and expected network access level, as defined by ACLs attached to these roles. Defining roles based on wireless entities allows an administrator to set the same WLAN access across the Enterprise and still control network access based on user identity.



5.1.6 Location Based Access Control

Enterprises often want the benefits of mobility to their employees and visitors, but want to restrict network access based on building location. A company may not want to give access to HR, Finance or new product documents in their lobby or cafeteria. They may want to restrict hotspot access to visitors only in certain areas, or prevent access to google in exam halls.

Location Based Access Control (LBAC) makes it possible to control access to a WLAN based on the current geographic location of the MU in conjunction with his authorization status. As the user roams around the corporation, his access to various resources is determined based on his current location. Thus, a guest user could have Internet access in a conference room, then have it disabled as soon as he steps out of the conference room.

LBAC can be combined with one or more IDs (like an RFID-enabled badge) allowing access only if the user has the right ID and authentication credentials. This takes into account the location of the MU, user ID and authorization status. This prevents the possibility an employee is using somebody else's laptop to obtain unauthorized access.

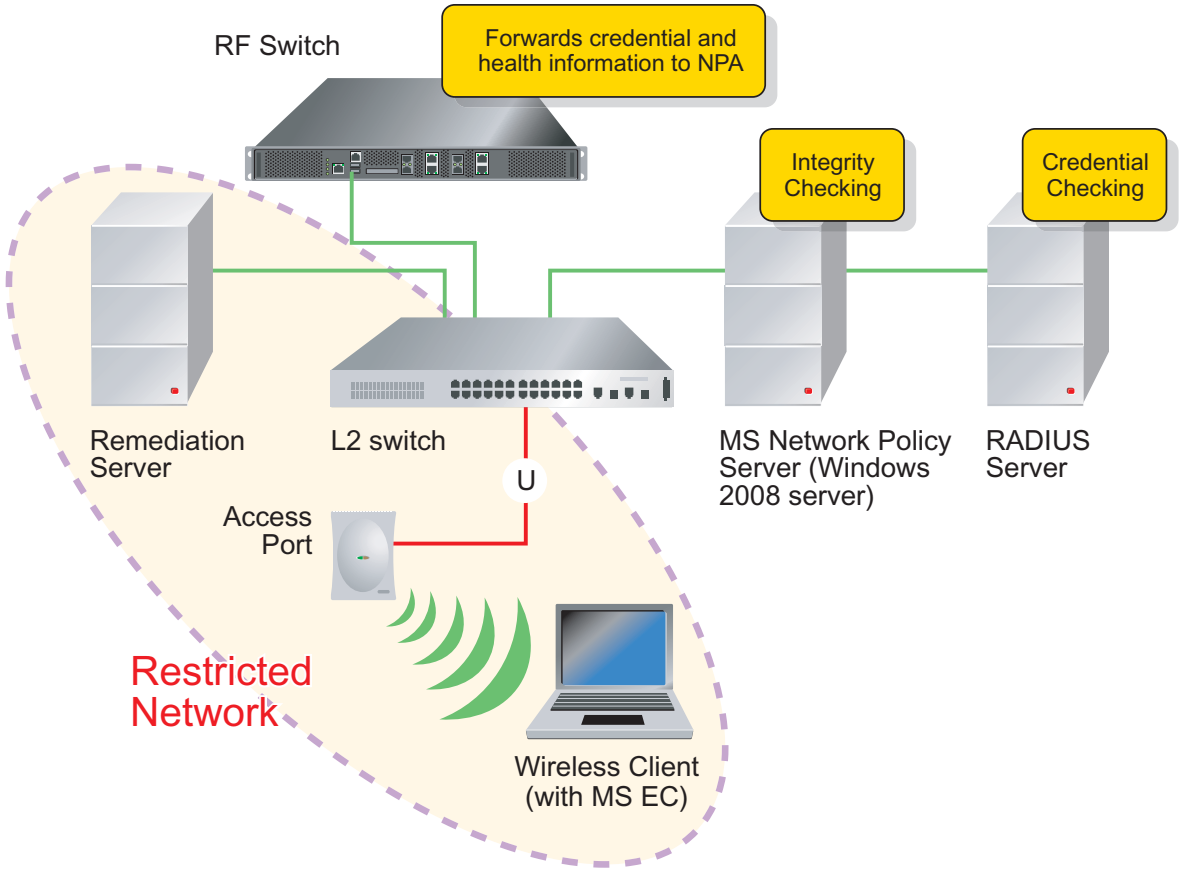
5.1.7 Network Access Control (NAC)

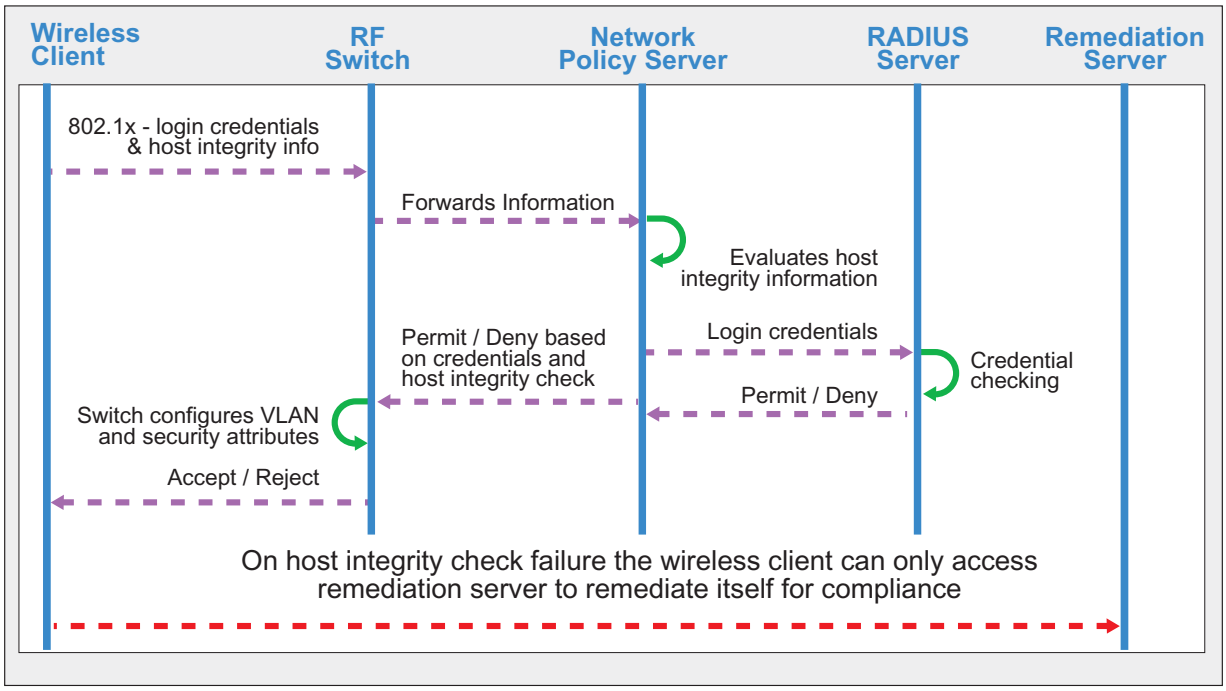
Today's mobile workforce uses their laptops at the office, home or public wireless networks while traveling. These systems can get infected and jeopardize the corporate network upon return to the office. In this scenario, the laptop bypasses perimeter security measures employed by the organization. Secondly, when the user gets back to office, he may not have all the necessary software (like the latest OS patch) and up to

date anti-virus definitions. It's important network users meet corporate health policy requirements before allowed access to the network. For wireless clients, this enforcement should happen at the network's edge (at the access points), which is their point of entry.

This enforcement can be achieved in conjunction with Symantec NAC or Microsoft *Network Access Protection* (NAP). These help an administrator enforce compliance with corporate health policies for network access. With these solutions, clients obtain access to the network only if they have mandated applications (OS, patches, firewall, etc) and anti-virus software. This helps the network administrator maintain the integrity of the wireless clients in the network.

If clients fail an integrity check, they are put in a quarantine VLAN, with access to a remediation server. They clients do not have access to any other corporate resources. The remediation server has the latest security and application software needed by the client to obtain compliance with corporate security policies. The client can install the required patches and gain entry to the corporate network when they properly authenticate.





5.2 Smart RF

Self Monitoring At Run Time RF Management (Smart RF) is a new Motorola innovation designed to simplify initial RF configuration for new deployments while (over time) providing on-going RF optimization and self-healing functions.

With new installations, Smart RF can reduce deployment time and cost by scanning the RF environment and automatically determining the best channel and transmit power configuration for each managed radio.

Unlike competing implementations, where RF decisions are made per controller or access point, Smart RF centralizes the decision process and makes intelligent RF configuration decisions using complete information obtained from the whole RF environment. This centralized approach results in a competitive advantage in medium or large deployments, since APs are distributed between multiple floors or managed by multiple switches.

As RF environments are dynamic and change over time, Smart RF can also reduce ongoing management and maintenance costs through periodic re-calibration. Re-calibration can be initiated manually or be

automatically scheduled to ensure the RF configuration is optimized to factor in new RF environment changes such as new sources of interference or neighboring APs.

Smart RF also provides self-healing functions by monitoring the managed RF environment in real-time and providing automatic mitigation from events such as RF interference, coverage holes and AP or radio failures. Self-healing allows a WLAN maintain station performance and coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

Smart RF is supported on WS5100, RFS6000 and RFS7000 switches managing AP300s in standalone or clustered environments.

NOTE: For optimum Smart RF deployment, a WLAN should have been planned and deployed correctly, with each radio being reachable by at least one other radio. Smart RF cannot compensate for a poorly planned design, or deployments where APs have been incorrectly located.

Smart RF management is comprised of the following two phases:

- *Smart RF Calibration*
- *Smart RF Monitoring*

Smart RF is well suited for clustered environments. Smart RF interacts with a number of existing features, (such as radio detection, MU load balancing and self-healing).

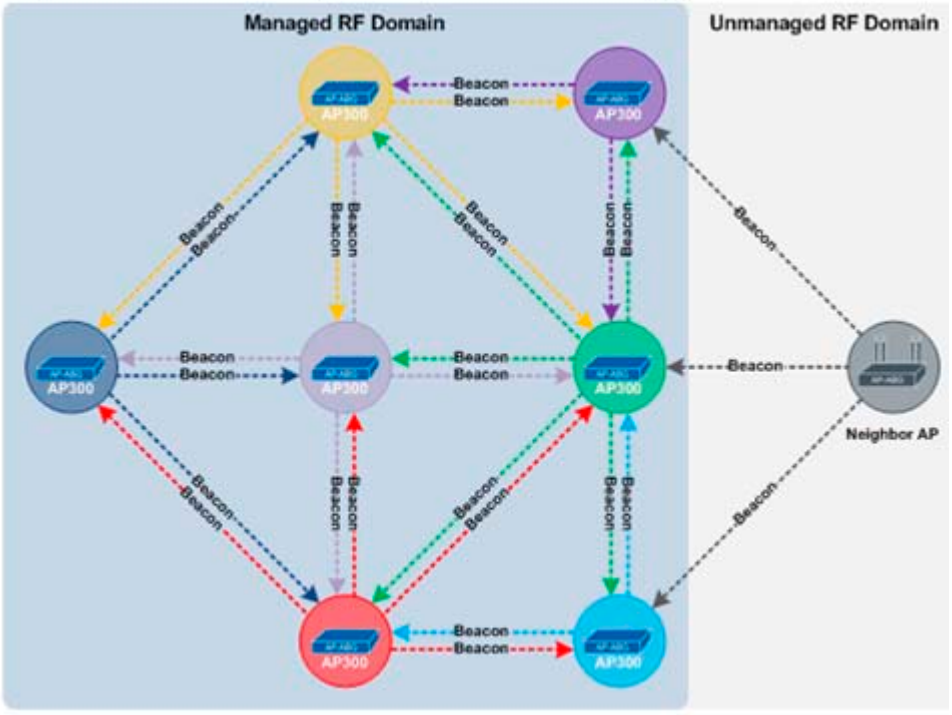
5.2.1 Smart RF Calibration

Smart RF calibration canbe initiated by a network administrator during a new deployment or scheduled to run at a specified time and frequency for ongoing WLAN performance optimization.

5.2.1.1 Scanning

When calibration begins, the Smart RF module instructs all adopted radios to beacon on a specific legal channel and transmit their power value. The Smart RF module measures the signal strength of each beacon received from managed and un-managed neighboring APs to define a RF neighborhood map. Smart RF uses

this scan information to calculate and define each managed radio's RF configuration and assign radio roles and self-healing parameters.



Smart RF calibration supports basic and extensive scanning modes. Basic scanning (default) results in faster calibration, as the beaconing/scanning cycle only occurs on each configured channel using the maximum transmit power value. The following describes the operation of a basic scan:

1. All radios change to the first configured legal channel
2. All radios increase their transmit power to maximum
3. All radios transmit and receive beacons based on the configured dwell time (default time is 1 second)
4. All radios change to the next configured legal channel
5. Steps 3 and 4 are repeated until all the configured legal channels have been scanned at the maximum transmit power value

Enhanced scanning results in longer calibration, since the beaconing/scanning cycle will occur on each configured channel on all transmit power values. The following describes the operation of an extended scan:

1. All radios change to the first configured legal channel
2. All radios increase their transmit power to maximum
3. All radios transmit and receive beacons based on the configured dwell time (default 1 second)
4. All radios change to the next configured legal channel
5. All radios reduce their transmit power by 1dBm
6. All radios transmit and receive beacons based on the configured dwell time (default 1 second)
7. Steps 4, 5 and 6 are repeated until all the configured legal channels have been scanned on all transmit power values

The decision of which scanning mode to select depends on the stage of deployment and the frequency of on-going optimization. For new WLAN deployments, it's recommended an extensive scan be performed, as it provides a more accurate RF neighborhood map resulting in better configuration decisions. For on-going RF performance optimization, it's recommended basic scanning be used, if re-calibration is being performed on a weekly or bi-weekly basis. If re-calibration is being performed monthly, quarterly or on a yearly basis, an extensive scan is recommended.

NOTE: The calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.

5.2.1.2 Configuration

Once calibration is complete, the following Smart RF tasks can be conducted:

- *Channel Assignment* - Smart RF can assign channels to working radios selected to avoid channel overlap between managed APs and interference from external RF sources
- *Transmit Power Assignment* - Smart RF can assign an operating and maximum transmit power to working radios. The operating and maximum transmit power configuration is determined based on each radios coverage in respect to neighboring APs, channel overlap and the self-healing parameters
- *Assigns Detectors Radios* - Smart RF can select detector radios to perform real-time monitoring and self-healing functions
- *Self-Healing* - Smart RF can automatically configure self-healing parameters such as assigning rescuer radios to working radios to increase transmit power to account for an AP failure

The configuration tasks performed during calibration can be enabled or disabled in the Smart RF global configuration. Administrators can exclude Smart RF configurations on a per radio basis.

5.2.1.3 Radio Roles

During calibration, radios within a WLAN are assigned a normal or detector role. Radios maintain these roles during WLAN operation. Detector radios provide monitoring for self-healing functions and normal radios service clients.

During self-healing, normal radios convert to *Rescuer* or *Filling* roles depending on the self-healing action performed. If neighborhood recovery is performed, a radio transitions to a Rescuer role. If coverage hole mitigation is performed, a radio transitions to a *Filling* role.

Radio Role	***Description***
Normal	Working radios function in a normal operating mode. A normal mode indicates a working radio is not monitoring or self-healing.
Detector	Detector radios are automatically defined and configured during calibration. They provide real-time monitoring for self-healing. Detector radios are dedicated for monitoring and do not provide client services.
Rescuer	Each working radio can assume the role of rescuer. When a radio is defective or fails its neighboring radios increase transmit power to compensate for coverage holes. These neighbors are called *rescuer* radios. Smart RF calibration automatically assigns rescuer radios for each working radio, along with the power needed to rescue each failed or defective radio.
Filling	During coverage hole mitigation, a normal radio increases transmit power to support the coveragearea. When a radio is performing coverage hole mitigation, its state changes to *filling*.

NOTE: By default, all radios participate in Smart RF, can be a detector and have rescuer radios assigned. Smart RF allows administrators to exclude radios from detector or rescuer roles, and can manually configure rescuer radios.

5.2.2 Smart RF Monitoring

Once calibration is complete, Smart RF transitions to a monitoring phase. Monitoring occurs continuously until the Smart RF module is disabled or calibration is performed. Smart RF monitoring performs the following functions:

- Detection and remediation for failed radios / APs
- Detection and remediation for interference
- Detection and remediation for coverage holes

Monitoring functions are enabled by default, but can be disabled using Smart RF global settings

5.2.2.1 Neighbor Recovery

When a radio fails or is faulty, Smart RF can provide automatic recovery by instructing assigned neighboring APs (called rescuers) to increase transmit power to compensate for the coverage loss. During calibration, each working radio can be assigned up to 5 rescuer radios. Each rescuer radio's operating and maximum

transmit power settings will be configured to provide adequate coverage for users and provide margin to compensate neighboring AP failures.

5.2.2.2 Coverage Hole Protection

Coverage holes occur when a station is unable to receive packets from a another station at the desired data rate. When packet transmissions are consistently below the working radios configured coverage rate, a coverage hole is detected and the transmit power for the radio needs to be raised to compensate.

When a coverage hole is detected, Smart RF first determines the power increase needed to bring the stations connection rate back to desired coverage rate and keep monitoring the stations connection rate. If the configured connection rate is met the radio will stay at that power level. If the connection is still under the coverage rate, more power would be applied. If the connection rate is higher than the configured connection rate ,Smart RF reduces the transmit power in 1dBm increments until the configured coverage rate for the radio is achieved. When the station roams to a new AP, Smart RF decreases the transmit power of the radio to its original value, completing the coverage hole healing action.

5.2.2.3 Interference Avoidance

802.11 WLANs are susceptible to sources of interference, such as neighboring 802.11 radios, cordless phones, microwave ovens and Bluetooth devices. When such disrupters are present, they can severely impact the performance of the WLAN and the user experience.

Smart RF provides mitigation from interference by monitoring retry rates on functional radios. When a retry rate threshold is exceeded, Smart RF can initiate a channel scan on the effected radio and select an

alternative channel with less interference. To avoid channel flapping, a hold time is defined which disables interference avoidance for a specific period.

5.2.3 Smart RF Cluster Operation

Smart RF is supported in both standalone and clustered environments. In standalone environments, an individual RF Switch controls the calibration and monitoring phases. In clustered environments, a single RF Switch is elected a Smart RF master, and remaining cluster members operate as Smart RF clients. The Smart RF master co-ordinates the calibration and configuration and (during the monitoring phase) receives information from Smart RF clients.

The Smart RF master switch maintains an active record of all adopted radios in the cluster and controls the calibration scan process, calibration configuration and decisions made during the monitor phase. The Smart RF master switch also synchronizes RF configuration within the cluster, including radio channel, transmit power, locks, radio operating mode, rescuers and all Smart RF global configuration

During calibration, the master switch instructs all radios to begin the scan process and the client's forward learned information to the master switch. The master switch makes the appropriate channel and power decisions for each adopted radio in the cluster and forwards the changes to the clients. Each maintains the

same identical radio configuration, so if a RF Switch fails, the effected radios receive the same configuration once re-adopted by the cluster.

During the monitoring phase, each client switch forwards information to master switch which determines actions to take. For example, if a radio or AP fails, the master instructs an appropriate rescuer radio (or radios) to increase power accordingly.

The master switch maintains an active copy of all adopted radio configuration for cluster clients in non volatile memory. If the Smart RF master fails the active information on the switch is lost. However, when a new master is elected it solicits radio information from the clients. Future events from clients are then forward to the new master switch.

5.3 Network Integrity Checks

In this section we'll discuss network data threats in the form of the following:

- Threats that bring the target system down to disrupt services to genuine users. These threats are commonly referred to as *Denial of Service* (DoS) attacks.
- Hackers that gain access to a target system to either steal information or to use their illegal access as a launchpad for additional (more threatening) attacks.

A security solution should not only attempt to protect against such attacks, but also alert administrators about their possible source (unprotected machines or suspicious activity observed on the network).

5.3.1 DoS Attacks

DoS attacks are intended to consume the resources of the target in such a way that the network is unable serve genuine users. DoS attacks can be very disruptive. It's imperative wireless infrastructure devices handle them at the point of origin. Existing wired infrastructures may not be sufficient to avert the threat, as damage may have already been done by the time the wired firewall detects it. Administrators need to be alerted immediately so corrective action can be taken. DoS attacks could include:

- *LAND attacks* - A TCP SYN packet is sent with the same source and destination IP address, causing the target system to keep replying to itself and eventually lock up.
- *IP fragmentation related attacks* - Send IP fragments with overlapping, oversized, payloads to the target machine. Some attacks in this category are teardrop attacks, teardrop2, ping of death or syndrop attacks.
- *Smurf attacks* - An ICMP ping packet is sent to a broadcast address with a spoofed source address of the target machine, causing it to be overwhelmed by the volume of replies.

Other common DoS attacks are Winnuke attack, Invalid IP Protocol attack, ICMP router advertisement, UDP short header, Twinge attack, IP Source Route option, Fraggle attack, Snork attack, TCP header fragmentation, TCP short header, TCP bad sequence number, TCP post-connection SYN, TCP invalid urgent offset, TCP SYN flood, SYN cookies, SYN proxying, SYN monitoring, RFProwl, FTP bounce, TCP XMAS scan, TCP NULL scan, TCP FIN scan, very small IP TTL, Mime flood, Ascend kill and Echo/chargen.

5.3.1.1 Wireless Intrusion Detection System

A wireless *Intrusion Detection System* (IDS) tracks various events and anomalies on the wireless network and looks for suspicious activity. For example, a large number of 802.11 frames with invalid length or non-supported frame types (a frame that is neither data, control or management), or when unencrypted data frames are seen on the network even when the network is configured to use encryption. It's possible to see such anomalous packets due to transmission errors (if the number of packets is large, it might signal

suspicious activity). The event should be logged and the network administrator should use a trap. Additionally, if the source is an MU, it should quarantined and any packets from that MU dropped.

An IDS generally detects unwanted manipulations to computer systems (mainly through the Internet). These manipulations can take the form of attacks by skilled malicious hackers.

An IDS detects malicious network traffic and computer usage that can't be detected by a conventional firewall. These include network attacks against vulnerable services, data driven attacks on applications, host based attacks (such as privilege escalation), unauthorized logins and access to sensitive files and malware (viruses, trojan horses, and worms).

An IDS is composed of several components. Sensors generate security events and a console monitors events. A centralized engine records events logged by the sensors in a database and uses a system of rules to generate alerts from the security events received. There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations, these components are combined in a single device or appliance.

Rogue AP detection uses different mechanisms (AP scans on its own channel; AP scans on all channels or scans by Motorola MUs). All of Motorola's Enterprise mobility products support Rogue AP detection by either scanning an AP on its own channel, scanning on all channels or leveraging MUs to report all the devices it sees in the network. Motorola wireless switch software supports integrated Rogue AP detection capability, and issues an alert when an AP is found that does not match the approved list.

For information on how Motorola's WIPS solution provides a means for detecting and eliminating the threat of rogue devices, see *Wireless Intrusion Detection System (WIPS) on page 5-18*.

Threats on the network are frequently defined by the following malicious activity:

- Excessive authentication /association requests
- Excessive probes
- Excessive disassoc/deauth
- Excessive decryption errors
- Excessive authentication failures
- Excessive 802.11 replays
- Excessive crypto IV failures (tkip/ccmp replay)

An analysis of an attack situation often produces the following event information:

- Source MAC = destination MAC
- Illegal frame sizes
- Source MAC is multicast
- TKIP countermeasures
- All zero addresses in addresses

Motorola provides a comprehensive IDS solution (built into the switch) with an SQL database for forensics and archiving, real-time performance and troubleshooting tools, and multi-sensor correlation to detect sophisticated attacks. Motorola maintains a wireless IDS system must monitor the air 24 x 7 using a dense pattern of dedicated sensors and provide significantly more that just Rogue detection/prevention.

The IDS built into the switch needs to be tuned or the data is somewhat meaningless. The tuning of these values can be configured in one of the following two ways:

- *Route 1* - Set the values extremely high to catch DOS style attacks.

- *Route 2* - Set values you do not expect to see at that installation.

If you go with the route 1 option, you should never get any false positives. Someone or something is on your network doing bad things, like sending line rate PROBE requests to disrupt the network.

Route #2 requires intimate knowledge of the RF environment. The flexibility always exists to set values lower to allow for testing and special cases.

If you are interested in setting these to not get false positives, set the Excessive entries to be in the 1000s per second.

Warnings generated from the implementation of an IDS could include:

- Excessive probes
- Excessive associations
- Excessive disassociations
- Excessive authentication failures
- Excessive crypto replays
- Excessive 802.11 replays
- Excessive decryption failures
- Excessive unassociated Frames
- Excessive EAP start frames
- Null destinations
- Same source and destination MAC
- Source multicast MAC
- Weak WEP IV
- TKIP countermeasures
- Invalid frame lengths

IDS is disabled by default. Setting a threshold value for any alarm enables it. Motorola does not have recommended threshold values, as each depends on the user environment and the noise (level of

interference) in that environment. If a user sees any of the following alarms and believes it to be an error, Motorola recommends increasing the threshold value.

#	Alarm	Explanation	Default Value
1	EXCESSAUTHSASSOCS	MU sent to many association authentication requests	Off
2	EXCESSPROBES	MU sent too many probe requests	Off
3	EXCESSDISASSOCS	MU sent too many disassociation requests	Off
4	EXCESSAUTHFAILS	MU failed authentication (EAP or Hotspot authentications only) too many times	Off
5	EXCESS80211REPLAY	Excessive replayed packets (802.11 retries)	Off
6	EXCESSCRYPTOREPLAY	Excessive replayed packets caught with encryption	Off
7	EXCESSDECRYPTFAILS	MU sent too many packets not decryptable	Off
8	IDSNULLADDR	MU with source MAC of 00:00:00:00:00:00	Off
9	IDSSAMEADDR	Same MU MAC on 2 different APs	Off
10	IDSMCASTSRC	Multicast source address from MU	Off
11	IDSWEAKWEPIV	Excessive MU selecting weak WEP IV	Off
12	DSCNTRMEAS	Excessive TKIP countermeasures	Off

5.3.2 Wireless Intrusion Detection System (WIPS)

Rogue APs are untrusted and unauthorized access points connected to the wired LAN that accept client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured access points that do not adhere to corporate policies. An attacker can install a rogue AP with the same ESSID as the authorised WLAN, causing a nearby client to associate to it. The rogue AP can then steal user credentials from the client, launch a man-in-the-middle attack or take control of MUs to launch denial-of-service attacks.

Wireless IPS (WIPS) systems provide continuous protection against wireless threats and act as a key layer of security complementing wireless VPNs, encryption and authentication. They typically use dedicated sensor devices for actively detecting and locating rogue AP devices. After detection, they use mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

WIPS specializes in three specific data protection requirements, including:

5.3.2.1 Rogue AP Detection

Rogue AP detection involves keeping track of access points in the network and identifying rogue devices within their coverage area. This can be accomplished by the regular access points themselves, by

periodically scanning the network and keeping track of any unauthorized APs, or have dedicated APs (sensors) scan for rogues full time.

If you are using clients and infrastructure from the same vendor, the clients can also be used for supporting rogue AP detection. Motorola client devices can help detect rogue APs even in areas infrastructure APs cannot reach.

5.3.2.2 Rogue AP Locationing

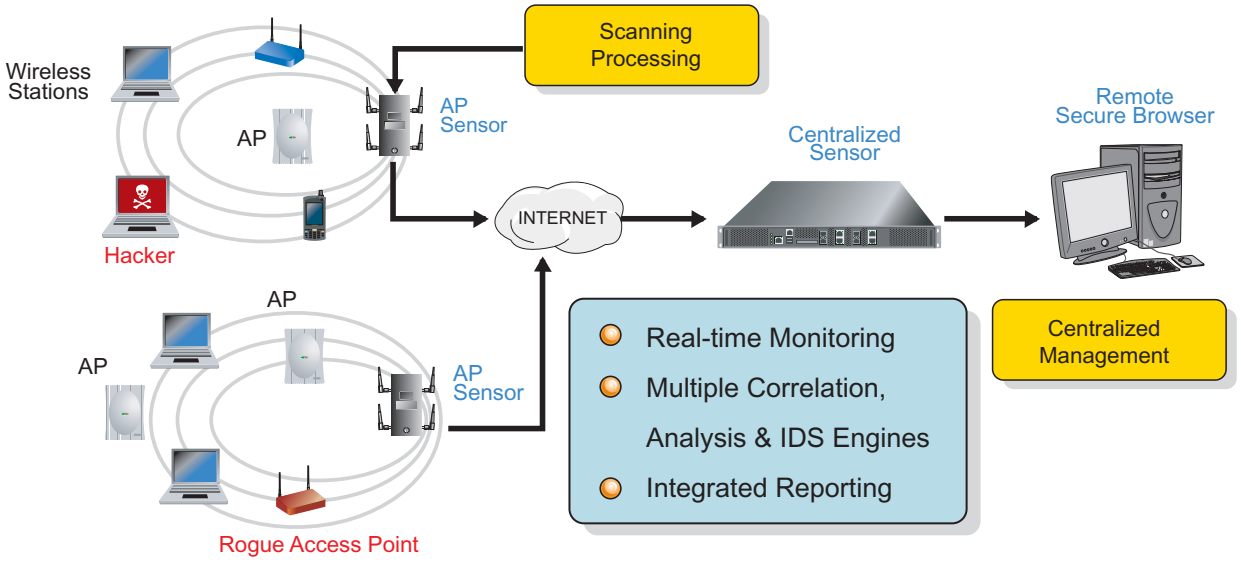
Simply detecting rogue APs is not enough, since rogue APs could be located anywhere in the Enterprise or outside the corporate boundaries. Locationing plays a vital role in intrusion prevention by pin-pointing the exact location of the rogue devices. This is done by tracking the signal strength of packets received from rogue APs. The packets provide the distance of the rogue AP from the sensor AP. Obtaining measurements from multiple sensors simultaneously increases the accuracy of the rogue device location calculation.

5.3.2.3 Rogue AP Containment

Once a rogue AP is detected, it needs to be blocked to prevent possible damage to the network. This can be done by sending deauthentication messages to the clients connected to the rogue AP (blocking the network port to which the rogue AP is connected to the network) or by a technique called *air lockdown*.

WIPS is an overlay security architecture that monitors wireless traffic, searching for rogue devices and other activities that present a threat to integrity or performance of the network. WIPS has the ability to identify unwanted intruders, physically locate them and prevent and terminate all unauthorized connections to the network. WIPS can also identify and prevent attacks to the network, such as denial-of-service and zero-day attacks. All activities are recorded into the system's database for easy recreation and forensic analysis of system performance over time. A built-in reporting system allows easy preparation of proof-of-compliance reports to industry regulators such as VISA-CISP, HIPAA, GLBA, DOD, and SOX (Sarbanes Oxley).

Motorola devices (such as the RFS7000 and WS2000) support rogue AP detection, location and containment natively. A WIPS server can alternatively be deployed as a dedicated solution within a separate enclosure.



5.3.3 Stateful Firewall Inspection at the Layer 2 level

Traditional firewall functionality is based on access control policies applied to the WLAN, VLAN or MAC/IP address in a static way. Incoming packets are matched against the entire set of ACL rules to determine whether they should be allowed or denied. However, they don't recognize the state of the network connections to which the packet belongs and thus are prone to spoofing attacks and other nefarious exploits.

Stateful packet inspection keeps track of network connection states (such as TCP stream) and determines which packets are legitimate based on the current state of the connection. Only packets matching a known connection state are allowed by the firewall, the others are rejected. For example, a packet claiming to part of a data transfer over FTP will be blocked until the firewall has seen the FTP control connection established and the data port dynamically opened.

Stateful packet inspections provide protection against various protocol header attacks, IP spoofing attacks, IP fragmentation and reassembly based attacks and TCP protocol state based attacks.

Having a firewall at the Layer 2 level helps detect Layer 2 protocol attacks, including:

- ARP cache poisoning and spoofing detection and protection
- Intelligent transmission of broadcast traffic
- Various fragment attack check
- Un-authorized MU activity monitoring and detection
- MAC or IP spoof

5.3.3.1 ARP Cache Poisoning/Spoofing

ARP cache poisoning is the act of introducing a specious IP-To-Ethernet mapping in another host's ARP cache. This results in a diversion of traffic, either to a different host in the LAN or to no host at all. ARP spoofing, also known as a *Man in the Middle* attack, can therefore be used to compromise a subnet.

Consider nodes A, B and C within a network. In general, when node A wants to communicate with node C, it sends an ARP request. Node C sends an ARP reply including a MAC address. Even in a switched environment, the initial ARP request is sent in a broadcast manner. It is possible for node B to craft and send an unsolicited, fake ARP reply to node A. This fake ARP reply specifies node B has the MAC address of node C. Node A will unwittingly send traffic to node B, since it professes to have the intended MAC address.

Stateful firewalls can maintain flows for DHCP requests by wireless clients and t a DHCP binding table can be built to maintain and verify the MAC-IP binding, helping in mitigating the threat.

5.3.3.2 Intelligent Broadcast Traffic Transmission

By observing network traffic over a period of time, a firewall can build a database to optimize the transmission of broadcast traffic instead of blindly forwarding it to everybody. For example, a gateway port and DHCP server port can be learned by the firewall to optimize broadcast traffic transmissions to certain ports, because that response is going to be anticipated from only that port.

Therefore, a layer 2 stateful firewall proves much more effective in mitigating attacks than a layer 3 firewall.

5.4 Network Privacy

A WLAN uses air as its transmission medium. When confidential company secrets, intellectual property, financial or personal information are transmitted over air, it can be accessed by an unauthorized individual capturing it. Encryption is a method of encoding data in a manner that no one but its intended recipient can

interpret its content. Secure encryption protocols should be used for the encryption of data while traversing the air, or preferably until it reaches its the final destination.

5.4.1 WPA/WPA2

Since it's easy to capture wireless traffic using freely available tools, it's imperative the data is encrypted using secure cryptographic methods. A WLAN should ideally use *Advanced Encryption Standards* (AES) available through WPA2 (802.11i) in combination with secure authentication protocols provided by 802.1x. AES is considered secure, but it might not be available for legacy hardware. Legacy hardware should use TKIP for encryption (available through WPA) and avoid WEP which can be cracked in minutes using widely available tools.

5.4.2 IPSec VPN

A VPN ensures privacy of data between two end points even while using a communication medium which is itself insecure (like the Internet). VPNs create a secure tunnel between two end points, as if they are directly connected over a secure connection. Traffic is secured using robust encryption techniques, like IPSec or SSL.

You can get the safety of a VPN in a WLAN by hosting the VPN server at the AP (or wireless controller), and installing the VPN client software on the MU. For that reason, a VPN provides secure WLAN access to MUs. A VPN solution was more common before 802.11i was introduced, but is not as common now, since 802.11i/WPA2 is considered more secure.

VPN tunnels can also be used to secure traffic to an external syslog or Radius server, if they support VPN. The only issue with a VPN solution is interoperability between different vendor solutions is not guaranteed.

5.4.3 End to End Security

When taking precautions to secure wireless traffic from a MU to an access points, one should not lose sight of the security solution in it's entirety, since the chain is as weak as its weakest link.

5.4.3.1 Traffic Between a Controller and Thin Access Points

Wireless access is no longer limited to corporate premises, it extends to the cafeteria, reception area and even the parking lot where visitors can access. Access points can be extended to these areas using an Ethernet cable vulnerable to a hacker. With some wireless controllers, encryption occurs at the access point, so data is only secure until it reaches the access point. It's important data be secure even when traversing this segment. Consequently, decryption should occur at the wireless controller instead of the AP, or the link between the controller and the AP should be secured using a method such as a VPN.

5.4.3.2 Mesh Links

When a WLAN is extended using a mesh network, the security of the mesh links should be ensured. Mesh links are prone to the same attacks as any wireless link between a MU and an access point. The mesh link can be secured using a IPSec VPN connection, or by using a WLAN security protocol such as WPA or WPA2.

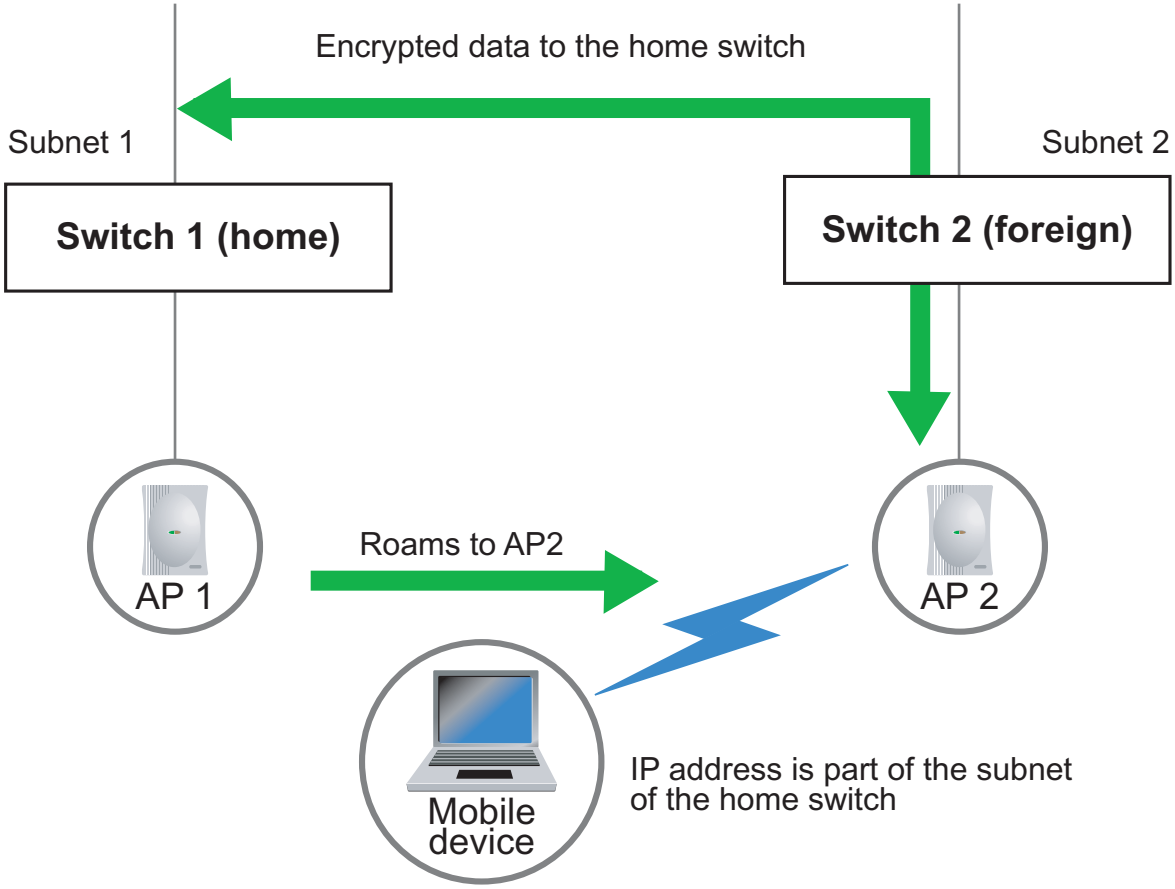
5.4.3.3 Layer 3 Roaming

Layer 3 roaming entails a MU roaming across a layer 3 boundary but still keeping the original IP address of the client. It happens when a MU leaves its currently associated switch (home switch) in one subnet and

associates with another wireless switch in different subnet within it's mobility domain (within the same WLAN).

When the MU roams to an AP adopted by a foreign switch (switch-2), the switch sends a notification to the home switch and all packets to and from the MU are routed through the home switch.

If data decryption takes place at AP2, the data flows un-encrypted from AP2 to the home switch (which is insecure). It should be ensured the foreign switch sends the encrypted packet to the home switch (where decryption takes place). Or a secure tunnel (an IPSec VPN for example) should be formed between the two switches, so the data remains encrypted and protected between the home switch and the AP the MU is currently associated with.



5.5 Certifications and Legal Requirements

The following sections describe the certifications and legal requirements addressed in the development of Motorola's Enterprise WLAN offerings. These certifications and requirements include:

- *FIPS 140 Certification and Common Criteria (CC)*
- *PCI Compliance*
- *Wi-Fi Certification*
- *Senior Management Liability*

For an overview of the WiFi security standards impacting your Motorola Enterprise WLAN deployment, refer to *WiFi Security Standards Overview on page 5-30*.

5.5.1 FIPS 140 Certification and Common Criteria (CC)

The *Department of Defense* (DoD) requires commercial WLAN systems incorporate extensive measures to protect the voice and data traffic proliferating a wireless network. In standardizing their WLAN security requirements, the DoD defined *Federal Information Processing Standards* (FIPS) 140-2 and Common Criteria, including WLAN Access System Protection Profile requirements.

The FIPS 140 standards are a series of US government computer security standards that specify requirements for cryptography modules. For the certification, a wireless solution must pass a series of comprehensive security tests, including a vulnerability and penetration analysis. The wireless solution's design metaphor and source code are scrutinized by experts to ensure its compliance with advanced cryptographic standards.

Like most typical DoD WLAN deployments (and their inherent data protection challenges), retail, health care, financial and wireless carrier businesses are under increasing pressure to ensure information is secure across their wireless networks. The majority of these institutions are implementing the same standards mandated by the U.S. government. For this reason, FIPS certification has become central to demonstrating a WLAN security deployment acceptable for its maturity.

Motorola's WS5100 and RFS7000 are certified to meet the most stringent security requirements set forth in DoD Directive 8100.2. Motorola's WS5100 and RFS7000 have the following pedigree:

- Compliant with DoD Directive 8100.2
- US Government Wireless Local Area Network (WLAN) Access System Certified with Protection Profile for Basic Robustness Environments
- FIPS 140-2 - Certified for Level 2
- Common Criteria (CC) - Certified for Evaluation Assurance Level 4 (EAL4)

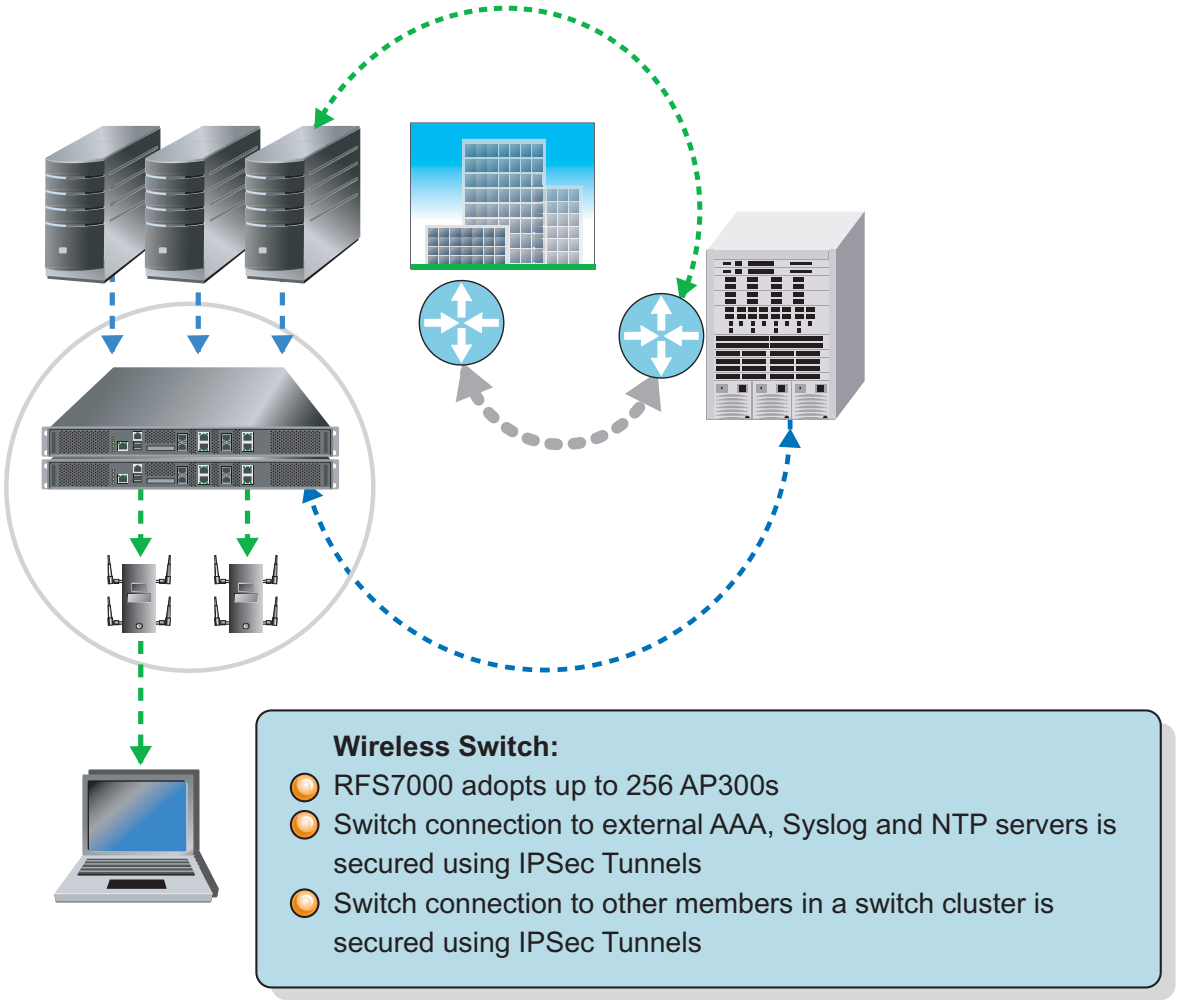
For more information on FIPS and Common Criteria and Motorola's FIPS offerings, refer to:

- *Targets for FIPS and CC*
- *Protection Profile*
- *FIPS 140-2*
- *Common Criteria*
- *FIPS and Common Criteria Additions and Modifications*
- *Robustness Profile Requirements*
- *Motorola's FIPS and CC Unsupported Features*
- *Motorola's FIPS and CC Additions*

5.5.1.1 Targets for FIPS and CC

The primary targets for FIPS and CC certified wireless infrastructures include:

- Government organizations
- Financial institutions
- Other verticals requiring the highest levels of security



5.5.1.2 Protection Profile

US Government *Wireless Local Area Network* (WLAN) Access System Protection Profile For Basic Robustness Environments

This is the final step in achieving total DoD Directive 8100.2 compliance. All new DoD acquisitions for *commercial off-the-shelf* (COTS) WLAN systems MUST be evaluated against this protection profile.

5.5.1.3 FIPS 140-2

The FIPS 140-2 standard defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems. The requirements include:

- Basic design and documentation
- Module interfaces
- Authorized roles and services
- Physical security
- Software and operating system security
- Key management

- Cryptographic algorithms
- EMI/EMC and self-testing

Security level 2 enhances physical security by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers on doors of the module.

5.5.1.4 Common Criteria

The common criteria was developed as a standard to replace existing security evaluation criteria used by different countries around the world.

The criteria includes an assurance scale (evaluation assurance levels) applied to generate confidence levels in the security of products. How much confidence is required is a matter for users to determine, in relation to the value of the assets to be protected, the threat potential, and available budget.

5.5.1.5 FIPS and Common Criteria Additions and Modifications

Refer to the following FIPS and common criteria additions and modifications to understand its relevance for potential DoD supported deployments:

FIPS Feature Additions

The FIPS baseline has had the following recent additions:

- KAT, CRNG and power on self tests for QuickSec and OpenSSL libraries
- Changing static OpenSLL into dynamic library.
- Security between switch and NTP server.
- Security between switch and auth server (Radius)
- Security between switch and log server (SYSLOG)
- WIPE command to erase all keys and passwords.
- Firmware and Writable date integrity check
- Zeroization of keys.
- Introduction of crypto officer and other roles (different from regular roles that we have in our existing CLI)
- Upgrade and downgrade support (this includes new digitally signed key to be added which should be through FIPS approved algorithm used)
- Authentication strength for CLI management access
- Authentication strength for applet management access
- Role based authentication
- Test for hardware components
- Any test failure- handle the state machine and reboot the box

FIPS Feature Modifications

The FIPS baseline has had the following recent modifications:

- Cert manager, DHCP, Radius, stunnel, OpenSSH modified for CRNG, version compatibility and FIPS approved algorithm usage
- Wireless - power on self-test, KAT test for current AES library
- Removing/suppressing all non-approved commands as part of FIPS (including debug and other commands)
- Core dump, panic dump and root shell access removal.
- VPN and IPSec tunnel for switch to server communication
- Display of crypto keys. (Getting more than one confirmation)
- QuickSec changes to have approved algorithm.
- Disable capabilities for SNMP and applet
- FIPS documentation support for security target and protection profile documents
- Layer 3 mobility and cluster peers formed under IPSec/VPN tunnels

FIPS Common Criteria Additions

The FIPS Common Criteria has had the following recent additions:

- Audit event generation and configuration
- Cryptographic key destruction
- Access banner to intercept EAP and other authentication packets exchanged between the MU and Radius server in order to locate a user-name
- Additional self test requirements based on user request
- Verification of integrity of data on the switch (non binary)
- Hardware critical test
- Automatic power-up tests for crypto key generation
- Event audit management and configuration
- Switch-lockup when admin reaches max password attempt (only the serial port is then accessible)

FIPS Common Criteria Feature Modifications

The FIPS Common Criteria baseline has had the following recent modifications:

- Packet zeroization and overwrite
- Overwrite capabilities for all intermediate, private and plain test keys
- Logging on/off for audit events

Robustness Profile Requirements

The US Government WLAN Access System Protection Profile For Basic Robustness Environments Mandates a Secure connection be established with any external server or device.

Motorola's WS5100 and RFS7000 wireless LAN switches in FIPS and CC mode establish an IPSec Tunnel for:

- Security between the switch and NTP server.

- Security between the switch and AAA (Radius)
- Security between the switch and log server (SYSLOG)
- Security between switches within a cluster

5.5.1.6 Motorola's FIPS and CC Unsupported Features

Refer to the following for an understanding of those features supported by the Motorola wireless switch platform, but not within the Motorola FIPS and CC offerings:

#	*Feature*	*WIOS Version*	*Incorporated*
1	Rogue AP detection enhancements	2+	Not Sure
2	Adaptive AP (not FIPS compliant)	2+	No
3	Adaptive AP statistics (not FIPS compliant)	2+	No
4	Enhanced wireless IDS (not FIPS compliant)	2+	No
5	NAC (not FIPS compliant)	2+	No
6	Auto-Install (not FIPS compliant)	2.0	No
7	EAP-TTLS (PAP and CHAP) (not FIPS compliant)	2.0	No
8	WEP 64, 128 and TKIP (not FIPS compliant)	2.0	No
9	Copy tech support (not FIPS compliant)	2.0	No
10	FTP, TFTP and copy commands (not FIPS compliant)	2.0	No
11	Upgrade and downgrade using TFTP, FTP and HTTP (not FIPS compliant)	2.0	No
12	External Kerberos Server (not FIPS compliant)	2.0	No
13	Applet	2.0 and 2+	No
14	SNMP	2.0 and 2+	No
15	Open SSH (not FIPS compliant)	2.0	No
16	Telnet	2.0	No
17	Root shell access	2.0	No
18	Help desk user roles	2.0	No
19	NTP client with broadcast discovery server	2.0	No
20	IPSec/VPN tunnels using Public key crypto-graph protocols (RSA and DSA)	2.0	No
21	CLI password reset without logging into CLI	2.0	No
22	GDB, Strace (not FIPS compliant)	2.0	No
23	Debug commands (not FIPS compliant)	2.0	No
24	RFMS (since there's no SNMP support)	2.0	No
25	MSP (since there's no SNMP support)	2.0	No
26	Packet capture	2.0 and 2+	No

5.5.1.7 Motorola's FIPS and CC Additions

Refer to the following for a review of the features added by Motorola to their FIPS and CC offerings:

#	Feature	WIOS Version	Incorporated
1	Power on self test for RNG, KAT and key pair generations		Yes
2	IPSec/tunnels between cluster, layer 3 mobility peers and between the switch and external servers (Radius, Syslog and NTP server)		Yes
3	Zeroization of keys		Yes
4	Switch access authentication strength		Yes
5	Audit event generation and management		Yes
6	Firmware integrity		Yes
7	Data integrity		Yes
8	On demand self test execution		Yes
9	Access banner		Yes
10	Crypto keys destruction		Yes

5.5.2 PCI Compliance

The *Payment Card Industry Data Security Standard* (PCI-DSS) was established in 2005 by a group of major credit card companies to provide a set of security guidelines to help retailers prevent credit card fraud and identity theft. The standards include a secure network with a firewall and access control measures, the maintenance of a network vulnerability management program (the latest anti-virus software) and protection for a cardholder's personal data.

Any retailer that accepts, processes or stores credit card information must comply with the standards set by the *Payment Card Industry* (PCI) Security Standards Council or risk a substantial penalty. It's in a retailers best interests to ensure any technology they invest in is PCI compliant.

If a retailer is not PCI compliant at the time a breach occurred, that retailer will likely be responsible for the damages incurred during the breach. However, the credit card company is generally liable for damages (if the retailer was PCI compliant at the time of breach). Many credit card companies charge hefty fines (up to $500,000 per violation) in cases of non-compliance, regardless of whether the network has been compromised.

A WLAN is considered a public network, and the PCI standard includes several guidelines specific to WLANs. A WLAN infrastructure should adhere to these stringent guidelines to be PCI compliant. Some of these requirements include preventing wireless access to credit card data using a firewall, changing the default (out of box) settings of wireless devices and mandating an encryption scheme encryption (using WPA/WPA2

or IPSec). It is invaluable to have the reporting and forensic tools necessary to keep comprehensive records of network activity.

5.5.3 Wi-Fi Certification

The Wi-Fi alliance was formed in 1999 by several industry leaders to drive a single worldwide accepted standard for WLAN. It conducts Wi-Fi certification of wireless devices to ensure they implement universal 802.11 specifications through a series of rigorous tests. Checking for Wi-Fi certification within a WLAN and its infrastructure ensures the deployment supports standards based Wi-Fi Protected Access (WPA/WPA2) security (mandatory for all wireless LAN devices).

5.5.4 Senior Management Liability

If you think the law only goes after the criminal/hacker in cases of data loss due to a security breach, you may only be partially correct. Federal sentencing guidelines recognize the responsibility of senior management in ensuring resources and policies are in place to maintain the security of business systems and sensitive corporate information. Senior management can be held personally liable if it is proved security systems and policies are lacking. In 1997, federal sentencing guidelines were extended to apply to computer crime, and senior management can be personally liable up to $290 million in fines. It is in the best interest of a company and its management that corporate security is top priority and all aspects are careful considered.

5.6 WiFi Security Standards Overview

802.1x is an IEEE standard used as a basis for authentication on all 802 networks, including Ethernet, token ring and WLANs. IEEE 802.1X specifies how EAP information should be encapsulated in frames.

To effectively enable mobile security, 802.1X must be supported by WLAN infrastructure equipment as well as mobile-device operating systems and authentication services.

For information on the 802.1x standards and how they impact the deployment of Motorola Enterprise WLAN infrastructure, refer to the following:

- *802.1x Framework and EAP Overview*
- *802.11 Deployment and Security Issues*
- *IEEE Security Options*
- *802.1x Motivation and Overview*
- *EAP Overview*
- *Windows Implementations - Transaction Level Security (EAP-TLS)*
- *802.1x and IEEE 802.11*
- *Roaming Issues*
- *802.1x Summary*

5.6.1 802.1x Framework and EAP Overview

802.11 WLANs are being increasingly used in public and semi-public spaces. One of the major drawbacks to current [802.11] WLAN systems is the lack of effective and scalable Enterprise security mechanisms that prevent growing deployments from properly scaling. The following sections provide an overview of the

802.1X security framework and how it can improve upon the security implementations in IEEE 802.11 networks.

5.6.2 802.11 Deployment and Security Issues

There are three major issues that need to be considered while deploying 802.11 systems:

- *Integration with user administration tools*

  There is a need to provide a mechanism to associate end-user identity with the port used to access to a LAN. Currently, the identification mechanism used is based on MAC address, but identification based on user name is easier to administer within large network environments. This makes it easier to enable billing and accounting services and personalize network access. I

- *Key Management*

  Currently, MUs and APs have static encryption keys that are difficult to manage, especially as the number of users grows. There is a need for dynamic, per-session, key management that circumvents this problem.

- *Security*

  There are a number of security issues with the way current IEEE 802.11 systems are implemented. Primary among them:

  - IEEE 802.11 systems are vulnerable to a number of security attacks
  - There is no mechanism for user identification and authentication
  - No support for centralized authentication, authorization, or accounting support
  - No management of dynamic session keys
  - There is no per packet authentication

5.6.3 IEEE Security Options

Authentication and encryption services for 802.11 systems are based on the WEP algorithm.

- *Authentication* - There are two subtypes of authentication services supported: Open system and shared key. Open system is a default null authentication algorithm that involves a 2-step process consisting of an identity assertion and request for authentication followed by an authentication result.

  Shared key supports the authentication of an MU as either a member of those who know a shared key or those who do not. The current standard assumes the shared key is supplied to the MU over a secure channel, independent of the 802.11 wireless communication channel.

- *Encryption* - WEP provides encryption services (comparable to a wired medium) to protect against unauthorized access to a WLAN. A WEP algorithm defines the use of either 40 or 104-bit keys for authentication and encryption. With a symmetric algorithm the same key is used for cipher and decipher.

5.6.4 802.1x Motivation and Overview

The IEEE 802.11 *Task Group I* (TGi) is adopting the 802.1X framework to improve security implementations. The growing use of 802.11 supported WLANs in public spaces and Enterprises, coupled with the need for a secure user-based authentication service were some of the motivating factors in the adoption the 802.1X

security framework. There is also a need for integrating accounting and billing mechanisms as well as personalizing the network access environment.

IEEE 802.1X is a draft standard for *port-based* network access control to provide authenticated network access for Ethernet networks. It specifies:

- A protocol between devices requiring access to a bridged LAN and devices providing access to the bridged LAN.
- Requirements for a protocol between an authenticator (AP) and an authentication server (Kerberos) as well between MUs and APs. An authenticator is the entity requiring the entity on the other end of its link to be authenticated.
- Different levels of access control and the behavior of the port providing access to the bridged LAN.
- Management operations via SNMP

A central issue, is the lack of a WEP key-management protocol that limits security services, especially in large wireless infrastructures.

802.1X is a flexible security framework implemented in the upper layers, which allows the plug-in of new authentication or key management methods without changes to an AP or a MU. 802.1X builds on existing network access control protocols (such as EAP and Kerberos). 802.1X supports user authentication and dynamic key management.

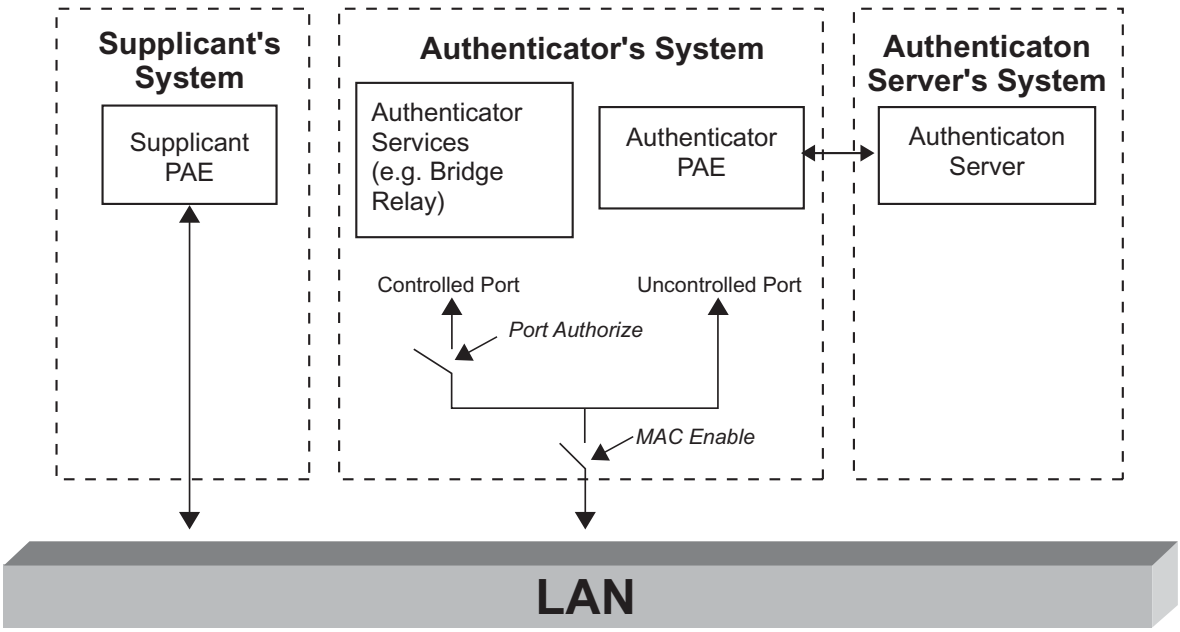
Port-based network access control utilizes physical characteristics of the switched LAN infrastructure to provide a means of authenticating devices attached to a LAN port, and for preventing access to that port in cases where authentication fails. 802.1X defines a *Port Access Entity* (PAE), which is a LAN port that can adopt one of two roles in an access control interaction (the role of *supplicant* or *authenticator*). The

supplicant is a port requesting access to services accessible via the authenticator's port. An authenticator is a port that enforces authentication before allowing access to services accessible via that port.

The 802.1X standard enables a switch to deny access to network resources until authentication between the supplicant (MU), AP and authentication server has been completed.

802.1X adds security by preventing users from attempting DoS attacks or other malicious actions while the network is determining whether a DHCP lease should be assigned to the user.

General 802.1X operation can be illustrated as follows:



5.6.5 EAP Overview

Extensible Authentication Protocol (EAP) is an IEF-proposed extension to *Point-to-Point Protocol* (PPP) that allows arbitrary authentication mechanisms to be employed for the validation of a PPP connection (RFC 2284). EAP has been made available in response to an increasing demand to augment *Remote Access Server* (RAS) authentication with third-party security devices. These authentication schemes include token cards, Kerberos V5 protocols, one-time passwords, and public key authentications (using smart cards and certificates). EAP works with dial-up, PPTP and layer 2 clients. EAP is a critical technology component for secure *Virtual Private Networks* (VPNs) because it provides more security against brute force or dictionary attacks (where all possible combinations of characters are attempted) than other authentication methods, such as CHAP (*Challenge Handshake Authentication Protocol*). With PPP authentication protocols, a specific authentication mechanism is chosen during the link establishment phase. Then, during the connection authentication phase, the negotiated authentication protocol is used to validate the connection. The authentication protocol itself is a fixed series of messages sent in a specific order.

With EAP, the specific authentication mechanism is not chosen during the link establishment phase. Instead, each PPP peer negotiates EAP during the connection authentication phase. Once the connection authentication phase is reached, PPP peers must first negotiate the use of a specific EAP authentication scheme (known as an EAP type). Once the EAP type is agreed upon, EAP allows an open-ended conversation between the remote access client and the remote access server that can vary based on the parameters of

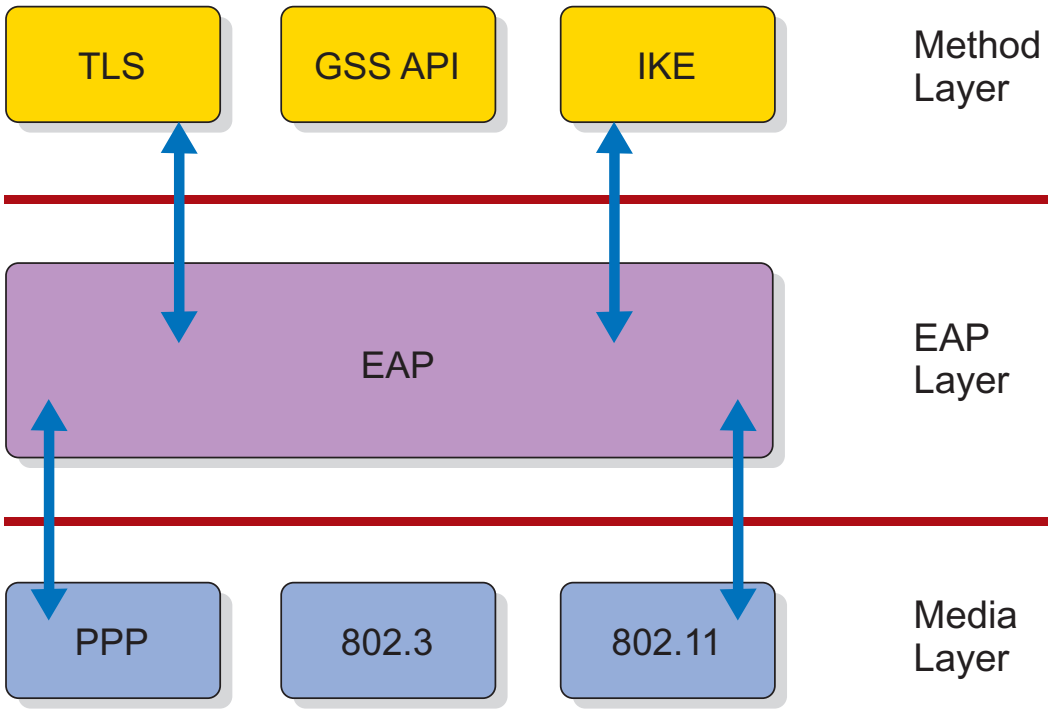
the connection. The conversation consists of requests for authentication information and responses. The length and detail of the authentication conversation is dependent on the EAP type.

EAP is a simple encapsulation protocol that provides a flexible link layer security framework and has no IP dependency. In addition to PPP, it also runs over 802.3 and other link layers. It does not assume a physically secure link, as EAP provides the security services and it can run over lossy or lossless media.

When EAP is used with security token cards, the remote access server can separately query the remote access client for a name, PIN, and card token value. As each query is asked and answered, the user passes through another level of authentication. When all questions have been answered satisfactorily, the user is authenticated and permitted access to the network.

Architecturally, EAP is designed to allow authentication plug-in modules at both the client and server ends of a connection. By installing an EAP library file on both the remote access client and the remote access server, a new EAP type can be supported. This presents vendors with the opportunity to supply a new authentication scheme at any time. EAP provides the highest flexibility in authentication uniqueness and variations.

The following figure illustrates the EAP architecture:



5.6.6 Windows Implementations - Transaction Level Security (EAP-TLS)

EAP methods supporting mutual authentication are recommended for use with 802.1X to guarantee a key is transferred to the right entity in order to prevent man-in-the-middle and rouge attacks. EAP methods supporting mutual authentication include:

- *Transport Level Security* (TLS)
- *Internet Key Exchange* (IKE)
- *GSS_API (Including Kerberos)*

EAP-TLS has been submitted to the IETF as a draft proposal for a strong authentication method based on public key certificates. With EAP-TLS, a client presents a user-certificate to a dial-in server, while at the same time, the server presents a server certificate to the client. The first provides strong user authentication to the server, the second provides assurance the user has reached the server expected. Both systems rely on a chain of trusted authorities to verify the validity of the offered certificate.

The user's certificate could be stored on the dial-up client PC, or stored in an external smart card. In either case, the certificate cannot be accessed without some form of user identification (PIN number or name/password exchange) between the user and the client PC. This approach meets the *something you know plus something you have* criteria recommended by most security experts.

EAP-TLS is the EAP method implemented in Windows NT 5.0. Like MS-CHAP, EAP-TLS returns an encryption key to enable subsequent data encryption. Microsoft® Windows® 2000 supports the EAP. It allows third-party authentication modules to interact with the implementation of PPP included in Windows 2000 RAS. The EAP client is supported on Windows 2000 Professional. However, the RAS server provided with Windows 2000 Professional does not support EAP server functionality.

5.6.7 802.1x and IEEE 802.11

An extension to the basic IEEE 802.1X protocol is required to allow a wireless access point to securely identify the traffic of particular clients. This is done by passing an authentication key to the client and to the wireless access point as part of the authentication procedure. Only authenticated clients know the authentication key, and the authentication key encrypts all packets sent by a client. Without a valid authentication key, an AP (authenticator) inhibits all traffic flow through it.

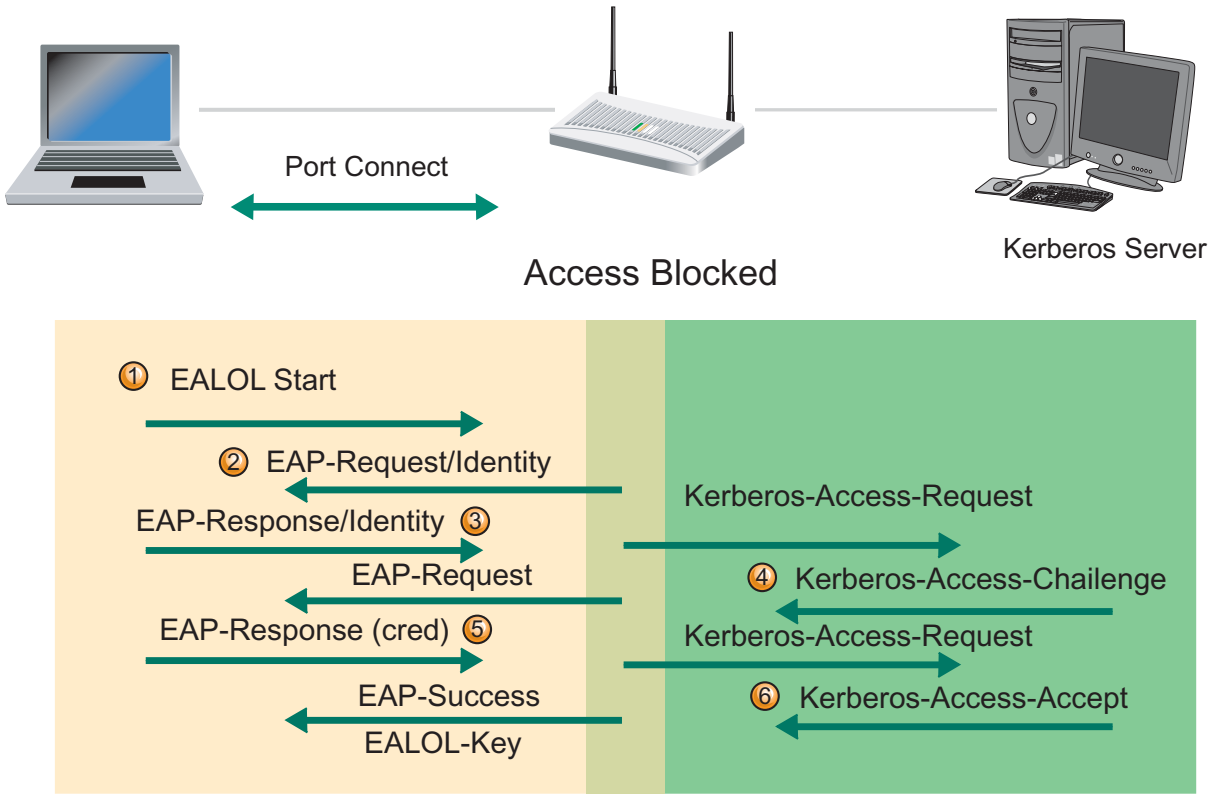
When an MU comes in range of a wireless AP, the following sequence occurs:

8. The wireless AP issues a challenge to the wireless MU. The protocol encapsulates EAP in 802 frames.
9. Upon receiving the challenge from AP, the MU sends its identity to the AP.
10. The AP forwards the MU's identity to the authentication server to initiate authentication.
11. The authentication server requests the credentials of the MU, specifying the type of credentials required to confirm identity.

    Information is exchanged between the MU and authentication server through an uncontrolled port on the AP, as the MU cannot directly reach the authentication server. The AP does not allow communication via the controlled port because the MU does not possess an authentication key.
12. The MU sends the credentials to the authentication server.
13. Upon validating the credentials, the authentication server transmits an EAP-Success packet to the peer. It then sends an authentication key to the AP. The authentication key is encrypted so only the AP can access it.
14. If the authentication server cannot validate the credentials (unacceptable responses to one or more requests), LAN access is blocked for the MU.

    The authenticator in this case transmits an EAP-Failure packet.
15. The AP uses the authentication key received from the authentication server to securely transmit a MU unicast session key and a multicast/global authentication key to the MU.

    An 802.1X conversation (with a Kerberos authentication server as an example) is illustrated below:



Following authentication, the IEEE 802.1X protocol should be configured to request the MU to periodically re-authenticate, at a user-defined interval. The authentication process is as follows:

1. A wireless AP is configured to inhibit data traffic from being forwarded either to a wired network (such as the Ethernet) or to another wireless MU without valid authentication keys.

   The wireless AP and MU must support a multicast/global authentication key. It is also acceptable for them to support a per-MU unicast session key. The wireless AP has a process that listens for IEEE 802.1X traffic both with and without authentication keys.

2. If the AP observes a new MU associating with it, the IEEE 802.1X process in the AP transmits an EAP-request (identity) to the new MU.

   If the AP IEEE 802.1X process receives an EAP-start message from the MU, the IEEE 802.1X process transmits an EAP-request (identity) to the MU. The MU transmits an EAP-start on associating with a new AP.

3. A MU transmits an EAP-response (identity) containing the machine name in response to the EAP-request (identity) if there is no user logged on to the machine.

   A MU transmits an EAP-response (identity) containing the user name in response to an EAP-request (identity) if there is a user logged on to the machine.

4. The wireless AP forwards the EAP-response (identity) message to a Kerberos server.

   The Kerberos server sends an EAP-request (either MD5 challenge or TLS) in response to the EAP-response (identity) message from the MU (TLS is required for wireless). The wireless AP forwards the EAP-request from the Radius server to the MU.

5. The MU transmits an EAP-response (containing its credentials) to the Kerberos server via the wireless AP. The wireless AP forwards the MU's credentials to the Kerberos server.
6. The Kerberos server validates the MU's credentials and generates a success message to MU.

   The Kerberos server's response to the wireless AP contains the MU message and the encryption key derived from the EAP-TLS session key. The wireless AP generates the multicast/global authentication key by generating a random number or selecting it from an existing value. On receiving the Kerberos server message, the wireless AP forwards the success message to the MU.
7. The wireless AP transmits an EAP-key message to the MU containing the multicast/global authentication key encrypted using the per-session encryption key.

   If the wireless AP and MU support the per-MU unicast session key, the AP uses the encryption key sent from the Radius server as the per-MU unicast session key.
8. When the wireless AP changes the multicast/global authentication key, it generates EAP-key messages, where each message contains the new multicast/global authentication key encrypted with the particular MU's per-MU unicast session key.

   The wireless AP adds the per-MU unicast session key, if supported, to the per-MU list of unicast session keys.
9. The MU, on receiving the EAP-key message, uses the per-MU unicast session encryption key to decrypt the multicast/global authentication key.

   If the wireless AP and MU support per-MU unicast session keys and a multicast/global authentication key has been received, the encryption key derived from the EAP-TLS session key is passed to the wireless MU as the per-MU unicast session key.
10. When the wireless network adapter driver receives the authentication keys, it must program the wireless MU network adapter.

    Once the authentication keys have been programmed, the MU invokes DHCP to restart the DHCP process.

5.6.8 Roaming Issues

When a MU roams between APs, the previous AP's address should be passed to the new AP by the MU. If however, the APs do not offer inter-AP support, the MU will have to go through a re-authentication process with the new AP. Criteria need to be defined allowing the new AP to obtain authentication information from the old AP and send a new EAPOL-key message to the MU with a new set of WEP keys.

These roaming issues can be addressed in one of two ways:

- Non-Motorola products can use the on-board Radius server built into the switch
- If the MU has a Motorola radio, no-reauthentication will talk place

5.6.9 802.1x Summary

802.1X is a flexible security framework implemented in the upper layers and enables the plug-in of new authentication and key-management methods without changing the MU or AP. In this framework, security conversations are carried out between the MU and the authentication server. The NIC and AP act as pass through devices. 802.1X uses the EAP framework with the following features:

- Provides user identification and strong authentication
  - 802.1X users identified by user names; not MAC addresses
- Dynamic key derivation
  - 802.1X enables secure derivation of per-user session keys
  - Makes per-user WEP keys easy to administer - There is no longer a need to store WEP keys on the NIC or AP
  - Attacks are more difficult since WEP key varies from session to session
  - Global keys can be sent from AP to client encrypted in session key
- Mutual authentication
  - EAP methods supporting mutual authentication is used (TLS, IKE, GSS_API (Kerberos))
- Dictionary attack precautions
  - Primary focus is non-password based authentication
  - Token cards, Certificates, Smartcards, one-time passwords, biometrics not vulnerable to dictionary attacks
- Some of the advantages of this framework include
  - Decreased hardware cost and complexity
  - Enables customers to choose their own security solution
  - Enables rapid response to security issues
  - Requires only modest hardware changes to implement the latest, more sophisticated authentication and key-management techniques

5.6.9.1 Conclusion

All of Motorola Enterprise wireless infrastructure products support 802.1x and all the EAP types. Which EAP type to use depends on the application and what the hardware platform supports.

6

Wireless Switch Architecture

This chapter describes Motorola's wireless switch architecture, including:

6.1 Wi-NG Architecture

Motorola's *Wireless Next Generation* (Wi-NG) architecture offers the superior performance required for Enterprise mobility and multimedia applications. Beyond traditional wireless networking, Wi-NG provides a single RF switching platform that allows administrators to easily deploy and manage evolving RF networks from one central location. Wi-NG optimizes voice performance and enables seamless campus-wide roaming across subnets without the need to re-authenticate. Highly scalable, it is designed to offer enhanced security, including advanced intrusion detection tools, making it ideal for large Enterprise, health care, manufacturing, education, and transportation and logistics environments. Wi-NG also lays the foundation to support emerging RF technologies including RFID, Mesh, WiMax and *fixed/mobile convergence* (FMC).

The switch builds on the power of Motorola's award-winning, industry's first wireless switch, the WS5000, adding more throughput and capacity to support the largest organizations. Ideal for health care, educational and retail/distribution and transportation/logistics industries, the switch delivers superior Enterprise class security, functionality, scalability, performance, and manageability and supports Motorola's family of *thin* access ports.

The Power of Centralized Intelligence

Motorola's switch platform delivers Enterprise class security and scalability, manageability, availability, reliability and total cost of ownership savings.

End-to-End Layered Security

Motorola's comprehensive security mechanisms include access-control, integrated authentication and encryption and intrusion protection systems that can be deployed at various locations (the perimeter, the network, servers and client devices). Motorola's RF switch is the wireless gate keeper for your Enterprise network with support for the wireless security standards of today and the ability to easily upgrade to tomorrow's standards.

Centralized Management

Motorola's RF switch supports the unified management of hardware, software configuration and network policies. Centralized management also enables the automatic configuration of access ports eliminating the need and costs of configure and managing individual access points.

Reliability

The low risk and high business value of multi-layer network designs is extended to wireless networks with the flexible overlay architecture of Motorola's RF switch. The RF switch is designed to be integrated with the reliable approach of multi-layer networking to enable predictable and high performance wireless networks, while preserving network integrity. In addition, the RF switch can be implemented using the standard networking best practices of modularity.

Lower Total Cost of Ownership

Motorola's RF switch removes the overhead and complexity of first generation access point-based wireless LANs. Extensive functionality, expandability and centralized management eliminate time and management costs associated with access point-based solutions, providing a lower total cost of ownership and outstanding investment protection. Motorola's *Enterprise Mobility Services* offer comprehensive support and technical expertise to design, deploy and maintain successful mobility solutions.

Refer to the following section for a further understanding of the technology and feature set supported by Motorola's Wi-NG architecture:

- *Interfaces*
- *ACS Support*
- *Virtual AP*
- *Clustering*
- *Management*
- *RF Switch Architecture*
- *Wi-NG Architecture Wired Features*
- *Radio Features*
- *Recent "Key" Wi-NG Enhancements*

6.1.1 Interfaces

Motorola's RF switch is an easily configurable system supported via Java applet, CLI and SNMP (v2, v3). In the wireless switch (centralized architecture), access ports are *discovered* using a Motorola proprietary protocol. Once discovered, the switch downloads the run time configuration to the access port over a layer 2 network. All the processing (including associations, encryption authentication, etc.) is done at the switch level. Motorola access ports come in both plenum (with external antenna connectors) and non-plenum (with internal antenna) ratings. The access ports have built in mounting options for ceiling tiles. Yagi antennas are used for outdoor coverage. There are several antennas (patch, omni directional, etc.) for internal use. Custom enclosures for APs are currently not available.

6.1.2 ACS Support

Currently the RF switch supports *Auto Channel Selection* (ACS). Using ACS, access ports move to a new channel based on interference detection on its current channel.

6.1.3 Virtual AP

Virtual AL enables true RF Virtual VLANs for better device and network performance. With Virtual AP, each access port can support four separate wireless broadcast domains (the wireless equivalent of Ethernet VLANs), providing the ability to map multiple ESSIDs to multiple BSSIDs that would otherwise require the installation of four first-generation access points. These true wireless VLANs enable separation of mobile end-users, ensuring broadcast traffic reaches only those recipients for which it is intended. Wireless traffic engineering capabilities control client to-client visibility, broadcast/multicast/unicast packet forwarding behavior and security policies. Virtual AP provides complete control over broadcast traffic, which is associated with a BSSID. This fits in very well with the requirement to provide separate user roles, and hence separate wired and wireless VLANs (increasing overall security). Overall network traffic is reduced, network and device performance is improved, and device battery life is increased. Each AP300 supports four BSSIDs and 16 ESSIDs per radio, enabling granular segmentation of the WLAN into multiple broadcast domains to meet specific Enterprise needs. Typical access points support only one BSSID, utilizing ESSIDs (instead of BSSIDs) to create VLANs.

The control of broadcast traffic, including network level messages, is extremely important because of its potentially negative effect on performance. Intelligent control of broadcast forwarding through proxy ARP and other mechanisms ensures only the intended recipients receive broadcast traffic. The resulting reduction in traffic maximizes bandwidth, network throughput and device battery life and overall performance is improved with the elimination of message processing for other recipients. A possible compromise in confidentiality and security is eliminated, since broadcast messages can no longer reach the wrong recipients.

Motorola's AP300 model access ports are equipped with third-generation 802.11a/b/g chipsets providing superior performance and RF control for mission-critical WLAN access. While one AP300 access port is sufficient to cover a 10,000 sq. ft. area, additional AP300s are recommended to provide coverage redundancy and allow dynamic load balancing and optimal roaming.

Motorola's RF switch supports wired VLAN mapping to WLANs (VLAN - ESSID mapping). Each switch supports 32 ESSIDs, each with its own security, network and QoS policies.

Motorola's RF switch supports WPA2 with all of its fast roaming options (pre-authentication and PMK caching). Additionally, it also supports opportunistic PMK caching, which takes advantage of a centralized switch architecture allow for fast MU roaming between APs connected to the same switch. The RF switch also supports an integrated AAA/Radius server (with a 500 username/password database). The Radius server natively supports EAP-TTLS and PEAP, thereby allowing WPA or WPA2 termination at the box. This functionality is a central part of the Wi-NG software (there is no additional license fee to support this feature).

6.1.4 Clustering

A computer cluster is a group of loosely coupled computers that work together closely so that, in many respects, they can be viewed as a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks. Clusters are usually deployed to improve performance and/or availability over a single computer, while typically being much more cost-effective than single computers of comparable speed or availability.

6.1.4.1 Advantages of a Cluster

Enabling clustering allows member switches to:

- Exchange licensing information
- Load balance access ports between switches

- Redistribute the load in the event of a switch/network failure
- Manage (configuration and monitoring) all switches in the cluster from any single switch using the cluster-cli feature
- Exchange important information like rogue detection, APs in self healing mode, number of APs and radios adopted and switch aP adoption capacity

The cluster can have a mix of primary and standby switches or all of them can be primary

- All primary switches are in an active state and adopt access ports
- The standby switch will adopt access ports when the primary fails or if there is an unadopted access port in the network

A maximum of 12 switches can be part of a cluster, the licenses will be aggregated

The enhanced redundancy/failover is achieved through the new Wireless Cluster Control Protocol (WCCP).

WCCP is used for:

- Managing switch auto port adoption within a cluster
- Sharing licenses within the cluster
- Actively monitoring other switches in the same cluster
- Exchanging runtime information such as AP adoption, detected rogue APs, APs operating in self healing mode, number of APs and radios adopted and switch AP adoption capacity
- Providing license and state information whether to adopt access ports (or not) to the adoption module
- Allows the configuration and management of all switches in the cluster from any member switch using the cluster-cli feature (not available in the applet or SNMP)
- Supports cluster specific commands unique to individual switches using a common config file from DHCP
- Acts as a tunnel between application modules of the core cell controller across switches
- Some layer 3 networks are locked down between boundaries, so each boundary need both UDP and TCP port number 51515 for cluster

6.1.4.2 Simple Redundancy

Clusters can be set to simply provide simple one-to-one redundancy. For instance, a site with 48 APs has purchased two WS5100 switches with 48 AP licenses per switch. In this scenario, there is no point to implement a cluster, as each switch is maxed on licenses. A WS5100, even when in a cluster, cannot control more than 48 access ports.

To implement redundancy, the site should implement:

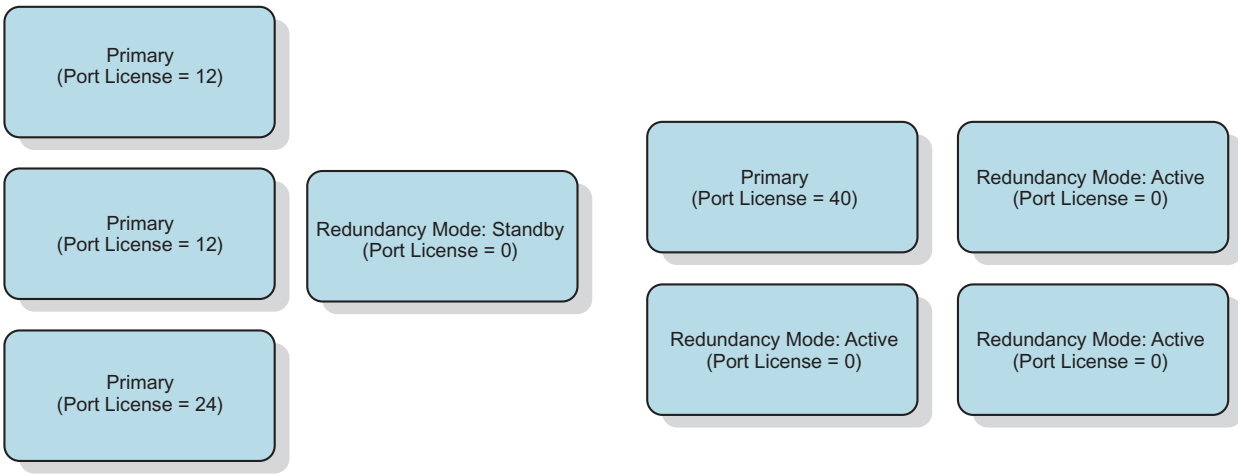
- One 48 port switch configured in primary redundancy mode
- One zero port switch configured in standby redundancy mode

In this configuration, the 48 port switch services all traffic. If the primary (licensed) switch were to experience a failure, the standby switch would adopt the APs orphaned by the failed switch. There is no load balancing in this scenario.

6.1.4.3 Sharing Licenses Across Cluster Members

Within a cluster, increasing aggregate throughput is as simple as adding a zero port license wireless switch. The total number of AP licenses across the switches is equal to, or greater than, the number of deployed APs.

AP license information is shared between cluster members. For example, if a site has one 48 port switch and eleven zero port switches, then the licensed switch could fail and the zero port switches would carry the remaining load, distributing the AP count across the remaining functioning switches. The licensed switch and 10 of the zero port switches could fail. Consequently, the one remaining zero port switch would have to carry the load. When all 12 switches are operating, the APs would load balance and there would be 4 APs servicing traffic on each switch.



Remember, up to 12 switches can be part of a cluster. The cluster can have multiple primary and standby switches. Motorola's recommended design is to have multiple primary switches and one standby switch. Each Switch cannot support more than its maximum capacity in the event of failover. For example in the case of WS5100, the upper limit per switch is 48. In a cluster, the licenses is aggregated.

In active/standby mode:

- The switch continues to operate as it did before it was a member of the cluster
- If the primary switch (having adopted 6 access ports) goes down, the standby switch adopts the 6 access ports.

In active/active mode:

- Once a cluster is established and there are 12 access ports to be adopted, the original primary switch (licensed) and the standby switch load balances the access ports
- The primary has access ports and the original zero-port license switch also has 6 access ports
- If the original licensed switch goes offline, the second switch adopts the access ports attached to the primary and ends up with 12 access ports

In one to many redundant cluster mode (three switch environment example):

- The initial load balancing after cluster establishment will lead to 16 ports adopted by each *active* switch
- If any of the 3 switches in the cluster fails, the standby adopt 16 access ports

In a four switch environment example:

- After cluster establishment, the 48 APs will be redistributed between the 4 switches, each switch will now adopt 12 access ports

- If the 48-port license switch goes down, the remaining 3 switches continue to support a total of 48 access ports

6.1.4.4 Clustering Configuration Parameters

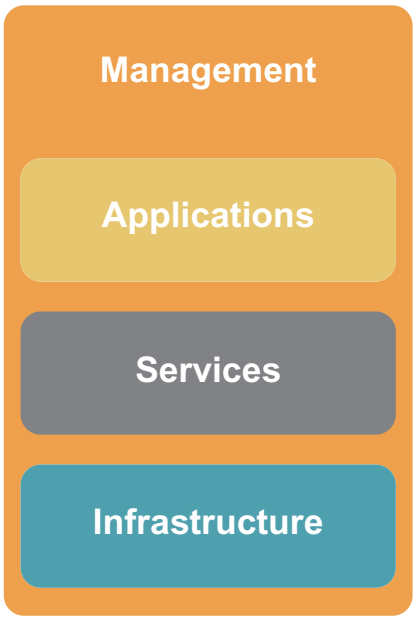
Refer the following for cluster configuration parameters:

Parameter	***Description***	***Minimum Value***	***Maximum Value***	***Default Value***
Redundancy Enable	Protocol should be operational or not	0 (disable)	1 (enable)	0
Redundancy Group ID	Group ID	1	65535	1
Discovery Time	The time the switch uses to discover other cluster members	10 seconds	60 seconds	30 seconds
Hold Time	The time the switch anticipates receiving a heartbeat message from another switch	3 times greater than heartbeat interval	255 seconds	15 seconds
Heartbeat Timer	The frequency heartbeat messages are sent.	1 second	255 seconds	5 seconds
Interface IP	The interface IP on which redundancy heartbeats need to be exchanged	IP	IP	0.0.0.0
Member IP	IP address of peer	IP	IP	0.0.0.0
Redundancy Mode	Primary or Standby	0 (standby)	1 (primary)	1

NOTE: When building redundant switches, the primary config can be cut and pasted. IP address need to be changed for each switch in the cluster. Motorola recommends Wordpad. Change the ASCII settings on the terminal, the line delay 300 ms and character delay to 30 ms.

6.1.5 Management

Refer to the following for an overview of the features and benefits per architecture:

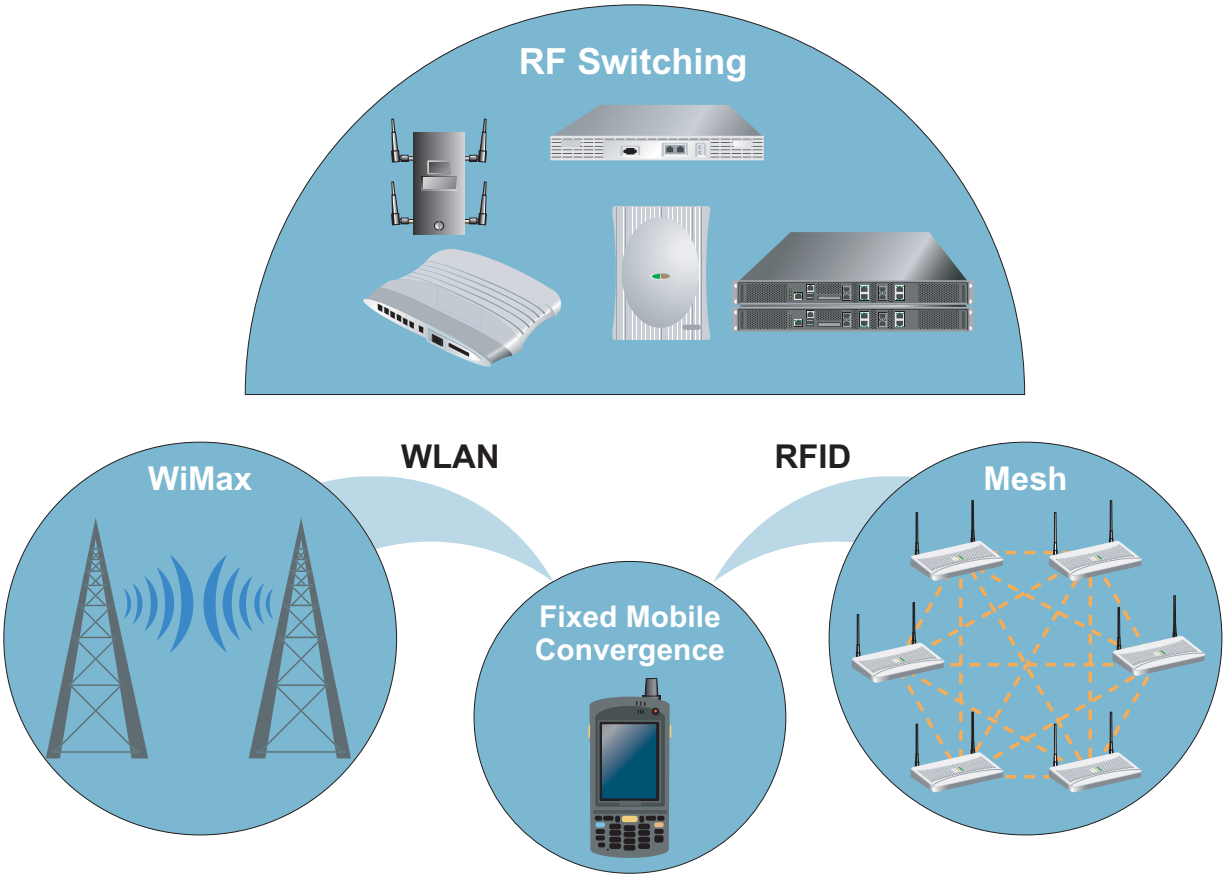


Architecture	Features	Benefits
Management	IDS/WIPS RF Planning/Mgmt. Firmware/Config. Mgmt.	Enhanced Security Significantly Lower TCO Regulatory Compliance High Uptime
Applications	Enterprise Connectivity Asset Tracking	Employee Productivity Reduce Costs, Enforce Compliance
Services	Symbol Client Extensions L2/L3 Mobility Mash Locationing Security	Enhanced Battery Life Seamless Voice/Video Roaming Extend Wireless Outside 4-walls Asset Tracking, Physical Security Simplified wireless security
Infrastructure	Linux based software RF & H/W abstraction, Services/ Diagnostics	Driving Business Efficiencies Enabling OEM Deals High Performance

6.1.6 RF Switch Architecture

The *RF Abstraction Layer* (RFAS) Wi-NG has the capability to adopt any radio as long as its definitions are known. The capability is largely through WiAP. Once a radio is adopted, the wireless switch doesn't care what radio it is adopting. Thus, the name change from wireless switch to RF switch. This provides the capability to gather dissimilar data from different radios and provide decision making data to a monitoring program. An example of this would be and an RFID tag read triggering an event like turning on a wireless video camera to focus on the tag just read.

It also supplies a platform to move information beyond RFID into WiMAX, FMC, Mesh etc. in order to blend all existing Motorola products.



6.1.7 Wi-NG Architecture Wired Features

Wired features of Motorola's *Wireless Next Generation* (Wi-NG) architecture include:

- Router support- WAN-LAN-WLAN routing functionality
- Firewall - Isolation of the LAN-WLAN from the WAN
- DHCP & NAT - LAN IP address management
- 802.1x wired-authentication.
- 802.1q trunking - VLAN support on the LAN port
- IPSec VPN client - Secure backhaul to a corporate network over the WAN
- Dual FE uplink (LAN + WAN)

NOTE: For hardware specific features unique to a WS5100, RFS6000 or RFS7000, refer to the documentation shipped with that model switch.

6.1.8 Radio Features

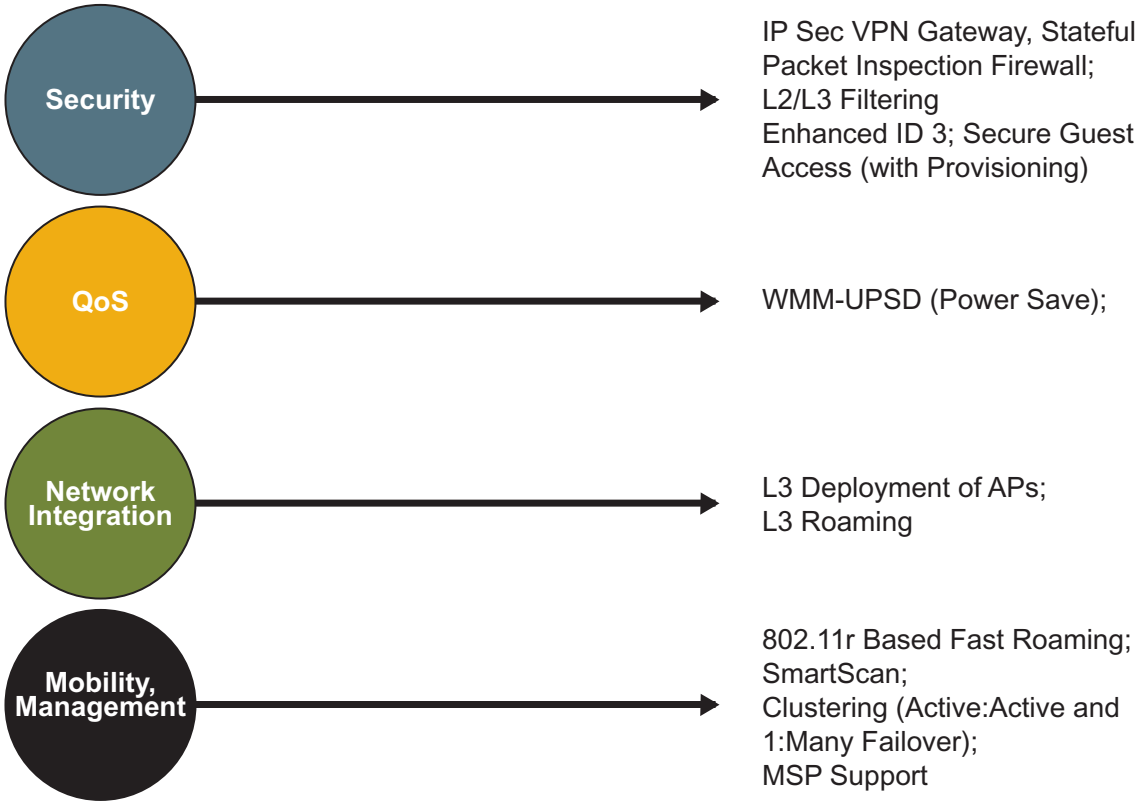
Radio features unique to Motorola's Wi-NG platform include:

- 4 BSSIDs per radio
- Support for 32 SSIDs per AP300. 16 SSIDs are supported for the 802.11b/g radio and 16 SSIDs for the 802.11a radio.
- Wi-Fi certified
- WPA, WPA2, KeyGuard, Kerberos Security (Passthrough)
- WMM certified
- 802.11a DFS/TPC - Radar detection and avoidance
- Dual-radio 802.11a+b/g support

6.1.9 Recent "Key" Wi-NG Enhancements

Wi-NG wireless is a modular and portable subsystem that provides the following recent enhancements:

- Full IEEE 802.11 and Wi-Fi Alliance standards support
- AP configuration and management
- QoS
- Identity driven MU management
- IDS
- Clustering
- Self healing
- Enterprise connectivity
- VoWLAN
- Motorola extensions
- Layer 2/3 mobility
- Layer 2/3 port adoption
- Dynamic VLAN load balancing
- Mesh
- Locationing
- Security
- Linux based software
- RF & H/W abstraction layer
- Services/diagnostics



Motorola's Wi-Fi supported products are divided into four product sets:

- *Centralized Infrastructure Products*
- *Distributed Infrastructure Products*
- *Client Products and*
- *Accessories*

Motorola supports a range of Wi-Fi embedded mobile handheld terminals based on Microsoft Pocket PC. There is also a management system that significantly reduces the costs of running a Wi-Fi mobility enabled Enterprise by managing not just the infrastructure, but the end devices and connection between them.

6.2 Locationing

Locationing (also called Real Time Location-based Services and Real Time Location Application Services) delivers end-user applications based on:

- The location of *mobile devices* (devices with location enabling technology, such as a WiFi supported handheld, Wi-Fi laptop or cell phone)
- The location of an attached *tag* (a location enabled mobile device in miniaturized form, for example a WiFi tag, UWB tag or RFID tag that is attached to a person, vehicles or a package)

A Motorola wireless LAN switches (such as a RFS7000) can facilitate true RF technology-agnostic mobility, allowing customers to view, manage and troubleshoot their RF network (Wi-Fi, RFID, UWB, mesh etc.) and provide accurate asset locationing information across multiple networks in real-time. This solution can also be packaged as a locationing appliance.

Motorola's wireless switches include a *Smart Opportunistic Location Engine* (SOLE), provided as an on-board software module, that eliminates the cost and complexity associated with managing separate location appliances. It also enables the real-time tracking of Wi-Fi devices and tags. In addition, SOLE is the first and only service in the market designed to compound and calibrate data from Wi-Fi and other sources (RFID etc.), delivering superior location accuracy.

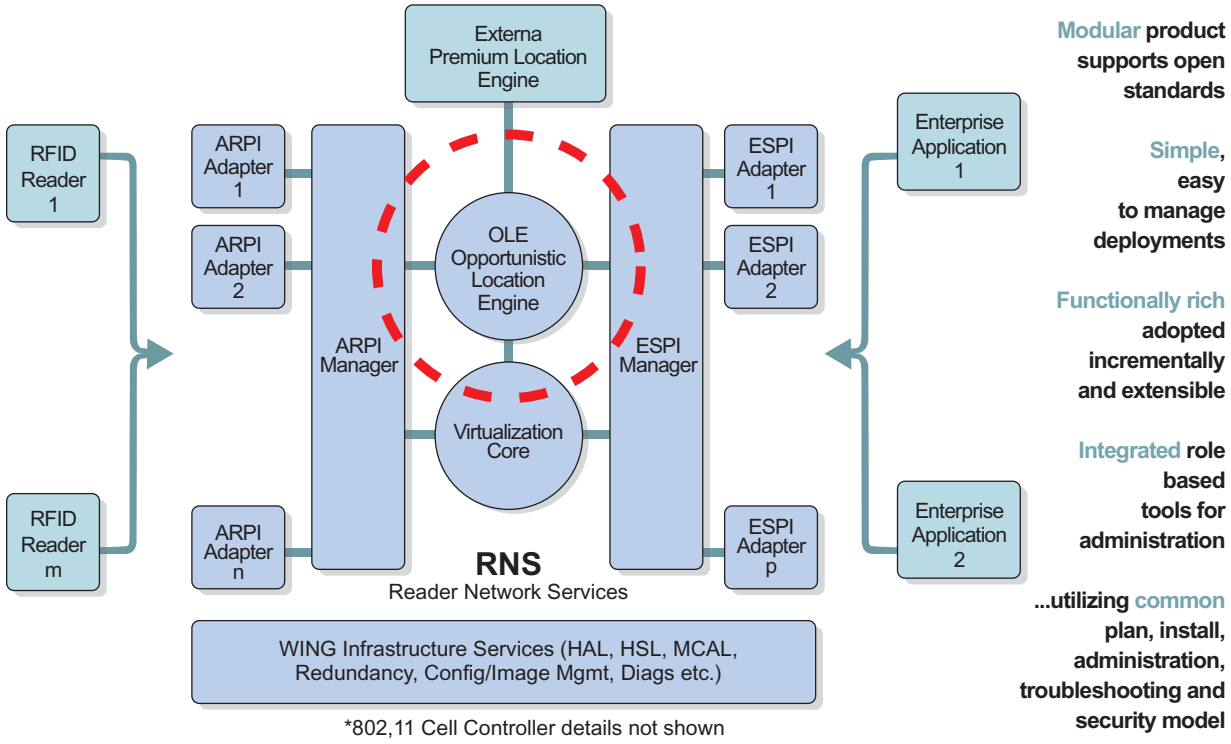
The RFS7000 leverages Wi-NG as a standards based open platform and modular architecture that works with various eco-system partners to add support for different types of tags. This enables customers to adopt new tag technologies without changing applications.

Often, locationing algorithms depend on the relationship between received signal strength and distance measurements. Thus, signal strength is susceptible to *Denial of Location Accuracy* (DoLA) attacks. Some examples include the introduction of ambient channel noise, fake beacons and probes and the altered transmit power of access ports. SOLE includes mechanisms to interpret and prevent DoLA attacks.

6.2.1 SOLE - Smart Opportunistic Location Engine

SOLE is an on-board location engine using a combination of innovative algorithms to determine location based on asset type. SOLE fuses the location information reported by several technologies into one seamless environment to get more meaningful results.

SOLE helps locate assets (including rogues) including passive tags, semi-passive tags, active tags (UWB, 802.11, RFID etc) and MUs. SOLE returns the location of passive tags as seen by mobile RFID readers (like a a MC9090) by combining the 802.11 reader's location with RFID antenna direction/location data.



Applications (users) inform SOLE (RF switch) about a facility map, location of infrastructure and zones. A zone is an area of specific interest with respect to whenever an asset becomes visible or invisible in that area.

SOLE uses the following input variables as needed for the specific tag type calculating location:

- User configurations

- RSSI propagation based on facility layout and RF barriers as specified by the user
- Smart surroundings (fixed wireless devices such as printers, price verifiers, near me tags as installed in the facility)
- Runtime RF environment
- The previous position of the tag
- TDoA
- AoA

SOLE is capable of receiving input of location from external 3rd party location engines such as Aeroscout, Ekahau and Newbury. SOLE also has a self learning process that adapts with a changing environment. SOLE also provides an open platform for supporting new architectures, future algorithms or newer asset types.

6.2.2 Locationing Terminology

Refer to the following to familiarize yourself with key locationing terms and concepts:

- *Passive RFID*
- *Active RFID*
- *Wi-Fi RFID*
- *Semi Passive RFID*

6.2.2.1 Passive RFID

Passive RFID tags have no internal power source. The lack of an onboard power source means the device can be relatively small. Some commercially available products can be embedded in a sticker or printed on paper. Passive RFID antenna/readers *interrogate* these tags. Electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the integrated circuit in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier wave from the reader. The response of a passive RFID tag is not necessarily just an ID number; the tag chip can contain non-volatile EEPROM for storing data.

6.2.2.2 Active RFID

Unlike passive RFID tags, active RFID tags have their own internal power source used to power integrated circuits and broadcast the signal to the reader. Active tags (due to their onboard power source) also transmit at higher power levels than passive tags, allowing them to be more effective in RF challenged environments like water, metal, or long distances. Active tags generate strong responses from weak requests (as opposed to passive tags, which work the other way around). In turn, they are generally bigger and more expensive to manufacture, and their potential shelf life is much shorter. Many active tags have practical ranges of hundreds of meters, and a battery life of up to 10 years. Active tags are available in Wi-Fi, UWB, ZigBee and many other frequencies such as 125KHz, 303Mhz, 315Mhz, 433Mhz.

6.2.2.3 Wi-Fi RFID

Wi-Fi based active RFID tags are small, battery-powered wireless devices that utilize standard Wi-Fi networks and can track assets and people in real-time. Using your existing Wi-Fi infrastructure in the Enterprise has obvious advantages, both economically and for an ease in installation.

6.2.2.4 Semi Passive RFID

Semi-passive tags are similar to active tags, as they have their own power source. However, the battery is used only to power the microchip and not broadcast a signal. The RF energy is reflected back to the reader like a passive tag. An alternative use for the battery is to store energy from the reader in order to emit a response in the future (by means of backscattering). Tags without a battery need to emit their response reflecting energy from the reader carrier on the fly. Semi-passive tags are comparable to active tags in reliability while supporting the effective reading range of a passive tag. They usually last longer than active tags as well.

6.2.3 Wi-Fi Locationing - An Architectural Approach

The RF switch has the ability to evolve with tag technologies (be extendible and adaptable with minimum disruption to the deployed infrastructure) and make use of robust adaptive reader programming to abstract a view of device tags so applications do not need to be aware of the device type or tag type being processed.

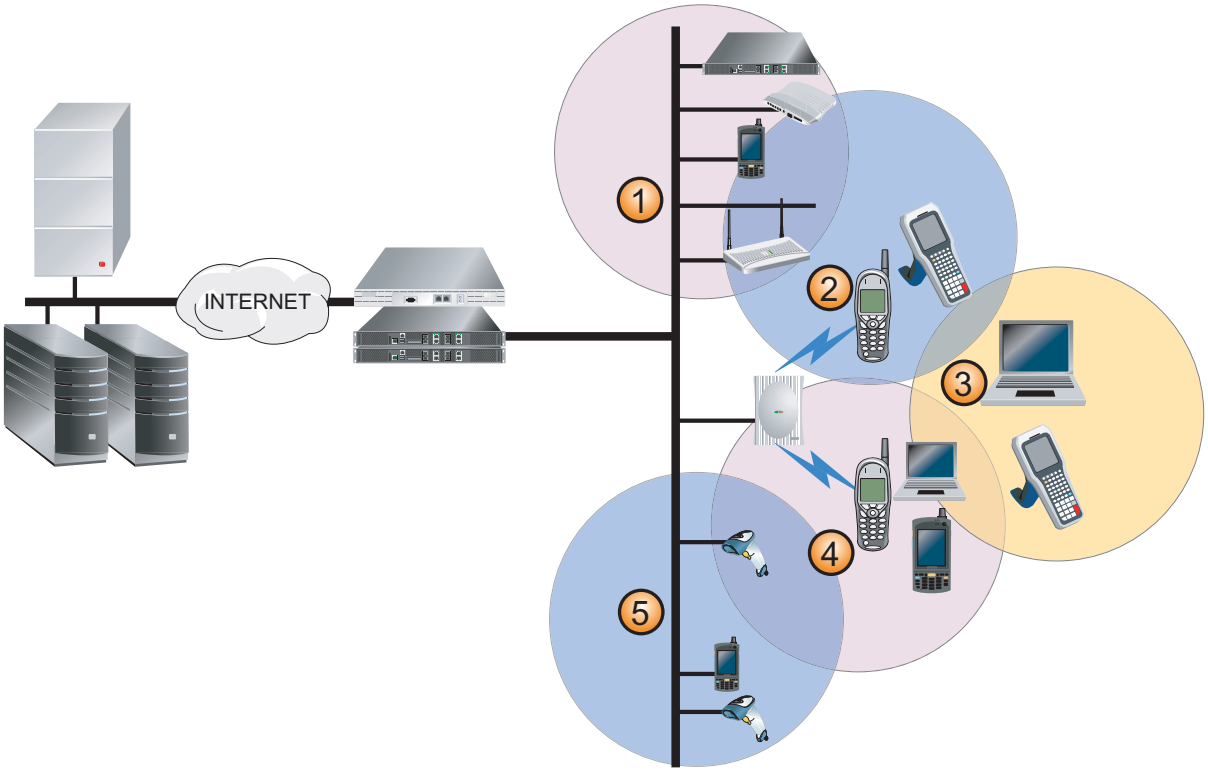
Adapters for standards-based protocols such as LLRP for RFID, native capabilities such as Wi-Fi and eco-system capabilities, are included by default and more can be added at runtime as patch upgrades.

Tag information includes location coordinates specified as (X,Y,Z), ZONE, GPS, telemetry data and tag specific data.

With Motorola's RF switch architecture, new adapters can be added with the published Motorola RF switch *Enterprise Services Programming Interface* (ESPI Adapter Writing Guide) for applications that do not make use of ALE or need a specific interface.

6.2.4 Wi-Fi Infrastructure Integration

Motorola locationing solution supports all Wi-Fi infrastructures allowing it to be deployed in a overlay configuration to track assets using RFID, UWB tags etc. For these technologies, any existing reader or sensor can be deployed on an existing Wi-Fi network, and these assets can be located using the Motorola locationing solution.



While native locationing Wi-Fi assets on is supported only on Motorola infrastructure, the RF switch makes use of a eco-system locationing engine to add support for non-Motorola infrastructures.

6.2.5 Locationing Technology

Locationing uses various *ranging techniques* to determine *symbolic distance* or *range measurement* coupled with *position estimation* techniques that derive position estimates from collection of reference points and their associated range measurements.

The ranging techniques for distance or range measurement can be based on different physical variables, such as:

- *Time difference of arrival* (TDoA)
- *Angle of arrival* (AoA)
- *Time of arrival* (ToA)
- *Received signal strength indicator* (RSSI)
- *Signal to noise ratio* (SNR)
- *Proximity*

The position estimation techniques can be based on various algorithms such as:

- Triangulation
- Trilateration
- Finger printing
- Nearest neighbor

- Least square algorithm
- Scene analysis
- min-max algorithms

Despite an abundance of established ranging and position estimation technologies, there is no single technology reliable in all environments to provide accurate location information. Each technology has its strengths and weaknesses. The RF switch's on board location engine, referred to as SOLE, uses existing systems/algorithms to fuse location information as reported by several sources.

Specifically, for Wi-Fi, SOLE uses trilateration and a probability distribution model fused with a RSSI propagation model in a runtime environment to view a facility in a topological model, where the whole building is divided into zones.

- The location engine for all types of tags is integrated in the switch
- Provides a standards based single interface/connection for applications/middleware to get information about tags of all types
- Provides robustness and accuracy, even when exposed to DoLA (denial of location accuracy) attacks.
- Provides one connection point for all location services. Motorola customers can take advantage of:
  - Compounding multiple technologies (such as Wi-Fi and passive RFID)
  - Locationing for tags identified by multiple/hybrid technologies
  - No application adjustments needed when a new tag technology (infrastructure) is introduced
- Investment protection for customers, as their applications can be RF network *agnostic*, meaning they can adopt or add newer tag technologies without having to change their infrastructure

6.2.6 Application, Business/Technology Partners

Motorola believes our locationing appliance is enhanced by a strong eco-system. Motorola has partners in four categories within our locationing eco-system:

- *Tag vendors* - These are the various tag vendors who provide standards-based tags for different technologies. These are Wi-Fi tag and Gen 2 passive tag vendors.
- *RF access point vendors* - These are access point vendors. The access points are for UWB, proprietary active RFID tags, proprietary semi-passive RFID tags and RFID readers used to locate UWB, active RFID, semi-passive RFID, RFID Gen2 tags, etc. These partners play an important part in the eco-system as some tag technologies work in some environments better than others (for cost or accuracy or other reasons). Motorola's RF switch architecture enables the interaction and management of these tag technologies as part of same the RF network, enabling applications to work seamlessly (not be tag type aware. The customer benefits from the technology that suiting them the closest.
- *Application (frame work) vendors* - These are the applications (frame work) vendors that interact with the RF switch and provide a framework that can be customized for various applications. For example, a hospital application needs to associate each tag with a hospital type asset - bed, nurse, pump etc.
- *Integrators* - These are the end solution providers who create their own application framework to develop solutions/applications that work for the end customer. They play a key part in eco-system, as they work with the end customer to solve specific problems

6.2.7 Security Applications Addressed by the Wi-Fi Location Platform

- *Location Based Access Control*

- *Restricting Physical Access Based on Location*
- *Tracking Critical Items*

6.2.7.1 Location Based Access Control

Motorola's locationing engine connects the physical to virtual. The most fundamental aspect of conventional network security is the location of a user. The firewall on a RF switch makes location a factor. It enables users to create virtual location-based firewalls around a facility or divide a facility into zones and establish virtual firewalls around the zones to prevent unauthorized access.

Examples include:

- The physical location of a wireless device in a specific portion of a building to access a wireless network
- Having the RFID tag in the premises and wireless device in specific zone in the building to access the wireless network, or a user in parking lot not able to connect at rate higher than 5 Mbps

6.2.7.2 Restricting Physical Access Based on Location

Geofencing is a term used to describe a virtual fence an administrator can draw around their facility to allow/prevent the authentication of users based on location, or receive alerts when a tag enters or exits the *fence*. The RF switch has a built-in application to support geofencing. For the graphical component, users can make use of Motorola RFMS.

6.2.7.3 Tracking Critical Items

The RF switch's locationing engine supports multiple service level agreements for an asset or group of assets. This allows administrators to track assets or groups of assets with specified seek/latency times.

With the switch, administrators can configure zones and alerts, such as an alert when an asset enters an unauthorized zone.

6.2.8 Location Based Hotspots

The RF switch enables network administrators to add location-based hotspots.

Examples include:

- A tourist at a historic monument can see a map, the nearest exit and all points of interest
- Customers at a department store can easily see advertised items and inventory not on display

6.2.9 On-Board Location Services

Using its on-board location engine, the RF switch provides location based services, including:

- *Location based authentication* - A user can configure zones and MAC addresses that are allowed in that zone. For example, they can disallow authentication for everyone in a training room, parking lot, disallow authentication for person X in zone A of the building, etc.
- *Location based hotspots* - The first page after the logon page is customizable for unique hotspots accessed from different locations
- *Location based ACLs/NAT* - User configurable zones and ACLs applied strategically
- *Location based radio rate limiting* - Define a zone only allowing a maximum of 5 Mbps from the parking lot or guest reception area
- *Sending Location to clients* - Enables clients to have location/context aware applications

6.2.10 Application Interface

Applications can get location information on all assets via ALE (*EPC Global Standard*). The RF switch/SOLE supports ALE 1.1 (more specifically ALE++). Motorola supports many value add vendor extensions.

Applications can use ALE to configure facilities, zones and then subscribe to get asset information autonomously (whenever the asset visibility changes).

The location information of assets includes:

- X, Y, Z
- Zones
- GPS coordinates

6.3 Access Port and Access Point Adoption

An access port is a thin AP and an access point is a fat AP. Before deploying wireless switches, you need to understand how an access point or access port adopts and is handled by a wireless switch.

The difference between these two APs is the amount of intelligence build in the AP. An access port shares its intelligence with its associated switch. For more information on access port and access point adoption, refer to the following:

- *WISP*
- *Port Adoption*
- *Radio Adoption*
- *Layer 3 AP Adoption*
- *Adoption Notes*

6.3.1 WISP

WISP is a Motorola defined layer 2 protocol for communication between an access port and a wireless switch. At its basic level, WISP is a 802.11 tunneling protocol. An access port takes 802.11 packets off the air, encapsulates them in WISP and forwards them to the wireless switch. The switch takes wired packets, turns them into 802.11 packets, encapsulates them in WISP and forwards them to the AP. This is a modification of WNMP.

802.3 header -> WISP header - > 802.11 header - > Payload

- *802.3 header* - Used to get packets to the AP
- *WISP header* - Determines what the AP or Switch should do with the packet
- *802.11 header* - This is the 802.11 packet the AP forwards or the 802.11 packet used by the switch to convert into a wired packet
- *Payload* - The TCP/UDP/ARP/etc payload

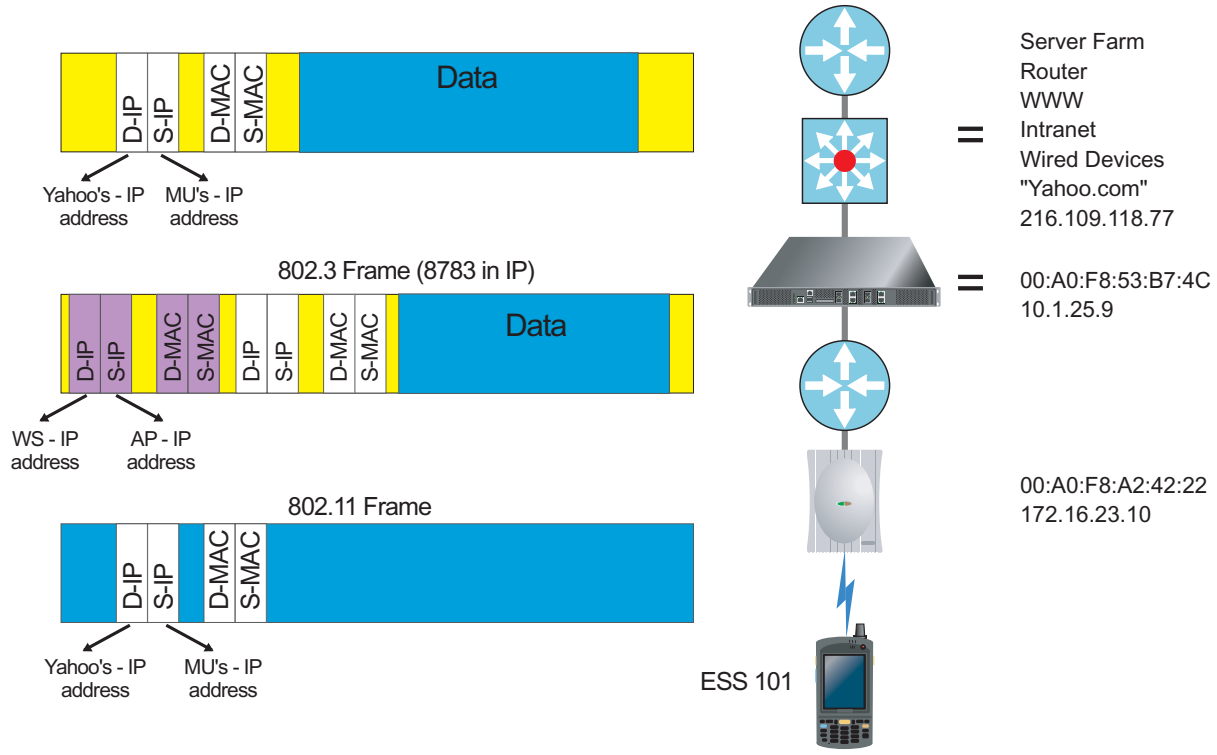
WISP has many more functions besides just passing data packets between the switch and the AP. It helps define configurations, status, flow control and statistics processing as well.

6.3.1.1 WISPE

WISPE is the protocol used by Motorola for communications between the switch and the AP.

Differences between WISPE and WISP include:

- There is no flow control in WISPE - it is assumed the AP has sufficient buffers that will render this unnecessary. This means an AP100 cannot be supported under WISPE, only the AP300 and AP-5131 can be supported.
- WISPE works over Layer 2 and Layer 3 networks, unlike WISP which is a pure Layer 2 protocol
- WISPE implements Motorola proprietary features, and undocumented CAPWAP features as vendor specific extensions to CAPWAP. For information on CAPWAP, see *CAPWAP on page 6-19*.
- CAPWAP itself has no provisions for working over a layer 2 or wireless link - This is yet another Motorola proprietary extension provided under WISPE



6.3.1.2 CAPWAP

The intent of the *control and provisioning of wireless access points* (CAPWAP) protocol is to facilitate the control, management and provisioning of *WLAN termination points* (WTPs) specifying services, functions and resources relating to 802.11 WTPs to allow interoperable implementations of WTPs and access controllers. WISPE looks very much like CAPWAP.

NOTE: The CAPWAP specification is an evolving document, and is not as rich as the WISP specification. Motorola plans to implement WISP features as vendor specific extensions to a yet-to-be-defined draft version of CAPWAP, and called the resulting baseline WISPE.

CAPWAP has a set of WLAN control functions not directly defined by IEEE 802.11 standards, but essential for effective control, configuration and management of 802.11 WLAN access networks. These include:

- *RF monitoring* - Noise and interference detection, and measurement
- *RF configuration* - Supports retransmission, channel selection and transmission power adjustment
- *WTP configuration* - For SSID configurations.
- *WTP firmware loading* - Automatic loading and upgrading of firmware for network wide consistency
- *Network-wide STA state information database* - Including the information needed to support value-added services, such as mobility and load balancing
- *Mutual authentication between network entities* - For example, support for AC and WTP authentication in a centralized WLAN architecture.

CAPWAP and WISPE

WISPE implements the split-MAC architecture defined in the CAPWAP drafts. The split-MAC architecture splits 802.11 functions between the switch and the AP differently from the current Motorola WISP-based architecture.

CAPWAP has the capability to adopted other AP models. However, the CAPWAP protocol has not been ratified and the reality of its ratification is slim. If there is an AP that matches closely to the CAPWAP implementation, our infrastructure probably could adopt it, but the results are unpredictable.

Split MAC Architecture

A split MAC architecture is a subgroup of a centralized WLAN architecture wherein WTPs networks only implement delay sensitive MAC services (including all control frames and some management frames) for IEEE 802.11, while all the remaining management and data frames are tunneled to the access controller for centralized processing. The IEEE 802.11 MAC, as defined by IEEE 802.11 is effectively split between the WTP and AC.

Usually, the decision of which 802.11 MAC functions need to be provided by the AC is based on the time-criticality of the services considered. In a split MAC architecture, the WTP terminates the infrastructure side of the wireless physical link, provides radio-related management, and implements time-critical functionality of the 802.11 MAC.

In addition, non-real time management functions are handled by a centralized AC, along with higher level services, such as configurations, QoS, policies and ACLs.

The key distinction between Local MAC and split MAC relates to non-real time functions, such as:

- In a split MAC architecture, the AC terminates 802.11 non real time functions
- In a local MAC architecture, the WTP terminates 802.11 non-real time functions and sends appropriate messages to the AC

Real Time versus Non-Real Time

There is no clear definition in the 802.11 specification as to which 802.11 MAC functions are considered *real time*. Each vendor interprets real time differently.

Most vendors agree that the following 802.11 MAC services of are examples of real time services, and are implemented on WTPs:

- Beacon generation
- Probe response/transmission
- The processing of control frames: RTS/CTS/ACK/PS-Poll/CF-End/CF-ACK
- Synchronization
- Retransmissions
- Transmission rate adaptation

The following are examples of non-real time MAC functions as interpreted by most vendors:

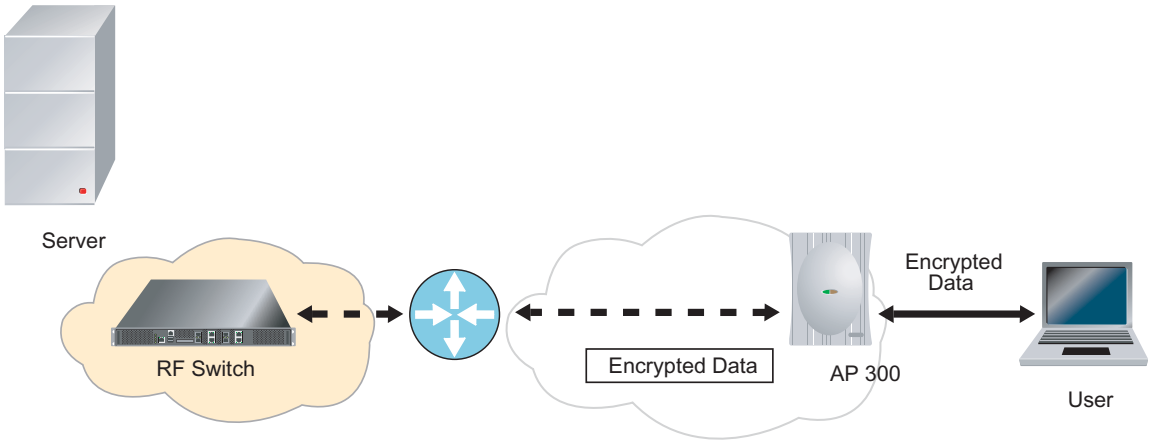
- Authentication/de-authentication
- Association/disassociation/re-association/distribution
- Integration services (bridging between 802.11 and 802.3)
- Privacy (802.11 encryption/decryption)

- Fragmentation/defragmentation

NOTE: Some vendors may classify non-real time functions as real time functions to support specific applications with strict QoS requirements. For example, re-association is sometimes implemented as a real time function to support VoIP applications.

6.3.2 Port Adoption

Port adoption is the process of a switch accepting a device radio for use. This could be an access port, access point or any other radio (including RFID readers) converted to Wi-AP. The device radio encapsulates every packet and sends it to the switch



6.3.2.1 Motorola's Layer 3 Port Adoption

Motorola's thin architecture design supports more than just the management of inexpensive radio ports (unlike our competitors, whose thick APs just send data to a controller). Since Motorola's access ports are created to fit into wired deployments and its existing physical security, spoofing an access ports is very difficult with respect to Motorola's heartbeat timing and encapsulation rules. Access ports have very little intelligence and are designed to be in the access layer of the network. A wired access layer is assumed to be *touched* by users. Consequently, *no* authentication, encryption or certificate cashing is conducted by the access port. Everything is pass-through and is sent to a switch typically locked in a closet.

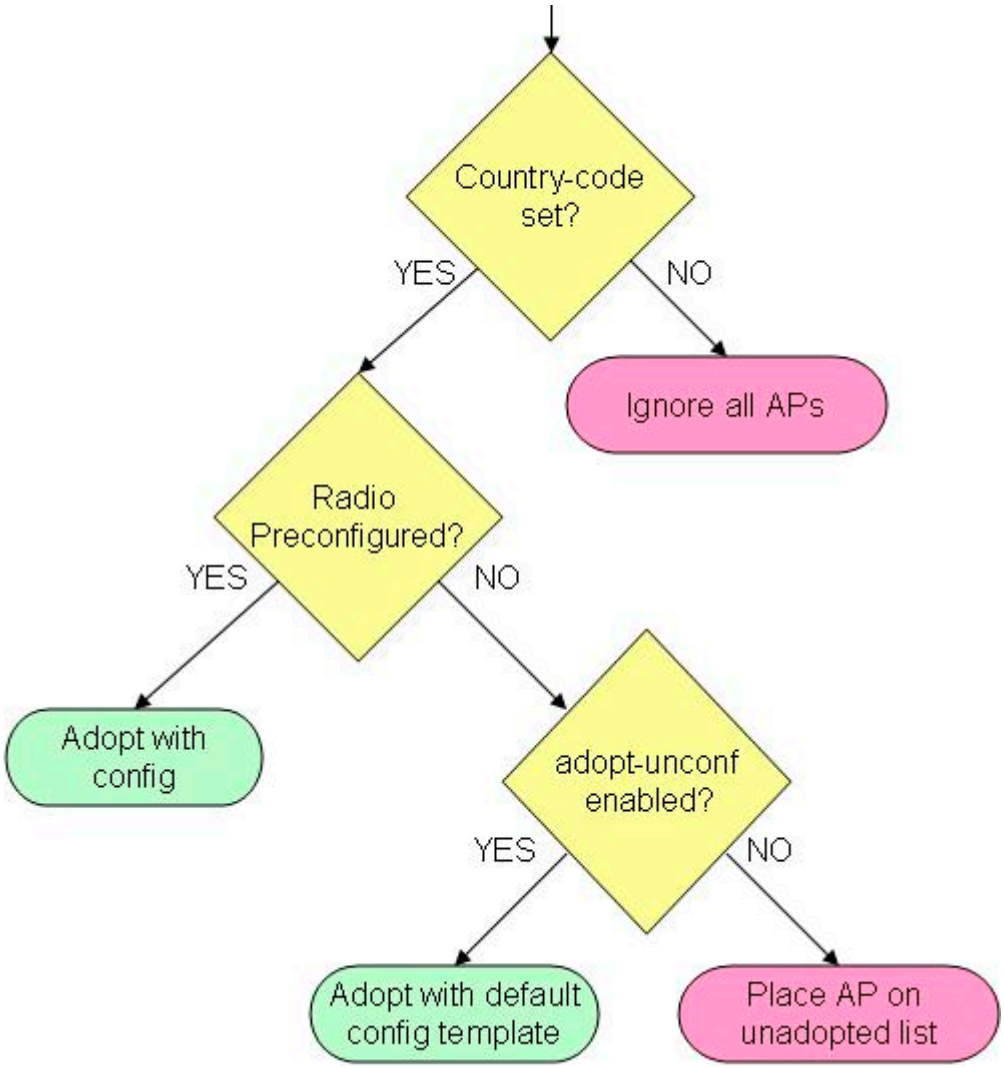
With a proper network design, the physical wire can be *locked*. This means if an access port is unplugged, and a hacker plugs their laptop in the Ethernet jack where the access port was connected, the hacker would not see any data, nor have access to the network.

Since traffic is pass-through, the data stays encrypted from the MU to the handheld. For example if an MU is using AES, the data would have AES encryption all the way to the switch. No further encryption is needed. This secures low overhead with superior performance on leaner bandwidths without protocol restrictions!

However, if the MU is connected using guest access privileges, or has no encryption for their wireless connection, the data is not encrypted on either the wired on wireless side. Hotspot safety precautions are required for this user.

6.3.3 Radio Adoption

This section describes what happens *if* a radio gets adopted. We say *if* because a switch may or may not adopt an AP/radio, and must meet several conditions prior in order for adoption to successfully occur.



You cannot adopt a radio without a country code. In fact, you cannot configure any radio parameters until the country code is set. Set the country code first.

The easiest way to adopt APs/radios is to pre-configure them. This is done with the following command:

```
radio 1 add 00:A0:F8:11:22:33 11bg
```

This tells the switch to look for an AP with MAC address 00:A0:F8:11:22:33 and adopt its 802.11bg radio. An AP and its radios must all be adopted by the same switch. An AP is adopted if the switch adopts one ore more of the AP's radios.

If a radio is not preconfigured, the switch can still adopt it. But the switch must be configured to adopt un-configured radios.

```
adopt-unconf-radio enable
no adopt-unconf-radio enable
```

This CLI command turns the auto-adoption feature on/off. The default is to have it enabled. When a radio is encountered without a configuration and auto-adoption is turned on, the switch copies the configuration template for that radio type (11a/11bg). It does this by adding the a radio *X add <MAC>* line into the configuration, and then copying any additional lines needed from the configuration template.

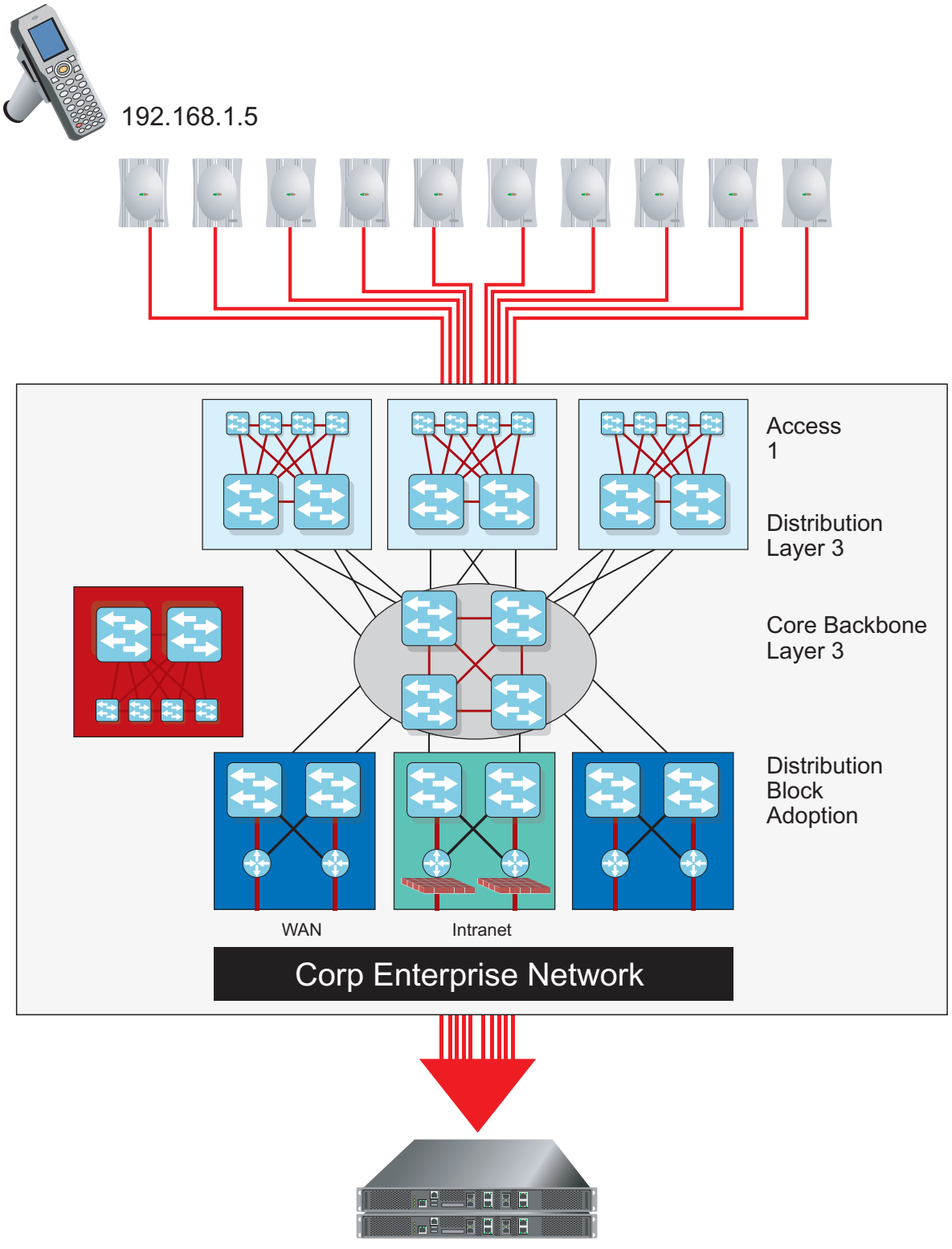
Configuration templates are implemented by a special radio index. The commands to configure the templates are the same as the commands to configure the radios themselves. For example:

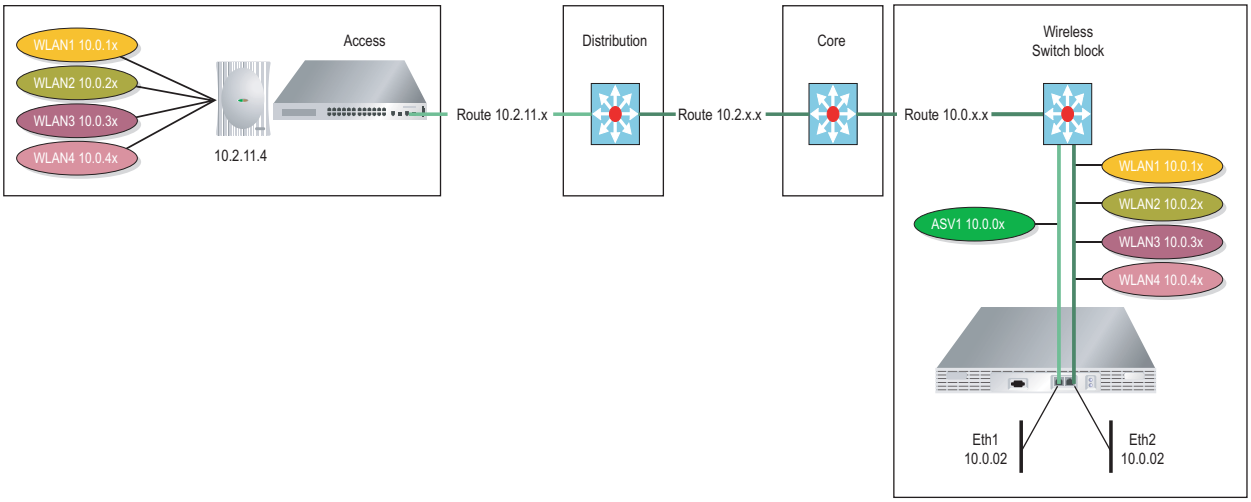
```
radio default-11a antenna-mode diversity
radio 1 antenna-mode diversity
```

Instead of using a radio index, you can specify which configuration template to use. Currently Motorola has 2 configuration templates: <default-11a|default-11bg>.

6.3.4 Layer 3 AP Adoption

Layer 3 AP adoption is the act of adopting access ports across a layer 3 boundary.


192.168.1.5
Access
1
Distribution
Layer 3
Core Backbone
Layer 3
Distribution
Block
Adoption
WAN
Intranet
Corp Enterprise Network



A switch can adopt ports anywhere in a layer 3 network using a layer 3 port. The WLAN connectivity provided by the layer 3 port is tunneled back to the switch, which puts that WLAN traffic on a single layer 3subnet. Effectively, the wireless devices are on a single layer 3 subnet, completely independent of the layer 3 subnet the access port is on. This topology allows a user to overlay a defined wireless layer 3 network on an arbitrary wired layer 3 network.

6.3.4.1 Dependencies

For a successful layer 3 port adoption, a DHCP Server with user options defined needs to configure an AP to point to the switch cluster. To accomplish this, a DHCP server is needed. Option 189 must be added to the resources the AP uses to obtain an IP address. Create a data type option with a string using code 189. The total number of switches listed should be 10. The switch IP address (or DNS name) must be separated by a space. In a linux environment, the switch IP addresses need to be separated by a comma. Layer 3 QoS needs to be implemented on the wired network to have QoS work properly. In the instance of a layer 2 adoption, a dedicated VLAN is required.

Refer to the following to understand various operating conditions impacting layer 3 AP adoption:

Roaming Quality

The following layer 3 scenarios should be noted, as they directly impact roaming quality:

- If the layer 3 link bandwidth is too meager, there is no way for a switch or AP to detect it until it begins to impact latency
- One might find the number of simultaneous roams becomes limited, and the quality of the roams poor (lossy). In such a situation, an infrastructure implementing Diffserv could be helpful.
- WISPE requires a minimum bandwidth of 10 Mbps between the switch and the WiAP to operate without substantial degradation in roaming quality

Wi-Fi Multimedia (WMM)

The following layer 3 scenarios should be noted, as they directly impact WMM:

- Since the AP performs WMM scheduling by itself (in contrast to WISP where the queue management is partially performed by the switch), WMM priorities will still be preserved across the layer 3 link, regardless of the latency
- Regardless of the type of tunnel, APSD and PSP are performed partially by the switch and partially by the AP
- A split-MAC architecture attempts to mask the effect of tunnel latencies

Throughput

The following layer 3 scenarios should be noted, as they directly impact throughput:

- Having a 10Mbps full-duplex link is a necessary for good roaming quality, but the throughput will still be limited by the throughput of the link

QoS (Voice)

The following layer 3 scenarios should be noted, as they directly impact voice quality:

- After an AP is adopted over an layer 3 tunnel, if the latency suddenly spikes, there is no way to protect against voice jitter buffer overflows
- While this may not affect SpectraLink round robin prioritization for a given latency, it will cause considerable lag in a conversation, depending on the latency
- Guaranteeing a latency of < 30m in the layer 3 path will go a long way towards improving voice performance
- Sudden changes in the bandwidth of an layer 3 tunnel will have a detrimental effect on voice quality. It is hoped the infrastructure pays attention to the TOS and .1p fields and implements differentiated services

6.3.5 Adoption Notes

If an AP is adopted and the 802.11a radio is in use, can the 11g radio be disabled and visa versa? If one of the radios is disabled, does it still send *adopt me* broadcasts on the wire? Can an unused radio be dedicated as a full time sensor?

Either radio can be disabled from the switch without affecting the status of the other radio. A disabled radio returns to an unconfigured state, and sends a config request every 5 seconds. Adoption is between a switch and an AP, not between a switch and a radio. Thus, disabling a radio does not affect adoption status. Any radio can be configured as an IDS sensor. However, in sensor mode the radio scans on all channels for beacons from rogue APs (perpetual ACS).

6.4 QoS and Wi-NG Port Adoption

Motorola's WiOS architecture supports various standards based and proprietary schemes for providing QoS over a 802.11 wireless network. These include *Spectralink Voice Prioritization* (SVP), both zero-backoff and round-robin-retries. Wi-NG supports the portion of the IEEE QoS standard 802.11e providing prioritized access to different traffic classes.

WiOS includes support for several new QoS features, while also enhancing the way some of the features have been implemented in previous baselines.

6.4.1 Unscheduled Automatic Power Save (WMM Power Save)

Wi-Fi Multimedia (WMM) power save or *unscheduled automatic power save delivery* (U-APSD) is a set of features for 802.11 networks that increase the efficiency and flexibility of data transmission to conserve power. Based on the IEEE 802.11e standard, WMM power save improves legacy device power efficiency by increasing the time a client can sleep and decreasing the number of frames a client can send and receive. These optimizations are for MUs running latency-sensitive applications such as voice or video.

This feature is supported on both on the switch and AP. It's also possible power save buffering (legacy as well as U-APSD) can be implemented on just the AP. In this case, the switch still needs to update the U-APSD per-AC setting on the AP (using WISPE ADD-MU and UPDATE-MU messages). Using the WMM power save mechanism:

- U-APSD and WPA/WPA2 can be used together
- U-APSD can work with 11b, 11g, 11b/g and 11a PHY
- ACs delivery/trigger behavior configurations via the QoS info field
- The simultaneous operation of U-APSD is supported

The switch advertises U-APSD capability in the QOS-Info fields of the WMM parameter element as well as the information element.

6.4.1.1 U-APSD Reserved Parameter Set Count

Power save is set for each WMM AC (voice, video, best effort, background) transmit queue independently. If some ACs are using legacy power-save, legacy mechanisms (TIM, power-save-poll etc.) are used to send those buffered frames. If all ACs are delivery enabled, TIM will not be updated for buffered frames, and the MU will only use WMM power save mechanisms to retrieve frames.

In addition to the U-APSD requirement on each AC, a MU also informs the switch about the number of frames it wants delivered (MAX SP length) each time it sends a trigger frame to the switch.

Every AC queue is marked for either WMM power save or legacy power save. The switch maintains the U-APSD state of every MU on a per-AC basis. The mechanism through which a MU reports it's sleep behavior is still the power-management bit in a frame sent to the AP.

If buffered data belongs to a legacy power-save queue, transmissions follow a legacy power save (response to PS-Poll, or indication the MU is now awake) mechanism. If the data belongs to a WMM power save queue, data frames are downloaded according to a trigger-and-delivery mechanism. The per-mu PSP queue is partitioned into one per-AC-per-MU.

The client sends a trigger frame on any of the ACs using WMM power save to indicate it's temporarily awake and ready to download any data frame an access point may have buffered on its behalf. This is acknowledged by the AP and forwarded to the switch. This is the start of an *unscheduled service period* (USP), and the MU now remains awake for a short interval. The switch dequeues and sends all buffered frames from delivery enabled ACs to the AP for transmission to the MU. If implemented on the AP, all the frames will get transmitted in one TXOP (*opportunity to transmit*), if these frames are coming from the switch, they hit the air depending on the AP queues (same as legacy power-save behavior with PS-poll). If the switch has no buffered data frames, it sends a QoS NULL frame to the MU.

On the last data frame (or the NULL frames if there was no data buffered), the switch marks the end of the service period by marking the *end of service period* (EOSP) bit on the frame. All frames to that point have the EOSP bit cleared.

This only impacts unicast frames sent to a MU. The transmission of broadcast/multicast frames is not changed by WMM power save. There is a small possibility the AP might re-order frames across two ACSs

spanning one service period. The switch dequeues packets in higher priority access categories before it dequeues the ones from lower ones to avoid this problem.

U-APSD is always enabled. The user is not required to enable or disable support for this feature. If clients are U-APSD capable, they'll use this feature, otherwise they'll use legacy power save mechanisms.

6.4.1.2 Traffic Prioritization

Multiple WLANs are typically mapped to the same radio, as users like to prioritize traffic from one WLAN versus another on the same radio. This is often done by:

- Ensuring a public access WLAN gets lower priority than a corporate WLAN
- Ensuring the WLAN dedicated to voice gets higher priority than the one used for data

Motorola's WLAN prioritization scheme is based on a user assigning weights (1-10) to WLANs., The packet-driver then ensures a number of packets is de-queued for every WLAN in a ratio corresponding to the weights assigned to the WLAN. This depends on the feedback mechanism the flow-control provides, thus allowing the switch to queue up packets. When the AP reports the flow-control window is open again, the switch de-queues packets from the appropriate WLAN queue, thus maintaining the correct ratios.

The new switch-AP protocol in WISPE is based on CAPWAP and does not implement flow-control. A new way of prioritizing traffic in different WLANs is required. There are two alternatives:

- Add some sort of flow-control, such as feedback to CAPWAP. However, this defeats the whole purpose of supporting a standards based AP-switch protocol.
- Have the switch rate-limit traffic automatically to an AP, and rely on periodic statistic updates from the AP to determine how transmissions are doing. From there either "hit the brakes" or the "accelerator." This requires constant fine tuning on the switch, and may not work ideally in a wireless deployment.

Within Wi-NG, these are implemented by mapping legacy WLANs requiring prioritization to one of the four access categories the AP supports. For each WLAN, the user picks one of the five following traffic prioritization schemes:

- *Automatic*
- *Voice*
- *Video*
- *Normal*
- *Low*

The automatic option assumes MUs are WMM enabled and traffic is automatically prioritized based on its type. Prioritization between such WLANs is possible in the upstream direction by changing WMM parameters for the WLANs. The next four traffic classifications result in traffic from the specified WLAN be placed in the corresponding access category. (voice = AC_VO, video = AC_VI, normal = AC_BE and low = AC_BK). This automatically ensures traffic from a voice WLAN gets higher priority than a normal WLAN.

This scheme addresses typical deployment scenarios for WLAN prioritization as used today Its simple to understand and implement, both on Motorola APs as well as vendor APs that wish to interoperate with Motorola's (HP fat-AP conversions).

NOTE: This scheme does not provide a way to prioritize voice traffic on a public WLAN over data traffic on a corporate WLAN. This prioritization scheme also does not handle downstream prioritization across two WMM enabled WLANs.

6.4.1.3 Configurable 802.1p/DSCP-AC Mappings

WiOS supports hard-coded mappings of *differentiated services code point* (DSCP) values and 802.1p priorities to WMM access categories. The values are set to Wi-Fi recommended values, however there is a perceived need to control the values.

The user can modify three different mapping types:

- *Wired to wireless* - DSCP to access category mappings
- *Wired to wireless* - 802.1p to access category mappings
- *Wireless to wired* - Access category to 802.1p mappings

The following default mappings allow a user to change the parameters in cells marked with a gray background:

Wireless to Wired - Access Category to 802.1p

WMM Access Category	*802.1p*
Voice	7
Video	5
Best Effort	3
Background	1

Wireless to Wired - 802.1p tag to Access Category

802.1p	*WMM Access Category*
0	Best Effort
1	Background
2	Background
3	Best Effort
4	Video
5	Video
6	Voice
7	Voice

Wireless to Wired - DSCP to Access Category

DSCP	*WMM Access Category*	*DSCP*	*WMM Access Category*
0	Best Effort	32	Video
1	Background	33	Video
2	Background	34	Video
3	Best Effort	35	Video
4	Video	36	Video
5	Video	37	Video
6	Voice	38	Video
7	Voice	39	Video
8	Background	40	Video
9	Background	41	Video
10	Background	42	Video
11	Background	43	Video
12	Background	44	Video

DSCP	***WMM Access Category***	***DSCP***	***WMM Access Category***
13	Background	45	Video
14	Background	46	Video
15	Background	47	Video
16	Background	48	Voice
17	Background	49	Voice
18	Background	50	Voice
19	Background	51	Voice
20	Background	52	Voice
21	Background	53	Voice
22	Background	54	Voice
23	Background	55	Voice
24	Best Effort	56	Voice
25	Best Effort	57	Voice
26	Best Effort	58	Voice
27	Best Effort	59	Voice
28	Best Effort	60	Voice
29	Best Effort	61	Voice
30	Best Effort	62	Voice
31	Best Effort	63	Voice

6.4.1.4 AP-Switch Traffic Prioritization

Traffic between a switch and AP can optionally be configured to use prioritization in encapsulation. For an AP with layer 2 connectivity, this means the use of 802.1p tags. For an AP with layer 3 connectivity, this implies the use of *differentiated services code point* (DSCP) values in addition to a possible 802.1p tag.

- WISPE/CAPWAP control frames use a 802.1p value of 7, and a DSCP value of 46 (these numbers are per the recommendation in the CAPWAP draft).
- Data frames from/to WMM MUs use 802.1p/DSCP values corresponding to the access category inside the 802.11 header.
- Data frames to legacy MUs have a 802.1p/DSCP value corresponding to the category the MU is placed in (default is best effort).
- Data frames from legacy MUs have an 802.1p/DSCP value corresponding to the MU's priority. The AP learns the priority of the MU as part of the ADD-MU or UPDATE-MU WISPE/CAPWAP commands.

An AP300 does not currently support 802.1p tagged frames, and in deployments using tagging the tagged frames terminate at an edge layer 2 switch. The handling of tagged layer 2 frames is a stretch goal and

consequently so is the layer 2 prioritization of frames from the AP to the switch. With layer 3, an AP uses an appropriate DSCP value.

The mappings should be the default ones specified in table section titled *Configurable 802.1p/DSCP-AC mappings*.

6.4.1.5 WMM Admission Control with TSPEC Negotiation

WMM admission control is a mechanism for limiting traffic on a given access category. Per the recommendation of the 802.11e specification, Motorola limits support of this feature to voice and video. The switch configures the AP to broadcast that admission control is mandatory.

Motorola's WiOS contains basic TSPEC negotiation. Noteworthy elements include:

- Support for the EDCF mode for channel access. Without some sort of dedicated time slot, or scheduled access to MUs, there is almost no way to guarantee the data rate, bandwidth or error rates a TSPEC tries to establish.
- Within Motorola's multi-BSS architecture, we have more than one WLAN per-BSSID, and more than one BSSID per radio. The resource (the air) MUs are trying to access is split across the WLANs mapped to the radio. Some of these WLANs might be WMM enabled, some might have admission control enabled on some ACs and others might not be WMM enabled at all. Enabling admission control on a WLAN radio (when 15 others are also mapped to it) may not always have the desired effect. When traffic shaping and MU/WLAN rate-limiting is implemented, Motorola will have slightly better control of radio bandwidth by different WLANs.
- Admission control and TSPEC negotiation have been noted by Spectralink as features they would like infrastructure to support in the future. The Voice group at WiFi is also in the planning stages of supporting admission control. Primary admission control users are likely VoIP phones. Motorola will drive its admission control implementation based on WiFi mandates, then test for interoperability.

Based on early drafts of the WiFi Admission Control MRD, the WiFi requirements for APs and switches include:

- Admission control and WPA/WPA2 being able to work together
- Admission control being able to work with 11b, 11g and11b/g mixed mode
- An AP setting flags in the WMM element for each access category
- APs being able to respond to admission requests for those ACs with a set flag (the AP will make a determination as whether to accept or deny requests). The AP will transmit a WMM TSPEC element to the requestor contained in an ADDTS response management action frame. If the AP accepts the request, it calculates and includes the medium time in the admission response that is returned.
- An AP supporting only one admitted TS per access category per MU
- To delete an explicit admission, a MU should transmit a DELTS management frame containing the WMM TSPEC element to the AP

Motorola's admission control/TSPEC implementation is geared towards voice and video, with an emphasis on the number of devices rather than the throughput of each device. Whether WiFi will test for oversubscription is in doubt at this point. For now (while we'll have a framework based on statistic updates from the access point) we will not implement checks for MUs exceeding allocated bandwidth on admitted ACs. Resources allocated and used by MUs will be tracked internally, but will only be used to make decisions whether to drop traffic.

An administrator will be allowed to configure the maximum number of devices to be granted access in each admission controlled access category (voice and video). The switch grants or denies the TSPEC based on MU

counts. A MU will be allowed to associate and pass traffic on non-admission controlled ACs. User interfaces (CLI/SNMP/GUI) will provide status on the number of devices on each access category.

Based on further testing, the switch may also dynamically restrict the number of MUs on an access category, tracking the total bandwidth utilization of a radio, and denying further access to the voice or video access categories if impacting existing calls.

Each MU will be allowed to set two TSPECs (one per access category), and other TSPEC requests will be denied by the switch. If the switch receives traffic from a MU in an access category not granted access, it will be dropped. If admission control is enabled for video, it will be enabled for voice, thus all high priority access categories. This will have to be enforced by the user interface.

An administrator will be able to enable/disable admission control on either voice or both voice and video access categories, on a per-WLAN basis. An administrator is also be able to configure the maximum number of MUs per-access category for each access category marked for admission control.

6.4.1.6 QBSS Load Information Element

The QBSS load balance element has been added to beacons and probes as part of 802.11e. It provides information about the load of an AP (traffic, number of MUs) so MUs can make informed decisions when roaming.

6.4.2 Adopting an AP300 to a WS2000

Using Motorola's *Wireless Next Generation* (Wi-NG) architecture, you can adopt an AP300 via layer 2 or layer 3 of the OSI model. Use the proprietary WISP protocol to adopt an AP300 to the switch.

With Motorola's latest offerings, use the WIPSE protocol to adopt an AP300. WISPE is based on CAPWAP. For more information on WISPE, see, *WISPE on page 6-18*.

When an AP300 is powered, it tries to adopt to a switch:

1. First the AP300 tries an EAPOL. Check if the Ethernet where it is connected is using 802.1x port authentication.
2. Next the AP300 broadcasts 0x8783 ethertype packets to discover the switch on layer 2.
3. If layer 2 adoption fails, the AP300 transmits DHCP discover packets in order to receive the switch IP address via option 189.
4. A layer 2 discovery is conducted based on the older WISP protocol.
5. If adoption fails, the process is started again.

The following network trace illustrates the search process, where 00:15:70:24:56:33 is the MAC address of the AP300:

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
45	00:15:70:24:56:33	Ethernet Broadcast		247	13.919950	ETHER-87-83	
46	IP-169.254.171.216	IP-169.254.255.255		96	14.149622	NB Name Svc	C QUERY NAME=ZUK35EX
47	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	14.778990	802.1	
48	IP-169.254.171.216	IP-169.254.255.255		96	14.910670	NB Name Svc	C QUERY NAME=ZUK35EX
49	00:15:70:24:56:33	Mcast EAP Port Acc...		64	14.943781	EAPOL-Start	
50	00:15:70:24:56:33	Ethernet Broadcast		247	14.943795	ETHER-87-83	
51	00:13:60:17:29:03	00:13:60:17:29:03		64	15.375552	Loopback	
52	IP-169.254.171.216	IP-169.254.255.255		96	15.660374	NB Name Svc	C QUERY NAME=ZUK35EX
53	IP-0.0.0.0	IP Broadcast		346	16.094790	DHCP	C DISCOVER
54	IP-169.254.171.216	IP-169.254.255.255		96	16.410392	NB Name Svc	C QUERY NAME=ZUK35EX
55	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	16.792287	802.1	
56	IP-0.0.0.0	IP Broadcast		346	17.730775	DHCP	C DISCOVER
57	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	18.805597	802.1	
58	IP-0.0.0.0	IP Broadcast		346	19.880582	DHCP	C DISCOVER
59	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	20.818916	802.1	
60	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	22.832212	802.1	
61	IP-0.0.0.0	IP Broadcast		346	24.174794	DHCP	C DISCOVER
62	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	24.845511	802.1	
63	00:13:60:17:29:03	00:13:60:17:29:03		64	25.382121	Loopback	
64	00:15:70:24:56:33	Ethernet Broadcast		203	26.516497	ETHER-87-83	
65	00:15:70:24:56:33	Ethernet Broadcast		66	26.516713	ETHER-87-83	
66	00:13:60:17:29:03	Mcast 802.1d Bridg...	*	124	26.858817	802.1	
67	00:15:70:24:56:33	Ethernet Broadcast		1046	27.642279	ETHER-87-83	
68	00:15:70:24:56:33	Ethernet Broadcast		1046	27.642724	ETHER-87-83	
69	00:15:70:24:56:33	Ethernet Broadcast		990	27.643292	ETHER-87-83	
70	00:15:70:24:56:33	01:80:C2:00:00:0E		82	27.643376	ETHER-88-CC	
71	00:15:70:24:56:33	Mcast EAP Port Acc...		64	27.643488	EAPOL-Start	
72	IP-169.254.171.216	IP-169.254.255.255		96	27.664943	NB Name Svc	C QUERY NAME=ZUK35EX
73	IP-169.254.171.216	IP-169.254.255.255		96	27.667942	NB Name Svc	C QUERY NAME=ZUK35EX
74	IP-169.254.171.216	IP-169.254.255.255		96	27.674439	NB Name Svc	C QUERY NAME=ZUK35EX

A closer analysis of the EAPOL start reveals the following:

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        64
  Timestamp:            21:07:50.469677000 05/06/2008
Ethernet Header
  Destination:          01:80:C2:00:00:03  Mcast EAP Port Access Entity
  Source:               00:15:70:24:56:33
  Protocol Type:        0x888E  802.1x Authentication
802.1x Authentication
  Protocol Version:     1
  Packet Type:          1  EAPOL - Start
  Body Length:          0

Extra bytes
  Number of bytes:
  15702...........  31 35 37 30 32 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ..........        00 00 00 00 00 00 00 00 00 00
FCS - Frame Check Sequence
  FCS:                  0x11211BDB
```

A closer analysis of the WISPE layer 2 discovery process reveals the following:

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        247
  Timestamp:            21:07:50.469691000 05/06/2008
Ethernet Header
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:15:70:24:56:33
  Protocol Type:        0x8783
Extra bytes
  Number of bytes:
  ..... .........p  00 80 00 E1 00 20 C0 00 00 00 00 00 06 00 15 70
  $V3.............  24 56 33 00 00 00 00 01 03 00 CC 00 00 00 00 00
  ......".@.......  00 13 00 01 00 00 22 00 40 02 02 00 00 00 00 01
  .... WIAP-300...  84 00 00 00 20 57 49 41 50 2D 33 30 30 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  .........0015702  00 00 00 00 00 00 01 00 10 30 30 31 35 37 30 32
  45633.....$....&  34 35 36 33 33 00 00 00 00 00 24 00 01 04 00 26
  ....'...........  00 01 01 00 27 00 05 00 00 00 00 05 04 17 00 10
  ......p&...d....  00 00 04 0A 00 15 70 26 E7 14 00 64 00 00 00 00
  .'..............  00 27 00 05 01 00 00 00 02 04 17 00 10 01 00 04
  ...p&.x.d.....+.  0A 00 15 70 26 F1 78 00 64 00 00 00 00 00 2B 00
  ......... .)....  07 00 00 00 00 00 00 02 00 20 00 29 00 00 01 84
  ..4. WSAP-5110-1  04 01 34 16 20 57 53 41 50 2D 35 31 31 30 2D 31
  00-WWR..........  30 30 2D 57 57 52 00 00 00 00 00 00 00 00 00 00
  .....             00 00 00 00 00
FCS - Frame Check Sequence
  FCS:                  0x7A17C5EA
```

The following is a DHCP discovery packet rom the AP300. Look at the DHCP options, the AP300 is looking for option 189:

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        346
  Timestamp:            21:07:53.256671000 05/06/2008
Ethernet Header
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:15:70:24:56:33
  Protocol Type:        0x0800  IP
IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5  (20 bytes)
  Differentiated Services:%00000000
                        0000 00.. Default
                        .... ..00 Not-ECT

  Total Length:         328
  Identifier:           1230
  Fragmentation Flags:  %000
                        0.. Reserved
                        .0. May Fragment
                        ..0 Last Fragment

  Fragment Offset:      0  (0 bytes)
  Time To Live:         64
  Protocol:             17  UDP
  Header Checksum:      0x74D8
  Source IP Address:    0.0.0.0
  Dest. IP Address:     255.255.255.255  IP Broadcast
UDP - User Datagram Protocol
  Source Port:          68  bootpc
  Destination Port:     67  bootps
  Length:               308
  UDP Checksum:         0x2B47
BootP - Bootstrap Protocol
  Operation:                    1  Boot Request
  Hardware Address Type:        1  Ethernet (10Mb)
  Hardware Address Length:      6  bytes
  Hops:                         0
  Transaction ID:               0
  Seconds Since Boot Start:     1
  BootP Flags:                  0x0000
  IP Address Known By Client:   0.0.0.0  IP Address Not Known By Client
  Client IP Addr Given By Srvr: 0.0.0.0
  Server IP Address:            0.0.0.0
  Gateway IP Address:           0.0.0.0
  Client Hardware Addr:         00:15:70:24:56:33
```

```
  Unused:                       0x0000000000000000000
  Server Host Name:
.....................................................................
  Boot File Name:
.....................................................................
.....................................................
DHCP - Dynamic Host Configuration Protocol
  DHCP Magic Cookie:    0x63825363
Message Type
  Option Code:          53
  Option Length:        1
  Message Type:         1  Discover

Client Identifier
  Option Code:          61
  Option Length:        7
  Hardware Type:        1
  Hardware Address:     00:15:70:24:56:33

Parameter Request List
  Option Code:          55
  Option Length:        10
  Requested Option:     6  Domain Name Servers
  Requested Option:     3  Routers
  Requested Option:     1  Subnet Mask
  Requested Option:     15  Domain Name
  Requested Option:     66  TFTP Server Name
  Requested Option:     67  Bootfile Name
  Requested Option:     13  Boot File Size
  Requested Option:     44  NetBIOS (TCP/IP) Name Servers
  Requested Option:     189
  Requested Option:     43  Vendor Specific Information

DHCP Option End
  Option Code:          255

  Data Area:
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ...               00 00 00
FCS - Frame Check Sequence
```

7

Voice Over Wireless LAN

This chapter describes Motorola's *Voice over Wireless LAN* (VoWLAN) architecture, including:

7.1 What is VoWLAN

VoWLAN s the use of a wireless broadband network for voice supported conversations. In other words, it's just like VOIP, but over a Wi-Fi network. VoWLAN can be conducted over any Internet accessible device, including a laptop, PDA or new VoWLAN units which look and function like cell phones. VoWLAN's chief advantages to consumers are cheaper local and international calls, free calls to other VoWLAN units and a simplified integrated billing of both phone and Internet service providers.

Although VoWLAN and broadband have certain feature similarities, VoWLAN is different in the sense that it uses a wireless Internet network (typically 802.11) rather than a cellphone network. Both VoWLAN and broadband are used in different ways.

For example, a company with fixed warehouses or locations can take advantage of their existing WiFi network and use VoIP (hence VoWLAN) for employees to communicate with one another. Another example would be a company that has mobile workers (like a FedEx delivery person or a Coca Cola delivery driver) that deliver goods to stores.

7.1.1 VoWLAN and Motorola's Enterprise Wireless LAN

Motorola's WS2000, WS5100, RFS6000 and RFS7000 switch platforms support call admission control. The implementation of QoS is also available for voice calls. Part of the non-standard QoS is the ability to prioritize non-standard voice traffic (such as SVP for Spectralink phones).

Motorola has been a pioneer in implementing VoWLAN and ensuring seamless voice calls on the wireless network. A recent enhancement is the implementation of a *Voice Quality Manager* (VQM) client software on our MC50 and voice enabled PDA's. The software works with the Avaya's soft-phone client to provide echo cancellation in speakerphone environments. A second enhancement is the ability to prioritize voice traffic on wireless and wired mediums by automatically detecting voice traffic. Motorola supports other leading VOIP equipment vendors in automatic detection and prioritization. Motorola also supports the most recently ratified WMMe standard for classifying Multimedia traffic. In addition, a voice feature unique to Motorola switches (DTIM per BSSID) makes it very easy to implement a short DTIM for voice traffic only, and maintain a longer DTIM interval for other devices (thus increasing their battery life.)

Customers can choose a variety of phones to use with the Motorola WLAN infrastructure. Mobility devices such as the MC50 and MC9000 are tested with Avaya Softphone client software and can be used to implement VoWLAN.

7.1.2 Motorola Extensions

The wireless switch sends information (current load, retries, RSSI etc.) in beacons to MUs. The MU makes use of it to roam to another access port. Currently, only Motorola MUs have the software drivers needed to support auto load balancing and pre-emptive roaming.

Motorola's wireless LAN products are optimized to use with mobile battery powered devices. In addition to the standard 802.11 power save polling mechanisms, Motorola implements proprietary power save schemes for even better client power management.

When client devices enter power save mode, the switch or AP buffers incoming packets for the client. When the client device polls the AP, the queued packets will be delivered.

The AP buffers frames to MUs in standby mode. The MU's current power save mode is tracked by examining the power save bit in received frames from the MU.

Management frames are the highest priority for scheduling, with a queue depth of 4 frames (all queue sizes are based on number of frames, not on number of bytes).

Broadcast and multicast frames are the next highest priority for scheduling. Each BSS has a unique BC/MC queue, with a queue depth of 16.

Data frames are next in priority. Each MU has 4 queues for data frames, one for each access category (voice, video, best effort, and background). Each queue's depth is 11. The number and size of the queues is unaffected by a MU's power save state

7.1.3 Layer 2 and 3 Mobility

Layer 2 and 3 mobility is the main product design goal when it comes to Motorola's wireless switch systems, in order to shorten roam times to ensure application persistence. Motorola's patented pre-emptive roaming mechanism allows for sub-30ms roam times by ensuring devices move their connections to a new and better AP before connection quality gets too poor to sustain performance. In addition, Motorola's secure fast roaming implementation (with extensions to the WPA2 standard, PMK caching and opportunistic PMK caching) eliminate the need to re-authenticate on each roam. Caching credentials for each device in the network allow the switch to reduce roam times to <50ms with full 802.11i security (even with 802.1x/EAP

and Radius based security mechanisms). Compare this speed to 200ms to 2 minute roam times without these extensions. The WPA2 and 802.11i extensions are fully interoperable with 802.11i supplicants from Microsoft, Funk and Interlink.

Layer three roaming is an action that refers to roaming across a layer 3 boundary while keeping the existing IP address of the client. This feature becomes critical with application like voice and video over WiFi WLANs. It also is critical with older devices where the only way to receive a DHCP address is rebooting.

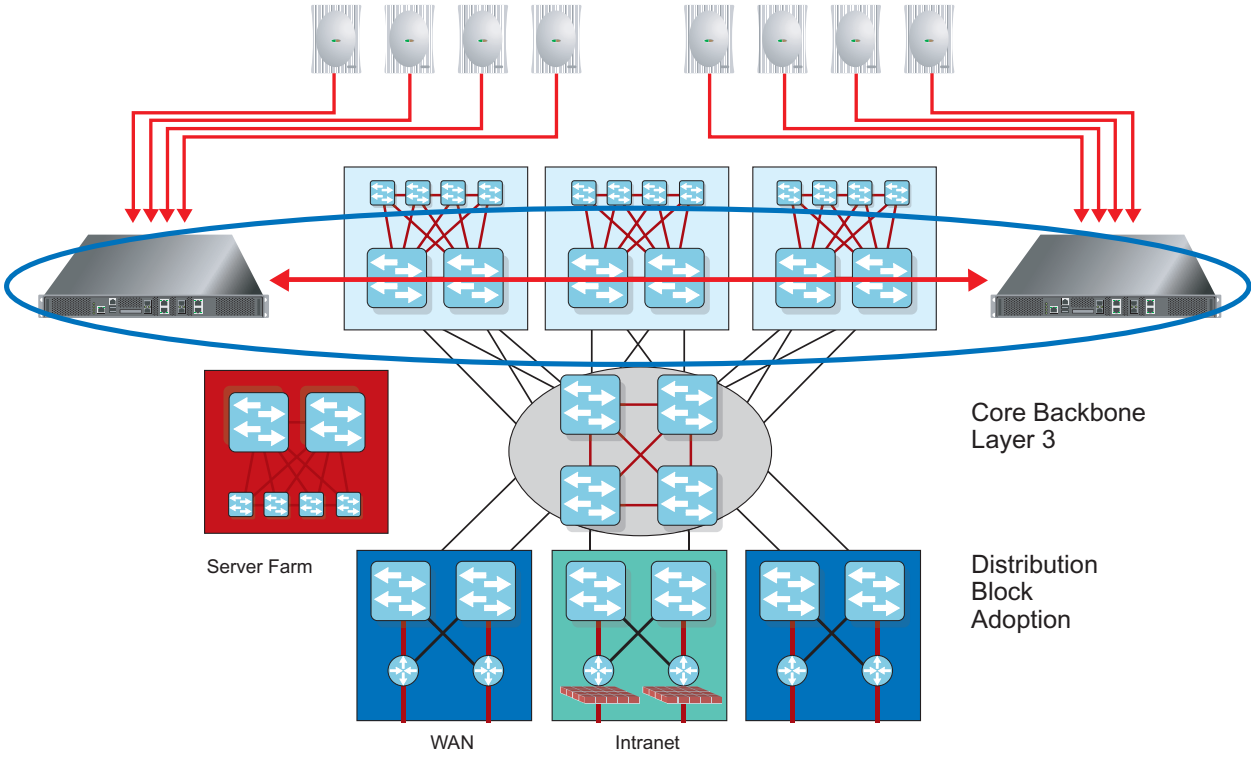
Layer 3 roaming occurs when a MU leaves a switch in the it's current subnet and roams to another wireless switch within its mobility domain.

With layer 3 roaming, mobility domains map multiple VLANs to the same wireless LAN (WLAN). An MU IP subnet is tied to the IP subnet the MU originally associated with. The MU's IP address is maintained as long as the MU stays associated to the WLAN. For IP address persistence, a mobility domain is established. A mobility domain consists of mobility peers. Mobility peers map the same WLAN to different VLANs. This solution is similar to mobile IP, where the client maintains its IP address as it roams from subnet to subnet by tunneling its traffic back to a home agent. Unlike mobile IP however, this solution does not involve client software and is implemented entirely by Motorola's wireless infrastructure.

7.1.4 The Mobility Domain

The mobility domain maps multiple VLANs to the same WLAN. The MU's IP subnet is tied to the IP subnet the MU originally associates. The MU's IP address is maintained as long as the MU is associated to the WLAN with a configurable MU time out interval. The default timeout is 30 minutes. For IP address persistence, a mobility domain is established. A mobility domain consists of mobility peers. A mobility domain should not be confused with a cluster. A wireless switch can be part of a cluster but be in a different mobility domain. Clusters deal with load balancing, while mobility domains deal with IP addressing.

Admittedly, there is continued pressure on performance requirements with the current explosion in voice and multimedia applications. Additionally, there is a market segment (large university campuses, very large Enterprise campuses, large hospitals, large financial institutions etc.) where it's not just the APs required for coverage, but the traffic supported does not require high performance infrastructure (like the Motorola RFS7000).



7.1.5 Planning for Layer 3 Roaming

When planning for layer 3 roaming support, there are some basic points to keep in mind.

Each RFS7000 supports up to 8000 users. Each switch maintains a separate table defining an MU's home or current switch. This table cannot exceed (2 x 8,000 = 16,000). 8,000 on the home switch and 8,000 on the current switch. If you have 2 switches peering with each other, you can potentially have all 8,000 MUs roaming from one to the other and still be under (or equal to) to the limit of 16,000.

7.1.6 Dynamic VLAN Load Balancing

Using dynamic VLAN load balancing (also known as VLAN pooling), each WLAN (ESSID) on the switch can be mapped to multiple VLANs. When a MU associates, it is dynamically assigned one of the VLANs in a manner optimally utilizing network resources. This form of load balancing keeps the number of MUs balanced across VLANs tracks the average bandwidth utilization on each VLAN to keep all the VLANs as uniformly loaded as possible.

7.1.7 Capacity

Each WLAN can be mapped to a maximum of 128 different VLANs. The number of VLANs per switch is not restricted (all 4094 allowed). The RFS7000 supports 256 WLANs, and up to 256 dual-mode access ports, that's 512 radios per switch and 3072 dual-mode access ports with 6144 radios per RFS 7000 switch cluster. Each of these WLANs can be mapped to a different set of VLANs.

VLAN pools are configured from the CLI as follows:

```
(config-wireless)# wlan <WLAN_INDEX> vlan <VLAN_LIST/RANGE>
 .... Eg: wlan 1 vlan 1-64
.......... wlan 2 vlan 100,200,300,500
```

7.1.8 Load Balancing Algorithm

The load balancing algorithm initially assigns MUs to VLANs in a round robin fashion. Once assigned, it periodically tracks VLAN usage based on the number of devices and average bandwidth utilization to output a weighted *usage-level* for each VLAN. VLAN assignments to subsequent MU associations are made based on this weighted VLAN utilization.

Consider the case where WLAN 1 is mapped to VLANs 1,2, 3. The first three MUs that associate are assigned to VLANs 1, 2, 3 respectively. However, if MU2 leaves the network, and MU4 associates, it will be assigned to VLAN 2. Depending on the network utilization of VLANs 1, 2, 3, the fourth MU associated could be assigned to any of the three VLANs.

The algorithm takes into account a MUs dynamic nature, and constantly works to keep the network uniform.

When a MU roams from one AP to another its VLAN is maintained in a *vlan-cache*, and reassigned on re-association. This avoids service disruption as MUs roam across the wireless network.

7.1.9 Maintaining Broadcast Separation

In the wired world, VLAN tags are used to ensure broadcast separation when two different broadcast domains share the same physical transport medium. In a wireless medium this is done using different BSSIDs. However, in a case of dynamic VLAN assignments, two MUs on the same BSSID are assigned to different VLANs. To ensure broadcast separation over the air, different broadcast keys per VLAN are used. This ensures even if a MU receives frames from both VLANs, it only decrypts the one from its own VLAN. The only packet that travels *up* the stack from the driver is the one from the right VLAN.

A MU is assigned a VLAN when it associates with the network. As part of either message #3 of the WPA2 handshake or the group-key-update message of the WPA handshake of 802.11i, the switch provides the MU with a broadcast key unique to its VLAN. This key is transmitted securely in a standards compliant manner.

Broadcast keys can also be periodically rotated by the switch for added security. The key rotation interval is configurable by the administrator and can be set on a per-WLAN basis.

7.1.10 Typical Packet Flows

Review the following (typical) VoWLAN packet flows:

- *Unicast from a MU* - The frame is decrypted, converted from 802.11 to 802.3, and switched to the wired side on to the VLAN dynamically assigned to the MU. If the destination is another MU on the wireless side, the frame is encrypted and switched over the air.
- *Unicast to a MU* - The frame is checked to ensure (in addition to the destination MAC address matching that of the MU), the VLAN is the same as the one assigned to the MU. It's then converted to an 802.11 frame, encrypted, and transmitted over the air.
- *Multicast/broadcast from a MU* - This is treated the same as a unicast frame from the MU, with the exception that (in addition to sending the frame to the wired side), it is encrypted with a per-VLAN broadcast key and transmitted over the air.
- *Multicast/broadcast from the wired side* - If a frame is received on a VLAN mapped to a WLAN, it's encrypted using a per-VLAN broadcast key and transmitted over the air. Only MUs on that VLAN have the broadcast key that can decrypt this frame, other MUs will receive but discard the frame.

7.2 VoWLAN Requirements for the Wireless Medium

Voice over WLAN solutions range from simple networks supporting a few voice-only handsets for specific users to multifunction systems. Many support dual-mode WLAN-cellular handsets along with smartphones and mobile computers and provide a variety of telephony, push-to-talk and data applications for different parts of the enterprise. To ensure the solution is extensible enough to meet all of these requirements, it is important to understand the scope of the enterprise's communications needs and opportunities available in the mobility space. That requirements assessment is a major step in determining the direction to follow for the VoWLAN implementation. Correctly implemented, WLANs can provide a robust, manageable and secure wireless infrastructure for both voice and data communications. The key is to choose products that incorporate state-of-the-art architectures and designs, and implement them in the most functional manner.

There are several requirements for VoWLAN networks to operate efficiently:

- *Robust, reliable WLAN infrastructure* - The foundation of any enterprise-grade VoWLAN deployment is a robust wireless infrastructure. That infrastructure must extend anywhere a user might be when they need to make or receive a call. The configuration must provide adequate capacity and good signal strength throughout the required coverage area. Poor signal conditions results in diminished voice quality, dropped connections and no-service-available conditions.
- *Voice-capable QoS and hand-off abilities* - To deliver enterprise-grade voice services, the infrastructure and user devices should make use of the IEEE 802.11e/WiFi Multi-Media (WMM) quality of service (QoS) standards. The network must be capable of handing off connections from access point to access point quickly and securely as the user moves throughout the coverage area.
- *Channel availability* - The 2.4 GHz ISM band used for the 802.11b and g radio links can accommodate only three non-interfering channels. When selecting voice-capable WLAN solutions ensure the equipment is also capable of supporting the 802.11a radio link that operates in the 5 GHz U-NII band and its 11 non-interfering channels.
- *Battery conservation* - Batteries are a critical concern in any mobile device. The WiFi Multi-Media (WMM) *Automatic Power Save Delivery* (APSD) standard can increase battery life 20 to 40%. However, that might not meet the requirements of many communications-intensive applications. Device capacity varies significantly, but there are VoWLAN solutions that can adequately cover even an extended shift.
- *Micro mobility* - Allows VoIP to roam from AP to AP within a WLAN coverage area without impacting voice quality or applications. APs can be on the same or different subnets. A wireless IP phone roams from one subnet to another within the same network with no call in progress or with a call in progress. Voice calls proceed normally during AP transitions, even between subnets. During a voice call, as the smartphone moves from AP to AP in the WLAN, it must remain reachable at its current assigned IP address, regardless of the location of its serving AP.

7.2.1 Toll Quality Voice

The first requirement in a VoWLAN solution is that the network provides toll-quality voice in all operating environments. Mobile voice can be a major boost to productivity, but if the user experience is unsatisfactory, they will avoid the network and find other means to make their critical communications. High-quality voice is the result of a sound infrastructure, high-quality handsets, and a network management system that ensures ongoing performance. A caller's experience includes four key factors: voice quality, call quality and service quality (experienced on every call), plus the usability of supplementary services that may also be employed.

- *Voice Quality* - Can the caller hear the other party? Can the speaker be recognized? Are the words garbled? Is there noise on the call? …These can be measured!

- *Call Quality* - Does the caller have a dial tone? Does the PBX or PSTN set up the call?
- *Service Quality* - Is the endpoint, or network, busy? Is the call lost? Can 800/900 numbers be accessed? Can 911 be accessed? There is a long list for service possibilities!
- *Usability of supplementary services* - Does the *interactive voice response* (IVR) application work properly, and does the voice mailbox have adequate storage for the calls?

7.2.2 VoIP Latency

VoIP is particularly sensitive to packet loss caused by weak signals, range limitations, and interference from other devices on the same frequency. A wireless network must be reliable, since users expect more dependability from their phone systems than from their computers. They expect a dial tone, no dropped calls, and high voice quality Consider the following affecting affect voice traffic:

- Latency (or packet delivery delay)
- Jitter (or the variation in arrival time between packets)
- Packet loss (occurring when too much traffic overflows buffers within the network causing dropped packets)
- Burstiness (when your network undergoes bursts of packet activity)

7.2.3 Enterprise WLAN Requirements

The backhaul network for a WLAN is the wired LAN. The backhaul network moves traffic from a users VoIP phone and WLAN to servers. It encompasses equipment not part of the WLAN. The customer supplies and maintains the backhaul. If capacity increases in the WLAN, the backhaul needs to expand to manage the traffic. The backhaul network equipment includes:

- Routers
- Switches
- Other networking gear

The backhaul network consists of two types:

- Local backhaul (layer 2), from the AP to the switch, which uses VLAN and switching
- Wide-area backhaul (layer 3) for cross-regional or wide-area sites

Quality of Service (QoS) is a requirement when setting up the backhaul. If an Enterprise uses a centralized deployment model, where the servers are located in a hub and spokes radiate from the hub to where various sites are located and from which WLAN traffic needs to be supported, then the signaling and voice traffic need to be backhauled to/from the VoIP servers and mobile phones. Routers and switches must comply with standards for QoS settings.

For voice traffic, the network mechanisms used to isolate and prioritize traffic within a given site (for example, VLANs) will probably be different from what is done with wide-area traffic, where layer 3 routing is often done (and VLANs are not typically used). Also, the wide-area network may not use 802.1 Q/p, but instead it may use other means to do gross or simple traffic prioritization.

WLAN infrastructure needs to be engineered to support voice and data on the same medium. This includes standards-based security features required in the WLAN (enterprises require a level of security in their wireless networks that is at least equal to the security available to other segments of their network).

A WLAN provides seamless mobility throughout the Enterprise with transparent handoffs between access points and subnets. Security in call admission control assures the availability of sufficient bandwidth before

a voice call enters the Wi-Fi network. QoS for packet prioritization needs to be designed throughout the entire network system (without any breaks in connectivity) to ensure voice calls have the highest priority on the Wi-Fi network. Voice must be allowed priority access with minimal jitter and delay and data is allowed use of the VoIP network only when it is not needed for voice calls.

7.3 Planning VoWLAN Deployments

Before considering VoIP device deployments, a careful survey should be performed by a network administrator to consider the network users will rely on and verify it is VoIP capable. Design considerations influence the success of integrating VoIP with an existing network. When transmitting voice over a data network, quickly detecting and fixing problems is central. VoIP traffic will quickly become the most important information the network transmits. You should dedicate time and effort into planning, implementing and preserving the VoIP network.

The following are considerations that should be adhered to when considering the deployment of a VoIP solution:

- *Document the Requirement of the VoIP Solution*
- *Characterize the Existing Wired LAN Voice Traffic*
- *Identify Existing LAN Servers for Compatibility and Capacity*
- *Separate Voice and Data When Possible*
- *Be Aware of Security*
- *Be Cognizant of Multiple Subnets*
- *Use QoS on the WLAN and Backbone*
- *Use Wi-Fi Multimedia (WMM)*
- *Use SIP for VoIP Connections*
- *Be Aware of Security*

7.3.1 Document the Requirement of the VoIP Solution

7.3.1.1 Existing Deployments

If the VoIP solution is intended for an existing wireless infrastructure:

- *Perform a VoIP assessment* - Existing wired, wireless, and telephony infrastructures should be evaluated for voice readiness. This involves an analysis of the existing wired and wireless network and telephony infrastructures and any recommendations for changes or additions to support the VoIP solution.
- *Perform network planning and design* - If additions or changes to the existing wired or wireless infrastructure are required, a network design is required to identify wired and/or wireless network changes such as the addition of APs, the addition or reconfiguration of switches or routers, or the addition of an IP PBX or TDM Gateway.

Perform the following specific checks to determine if the network infrastructure is voice-capable:

- *Evaluate the WLAN* - Ensure the WLAN supports QoS (WMM/WMM-PS), and uses equipment Motorola has either tested, or is in the same family as equipment tested by Motorola.
- *Conduct an inventory* - Inventory the number and model of existing wireless clients, 802.11b, 802.11g, and possibly 802.11a.

- *Evaluate the LAN* - Evaluate the existing PBX (circuit, packet, existing IP-PBX, capacity, interfaces etc.) for upgrade, replacement, or co-location.
- *Evaluate existing LAN equipment* - The LAN network needs to support QoS (802.1Q/p).
- *Determine system capacity* - Evaluate the existing network management system and capacity.

7.3.1.2 New Deployments

If the VoIP solution is intended for a new wireless infrastructure deployment:

- *IP telephony or a TDM gateway* - Besides supporting mobility, IP telephony provides numerous other benefits. These systems support a full complement of telephony features and call processing functions, and deliver these across the Enterprise IP network. A converged voice/data network simplifies network administration and reduces the cost of endpoint moves, adds, and changes. Significant savings are possible by routing IP voice calls over the corporate data network, instead of the costly public toll network. If an update to IP telephony is not feasible, a TDM gateway can provide the ability to deploy the TEAM solution with a TDM PBX.
- *WLAN design* - Designed from ground-up to support voice traffic, the WLAN delivers critical features such as intelligent no delay roaming, load balancing, advanced quality of service and end-to-end security. Additionally, centralized security and management capabilities have many benefits for traditional data applications.

7.3.2 Characterize the Existing Wired LAN Voice Traffic

This could be extended to a comprehensive plan including additional LAN ports needed to interface APs, additional bandwidth concerns and additional IP addressing concerns. This should also work with deployment loading tools to avoid re-entering common information. Deployment loading tools are used by an end-customer's planning team and/or *System Integration* (SI) vendor. Motorola RF Design software is used for measuring the existing environment (sniff) and planning (layout) the network(s); for more information, visit *www.motorola.com/RFdesign*. Essential tools for VoIP planning include:

- *Motorola LANPlanner* – Used to design, plan, and optimize the network.
- *Motorola SiteScanner* – Used to simulate network activity and perform site surveys for 802.11 Wi-Fi networks.
- *OmniPeek®* – Used for Wi-Fi and Ethernet sniffing (EtherPeek and AiroPeek are now OmniPeek).
- *Wireshark® (formerly Ethereal®)* – Used for Ethernet sniffing.
- *AirMagnet®, GL Communications, VXVoice, and ixChariot®* – Designed for various very low level assessments of network and audio performance.[

7.3.3 Identify Existing LAN Servers for Compatibility and Capacity

Identify the following if possible:

- Authentication, authorization, and accounting (AAA) servers
- Domain name services (DNS) servers
- Dynamic host configuration Ppotocol (DHCP) servers
- E-mail servers
- Voice mail servers
- Network time protocol (NTP) servers

- IP-PBX/Analog PBX
- Directory servers
- Existing WLAN infrastructures

7.3.4 Separate Voice and Data When Possible

The Motorola preferred solution for VoIP WLAN networks is 802.11a or 802.11a with 802.11g (no 802.11b clients). This solution maximizes capacity but does not address legacy 802.11b devices. 802.11b clients can be offered their own reserved channel for operation by installing 802.11b access points. This maximizes the throughput of 802.11b on their channel.

7.3.5 Be Aware of Security

A WLAN should optimally employ various security protocols at different layers within the system to protect the system from unauthorized access, intrusion and compromise. This includes security frameworks for authentication and authorization and for the encryption of signaling and voice traffic.

- The security framework protects the physical components of the system from attack
- Authentication and authorization determine if a smartphone and a subscriber should be granted access to the system
- Encryption ensures privacy of the voice and data being transmitted
- Separate security policies and measures are configured and deployed on interfaces between various elements within the Enterprise network as well as between the Enterprise network and remote subscribers
- Network management interfaces are secured with authentication and encryption mechanisms

The following framework provides a comprehensive standards based security solution:

- WPA/WPA2 (802.11i) on-the-air interface from the smartphone to the WLAN
- X.509 certificates on smartphones and servers for device authentication
- Extensible Authentication Protocol – Transport Layer Security (EAPTLS) on the system interface

Optimized approaches on security interfaces include:

- WLAN authentication with abbreviated 802.1x exchange during AP change
- Reuse of a single TLS/TCP connection between the smartphone and the SIP Proxy for both directions of the SIP signaling traffic

7.3.6 Be Cognizant of Multiple Subnets

A high number of subnets lead to more Layer 3 routing. A trade-off occurs between the number of subnets and the coverage domain. On a given subnet, all the subscribers hear all Layer 2 (L2) transmissions. This is due to the following:

- Broadcast packets sent to all destinations on L2 networks
- Increased likelihood of collisions

Do not use multiple subnets because:

- More routing between subnets could be needed while the smartphone is on a call. Smartphone keeps the same IP address within a call, even when crossing L2 subnets

- Routing packets consume the capacity of the wireless routers

7.3.7 Use QoS on the WLAN and Backbone

The Enterprise-provided WLAN and LAN equipment must meet QoS requirements. QoS is the prioritization of packets across a network. QoS becomes critical when voice is introduced over IP (VoIP). If any point the communication path does not support QoS, the effect is the same as not having QoS on the path at all. The effect on voice traffic is to deprioritize the packets, which results in additional jitter and delay. This causes the audio to degrade and may manifest as drop outs and additional noise in the background.

7.3.8 Use Wi-Fi Multimedia (WMM)

A Wi-Fi Alliance interoperability certification (based on the IEEE 802.11e draft standard) adds QoS extensions to the 802.11 standard. WMM allows the subscriber unit and the access point to categorize messaging between the endpoints and to prioritize the messaging. WMM prioritizes traffic according to four *Access Categories* (AC):

- AC_VO (Voice)
- AC_VI (Video)
- AC_BE (Best Effort)
- AC_BK (Background)

WMM-AC adds admission control to WMM access classes. It limits the number of simultaneous calls on a single AP. Admission control ensures adequate bandwidth is available for a voice call and contributes to overall voice quality. The bandwidth reservation record format has been described within the WMM specification. The implementation of bandwidth reservation has been previously limited to select vendor proprietary versions (such as Cisco APs). The WiFi Alliance is in the process of inter-vendor testing for WMM-AC.

7.3.9 Use SIP for VoIP Connections

The *Internet Engineering Task Force* (IETF) introduced *Session Initiation Protocol* (SIP) to simplify the process of running VoIP connections across the Internet. Networks running SIP can handle VoIP calls regardless of which vendor has created the smartphones or soft phones. SIP allows consistent inter-connectivity between products (such as between the WSM) the PBX and the smartphone, when used as the baseline call signaling protocol. SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.[

7.3.10 In Conclusion

VoIP equipment and installations have evolved into a working system for replacing *plain old telephone service* (POTS) equipment, provided the principles of QoS are followed from end to end. Existing WLANs more often than not require upgrades in equipment and backbone LANs to support VoIP users as they grow. Investigations must not fail to provide the type of network needed to the VoIP application chosen and those it might evolve into. A perfect execution of the three C's of network planning will bring about a working VoIP environment:

Context - The environment in which a VoWLAN is deployed

Coverage - Communication at a specified minimum transmit data rate at a given location

Capacity - Making sure all installations provide enough capacity for excellent user experiences on VoIP

7.4 Conducting a VoIP Site Survey

A RF site survey is used to supply enough information to determine the number and placement of APs to provide adequate coverage throughout the facility. Motorola offers tools that help design and subsequently monitor WLANs. In addition, Motorola offers professional services to perform site surveys. For more information, contact your Motorola Account manager.

For WLANs, it can be difficult to predict the propagation of radio waves and detect the presence of interfering signals without the use of test equipment. Even if you are using omni-directional antennas, radio waves do not travel the same distance in all directions. Walls, doors, elevator shafts, people, and other obstacles offer varying degrees of attenuation, which causes an irregular and unpredictable RF radiation pattern. As a result, it is necessary to perform an RF site survey to understand the behavior of radio waves within a facility before installing wireless network APs. In most implementations, adequate coverage means support of a minimum data rate. An RF site survey also detects the presence of interference coming from other sources that could degrade the performance of the WLAN. The need and complexity of an RF site survey varies depending on the facility.

When conducting an RF site survey, consider these general steps:

1. *Obtain a facility diagram* - Before beginning the site survey, locate a set of building blueprints. If none are available, prepare a floor plan drawing that depicts the location of walls, walkways, and any other obstructions.
2. *Visually inspect the facility* - Be sure to walk through the facility before performing any tests to verify the accuracy of the facility diagram. This is a good time to note any potential barriers that may affect the propagation of RF signals. For example, a visual inspection will uncover obstacles to RF such as metal racks and partitions, items that blueprints generally do not show.
3. *Identify subscriber areas* - On the facility diagram, mark the areas of fixed and mobile subscribers. In addition to illustrating where subscribers may roam, indicate where they may not roam.
4. *Determine preliminary AP locations* - Consider the location of subscribers and range estimations of the WLAN products you are using, to determine the locations of APs to provide adequate coverage throughout the subscriber areas. Plan for some propagation overlap among adjacent APs, but ensure that channel assignments for APs are far apart to avoid inter-AP interference.
    - Consider mounting locations, which could be vertical posts or metal supports above ceiling tiles
    - Recognize suitable locations for installing the AP, antenna, data cables, and power lines
    - Consider different antenna types when deciding where to position APs. An AP mounted near an outside wall, for example, could be a good location if you use a patch antenna with relatively high gain oriented within the facility.
    - Consider the worse case scenario in terms of subscribers and ensuring coverage
    - Use a tool, such as the Motorola LANPlanner to build a RF design
5. Ensure WLAN equipment meets requirements that make it voice-capable.
    - Include power requirements and power availability of WLAN equipment
    - Document A/C and floor space requirements, as well as distances to connect to LAN infrastructure (100 meter limits for 100BaseT and so on)
    - Determine the number and type of existing wireless clients – 802.11 b/g/a
    - Describe existing wireless clients and estimate the total capacity
    - Identify any existing 802.11a/b/g APs to be upgraded for WLAN use (other vendors, older non-

compliant APs, and so on)

- It is unlikely that an existing WLAN will support a VoIP solution. Most WLANs will require new access points, switches, and network QoS

6. Verify AP locations.

   This is when the real testing begins. Use a site survey tool available from Motorola (Site Scanner) or from a third-party company. For example, Berkeley Varitronics Systems offers a line of handheld devices, such as Grasshopper, Scorpion, AirMagnet and Yellowjacket that provide advanced site survey functions. Install an AP at each preliminary location, and monitor site survey software readings by walking varying distances away from the AP. You do not need to connect the AP to the distribution system because the tests merely ping the AP.

   However, you need AC power. Note the data rates and signal readings at different points as you move to the outer bounds of the AP coverage. In a multi-floor facility, perform tests on the floors above and below the AP. A poor signal quality reading indicates that RF interference is affecting the Wireless LAN. This would warrant the use of a spectrum analyzer to characterize the interference, especially if there are no other indications of its source. Based on the results of the test, you may need to reconsider the location of some APs and redo the affected tests.

7. Ensure smooth transition from subnet to subnet.

   Find locations to place APs to insure seamless roaming throughout the building.

8. Document the findings.

   Once you are satisfied that the planned location of APs will provide adequate coverage, identify the recommended mounting locations on the facility diagrams.Installers will need this information. Also, provide a log of signal readings and supported data rates near the outer propagation boundary of each AP as a basis for future redesign efforts.

8

Building Enterprise WLAN Solutions

A WLAN design is much more complex then simply measuring RF coverage in an area where mobility is enabled.

Refer to the following to review the Motorola solutions available to implement a Wireless LAN.

8.1 AP-5131 and AP-5181

The AP-5181 is a hardware variant of the AP-5131 designed specifically for outdoor use or in harsh environments requiring an extended operational temperature range. The AP-5181 supports the same software feature set as the AP-5131, and operates using same firmware.

An AP-5131 or AP-5181 (designed for outdoor deployments) provides an Enterprise-class 802.11a/b/g access point providing the following benefits:

8.1.1 High-Performance, Wired and Wireless Connectivity

Designed for small offices and retail locations, the AP-5131 delivers wired and wireless networking with Enterprise class performance and security in a single enclosure. This easy-to-deploy solution offers the flexibility to connect securely to remote corporate private networks, the Internet and local network resources with the speed and reliability to support the most demanding applications, including real-time video and

voice. The all-in-one AP-5131 delivers a new level of cost-efficiency and networking simplicity for employees in branch offices or telecommuters working at home. The AP-5131 boasts an integrated router, firewall, VPN, DHCP, AAA, hotspot gateway and other services in one remotely manageable device, simplifying network set-up and management.

8.1.2 Enterprise Class Security and Management

Support for today's standards-based security protocols ensures Enterprise-level protection for users on wireless laptops and other mobile devices, as well as wired computers. A wide variety of administration features provide powerful and secure control by either local, non-technical staff or remote IT professionals in the *Network Operations Center (*NOC).

8.1.3 Dual Radio 802.11 a/b/g Architecture

An AP-5131 and AP-5181's dual-radio architecture offers the flexibility to best meet wireless LAN networking and security needs through either dual-band data services, or single-band data services and full-band rogue AP detection, which identifies and reports unauthorized entities on the network. A complete suite of dual and single-band antennas provides the versatility to customize radio coverage for even the most challenging environments, with a minimal number of access points.

8.1.4 Mesh networking

To extend wireless network coverage to areas where Ethernet or fiber cabling is cost-prohibitive or otherwise impractical, the access point can operate wirelessly, connecting to other access points for data backhaul in a mesh topology. Enabling an array of applications, from simple point-to-point bridges connecting two wired networks, to complex multi-node multi-link networks, this feature provides a cost-effective way to extend the network outdoors and remote areas. Taking advantage of the dual-radio architecture and the easy-to-use configuration interface, it becomes a simple task to deploy a wireless network of access points connected securely via 802.11a, providing Enterprise-class 802.11b/g service.

8.1.5 Specifications

8.1.5.1 Wired Features

An AP-5131 and AP-5181 model access point support the following wired access point features:

- Router - WAN-LAN-WLAN routing function
- Firewall - Isolation of the LAN-WLAN from WAN
- DHCP & NAT - LAN IP address management
- PPPoE - Cable/DSL uplink support
- 802.1x wired-authentication
- 802.1q Trunking - VLAN support on LAN port
- IPSec VPN client - Secure backhaul to a corporate network over the WAN
- Dual FE uplink (LAN + WAN)

8.1.5.2 Radio Features

An AP-5131 and AP-5181 model access point support the following radio features:

- 4 BSSIDs per radio

- 16 WLANs, 8 BSSIDs total, 16 VLANs
- Supports 32 SSIDs. For a AP300 this means 8 SSIDs are supported for the 802.11b/g radio and 8 SSIDs for the 802.11a radio
- Wi-Fi certified
- WPA, WPA2, KeyGuard, Kerberos security
- WMM certified
- 802.11a DFS/TPC - Radar detection and avoidance
- Mesh networking with trunking
- Dual-radio 802.11a+b/g
- The 802.11 spec allows broadcasting a beacon for every BSSID (MAC address) on the radio. Motorola radios have 4 BSSIDs per access point. On each radio 4 of the 16 ESSIDs can be selected as primary ESSIDs and can broadcast. The other 12 are accessible by MUs via probe-responses

8.1.5.3 Memory

An AP-5131 and AP-5181 model access point support the following memory specifications:

- Volatile memory = 64MB (megabytes)
- Non-volatile memory = 2MB and 64MB (megabytes)

8.1.5.4 Management Features

An AP-5131 and AP-5181 model access point support the following management and user access features:

- Web-based Java UI
- CLI
- SNMP v3
- SSL v3.1
- SSHv2
- Motorola's *Mobility Services Platform* (MSP)

8.1.5.5 Security Features

An AP-5131 and AP-5181 model access point support the data protection and security features:

- Integrated VPN endpoint
- AAA Server with hotspot gateway
- Supports 25 Radius entries configured as the host or subnet
- Rogue AP detection
- Enterprise-class WPA2, 802.11i, KeyGuard, Kerberos security
- Enterprise-class management via RFMS
- Virtual AP technology for true broadcast domain separation in the air

8.1.5.6 VPN Terminations Tested

An AP-5131 and AP-5181 model access point support VPN terminations, including:

- Cisco ASA
- Nortel Contivity
- Netscreen
- Cisco PIX
- All standard IPSec modes

8.1.5.7 MTBF

AP5131 - ~245,000 hours

8.1.5.8 Port Adoption

The supports *Adaptive AP* (AAP) for port adoption. There's no *dumbing down* the AP to adopt to the switch

8.1.6 Real Time Locationing Support

An AP-5131 or a AP-5181 at a remote branch office or telecommuter site can now be controlled from a wireless switch at a central site over a WAN connection. The adaptive access points remain operational even if they loose their connection to the wireless switch. This enables an adaptive mesh network where mesh access points can be centrally configured from the wireless switch.

The following locationing features are supported by the access point:

- *Mobile Unit Locationing Support* - This feature, if enabled, creates a probe table for up to 200 MUs containing information that can be polled by SNMP using Motorola's *RF Management System* (RFMS). Using RF triangulation, RFMS can locate MUs in proximity of the access point with an accuracy of +/-10 meters.
- *Radius Time Based Authentication* - Extends the capability of the on-board Radius server on the access point to allow time based authentication for user groups when accessing a WLAN.
- *Rogue AP Detection Enhancement* - Dual radio access points now support a detector radio to perform dual-band scanning across A/B/G channels.

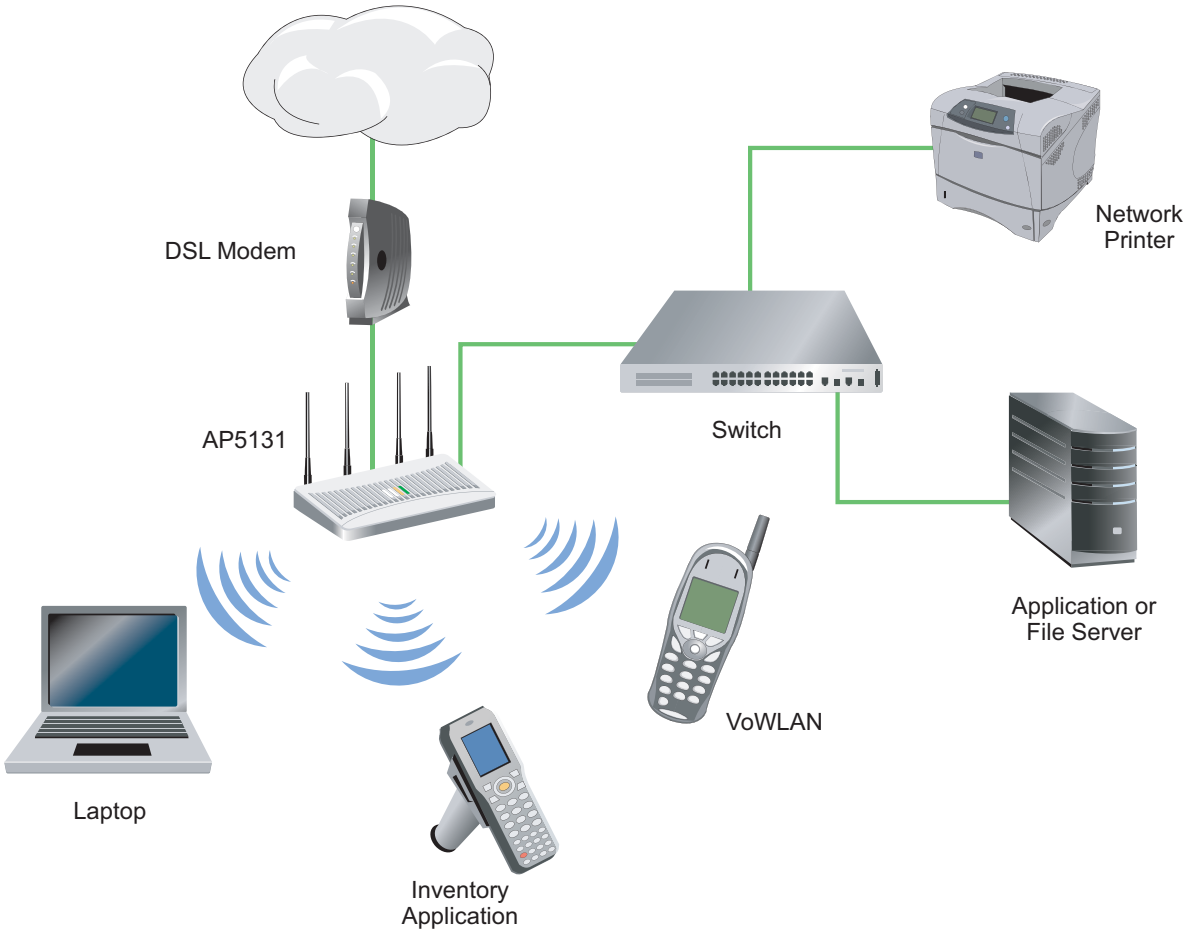
The AP-5131 provides a single-box solution which integrates all services required to extend secure broadband access to mobile users in a small or retail outlet.

8.1.7 Single Cell Deployments

A single cell deployment is the simplest form of deployment there is. A single cell is usually deployed in a small area where wireless is required for the flexibility of its usage, like a small store or small branch office.

With wireless, it is very easy to move users around or make the worker mobile for stock take applications in small retail stores.

A typical small SOHO type deployment may look as follows:



In the above deployment, you have a single ESSID mapped to a single BSSD to serve different applications of different verticals.

The DSL modem is used to bridge DSL and Ethernet connected to the AP5131's WAN port. The WAN port handles the PPPoE protocol to authenticate the subscriber to the DSL service.

The AP-5131 is the bridge between LAN and WLAN to serve wireless clients.

8.1.8 Adding Security to an Access Point Supported WLAN

Security can be provided in different levels and forms. One should take great care in what security is used to make their WLAN secure.

The reason for stating this so emphatically, is that securing the WLAN and the services of that WLAN are not always proportional, and neither is the cost of integrating the security mechanism used for securing its data. The access point supports the following security schemes:

For Authentication:

- Manually pre-shared key/no authentication
- Kerberos (Motorola proprietary)
- 802.1x

For Encryption:

- WEP 64 (40 bit key)
- WEP 128 (104 bit key)
- KeyGuard (Motorola proprietary)
- WPA/WPA TKIP
- WPA2/CCMP (802.11i)

The access point can flexibly integrate with a Radius server. The following is a summary of the access point's 802.1x security options:

- Built in Radius server with a local user database
- Built in Radius server with a central user database connected via LDAP
- External or remote Radius server
- Option for a secondary Radius server

8.2 Mesh Networking

The access point's mesh networking functionality allows it to function as a bridge to connect two Ethernet networks as a repeater to extend your network's coverage area without additional cabling. Mesh networking is configurable in two modes. It can be set in a wireless client bridge mode and/or a wireless base bridge mode (which accepts connections from client bridges). These two modes are not mutually exclusive.

In client bridge mode, the access point scans to find other access points using a selected WLAN's ESSID. The access point must go through the association and authentication process to establish its wireless connection. The mesh association process is identical to the access point's MU association process. Once the association/authentication process is complete, the wireless client adds the connection as a port on its bridge module. This causes the access point (in client bridge mode) to begin forwarding configuration packets to the base bridge. An access point in base bridge mode allows its radio to accept client bridge connections.

The two bridges communicate use the *Spanning Tree Protocol* (STP). The spanning tree determines the path to the root and detects if the current connection is part of a network loop with another connection. Once the spanning tree converges, both access points begin learning which destinations reside on which side of the network. This allows them to forward traffic intelligently.

After the access point (in client bridge mode) establishes at least one wireless connection, it will begin beaconing and accepting wireless connections (if configured to support mobile users). If the access point is configured as both a client bridge and a base bridge, it begins accepting client bridge connections. In this way, the mesh network builds itself over time and distance.

Once the access point (in client bridge mode) establishes at least one wireless connection, it establishes other wireless connections in the background as they become available. In this way, the access point can establish simultaneous redundant links. An access point (in client bridge mode) can establish up to 3 simultaneous wireless connections with other AP-5131s or AP-5181s. A client bridge always initiates the connections and the base bridge is always the acceptor of the mesh network data proliferating the network.

Since each access point can establish up to 3 simultaneous wireless connections, some of these connections may be redundant. In that case, the STP algorithm determines which links are the redundant links and disables the links from forwarding.

To familiarize yourself with mesh networking and understand how its deployed, review the following:

- *Mesh Overview*
- *The Access Point Client Bridge Association Process*
- *Mesh Spanning Tree Protocol (STP)*
- *Defining the Mesh Topology*
- *Mesh Networking and the Access Point's Two Subnets*
- *Normal Operation*
- *Importing and Exporting Configurations to a Mesh Network*
- *Configuring Mesh Network Support*
  - *Setting the LAN Configuration for Mesh Networking Support*
  - *Configuring a WLAN for Mesh Networking Support*
  - *Configuring the Access Point Radio for Mesh Support*
- *Mesh Deployment Scenarios*

8.2.1 Mesh Overview

An access point can be configured in two modes to support mesh networking. The access point can be set to a client bridge mode and/or a base bridge mode (which accepts connections from client bridges). Base bridge and client bridge mode can be used at the same time by an individual access point to optimally bridge traffic to other members of the mesh network and service associated MUs.

An access point in client bridge mode scans to locate other access points using the client's ESSID. Then it goes through the association and authentication process to establish wireless connections with located devices. This association process is identical to the access point's current MU association process. Once the association and authentication process is complete, the wireless client adds the connection as a port on its bridge module. This causes the client bridge to begin forwarding packets to the base bridge. The base bridge realizes it is talking to a wireless client bridge, and adds that connection as a port on its own bridge module. The two bridges at that point are communicating using STP.

Access points configured as both a base and a client bridge function as repeaters to transmit data to associated MUs in their coverage area (client bridge mode) as well as forward traffic to other access points in the mesh network (base bridge mode). The number of access points and their intended function within the mesh network dictate whether they should be configured as base bridges, client bridges or both (repeaters).

The spanning tree determines the path to the root and detects if the current connection is part of a network loop with another connection in the system. Each bridge can be configurable so the administrator can control the spanning tree to define the root bridge and what the forwarding paths are. Once the spanning tree converges, both access points begin learning which destinations reside on which side of the network. This allows them to forward traffic intelligently.

After the client bridge establishes at least one wireless connection (if configured to support mobile users), it begins beaconing and accepting wireless connections. If configured as both a client bridge and a base bridge, it begins accepting client bridge connections. Thus, the mesh network could connect simultaneously to different networks wherein a network loop is not created and the connection is not blocked. Once the client bridge establishes at least one wireless connection, it begins establishing other wireless connections as it finds them available. Therefore, a client bridge can establish simultaneous redundant links.

A mesh network must use one of the two access point LANs. If intending to use the access point for mesh support, Motorola recommends configuring at least one WLAN specifically for mesh networking support.

The client bridge creates up to three connections, if it can find a base bridge. If the connections are redundant (on the same network), then one connection will be forwarding and the others blocked. However, if each of the connections links to a different wired network, then none are redundant and all are forwarding. Thus, the bridge automatically detects and disables redundant connections, but leaves non-redundant connections forwarding. This gives the user the freedom to configure their topology in a variety of ways without limitations. This is important when configuring multiple access points for base bridge support in areas like a shipping yard, where a large radio coverage area is required.

NOTE: Since each access point can establish up to 3 simultaneous wireless connections, some of these connections could be redundant. If this is the case, the STP algorithm defines which links are the redundant links and disables those links from forwarding.

If an access point is configured as a base bridge (but not as a client bridge) it operates normally at boot time. The base bridge supports connections made by other client bridges.

A dual-radio model access point affords users better mesh optimization by enabling the access point to transmit to other mesh members using one independent radio and transmit with associated MUs using the second independent radio. A single-radio access point has its channel utilization and throughput degraded in a mesh network, as the AP's single radio must process both mesh network traffic with other access points and MU traffic with its associated devices.

8.2.2 The Access Point Client Bridge Association Process

An access point in client bridge mode performs an active scan to quickly create a table of nearby access points. The table contains access points matching the ESS of the client bridge AP's WLAN. The table is used to determine the best access point for connection (based on signal strength, load and the user's configured preferred connection list).

The client access point sends 802.11 authentication and association frames to the base access point. The base access point responds as if the client is an actual MU. Depending on the security policy, the two access point's engage in the normal handshake mechanism to establish keys.

After device association, the two access points are connected and the system can establish the bridge and run the spanning tree algorithm. In the meantime, the access point in client bridge mode continues to scan in the background attempts to establish an association with other access points using the same ESS on the same channel.

NOTE: Only Motorola AP-5131 or AP-5181 model access points can be used as base bridges, client bridges or repeaters within an access point supported mesh network. If utilizing a mesh network, Motorola recommends considering a dual-radio model to optimize channel utilization and throughput.

NOTE: An access point in base bridge mode logs out whenever a Client Bridge associates to the base bridge over the LAN connection. This problem is not experienced over the access point's WAN connection. If this situation is experienced, log-in to the access point again.

An access point in client bridge mode attempts to establish up to 3 simultaneous wireless connections. The second and third connections are established in the background while the system is running. The first connection needs to be established before the system starts bridging traffic.

A dual-radio model access point affords users better optimization of the mesh networking feature by allowing an access point to transmit to other access points (in base or client bridge mode) using one independent radio and transmit with its associated MUs using the second independent radio. A single-radio access point has its channel utilization and throughput degraded in a mesh network, as the access point's single radio must process both mesh network traffic with other access points and MU traffic with its associated devices.

For example:

Two access points are deployed with the following configurations:

- AP #1 base bridge
- AP #2 repeater (both a base and client bridge)

In the case of a mesh enabled radio, the client bridge configuration always takes precedence over the base bridge configuration. Therefore, when a radio is configured as a repeater (AP #2), the base bridge configuration takes effect only after the client bridge connection to AP #1 is established. Thus, AP #2 keeps scanning to find the base bridge, form the uplink and start beaconing as a base bridge for downstream client bridge connection. This is by design, as there is no reason to use a partially broken connection with no uplink to a base bridge.

8.2.3 Mesh Spanning Tree Protocol (STP)

The access point performs mesh networking using STP as defined in the 802.1d standard. Once a device association is complete, the client and base bridge exchange *Configuration Bridge Protocol Data Units* (BPDUs) to determine the path to the root. STP also determines whether a given port is a redundant connection or not.

8.2.4 Defining the Mesh Topology

When a user wants to control how the spanning tree determines client bridge connections, they need to control the mesh configuration. The user must be able to define one node as the root. Assigning a base bridge the lowest bridge priority defines it as the root. The access point can manipulate the path cost assigned to a bridge connection based on that connection's RSSI. This results in the spanning tree selecting the optimal path for forwarding data when redundant paths exist. However, this can be overridden using the preferred list. When using the preferred list, the user enters a priority for each bridge, resulting in the selection of the forwarding link.

Limit the wireless client's connections to reduce the number of hops required to get to the wired network. Use each radio's *preferred* base bridge list to define which access points the client bridge connects to.

8.2.5 Mesh Networking and the Access Point's Two Subnets

The access point has a second subnet on the LAN side of the system. This means wireless clients communicating through the same radio can reside on different subnets. The addition of this feature adds another layer of complexity to the access point's mesh networking functionality.

With a second access point LAN, the LAN's Ethernet port (and any of the 16 WLANs) can be assigned to one of two different subnets. From a layer 2 perspective, the system has two different bridge functionalities, each with its own STP. The WLAN assignment controls the subnet (LAN1 or 2) upon which a given connection resides. If WLAN2 is assigned to LAN1, and WLAN2 is used to establish a client bridge connection, then the mesh network connection resides on LAN1.

Therefore, (depending upon the WLAN-to-LAN mapping), the access point could have multiple mesh connections on either LAN1 or LAN2.

8.2.6 Normal Operation

Once the mesh network is defined, normal access point operations are still allowed. MUs are still allowed to associate with the access point as usual. The user can create WLANs, security polices and VLANs as with any other access point. DHCP services function normally and all layer 3 communications are allowed.

WNMP sends information about each mesh network so information can be displayed to the user from any access point on the system. WNMP messages are AP to AP information messages used to communicate system status.

8.2.7 Importing and Exporting Configurations to a Mesh Network

When using the access point's resident Configuration Import/Export functionality to migrate a configuration to other access points, mesh network configuration parameters get sent or saved to other access points. However, if using the Known AP Statistics screen's Send Cfg to APs functionality, *auto-select* and *preferred list* settings do not get imported.

8.2.8 Configuring Mesh Network Support

Configuring the access point for Mesh Bridging support entails:

- *Setting the LAN Configuration for Mesh Networking Support*
- *Configuring a WLAN for Mesh Networking Support*
- *Configuring the Access Point Radio for Mesh Support*

8.2.8.1 Setting the LAN Configuration for Mesh Networking Support

At least one of the two access point LANs needs to be enabled and have a mesh configuration defined to correctly function as a base or client bridge within a mesh network. This section describes the configuration activities required to define a mesh network's LAN configuration.

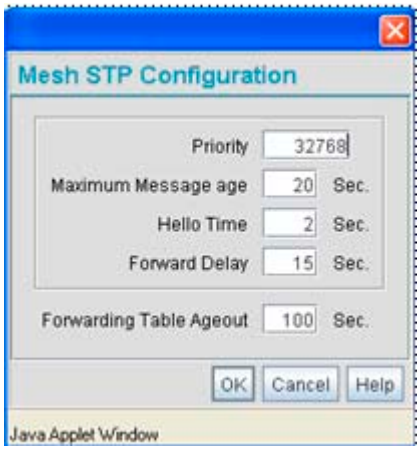
As the *Spanning Tree Protocol* (STP) mentions, each mesh network maintains hello, forward delay and max age timers. The base bridge defined as the root imposes these settings within the mesh network. The user does not necessarily have to change these settings, as the default settings will work. However, Motorola encourages the user to define an access point as a base bridge and root (using the base bridge priority settings within the Bridge STP Configuration screen). Members of the mesh network can be configured as client bridges or additional base bridges with a higher priority value.

To define a LAN's Mesh STP Configuration:

1. Select **Network Configuration -> LAN** from the AP-5131 menu tree.
2. Enable the LAN used to support the mesh network.

   Verify the enabled LAN is named appropriately in respect to its intended function in supporting the mesh network.
3. Select **Network Configuration -> LAN -> LAN1 or LAN2** from the AP-5131 menu tree.
4. Click the **Mesh STP Configuration** button on the bottom off the screen.

   Define the properties for the following parameters within the mesh network:



Priority	Set the **Priority** as low as possible for a to force other devices within the mesh network to defer to this client bridge as the bridge defining the mesh configuration (commonly referred to as the root). Motorola recommends assigning a Base Bridge AP with the lowest bridge priority so it becomes the root in the STP. If a root already exists, set the Bridge Priorities of new APs accordingly so the root of the STP doesn't get altered. Each access point starts with a default bridge priority of 32768.
Maximum Message age	The **Maximum Message age** timer is used with the Message Age timer. The Message Age timer is used to measure the age of the received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer
Hello Time	The **Hello Time** is the time between each bridge protocol data unit sent. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec. If you drop the hello time from 2 sec to 1 sec, you double the number of bridge protocol data units sent/received by each bridge. The 802.1d specification recommends the Hello Time be set to a value less than half of the Max Message age value.
Forward Delay	The **Forward Delay** is the time spent in the listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec. The 802.1d specification recommends the Forward Delay be set to a value greater than half the Max Message age timeout value.
Forwarding Table Ageout	The Forwarding Table Parameter value defines the length of time an entry will remain in the a bridge's forwarding table before being deleted due to lack of activity. If the entry replenishments a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table.

5. Click **OK** to return to either the LAN1 or LAN2 screen where updates to the Mesh STP Configuration can be saved by clicking the **Apply** button.
6. Click **Cancel** to discard the changes made to the Mesh STP Configuration and return to the LAN1 or LAN2 screen. Once the Mesh STP Configuration is defined, the access point's radio can be configured for base and/or client bridge support.

8.2.8.2 Configuring a WLAN for Mesh Networking Support

Each access point comprising a particular mesh network is required to be a member of the same WLAN. Therefore, each base bridge, client bridge or repeater within the mesh network must use the same WLAN in order to share the same ESSID, radio designation, security policy, MU ACL and Quality of Service policy. If intending to use the access point for mesh networking support, Motorola recommends configuring at least one WLAN (of the 16 WLANs available) specifically for mesh networking support.

To define the attributes of the WLAN shared by the members of the mesh network:

1. Select **Network Configuration -> Wireless** from the AP-5131 menu tree.

   The **Wireless Configuration** screen displays with those existing WLANs displayed within the table.

2. Select the **Create** button to configure a new WLAN specifically to support mesh networking.

   An existing WLAN can be modified (or used as is) for mesh networking support by selecting it from the list of available WLANs and clicking the **Edit** button.

3. Assign an **ESSID** and **Name** to the WLAN that each access point will share when using this WLAN within their mesh network.

   Motorola recommends assigning a unique name to a WLAN supporting a mesh network to differentiate it from WLANs defined for non mesh support. The name assigned to the WLAN is what is selected from the **Radio Configuration** screen for use within the mesh network.

NOTE: It is possible to have different ESSID and WLAN assignments within a single mesh network (one set between the Base Bridge and repeater and another between the repeater and Client Bridge). However, for ease of management and to not waste network bandwidth, Motorola recommends using the same ESSID across the entire mesh network.

4. Use the **Available On** checkboxes to specify the access point radio(s) used with the target WLAN within the mesh network.

   The Available On checkboxes are for making this WLAN available for base bridges or repeaters to connect to. The Available On checkbox should only be selected for a mesh WLAN if this target access point is to be configured as a base bridge or repeater on the radio. If the WLAN is to be defined for client bridge support only, the Available On checkbox should not be selected. Instead, it only needs to have the Enable Client Bridge Backhaul option selected.

5. Use the **Maximum MUs** field to define the number of MUs allowed to associate with this WLAN. This number should be defined based on the number of client bridge and repeaters within this mesh network. This value can be increased as the mesh network grows and devices are added.

   Only advanced users should define the number of devices allowed to associate with the WLAN, as setting the value too low could restrict devices from joining an expanding mesh network, and setting it too high could prohibit other WLANs from granting access to the all the devices needed.

6. Select the **Enable Client Bridge Backhaul** checkbox to make this WLAN available in the **Mesh Network Name** drop-down menu within the **Radio Configuration** screen. Only WLANs defined for mesh networking support should have this checkbox selected, in order to keep the list of WLANs available (within the Radio Configuration screen) restricted to just WLANs configured specifically with mesh attributes.

7. Refer to the **Security Policy** drop-down menu to select the security policy used within this WLAN and mesh network.

   A security policy for a mesh network should be configured carefully since the data protection requirements within a mesh network differ somewhat compared to a typical wireless LAN. **No Encryption** is a bad idea in a mesh network, since mesh networks are typically not guest networks, wherein public assess is more important than data protection. Motorola also discourages user-based authentication schemes such as Kerberos and 802.1x EAP, as these authentication schemes are not supported within a mesh network

   If none of the existing policies are suitable, select the **Create** button to the right of the **Security Policy** drop-down menu and configure a policy suitable for the mesh network.

8. ACL policies should be configured to allow or deny a range of MAC addresses from interoperating with the WLAN used with the mesh network. ACLs should be defined based on the client bridge and repeater (an access point defined as both a base and client bridge) association requirements within the mesh network.

NOTE: The **Kerberos User Name** and **Kerberos Password** fields can be ignored, as Kerberos is not supported as a viable authentication scheme within a mesh network.

9. Select the **Disallow MU to MU Communication** checkbox to restrict MUs from interacting with each other both within this WLAN, as well as other WLANs.

   Selecting this option could be a good idea, if restricting device “chatter” improves mesh network performance. If base bridges and client bridges are added at any given time to extent the coverage are

of a mesh network, the data going back and forth amongst just those radios could be compromised by network interference. Adding mesh device traffic could jeopardize network throughput. If however, MU to MU communication is central to the organization (for example, scanners sharing data entry information) then this checkbox should remain unselected.

10. Select the **Use Secure Beacon** checkbox to not transmit the ESSID amongst the access points and devices within the mesh network. If a hacker tries to find an ESSID via an MU, the access point's ESSID does not display since the ESSID is not in the beacon. Motorola recommends keeping the option enabled to reduce the likelihood of hacking into the WLAN.
11. Select the **Accept Broadcast ESSID** checkbox to associate an MU that has a blank ESSID (regardless of which ESSID the access point is currently using). Traffic within a mesh network probably consists of known devices, so you may want to leave the checkbox unselected and configure each MU with an ESSID. The default is selected. However, for WLANs used within a mesh network, Motorola recommends unselecting this option as it would prevent the AP from answering to blank ESSID probes from other mobile units.
12. If there are certain requirements for the types of data proliferating the mesh network, select an existing policy or configure a new QoS policy best suiting the requirements of the mesh network. To define a new QoS policy, select the **Create** button to the right of the Quality Of Service Policy drop-down menu.
13. Click **Apply** to save the changes made to the mesh network configured WLAN. An access point radio is now ready to be configured for use with this newly created mesh WLAN.

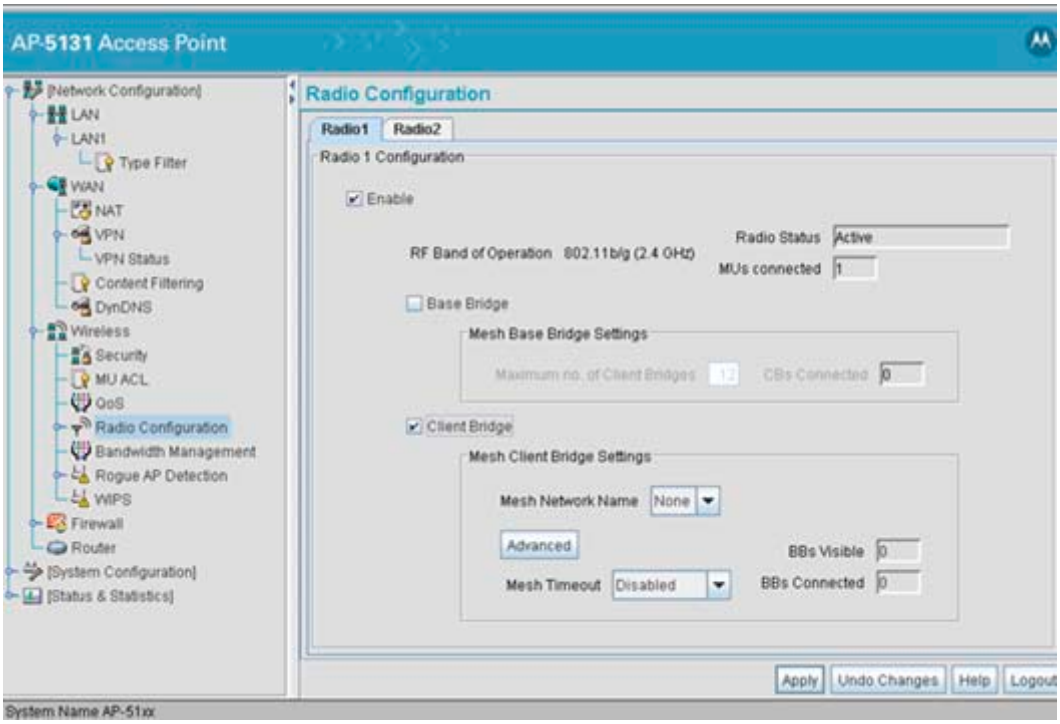
8.2.8.3 Configuring the Access Point Radio for Mesh Support

An access point radio intended for use within a mesh network requires configuration attributes unique from a radio intended for non-mesh support.This section describes how to configure an access point radio for mesh network support.

To configure the access point radio for mesh networking support:

NOTE: The dual-radio model access point affords users better optimization of the mesh network feature by allowing the access point to transmit to other access points (in base or client bridge mode) using one independent radio and transmit with its associated devices using the second independent radio. A single-radio access point has its channel utilization and throughput degraded in a mesh network, as the AP's single radio must process both mesh network traffic with other access points and MU traffic with its associated devices.

1. Select **Network Configuration** -> **Wireless** -> **Radio Configuration** from the AP-5131 menu tree.



2. Enable the radio(s) using the **Enable** checkbox(es) for both Radio 1 and Radio 2.

   Refer to **RF Band of Operation** parameter to ensure you are enabling the correct 802.11a or 802.11b/g radio. After the settings are applied within this Radio Configuration screen, the **Radio Status** and **MUs connected** values update. If this is an existing radio within a mesh network, these values update in real-time.

CAUTION: If a radio is disabled, be careful not to accidentally configure a new WLAN, expecting the radio to be operating when you have forgotten it was disabled.

3. Select the **Base Bridge** checkbox to allow the access point radio to accept client bridge connections from other access points in client bridge mode. The base bridge is the acceptor of mesh network data from those client bridges within the mesh network and never the initiator.

CAUTION: A problem could arise if a Base Bridge's Indoor channel is not available on an Outdoor Client Bridge's list of available channels. As long as an Outdoor Client Bridge has the Indoor Base Bridge channel in its available list of channels, it can associate to the Base Bridge.

4. If the Base Bridge checkbox has been selected, use the **Max# Client Bridges** parameter to define the client bridge load on a particular base bridge.

   The maximum number of client bridge connections per access point radio is 12, with 24 representing the maximum for dual-radio models.

CAUTION: An access point in Base Bridge mode logs out whenever a Client Bridge associates to the Base Bridge over the LAN connection. This problem is not experienced over the access point's WAN connection. If this situation is experienced, log-in to the access point again.

   Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of client bridge connections for this specific radio displays within the **CBs Connected** field. If this is an existing radio within a mesh network, this value updates in real-time.

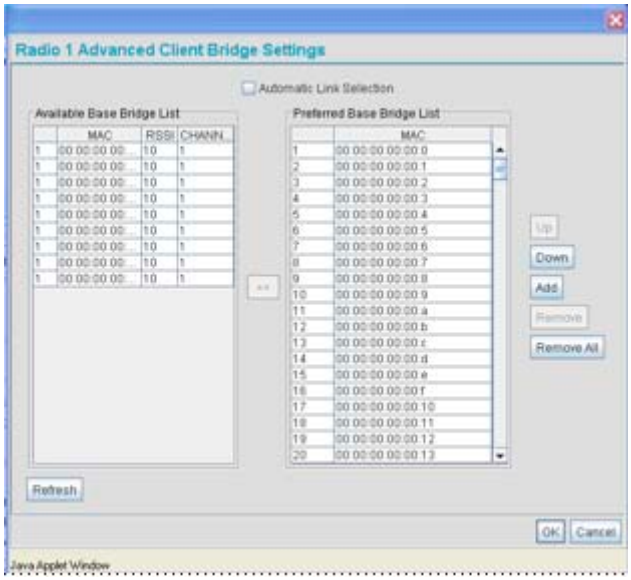
5. Select the **Client Bridge** checkbox to enable the access point radio to initiate client bridge connections with other mesh network supported access points radios on the same WLAN.

   If the Client Bridge checkbox has been selected, use the **Mesh Network Name** drop-down menu to select the WLAN (ESS) the client bridge uses to establish a wireless link. The default setting, is (WLAN1). Motorola recommends creating (and naming) a WLAN specifically for mesh networking support to differentiate the Mesh supported WLAN from non-Mesh supported WLANs. For more information, see *Configuring a WLAN for Mesh Networking Support on page 8-12*.

   Once the settings within the Radio Configuration screen are applied (for an initial deployment), the current number of base bridges visible to the radio displays within the **BBs Visible** field, and the number of base bridges currently connected to the radio displays within the **BBs Connected** field. If this is an existing radio within a mesh network, these values update in real-time.

NOTE: Ensure you have verified the radio configuration for both Radio 1 and Radio 2 before saving the existing settings and exiting the Radio Configuration screen.

6. Click the **Advanced** button to define a prioritized list of access points to define mesh connection links.



7. Select the **Automatic Link Selection** checkbox to allow the access point to select the links used by the client bridge to populate the mesh network. Selecting this checkbox prohibits the user from selecting the

order base bridges are added to the mesh network when one of the three associated base bridges becomes unavailable.

NOTE: Auto link selection is based on the RSSI and load. The client bridge will select the best available link when the **Automatic Link Selection** checkbox is selected. Motorola recommends you do not disable this option, as (when enabled) the access point will select the best base bridge for connection.

8. Refer to the **Available Base Bridge List** to view devices located by the access point using the WLAN selected from the Radio Configuration screen. Refer the following for information on located base bridges:

MAC	The MAC field displays the factory set hard-coded MAC address that serves as a device identifier.
RSSI	The *Relative Signal Strength Indicator* (RSSI) displays the located device's signal strength with the associated access point in client bridge mode. Use this information as criteria on whether to move a particular device from the available list to the preferred list.
CHANN	The CHANN displays the name of the channel that both the access point and base bridge use. A client bridge can only connect to access points (Base Bridges) on the same channel. If the user selects multiple base bridges on different channels, the access point will only be able to connect to those bridges on the same channel and the others will not be able to join this particular mesh network.

9. Click **Refresh** at any time to update the list of available Base Bridge devices available to the access point.
10. Use the **>>** button to move a selected base bridge MAC address from Available Base Bridge List
11. Refer to the **Preferred Base Bridge List** for a prioritized list of base bridges the mesh network's client bridge uses to extend the mesh network's coverage area and potentially provide redundant links. If a device does not appear on the Available Base Bridge List, there is no way it can be moved to Preferred Base Bridge List as the device has not yet been *seen*. However, if you know the MAC Address corresponding to that Base Bridge, you can add that to the Preferred List using the add button.
12. Highlight a MAC address from the Preferred Base Bridge List and click the **Up** button to assign that device's MAC address a higher priority and a greater likelihood of joining the mesh network if an association with another device is lost.
13. If a MAC address is not desirable as others but still worthy of being on the preferred list, select it, and click the **Down** button to decrease its likelihood of being selected as a member of the mesh network.

    If a device MAC address is on the Preferred Base Bridge List and constitutes a threat as a potential member of the mesh network (poor RSSI etc.), select it and click the **Remove** button to exclude it from the preferred list.

    If all of the members of the Preferred Base Bridge List constitute a risk as a member of the mesh network, click the **Remove All** button. This is not recommended unless the preferred list can be re-populated with more desirable device MAC addresses from the Available Base Bridge List.
14. Click **Ok** to return to the Radio Configuration screen. Within the Radio Configuration screen, click **Apply** to save any changes made within the Advanced Client Bridge Settings screen.
15. Click **Cancel** to undo any changes made within the Advanced Client Bridge Settings screen. This reverts all settings for the screen to the last saved configuration.

16. If using a dual-radio model access point, refer to the **Mesh Timeout** drop-down menu (from within the Radio Configuration screen) to define whether one of the access point's radio's beacons on an existing WLAN or if a client bridge radio uses an uplink connection. The Mesh Timeout value is not available on a single-radio access point, since the radio would have to stop beaconing and go into scan mode to determine if a base bridge uplink is lost. The following drop-down menu options are available:

Disabled	When disabled, both radios are up at boot time and beaconing. If one radio (radio 1) does not have a mesh connection, the other radio (radio 2) is not affected. Radio 2 continues to beacon and associate MUs, but MU's can only communicate amongst themselves using the access point. Disabled is the default value.
Upload Detected	When Uplink Detect is selected, the access point only boots up the radio configured as a client bridge. The access point boots up the second radio as soon as the first mesh connection is established. However, if the client bridge radio loses its uplink connection, the second radio shuts down immediately.
Enabled	If the mesh connection is down on one radio (radio 1), the other radio (radio 2) is brought down and stops beaconing after the timeout period (45 seconds). This allows the client bridge (radio 1) to roam without dropping the MU's associated to radio 2. The disadvantage is that radio 2 may beacon for the 45 second timeout period and have to drop associated MU's because radio 1 could not establish its uplink.

NOTE: The Mesh Time Out variable overrides the *Ethernet Port Time Out* (EPTO) setting on the LAN page when the access point is in bridge mode. As long as the mesh is down, the access point acts in accordance to the Mesh Time Out setting regardless of the state of the Ethernet. However, if the Ethernet goes down and the mesh link is still up, the EPTO takes effect.

17. Click **Apply** to save any changes to the Radio Configuration screen. Navigating away from the screen without clicking Apply results in all changes to the screens being lost.

CAUTION: When defining a Mesh configuration and changes are saved, the mesh network temporarily goes down. The mesh network is unavailable because the access point radio goes down when applying the changes. This can be problematic for users making changes within a deployed mesh network. If updating the mesh network using a LAN connection, the access point applet loses connection and the connection must be re-instated. If updating the mesh network using a WAN connection, the applet does not lose connection, but the mesh network is unavailable until the changes have been applied.

18. Click **Undo Changes** (if necessary) to undo any changes made. Undo Changes reverts the settings displayed on the Radio Configuration screen to the last saved configuration.
19. Click **Logout** to securely exit the access point applet. A prompt displays confirming the logout before the applet is closed.

    Once the target radio has been enabled from the **Radio Configuration** screen, configure the radio's properties by selecting it from the AP-5131 menu tree.

8.2.9 Mesh Deployment Scenarios

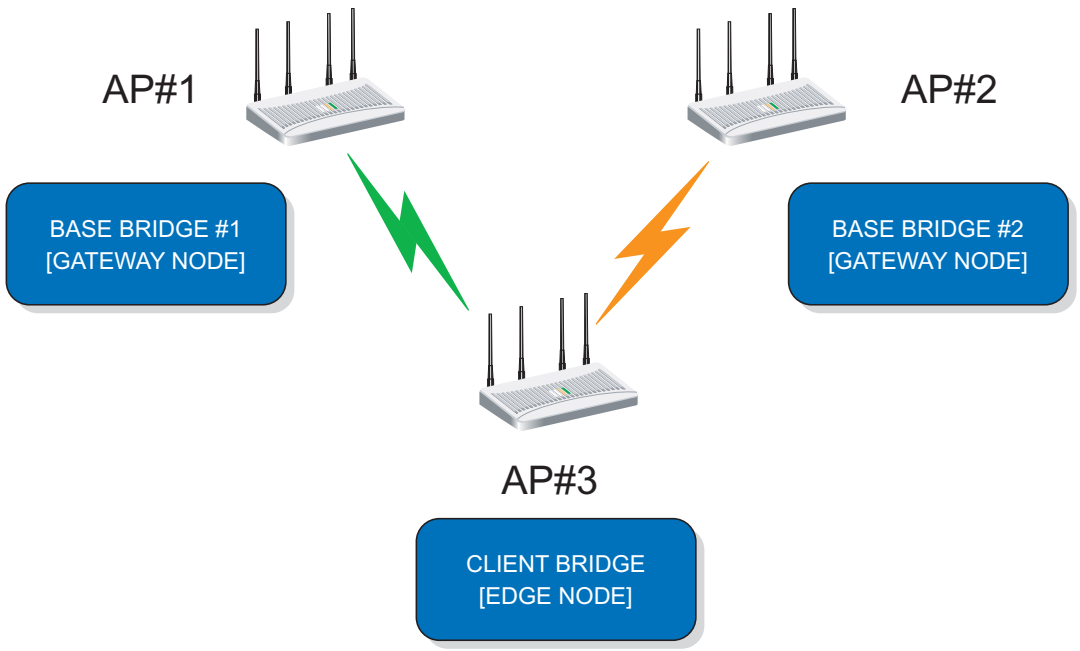
This section provides instructions on how to quickly setup and demonstrate mesh functionality using three access points. Two following two deployment scenarios will be addressed:

- *Scenario 1* - Two base bridges (redundant) and one client bridge

- *Scenario 2* - A two hop mesh network with a base bridge, repeater (combined base bridge and client bridge mode) and a client bridge.

8.2.9.1 Scenario 1 - Two base bridges (redundant) and one client bridge

A conceptual illustration of scenario one is as follows:



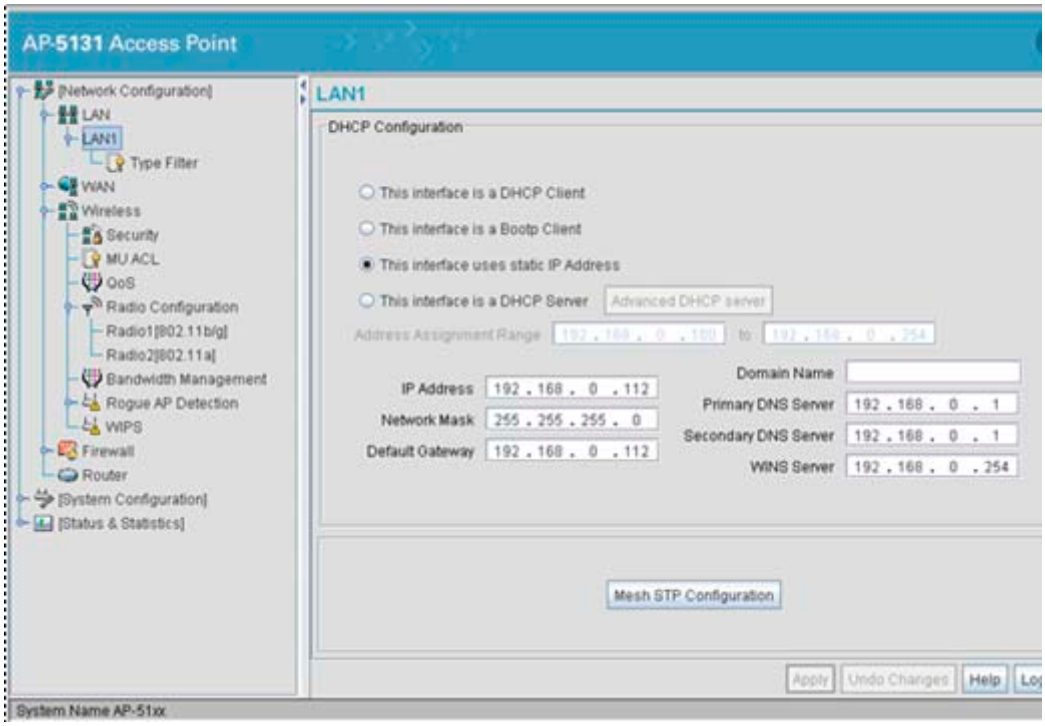
In scenario 1, the following three access point configurations will be deployed within the mesh network:

- *AP#1* - An active base bridge
- *AP#2* - A redundant base bridge
- *AP#3* - A client bridge connecting to both AP#1 and AP#2 simultaneously.

AP#1 and AP#2 will be configured somewhat the same. However there are some important (yet subtle) differences. Therefore, the configuration of each access point will be described separately.

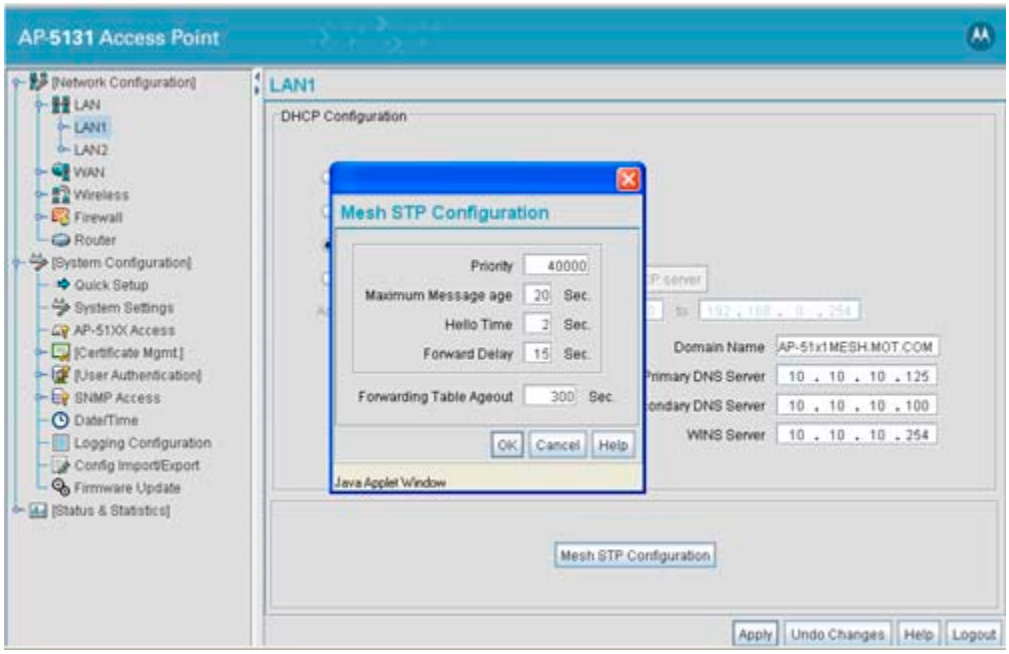
Configuring AP #1

1. Provide a known IP address for the LAN1 interface.

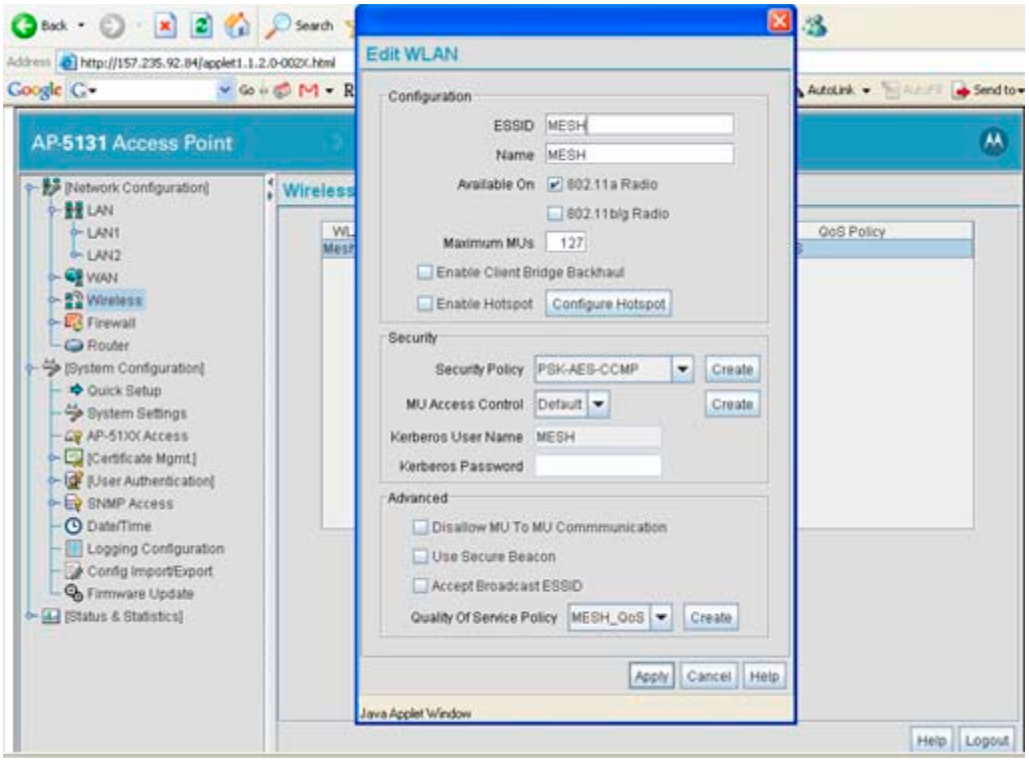


NOTE: Enable the LAN1 Interface of AP#1 as a DHCP Server if you intend to associate MUs and require them to obtain an IP address via DHCP.

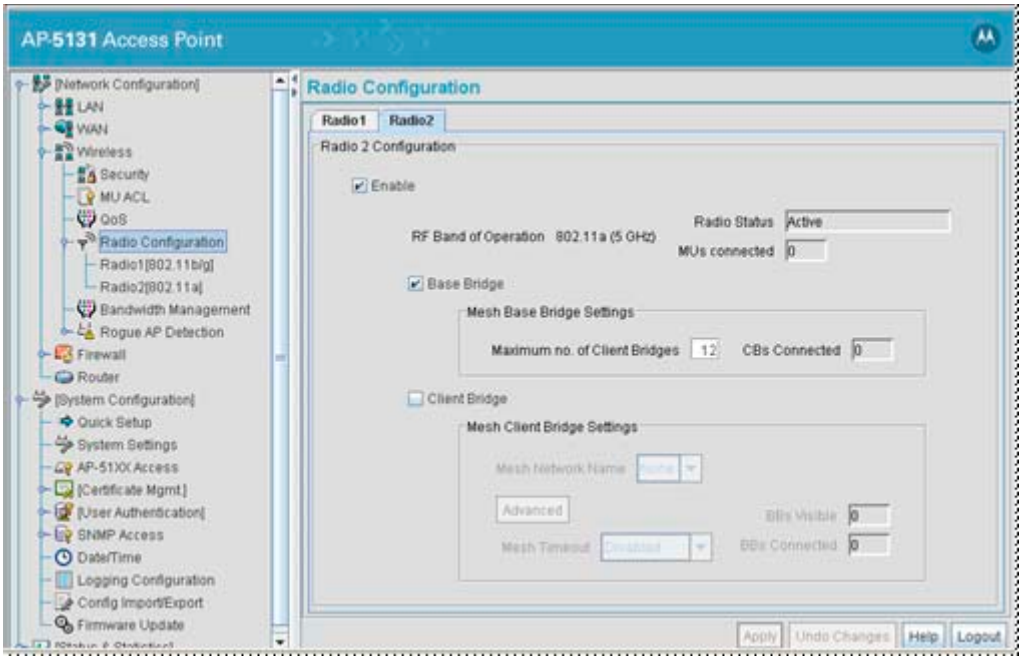
2. Assign a Mesh STP Priority of 40000 to LAN1 Interface.



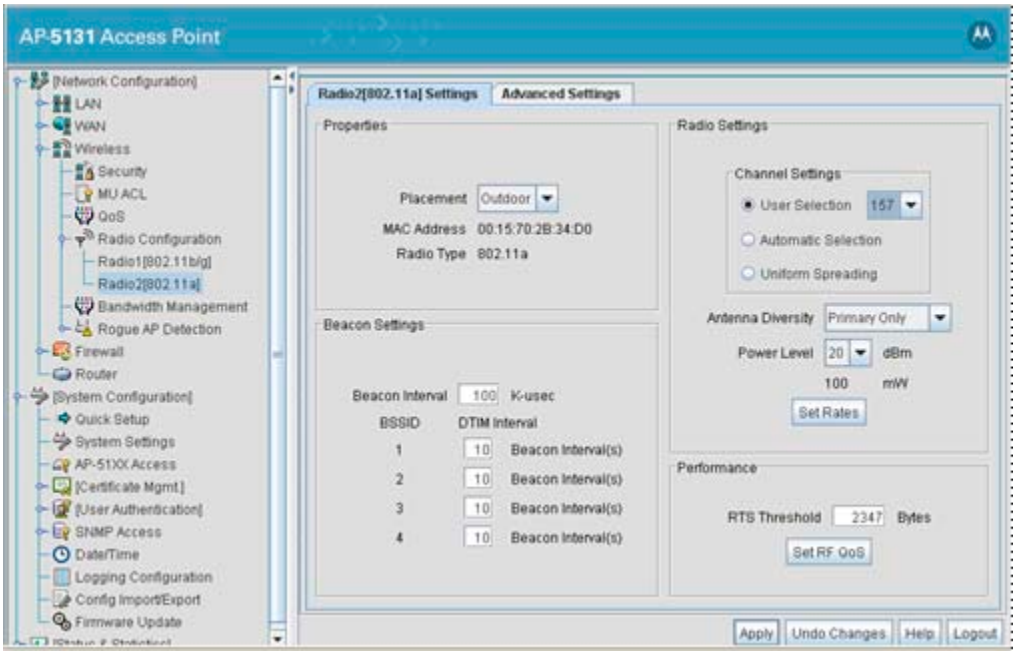
3. Define a mesh supported WLAN.



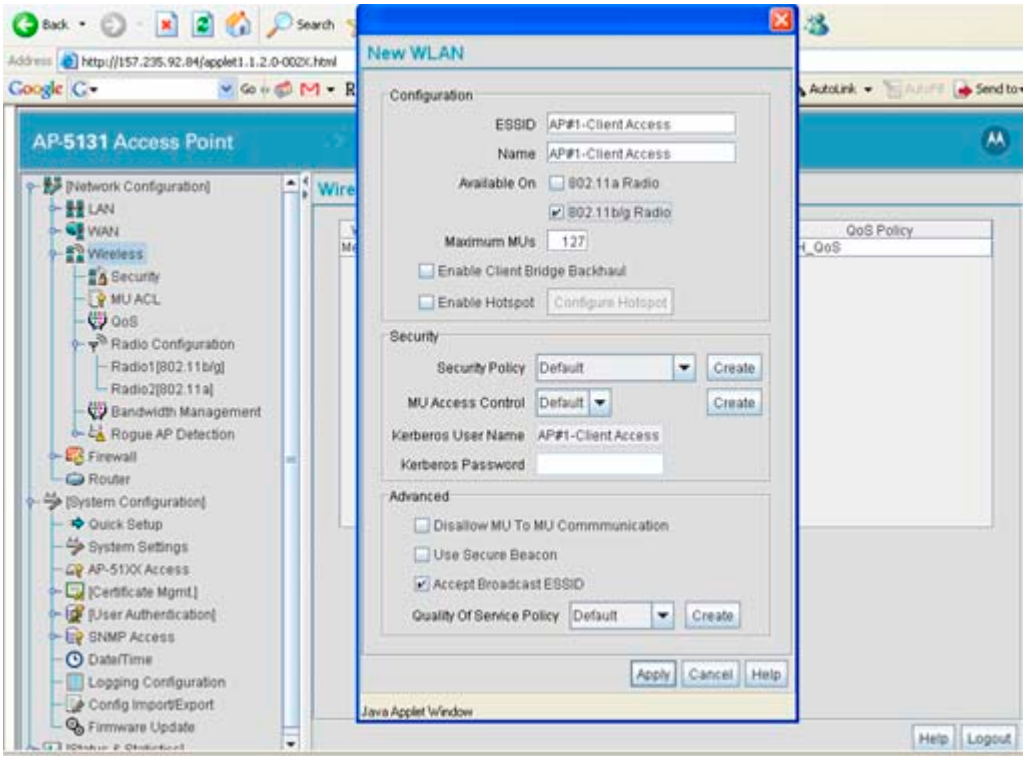
4. Enable base bridge functionality on the 802.11a radio (Radio 2).



5. Define a channel of operation for the 802.11a radio.



6. If needed, create another WLAN mapped to the 802.11bg radio if 802.11bg support is required for MUs on that 802.11 band.



Configuring AP #2

AP#2 can be configured the same as AP#1 with the following exceptions:

- Assign an IP Address to the LAN1 Interface different than that of AP#1

- Assign a higher Mesh STP Priority 50000 to the AP#2 LAN1 Interface.

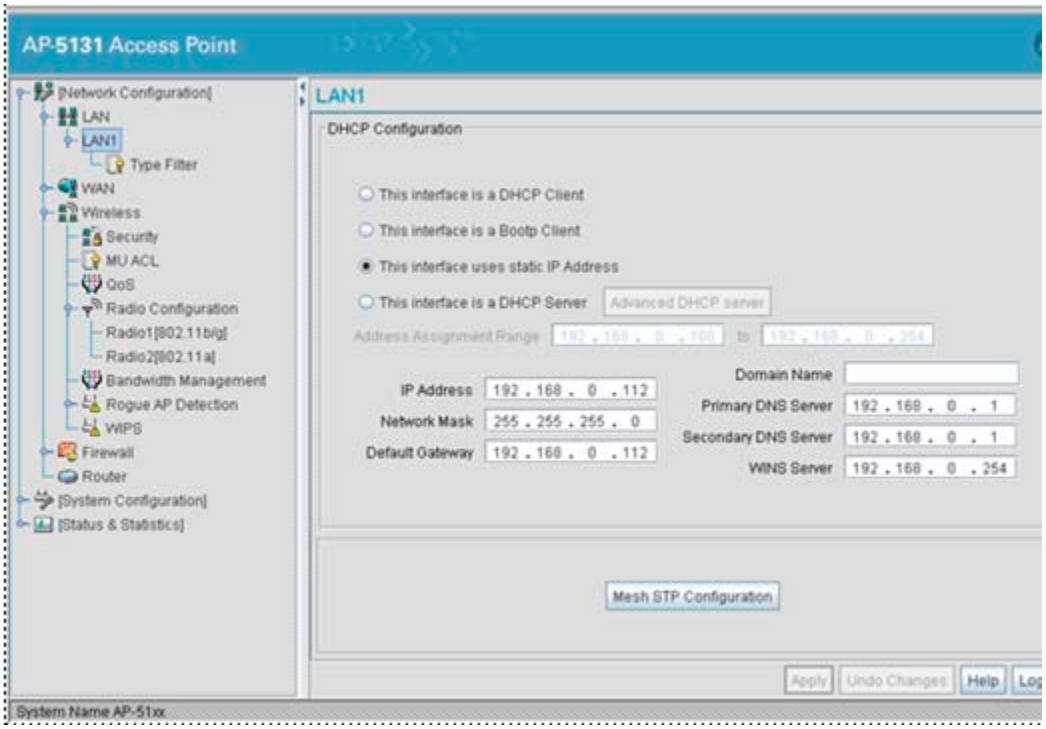
NOTE: In a typical deployment, each base bridge can be configured for a Mesh STP Priority of 50000. In this example, different values are used to force AP#1 to be the forwarding link since it's a small mesh network (of only three APs) with AP within close proximity of one another.

NOTE: Ensure AP#1 and AP#2 use the same channel for each 802.11a radio, or the APs will not be able to "hear" each other over different channels.

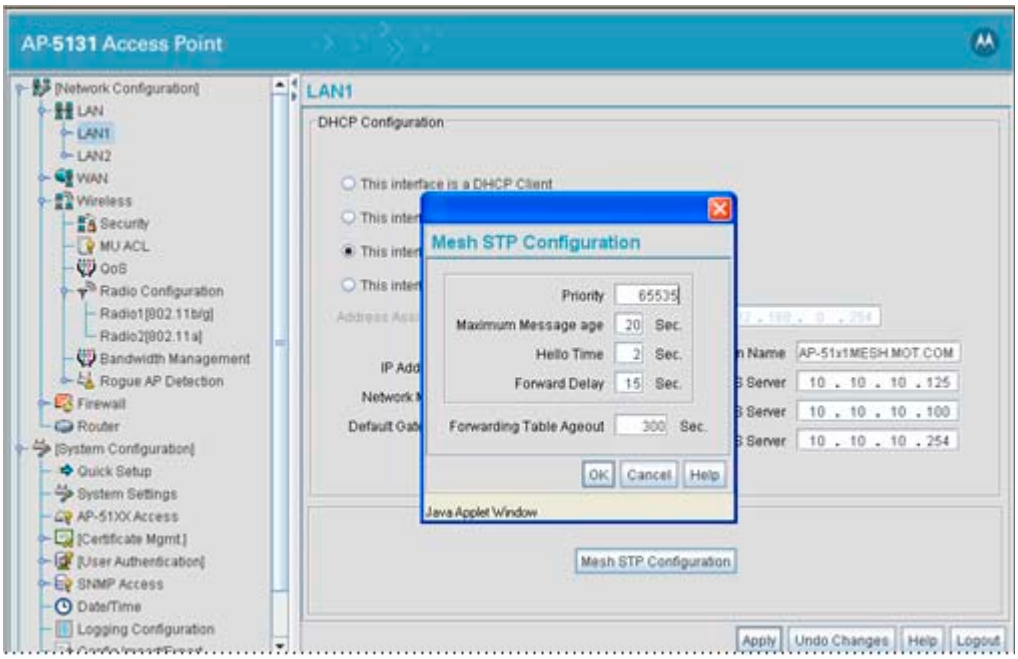
Configuring AP #3

To define the configuration for AP#3 (a client bridge connecting to both AP#1 and AP#2 simultaneously):

1. Provide a known IP address for the LAN1 interface.

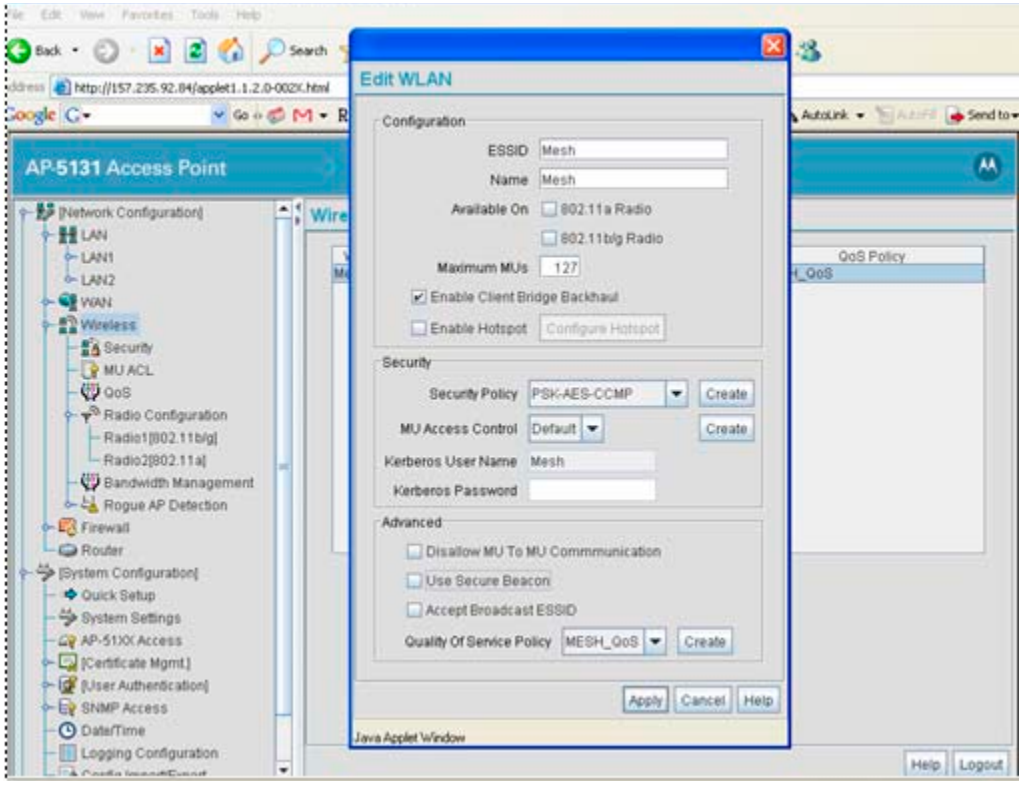


2. Assign the maximum value (65535) for the Mesh STP Priority.



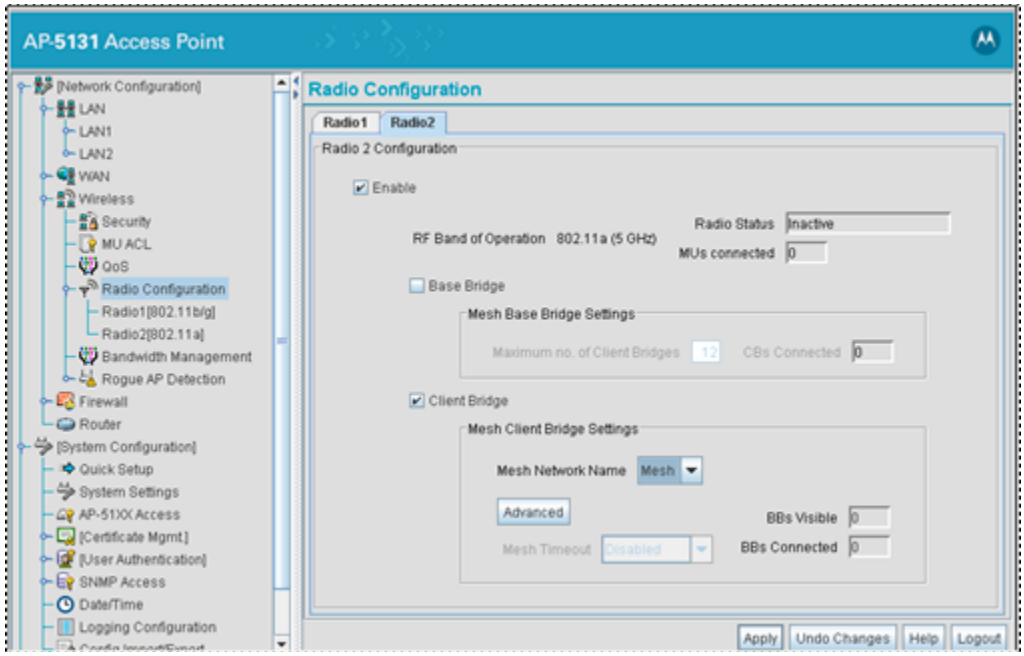
3. Create a mesh supported WLAN with the **Enable Client Bridge Backhaul** option selected.

NOTE: This WLAN should not be mapped to any radio. Therefore, leave both of the "Available On" radio options unselected.



4. Select the Client Bridge checkbox to enable client bridge functionality on the 802.11a radio. Use the Mesh Network Name drop-down menu to select the name of the WLAN created in step 3.

NOTE: You don't need to configure channel settings on the client bridge (AP#3). It automatically finds the base bridges (AP#1 and AP#2) and uses the channel assigned to them.



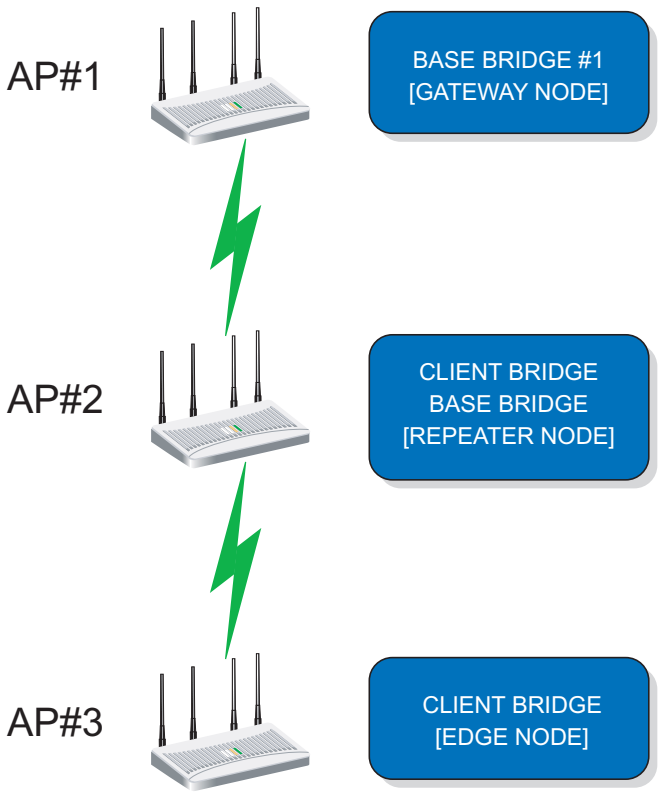
5. If needed, create another WLAN mapped to the 802.11bg radio if 802.11bg support is required for MUs on that 802.11 band.

Verifying Mesh Functionality

You now have a three AP mesh network ready to demonstrate. Associate a single MU on each AP WLAN configured for 802.11bg radio support. Once completed, pass traffic among the three APs comprising the mesh network.

8.2.9.2 Scenario 2 - Two Hop Mesh Network with a Base Bridge Repeater and a Client Bridge

A conceptual illustration of scenario two is as follows:



By default, the mesh algorithm runs an automatic link selection algorithm to determine the best possible active and redundant links. If member APs are not far apart (in physical distance), the algorithm intelligently chooses a single hop link to forward data. To force APs to use multiple hops for demonstrations, use manual links.

In scenario 2, the following three AP configurations comprise the mesh network:

- *AP#1* is a base bridge
- *AP#2* is a repeater (client bridge/base bridge combination)
- *AP#3* is a client bridge

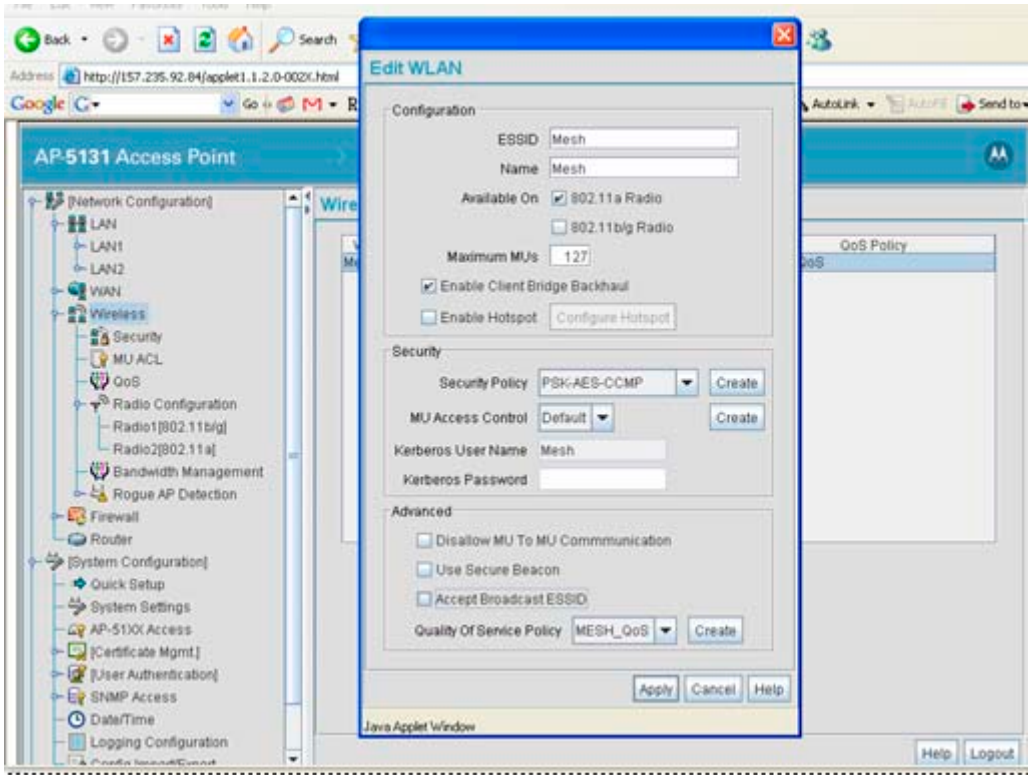
Configuring AP #1

The setup of AP#1 within this usage scenario is exactly the same as the AP#1 configuration within *Scenario 1 - Two base bridges (redundant) and one client bridge* for step by step instructions for configuring AP#1, see *Configuring AP #1 on page 8-19*. Once completed, return to *Configuring AP #2 on page 8-26* within this section.

Configuring AP #2

AP#2 requires the following modifications from AP#2 in the previous scenario to function in base bridge/client bridge repeater mode.

1. Enable client bridge backhaul on the mesh supported WLAN.



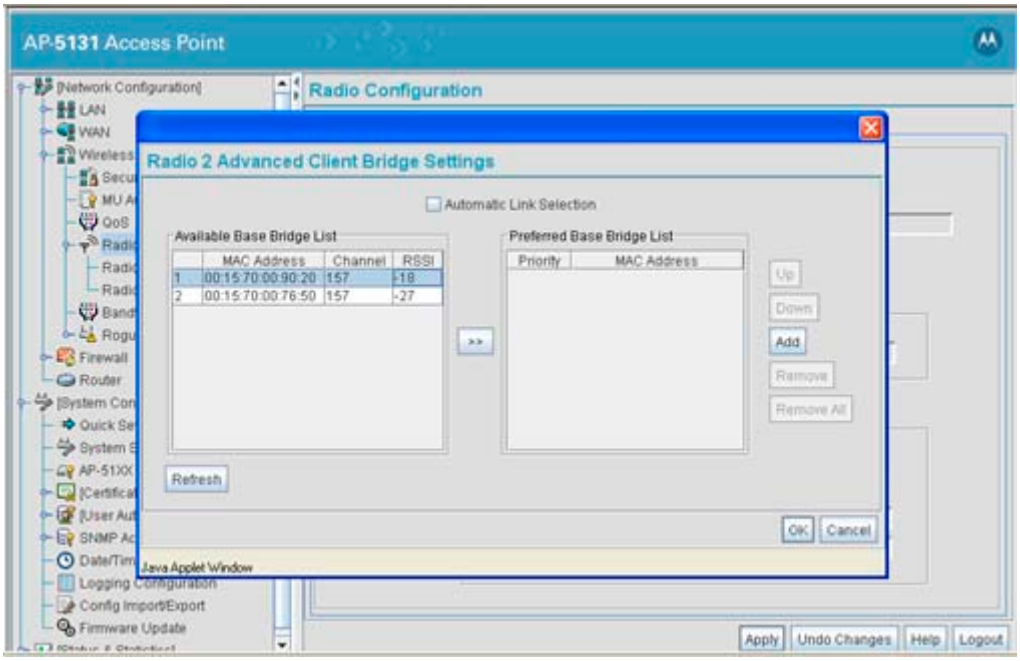
2. Enable client and base bridge functionality on the 802.11a radio.

Configuring AP #3

To define AP #3's configuration:

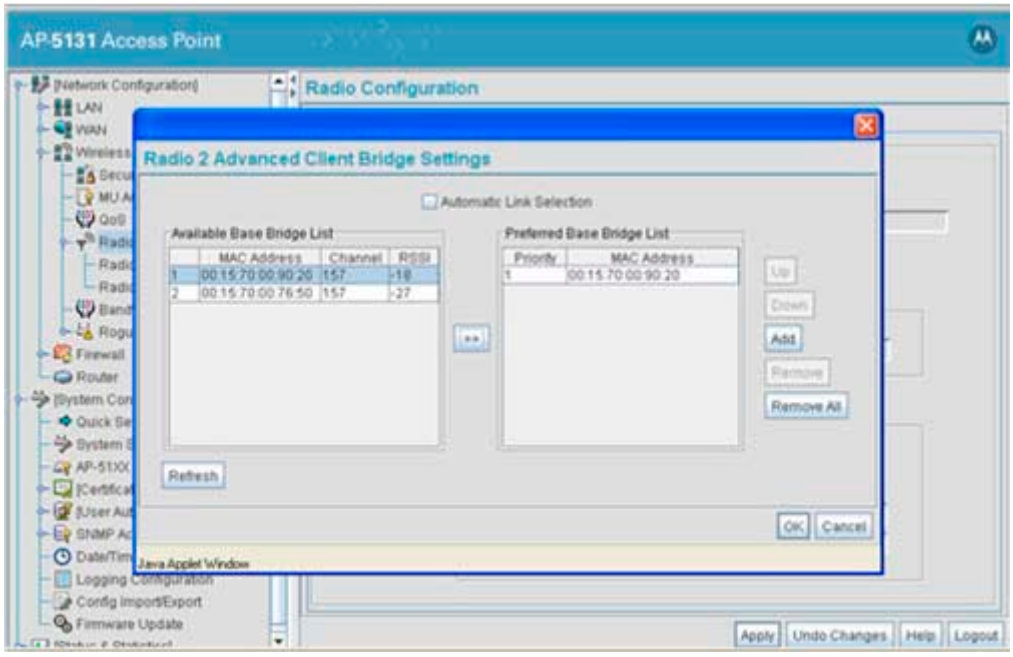
1. The only change needed on AP#3 (with respect to the configuration used in scenario #1), is to disable the **Auto Link Selection** option.

   Click the **Advanced** button within the **Mesh Client Bridge Settings** field.

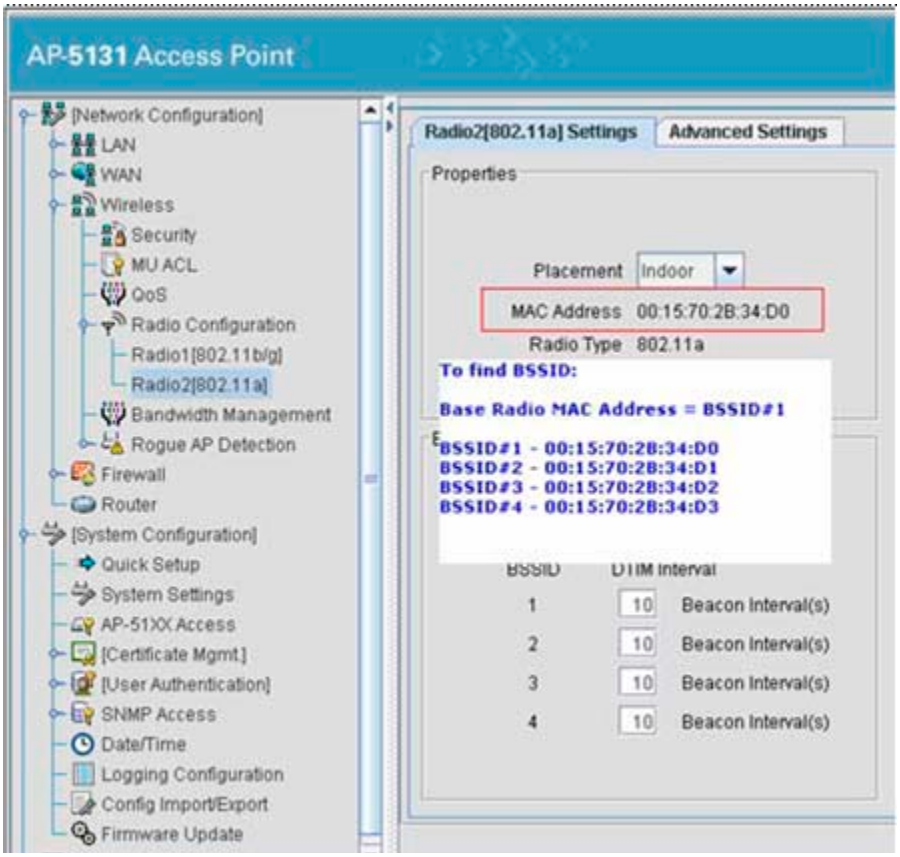


2. Add the 802.11a Radio MAC Address.

   In scenario #2, the mesh WLAN is mapped to BSS1 on the 802.11a radio if each AP. The Radio MAC Address (the BSSID#1 MAC Address) is used for the AP#2 Preferred Base Bridge List. Ensure both the AP#1 and AP#2 Radio MAC Addresses are in the Available Base Bridge List. Add the AP#2 MAC Address into the Preferred Base Bridge List.



3. Determine the Radio MAC Address and BSSID MAC Addresses.



Verifying Mesh Network Functionality for Scenario #2

You now have a three AP demo multi-hop mesh network ready to demonstrate. Associate an MU on the WLANs configured on the 802.11bg radio for each AP and pass traffic among the members of the mesh network.

8.3 Integrating a WS2000 Supported WLAN

A WS2000 wireless switch is a powerful all-in-one solution that simplifies and reduces the costs of managing wired and wireless (802.11a/b/g) networks in Enterprise branch offices. A WS2000 is designed for the small-medium Enterprise markets requiring an integrated, secure, remotely manageable wired and wireless networking solution at a low cost. The WS2000's integrated router, gateway, firewall and *Power-over-Ethernet* (PoE) eliminate the complexity of managing multiple pieces of equipment. WMM support enables a WS2000 to provide peak performance for even the most demanding applications, including voice and video. The ability to easily and cost-effectively scale to meet growing needs, as well as upgrade to support new security, radio and other standards provides the assurance that a WS2000 will meet your needs today and tomorrow.

A WS2000 is optimal for small to medium sized sites (1-4 cells). It provides the same centralized packet switching architecture as a WS5100 model switch. The Ws2000 supports integrated PoE and gateway functionality, mesh, mesh trunking and integrated wired networking capability. A WS2000 supports

- The same port adoption strategy as a WS5100's layer 2/3 port adoption
- 802.11b
- 802.11a

- 802.11a/g
- CF memory for storing AirBeam packages
- Software management of MUs
- External power supply
- Rack, wall and desk mount options
- Support for 32 SSIDs. This means 8 SSIDs are supported for an AP300's 802.11b/g radio and 8 SSIDs for the AP300's 802.11a radio

For more information on the WS2000, see:

- *WS2000 Security*
- *WS2000 Management*
- *Low Total Cost of Ownership*
- *Key WS2000 Features*
- *WS20000 Mesh Integration Example*

8.3.1 WS2000 Security

A W2000 protects your network and data with end-to-end Enterprise-class security with support for WPA2, integrated AAA (authentication, authorization and accounting) server for authenticating users, rogue access AP detection and a stateful packet inspection firewall. Your WS2000 supported network resources are safe, as only authorized users are granted access to the network. The WS2000 supports:

- VPN client technology for site-to-site communication
- An integrated IPSec engine with complete configuration and management support
- IKE engine
- DES, 3DES, AES encryption
- NAT Traversal support
- Support for 20 VPN tunnels

8.3.2 WS2000 Management

A WS2000 provides administrative simplicity and flexibility eliminating the need and cost for site IT personnel to manage a wireless network. You can easily manage a wired and wireless network using the WS2000's intuitive web-based interface to centrally manage access ports. For larger WS2000 deployments, secure remote management capabilities (with SSH and SNMP v3 support) and auto deployment capabilities (with DHCP options) enable staff to easily control and manage devices anywhere in the world.

Implementing a WS2000 is fast and easy, as the plug-and-play WS2000 automatically detects and configures access ports with the best channel. Tight integration with the wired network simplifies the extension of wired virtual LANs (VLANs), improving network performance as well as providing added protection against unauthorized access.

8.3.2.1 WS2000 Hotspot Deployments

A WS2000 is uniquely suited for hotspots, enabling, hotels, airports, lounges and restaurants to provide patrons convenient access to the Internet, email and corporate applications. Support for authentication and

Radius accounting enables organizations and service providers to offer secure wireless public access, either as a complimentary service or as an additional revenue stream.

8.3.3 Low Total Cost of Ownership

A WS2000 reduces the complexities and costs associated with deploying, managing, securing, upgrading and scaling your network. Motorola's Enterprise Mobility Services provide the comprehensive support and technical expertise you need to design, deploy and maintain a highly successful mobility solution.

The WS2000 is an integrated wired and Wi-Fi wireless networking solution. Built on the same centralized packet switching architecture as Motorola's WS5100 wireless switch, the WS2000 offers enterprise class security (802.11i/WPA2, site-to-site IPSec VPN), public/private network segmentation and 802.11a/b/g standards support. The elegant all-in-one design of the WS2000 supports multiple wireless LAN protocols (Wi-Fi® IEEE 802.11b, 802.11a, 802.11g), integrated Ethernet switching (6 LAN ports), routing (RIP, static routes), integrated gateway and PoE. The WS2000 includes an integrated stateful packet inspection firewall, a DHCP server (on multiple subnets) and WAN connectivity for flexible low cost installation.

WS2000 provides end-to-end layered security and supports a comprehensive suite of security mechanisms-including access-control, IPSec VPN (site-to-site), integrated AAA/Radius server (with support for PEAP and EAP-TTLS termination) an 802.1X based authentication, and strong encryption.

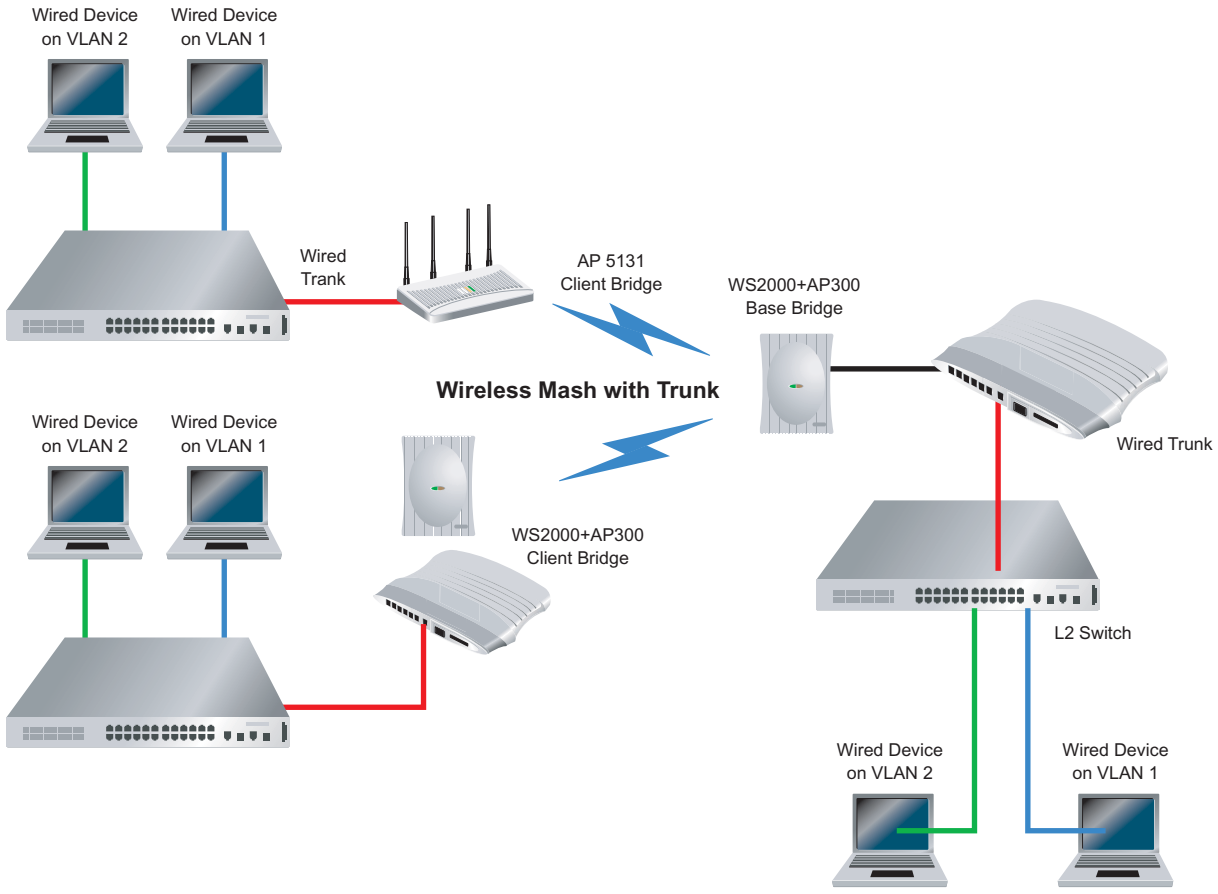
8.3.4 Key WS2000 Features

A WS2000 supports the following key features differentiating it from its competition:

- Wireless bridging with an AP-5131, AP-5181 and AP300
- Rogue AP containment
- Self healing
- WMM U-APSd
- Smart scan support
- Dual boot configuration
- Enhanced IDS and hotspot support
- Vendor specific attributes
- Bandwidth throttling on the WLAN

8.3.5 WS20000 Mesh Integration Example

With its integrated on-board Radius server, DHCP server and QoS, a WS2000 is ideally suited for the SOHO space. In the diagram below, you can see how to extend your outdoor or remote office across the street using the mesh support provided by a WS2000 (the WS2000 supports mesh and trunking over mesh).



8.4 Integrating a RFS7000 Supported WLAN

An RFS7000 can support Motorola and third-party vendor services, providing significant value to large businesses requiring a wireless LAN for their Enterprise mobility needs.

"As Wi-Fi networks become critical to business operations, we continue to rapidly enable more innovative ways to utilize the networks with easy to deploy add-on Enterprise mobility services," said Sujai Hajela, vice president and general manager of Enterprise WLAN, Motorola Enterprise Mobility business. "With the RFS7000 RF Switch, large businesses in carpeted offices, health care, warehousing and distribution, manufacturing, education, retail and government can deploy location services to track high-value asset and resources to increase utilization and safety."

The RFS7000 supports the real-time tracking of Wi-Fi devices and active tags to help simplify asset locationing. Businesses have the ability to locate employees for safety or track high-value and mission-critical assets to increase their utilization. In a health care setting, locationing services can be used to track life-saving crash carts, transfusion pumps, defibrillators, portable X-ray and dialysis machines. Locationing can also be used to find and track inventory for customers, providing better and faster service.

"We needed a solution for pin-pointing the location of cars in a parking lot in real-time," said Joseph Owusu, partner, Mieloo & Alexander. "We selected Motorola's Wi-Fi network infrastructure for its ability to integrate third-party ultra wideband (UWB) sensors that will work both indoors and outdoors."

Motorola's RF Management Suite (RFMS) is a set of tools to help Enterprises easily and centrally plan, deploy and manage their RF infrastructure and environment. RFMS simplifies a business' RF environment. The

ability to locate mobile and rogue devices greatly enhances the value of the management suite to Enterprises. Motorola's Wireless IPS detects and locates rogue devices, protecting the network against denial-of-service attacks as well as providing compliance reporting and advanced forensics. Motorola's comprehensive sensor-based Wireless IPS monitors, detects, protects and prevents network intrusions. The RFS7000 optimizes these security features to deliver a mobile client-based intrusion detection system that can disable difficult to detect rogue clients to ensure maximum up-time and peak network performance.

The RFS7000 is the industry's first RF wireless switch that bridges the gap between Wi-Fi and RFID, future RF technologies and indoor and outdoor wireless networks. The Enterprise-class RFS7000 is 802.11n-ready, and capable of supporting 256 device radios. The RFS7000 supports a new switch clustering concept, providing redundancy and high-performance scalability for up to 3,000 access points.

An RFS7000 deployment makes WLANs *smarter*. By smarter, we mean:

- *Secure and scalable*
- *Manageable*
- *Available*
- *Reliable*
- *Affordable with a low total cost of ownership*

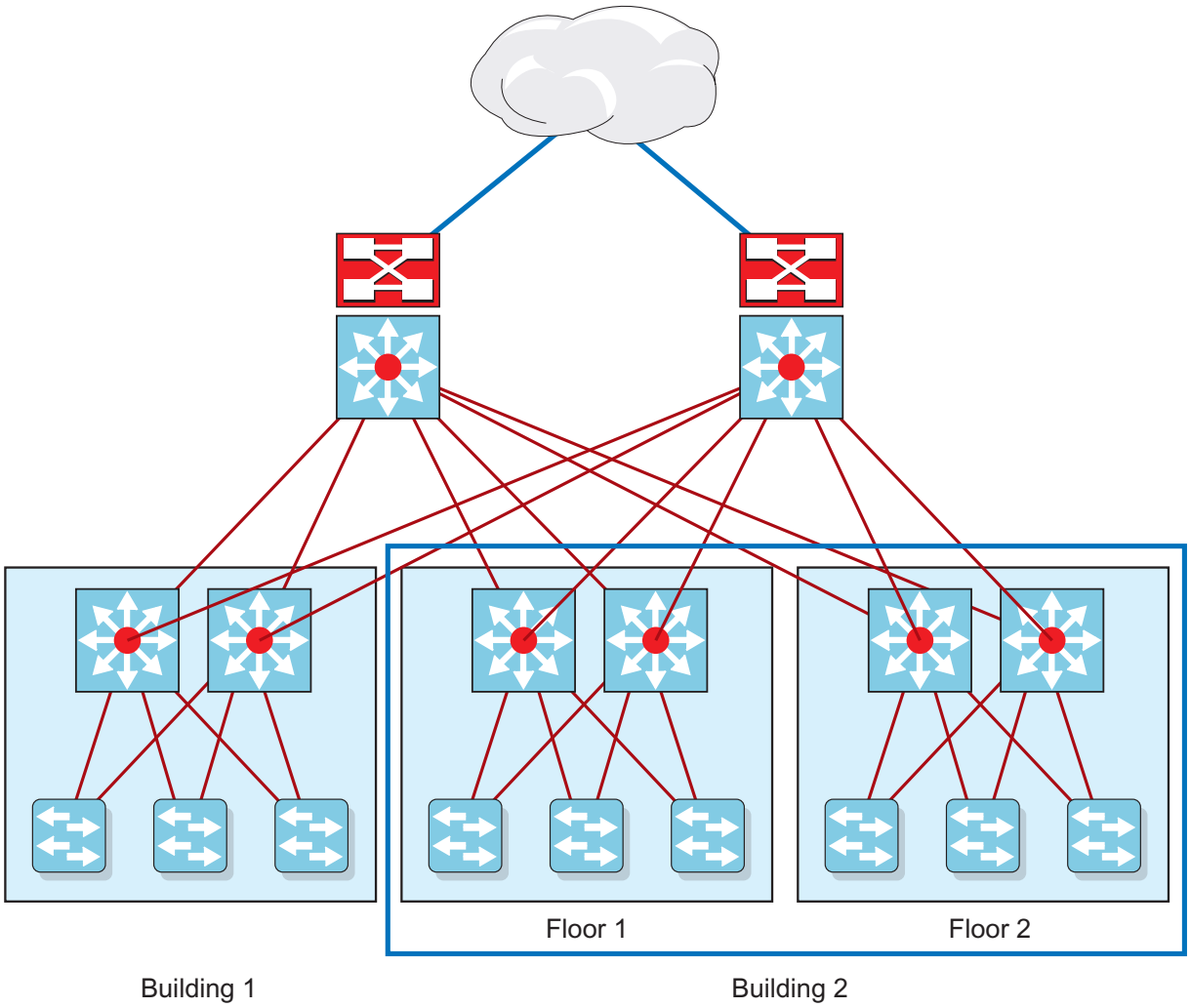
For more information on deploying an RFS7000, see:

- *Creating a Redundant WLAN with an RFS7000*
- *Redundancy Examples*

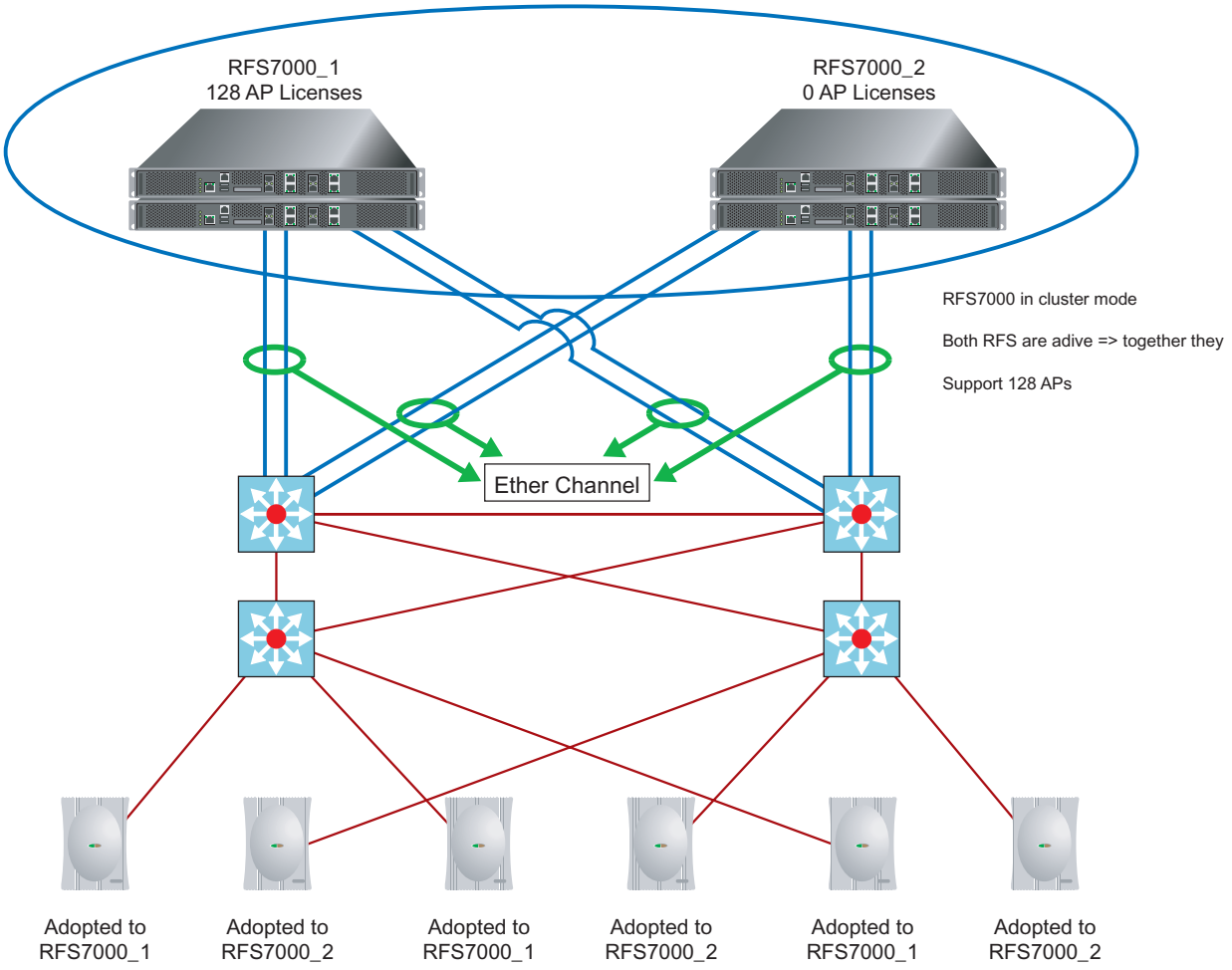
8.4.1 Creating a Redundant WLAN with an RFS7000

Redundancy (also referred to as clustering) is required to provide network traffic continuity. Optimally, when one switch goes down another ethernet switch should take over to provide uninterrupted data management support.

Such a RFS7000 supported wired deployment could appear as follows:



As illustrated above, there is redundancy on different layers of the network. This form of redundancy applies to wireless traffic as well. A wireless RFS7000 redundant design appears as follows:



Within the illustration above, there are several survivability routes, including:

- *Redundancy at the RF Level*
- *Redundancy at the AP Layer and Access Layer*
- *Redundancy at the Distribution Layer*
- *Redundancy at the Switch Level*

8.4.1.1 Redundancy at the RF Level

Redundancy is set at the RF level by creating enough RF overlapping across for installed APs.

There are a few ways to accomplish this:

- *100% cell overlapping* - Full redundancy when an AP goes down. If an AP goes down, there is always a second one that takes over. However, this is very hard to achieve with 802.11b/g, since there are only 3 non-overlapping channels. 100% cell overlap is much easier to achieve with an 802.11a AP, since you have many more non-overlapping channels then 802.11b/g. The amount of available non-overlapping 802.11a channels is dependant on the geographical region you would like to install the WLAN in and the version of DFS the AP is supporting.

- *Redundancy via rate scaling* - With this type of redundancy, perform a site survey based on the highest basic rate. Remember, the RF footprint of a 1 Mbps data rate is much larger then the RF footprint of a 54 Mbps data rate.
- *Self healing* - Self healing is great using 802.11a, since there are more non overlapping channels. With 802.11b/g, it is not always recommended. Its effectiveness depends on the required throughput and the criticality of the application.

Self Healing

Self healing is the automatic adjustment of transmit power if one an AP in the network goes offline. A good seal healing supported network requires the proper initial planning of AP deployments, as APs are required to provide full coverage.

However, there are several key performance characteristics that should be noted within a self healing supported WLAN, including:

- Scaling an access port's cell size can cause hidden node problems for MUs on the fringe of a current cell
- Self healing interferes with an MU's roaming algorithms and power scaling
- MUs can perform power scaling if they so choose

There are 2 types of self-healing within Motorola's *Wireless Next Generation* (Wi-NG) architecture. One is called interference avoidance (where an AP selects a new channel with ACS if it detects interference, the other is called neighbor recovery.

Interference avoidance is run on all radios performing ACS (it only works on radios in ACS mode). When you detect the average number of radio retries exceeds a configured value, the ACS algorithm is re-run.

Remember, a high number of retries does not mean interference. Additionally, there is no guarantee running ACS actually fixes the problem.

```
self-heal interference-avoidance enable
no self-heal interference-avoidance enable
```

This enables and disables the interference avoidance feature. It is disabled by default.

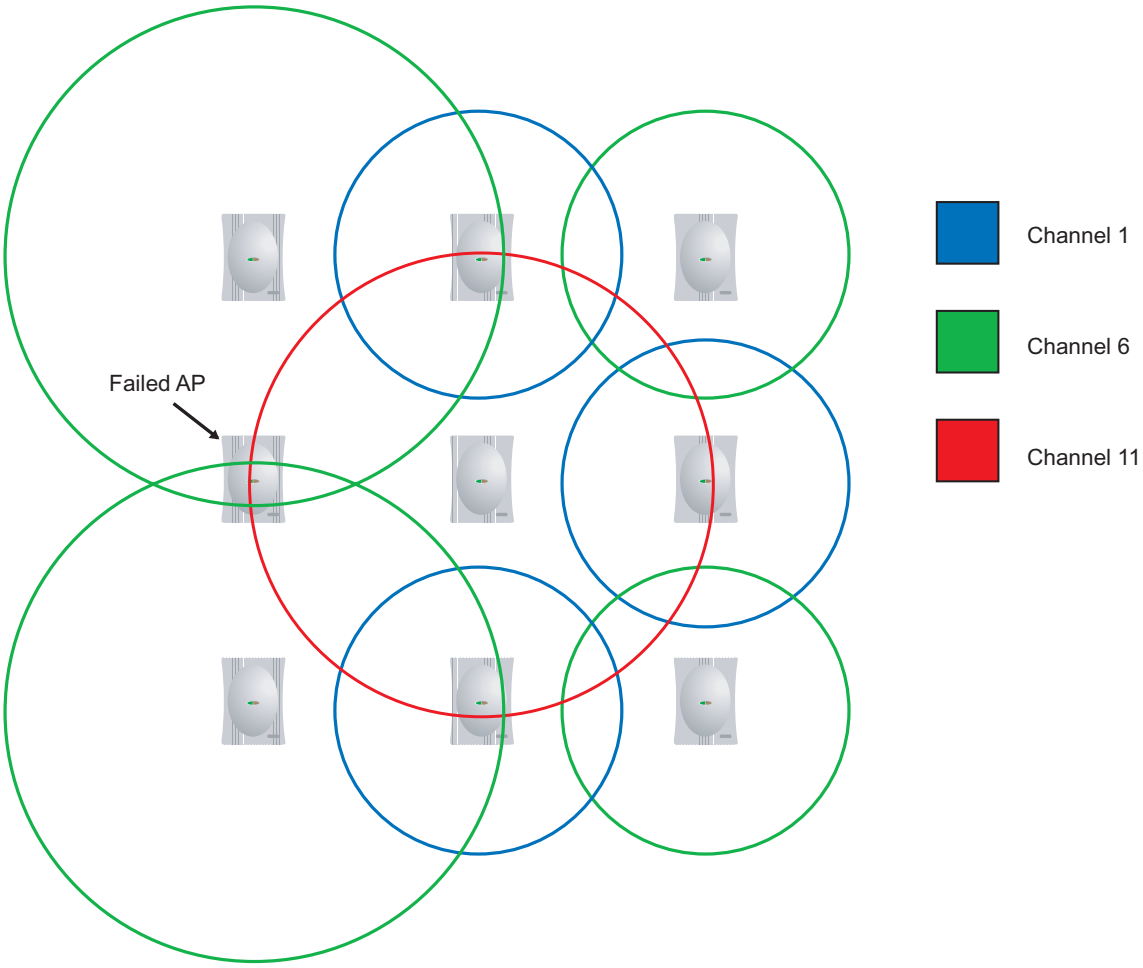
```
self-heal interference-avoidance hold-time <0-65535>
no self-heal interference-avoidance hold-time
```

These commands define the time interval interference avoidance is disabled after an interference avoidance event. This prevents thrashing when there is interference on all channels. The value is defined in seconds. The default hold time is 3600 seconds. The *no* command returns the value to 3600.

```
self-heal interference-avoidance retries <0.0-15.0>
no self-heal interference-avoidance retries
```

This command sets the average number of retries threshold value to determine when to perform interference avoidance. The default value is 14.0. The 'no' command returns it to this value.

Neighbor recovery was the original self-healing concept designed for Motorola's WLAN infrastructure. With neighbor recovery APs can cover for other APs that might be down. The idea is that you operate your radios at lower power or higher rates to shrink cell sizes. This lets you deploy a higher density, and cover for down radios when needed.



There are 4 steps to the neighbor recovery process, including:

1. Figuring out who your neighbors are
2. Detecting whether an AP is down
3. Taking action when the AP is down
4. Recovering back to a normal state if the AP comes back up

   First, ensure neighbor recovery is enabled.

   ```
   self-heal neighbor-recovery enable
   no self-heal neighbor-recovery enable
   ```

   These 2 commands enable/disable neighbor recovery. It is disabled by default. When self-healing is enabled, all radios forward beacons to the switch (just like rogue AP detection). The reason for this is so you can monitor the status of your radios.

   You can configure the neighbor list or have the switch generate it automatically. Generating it automatically should be done when the switch is first installed, not during normal operation.

   ```
   self-heal neighbor-recovery neighbors <1-1000> <1-1000>
   no self-heal neighbor-recovery neighbors <all|1-1000> <all|1-1000>
   ```

   Configure radio 1 as a neighbor of radio 2. Neighbor lists are reflexive, therefore radio 2 is automatically a neighbor of radio 1.Each radio can have a maximum of 10 radios. The *no* command has flexibility built

into it allowing you to wildcard either of the radio entries. 'all all' removes all radio neighbor mappings on the system.

```
self-heal neighbor-recovery run-neighbor-detect
```

Run this command to automatically detect neighbors. However, this is disruptive to your network. It takes down all the radios and temporarily has them beacon on the same channel. It then marks the three loudest radios (in dbm) heard as neighbors. Due to the reflexive nature of the neighbors, some radios can end up with more than three neighbors after running the command.

This command actually adds *self-heal neighbor-recovery neighbors X X* commands to the configuration. It most likely isn't the final solution for your neighbor map, but is a good starting place.

There are two ways to detect a radio is down. The first is simply that the radio becomes *unadopted*. This will happen if unplugged, the radio loses power or loses connectivity to the switch.

The second way, is the switch monitoring to check a radio is still beaconing. The switch uses beacons it is hearing to create an internal map of which radios can hear one another. Once a radio hears another radio's beacons for 30 seconds (continuous), it begins monitoring that radio. For example, both radio 1 and radio 6 are on channel 6 and consistently hear each other's beacons. After 30 seconds, radio 1 begins monitoring radio 6, and radio 6 monitors radio 1. If either radio stops hearing beacons from the other, the absentee radio is flagged as down.

It is important to understand the difference between *monitoring* and *neighbors*. You don't want neighbors to be able to hear each other. You want to minimize interference between radios close to each other by placing them on separate channels. Thus, neighbors will not be able to monitor each other.

Throwing detector radios into the mix complicates things a bit more. Detectors can be neighbors of other radios. They are very useful for monitoring other radios. A detector scans channels it will be able to monitor all the radios that are close to it. Since detectors never send any beacons, it is impossible to monitor a detector.

Self-Healing actions are defined on a per radio basis. Define what you want a radio to do when its neighbor goes down, as opposed to what action a neighbor should take when this radio goes down.

Up to 4 different actions can be configured.

```
self-heal neighbor-recovery action <none|open-rates|raise-power|both> radio
<1-1000>
```

Open rates place a radio back into its default rate (allowing all rates). Raising the power sets the radio to maximum power. The *both* setting does both of these things. You can also specify a radio does nothing. The nothing value is the default setting. In theory, when raising the power to maximum, you could become non-compliant (and operating illegally) for the country you are in, especially if using large gain external antennas. The work around for this is as follows:

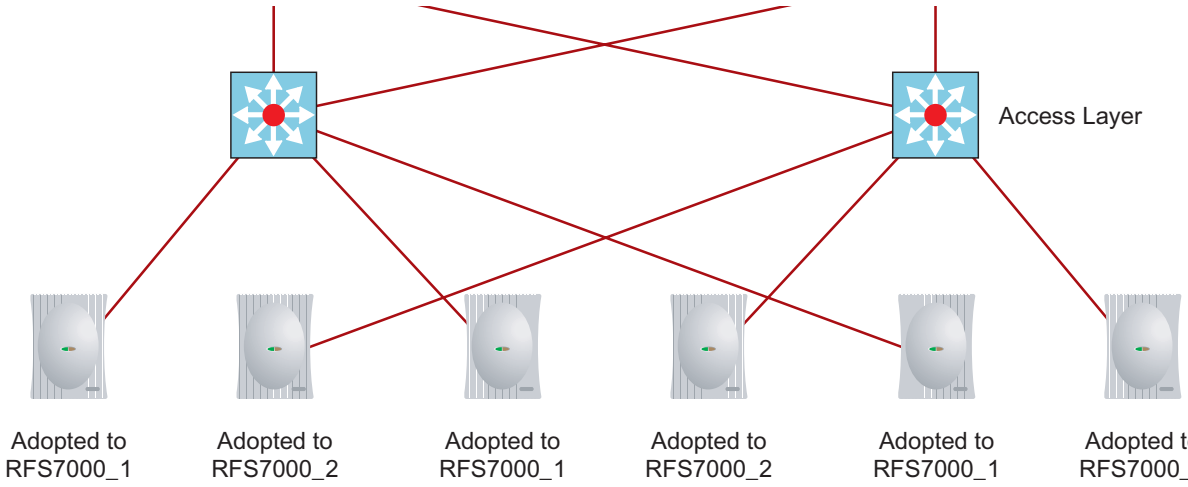
```
radio 1 self-healing-offset <0-65535>
no radio 1 self-healing-offset
```

This allows a user to input a dbm offset value when raising the power due to self healing. The new power is max - offset. The default value for this parameter is 0. The *no* command returns this to default. Recovering back to a normal state (when an AP comes back up) is something done automatically by the switch when either:

- A radio that was unadopted becomes adopted again
- A radio that was not beaconing begins beaconing again

8.4.1.2 Redundancy at the AP Layer and Access Layer

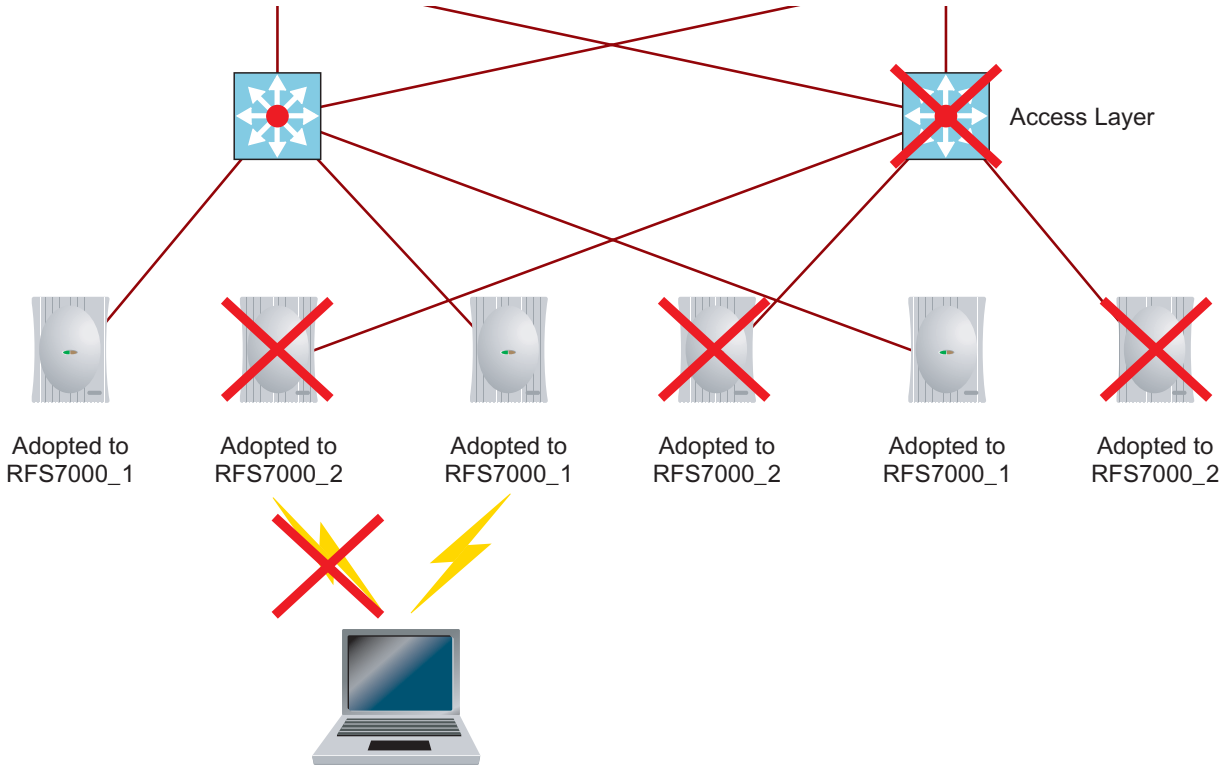
Its possible to have each AP adopted by each deployed switch.



When you connect all APs to the same switch you create on single point of failure. The same is true when you connect one side of a building (or a floor of a building) to one switch. In both cases, when the access switch is down, you have no access in that coverage area.

Having every other AP connected to every other switch provides redundancy on the RF network when one of the switches fails (as illustrated above).

Imagine a WLAN installation within a floor of a building. When one switch goes down, the PC connected to the failed AP simply associates to the next AP.



Layer 2 AP Adoption

The configuration of layer 2 adoption on the switch is defined as follows:

1. First you have to assign an adoption preferred ID to the switch:

   For the first switch:

```
RFS7000_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RFS7000_1(config)#wireless
RFS7000_1(config-wireless)#
RFS7000_1(config-wireless)#adoption-pref-id 500
```

   For the second switch:

```
RFS7000_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RFS7000_2(config)#wireless
RFS7000_2(config-wireless)#
RFS7000_2(config-wireless)#adoption-pref-id 1500
```

2. Now that you have assigned a preferred adoption ID to the switch, you need to assign a preferred adoption ID to the radio.

NOTE: The preferred adoption ID is assigned to the radio, not the AP.

   Define the radio configuration as follows:

```
RFS7000_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RFS7000_1(config)#wireless
RFS7000_1(config-wireless)#radio 3,4 adoption-pref-id 1500
```

Layer 3 Adoption

Creating a layer 3 wireless network provides even better redundancy then wired connections. A wireless redundancy approach aides a support team when an access switch goes down. In fact, in the case of a failed access switch, a wireless PC simply associates to the next available AP (the AP connected to the next switch). This is not the case for a wired PC, as the access switch has to be replaced immediately or all the connected PCs will lose connectivity.

8.4.1.3 Redundancy at the Distribution Layer

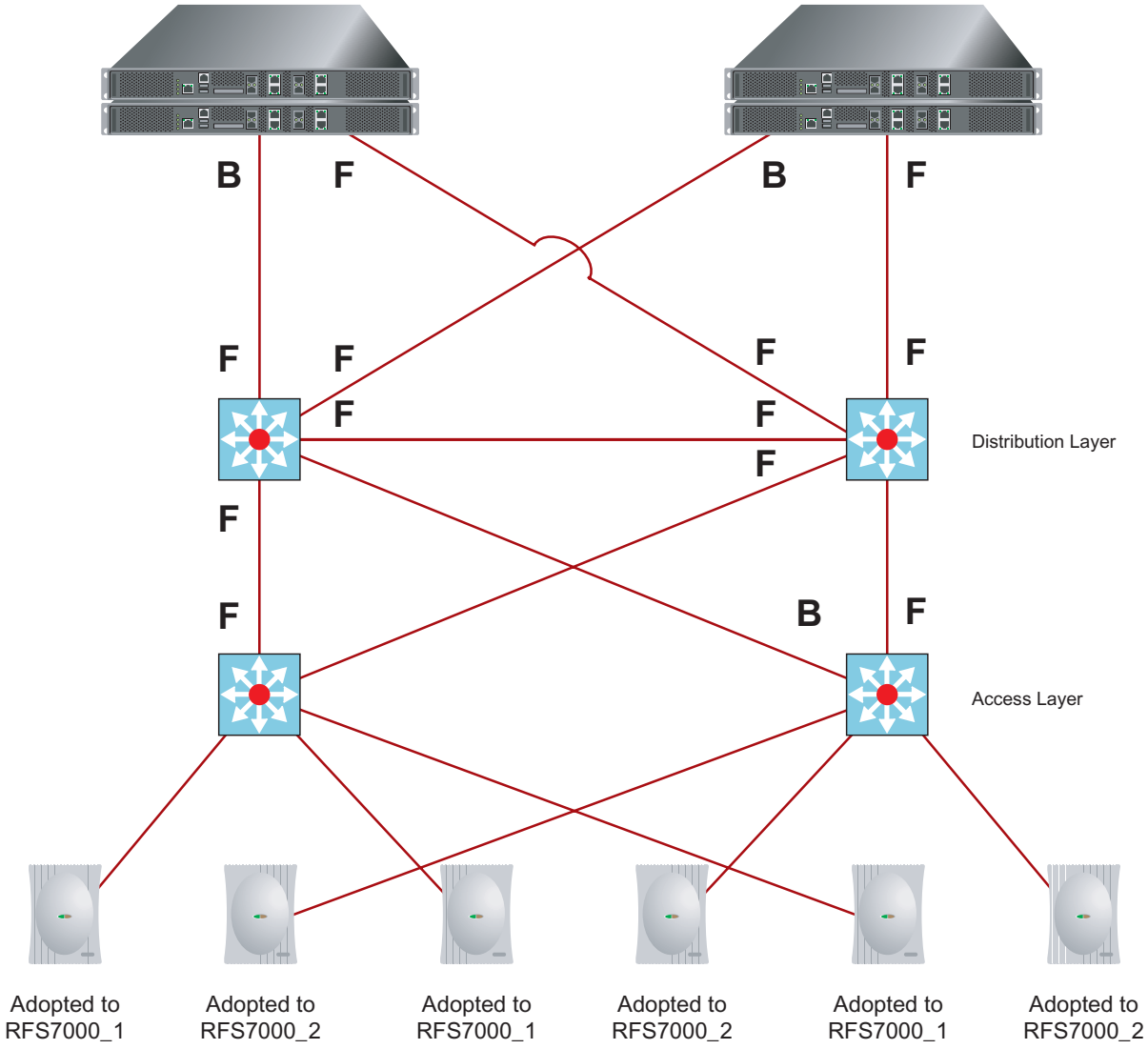
Creating redundancy within a core distribution access network is accomplished by cross connecting all the network devices. The only downside to this, is you can have packet storm problems leading to connectivity issues.

The solution is a spanning-tree protocol. The following is a list of the possible spanning-tree protocols:

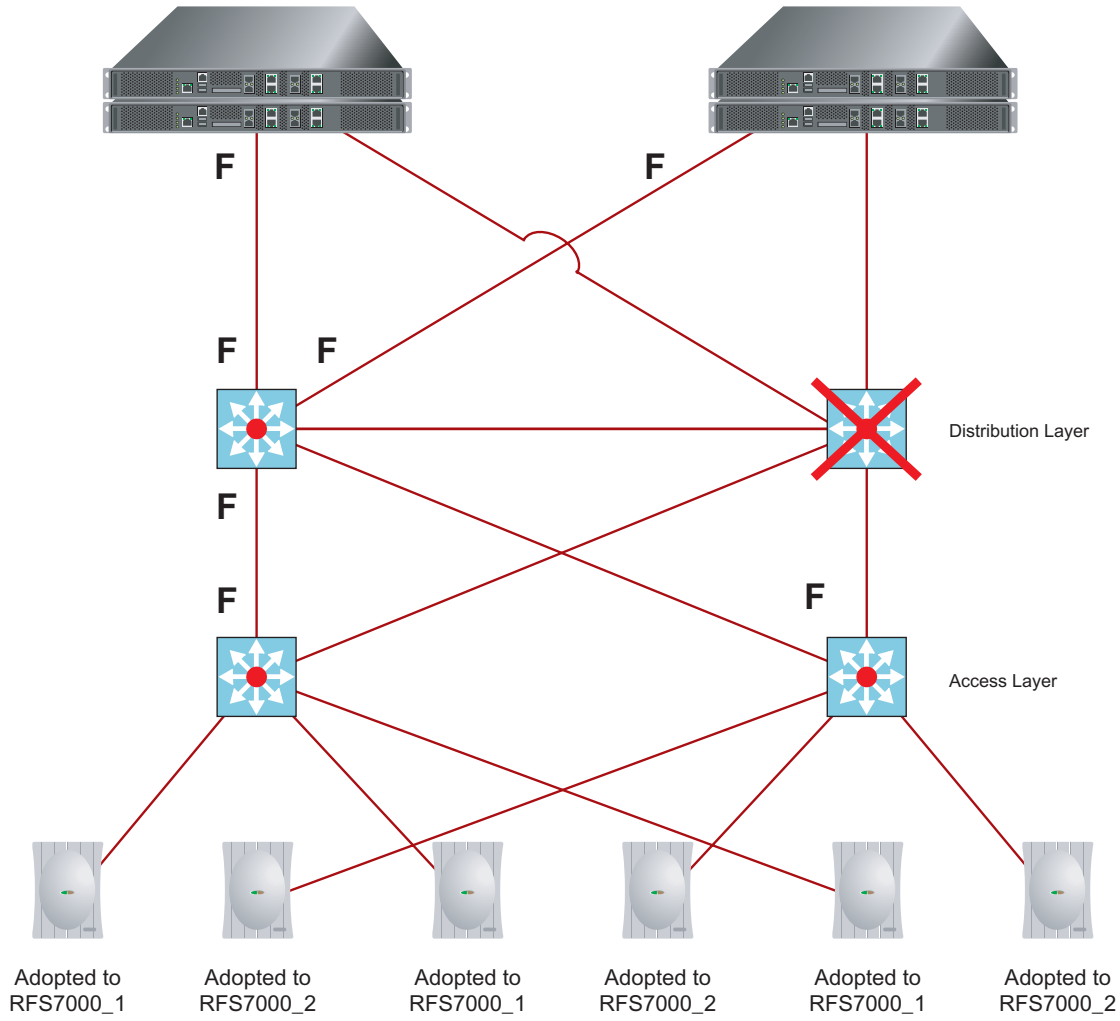
- STP
- RSTP
- MSTP
- PVST+
- Rapid PVST+

MSTP is an ideal spanning-tree implementation. With MSTP, you do not need to create an STP instance for each VLAN. MSTP runs on top of RSTP and therefore ideal within Motorola's wireless redundancy architecture. When one distribution switch fails, it's good to have each AP connected through the distribution switch immediately re-routed through the redundant distribution switch.

In the following illustration, forwarding and blocking states are accounted for in normal operation:



The following illustrates a network's traffic path when one of the distribution switches is down:



To configure MSTP on the switch, type the following command:

`RFS7000(config)#spanning-tree mstp configuration`

The following is a list of switch MSTP commands:

Instance *ID* ***vlan*** *vlan-id*	Defines the MSTP instance value between (0-15). The vlan is the vlan-id(s) associated to this instance.
Name *WORD*	Name of the MSTP region.
Revision *revision_num*	MSTP revision number (0-255).

This is how the MSTP config looks from the startup-config (of our example):

```
!by default cisco mst interoperable is enabled
spanning-tree mst cisco-interoperability enable
!here is the actual mst configuration, in this redundant scenario we have one
instance, however you could have multiple instances for the data to perform
loadbalancing with the distribution switches
spanning-tree mst configuration
 instance 1 vlan 50,100,200,300,400
 name Region_RFS
```

```
 revision 1
```

The following is a more detailed view of the MST configuration:

```
RFS7000(config-mst)#sh spanning-tree mst configuration
%
%  MSTP Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : Region_RFS
%  Revision Level : 1
%  Digest         : 0xA47081E64BFABCDFE0D45226BA3E5A86
%-------------------------------------------------------
```

This is how it looks on the Cisco switches (the config of the primary root):

```
spanning-tree mst configuration
 name Region_RFS
 revision 1
 instance 1 vlan 50, 100, 200, 300, 400
! This part is to set the primary or secondary root, compared to the secondary
config this priority value is lower, so this switch becomes the primary root
spanning-tree mst 1 priority 24576
```

This is how it looks on the secondary root:

```
spanning-tree mst configuration
 name Region_RFS
 revision 1
 instance 1 vlan 50, 100, 200, 300, 400
! This part is to set the primary or secondary root, compared to the primary
config this priority value is higher, so this switch becomes the secondary root

spanning-tree mst 1 priority 28672
```

The role of the MSTP ports are as follows:

- *Root port* - Provides the best path (lowest cost)
- *Designated port* - Connects to the designated switch
- *Alternate port* - Offers an alternate path toward the root switch
- *Backup port* - Acts as a backup for the path provided by a designated port

This is important to understand if you want to optimize your configuration with short path or alternative routes.

By default, the MSTP protocol provides a path for data traffic. However, in the case where no cost or priority for the port is provided, the port with the lowest MAC address becomes the forwarding port, and this is not always an ideal situation.

Another poor situation would be the switch serving all pass through traffic of each VLAN. This functionality is designed for distribution and access Switches, but not ideally for a normal switch. The switch in this case should only be occupied with wireless data traffic. Therefore, set the priority of the connected switch ports in a way where one port is blocking and the other port is forwarding traffic.

Use the following commands to check which ports are forwarding or blocking:

```
! this command will show the mst situation for each instance you ask for that
are configured on your switch
RFS7000#sh spanning-tree mst instance 1
! Optional you can add : spanning-tree mst instance 1 interface ge 1. In this
case your will see the situation for GE 1
% 1: MSTI Root Path Cost 20000 - MSTI Root Port 2004 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 6001001360172900
% 1: MSTI Bridge Id 8001001570380176
!you see port 1 is discarding since it is not connected at this time
%   ge1: Port 2001 - Id 87d1 - Role Disabled - State Discarding
%   ge1: Designated Internal Path Cost 0  - Designated Port Id 0
%   ge1: Configured Internal Path Cost 20000000
%   ge1: Configured CST External Path cost 20000000
%   ge1: CST Priority 128  - MSTI Priority 128
%   ge1: Designated Root 0000000000000000
%   ge1: Designated Bridge 0000000000000000
%   ge1: Message Age 0 - Max Age 0
%   ge1: Hello Time 0 - Forward Delay 0
%   ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
!GE2 is discarding not forwarding, however is connected
%   ge2: Port 2002 - Id 87d2 - Role Alternate - State Discarding
%   ge2: Designated Internal Path Cost 20000  - Designated Port Id 8017
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 240
%   ge2: Designated Root 6001001360172900
%   ge2: Designated Bridge 70010012da87ab80
%   ge2: Message Age 0 - Max Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1
%
! GE3 is discarding since this is not connected at this time
%   ge3: Port 2003 - Id 87d3 - Role Disabled - State Discarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0
%   ge3: Configured Internal Path Cost 20000000
%   ge3: Configured CST External Path cost 20000000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 0000000000000000
%   ge3: Designated Bridge 0000000000000000
%   ge3: Message Age 0 - Max Age 0
%   ge3: Hello Time 0 - Forward Delay 0
%   ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
! GE4 is set to forwarding
%   ge4: Port 2004 - Id 87d4 - Role Rootport - State Forwarding
%   ge4: Designated Internal Path Cost 0  - Designated Port Id 8017
%   ge4: Configured Internal Path Cost 20000
```

```
%   ge4: Configured CST External Path cost 20000
%   ge4: CST Priority 128  - MSTI Priority 240
%   ge4: Designated Root 6001001360172900
%   ge4: Designated Bridge 6001001360172900
%   ge4: Message Age 0 - Max Age 0
%   ge4: Hello Time 2 - Forward Delay 15
%   ge4: Forward Timer 0 - Msg Age Timer 5 - Hello Timer
```

A shorter (less detailed) way to find out which port is forwarding or blocking is as follows:

```
RFS7000#more system:/proc/net/dataplane/bridge/ports
ports
# of tagged external ports: 2
STP forwarding: 0
0: "ge1" external port, MAC 00-15-70-38-01-76, native vlan 1, vlan tag none,
MSTP state not forwarding
1: "ge2" external port, MAC 00-15-70-38-01-77, native vlan 50, vlan tag non-
native, MSTP state not forwarding
2: "ge3" external port, MAC 00-15-70-38-01-78, native vlan 1, vlan tag none,
MSTP state not forwarding
3: "ge4" external port, MAC 00-15-70-38-01-79, native vlan 50, vlan tag non-
native, MSTP state forwarding
4: "sa1" external port, MAC 00-00-00-00-00-00, native vlan 1, vlan tag none,
MSTP state not forwarding
5: "sa2" external port, MAC 00-00-00-00-00-00, native vlan 1, vlan tag none,
MSTP state not forwarding
6: "sa3" external port, MAC 00-00-00-00-00-00, native vlan 1, vlan tag none,
MSTP state not forwarding
7: "sa4" external port, MAC 00-00-00-00-00-00, native vlan 1, vlan tag none,
MSTP state not forwarding
8: "local" native vlan 1
9: "mobility" native vlan 0
```

The command used to check a Cisco switch's MST port status is as follows:

```
Dist_Pri_11#sh spanning-tree mst

###### MST00        vlans mapped:   1-49,51-99,101-199,201-299,301-399
                                     401-4094
Bridge      address 0013.6017.2900  priority  32768 (32768 sysid 0)
Root        address 0012.da87.ab80  priority  32768 (32768 sysid 0)
            port    Gi0/22          path cost 0
IST master  address 0012.da87.ab80  priority  32768 (32768 sysid 0)
                                    path cost 20000     rem hops 19
Operational hello time 2, forward delay 15, max age 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/19           Desg FWD 20000     128.19   Edge P2p
Gi0/21           Desg FWD 20000     128.21   P2p
Gi0/22           Root FWD 20000     128.22   P2p
Gi0/23           Desg FWD 20000     128.23   P2p
Gi0/24           Desg FWD 20000     128.24   P2p
!the following part is for the mst instance we used in our setup, namely
instance 1
###### MST01        vlans mapped:   50,100,200,300,400
Bridge      address 0013.6017.2900  priority  24577 (24576 sysid 1)
Root        this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/19           Desg FWD 20000     128.19   Edge P2p
Gi0/21           Desg FWD 20000     128.21   P2p
Gi0/22           Desg FWD 20000     128.22   P2p
Gi0/23           Desg FWD 20000     128.23   P2p
Gi0/24           Desg FWD 20000     128.24   P2p
```

8.4.1.4 Redundancy at the Switch Level

Creating redundancy on the switch is easy, scalable and transparent.

However, you need to understand of the following :

Maximum Number of APs Supported by Switch Model

WS5100	48
RFS6000	48
RFS7000	256

NOTE: The only other thing you have to understand besides the amount of APs a switch can adopt is the number of switches that can be added to one cluster. Currently, 12 switches can be supported in one cluster.

Switches are Available in 2 Modes

- *Active*
  - The RFS7000 can be ordered with 64, 128 or 256 AP licenses. There are license packs of 16 AP available to upgrade the 64 or 128 based RFS7000 switches.
  - The RFS6000 can be ordered with 8, 24 or 48 AP licenses. There are license packs of 8 AP available to upgrade the 8 or 24 based RFS6000 switches.
  - The WS5100 can be ordered with 6, 12, 18, 24, 30, 36, 48 AP licenses. There are license packs of 6 AP available to upgrade the 6, 12, 18, 24, 30 or 36 based RFS6000 switches.
- *Redundant*
  - This is just a RFS (6000 or 7000) with a zero port license. There are no upgrade packs available for this product.

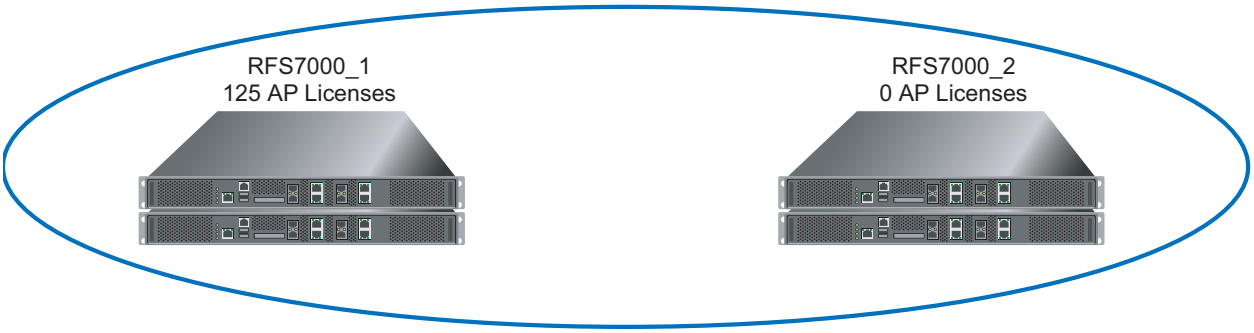
AP300 Boot Process

An AP300 model access port boots as follows:

1. The AP300 looks for a switch via layer 2 broadcasts.
2. If the AP300 fails to detect a switch via layer 2, it starts to look for a DCHP server.

8.4.2 Redundancy Examples

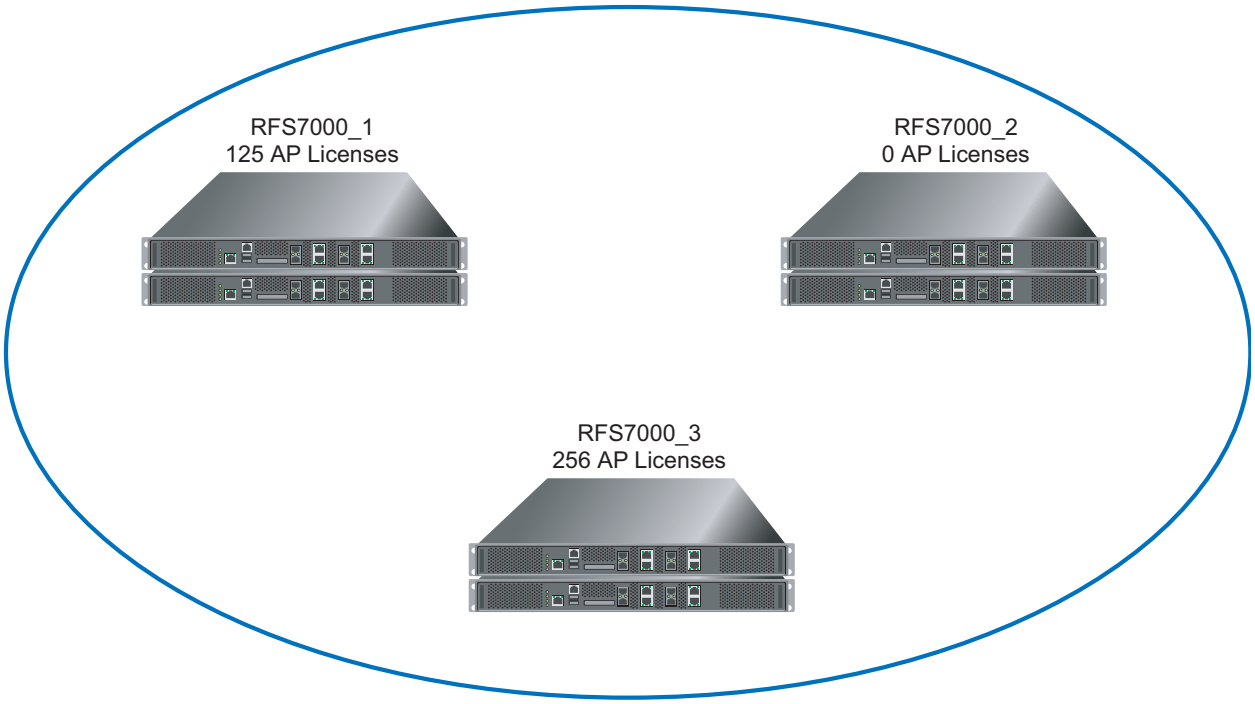
You can create a 1 to 1 or 1 to *n* redundant solution with the switch. The easiest form of redundancy is to make both switches active and license the 2 switches to aggregate to 1 common license. In other words, if you have one switch with 128 port licenses and 1 redundant switch with 0 (zero) port licenses, the 2 switches will together support 128 ports.



RFS7000 in cluster mode
Both RFS are adive => together they
Support 128 APs

Making the 2 switches active has clear advantages. The switches can load balance by negotiating the number of APs per switch and load balance an AP with heavy traffic between the two switches.

Another example is as follows:



RFS7000 in cluster mode
Both RFS are adive => together they
Support 384 APs

NOTE: If possible, avoid an active - standby configuration, as the active switch carries the load while the standby does nothing and consumes energy until the active switch is not available.

8.4.2.1 Configuring Redundancy Between Switches

Configuring redundancy between multiple switches is relatively easy. This section examines the configuration parameters and options required to set up a cluster (redundancy group).

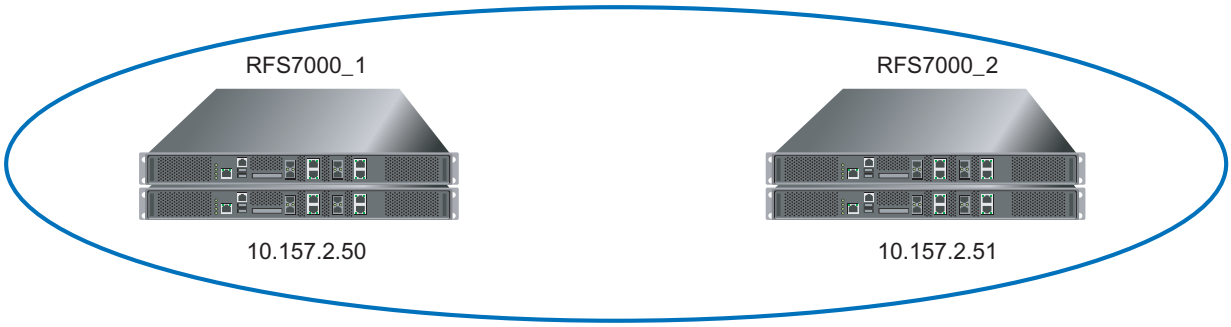
1. Move to the cluster configuration part of the switch by entering the privilege mode (on the switch CLI):
2. Refer to the following configuration commands (or switch applet options) to help define the redundancy group:

auto-revert *enable*	Check this option to enable the auto revert feature and specify the time (in minutes) for the switch to revert.
auto-revert-period *<1-1800>*	Define an interval between 1 and 1800 minutes. The default revert time is 5 minutes. When a primary switch fails, the standby switch takes over APs adopted by the primary. If the auto revert feature is enabled, when the failed primary switch comes back up, the standby will start a timer based on the auto-revert interval. At the expiry of auto-revert interval if the primary switch is still up, the standby switch would release all its adopted APs and goes back to monitoring mode. The expiry timer either will be stopped or restarted if primary switch goes down and comes up again during the course of the auto-revert interval timer.
Dhcp-server *enable*	The DHCP Redundancy feature allows administrators to have only one DHCP server running at any given time in a cluster. The clustering protocol will enable all peers participating in a DHCP redundancy to decide the active DHCP server among them. The switch with lowest Redundancy IP will be selected to serve as an active DHCP server in a cluster. This selected active DHCP server switch can be either a primary or standby switch. The other switches will not provide DHCP service as long as the selected active DHCP server running switch is alive.
discovery-period	Use the **Discovery Period** field to configure the member Discovery Time. During the Discovery Time, a switch discerns the existence of other switches within the redundancy group. Configure an interval between 10 and 60 seconds. The default value is 30 seconds.
enable	Refer to the **Enable** redundancy checkbox to enable/disable the redundancy feature. Redundancy must be disabled to set any redundancy related parameter. All the modifiable fields are grayed out if redundancy is enabled.
Group-id	Use the **Redundancy ID** field to set the Cluster ID. All the switches configured in the cluster should have the same Cluster ID. The valid range for a cluster id is 1-65535.
Handle-stp	Refer to the **Handle STP Convergence** field to enable Handle STP convergence for the switch. STP stands for *Spanning Tree Protocol*. In general, this protocol is enabled in layer 2 networks to prevent network looping. If the network is enabled for STP to prevent looping, the network forward is data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine execution is important to load balance access ports at startup.

Heartbeat-period	The **Heartbeat Period** is used to configure the Heartbeat time. The heartbeat time is the interval heartbeat messages are sent. These heartbeat messages discover the existence and status of other members within the redundancy group. Configure an interval between 1 and 255 seconds. The default value is 5 seconds.
Hold-period	If there are no heartbeats received from a peer during the hold time, the peer is considered to be down. In general, hold period is configured for three times the heartbeat period. Meaning, if three consecutive heartbeats are not received from the peer, the peer is assumed down and unreachable. Configure a hold time between 10 and 255 seconds. The default value is 15 seconds.
Interface-ip	The **Interface IP** is the redundancy switch IP used to configure the IP address with which the redundancy feature operates to send heartbeats and update messages.
Manual-revert	Manually reverts switches back to primary. The standby switch will un-adopt all its adopted APs and move into a standby (passive) mode only if all configured members are up again. The revert function does not push APs to the primary switch unless the primary switch has failed over.
Member-ip	This is the IP address of the member switch that is part of the cluster.
Mode	A member can be in either an active or standby mode. In a redundancy group, all active members adopt radio-ports. Standby members adopt radio-ports only when an active member has failed or sees an access-port not adopted by a switch.

3. For each switch, define the IP addresses you want to enable redundancy on. Then define each switch's redundancy members.

NOTE: In the following example, there are 2 switches. The CLI commands displayed define how they are made redundant.



For the first switch (RFS7000_1):

```
!this is the IP address where the cluster protocol is communicating on
redundancy interface-ip 10.157.2.50
!Here are the redundancy members added and listed
redundancy member-ip 10.157.2.51
!this is the redundancy mode Primary or Standby
redundancy mode primary
```

```
redundancy enable
```

For the second switch (RFS7000_2):

```
redundancy interface-ip 10.157.2.51
redundancy member-ip 10.157.2.50
redundancy mode primary
redundancy enable
```

4. Verify redundancy status for the group members:

```
RFS7000_1#sh redundancy-members
Member ID                     : 192.168.1.63
Member State                  : Peer Established
Member First Seen             : May 08 01:59:43 2008
Member Last  Seen             : May 08 02:10:19 2008
Number of HB sent             : 134
Number of HB received         : 128
Number of Update sent         : 1
Number of Update received     : 1
Member Standby Mode           : Primary
Member AP adoption count      : 1
Member Installed License Count: 128
Member Radio portal Count     : 2
Member Associated MU Count    : 0
Member Rogue AP detected Count: 0
Member Self Healing AP Count  : 0
Member Switch Adopt Capacity  : 256
Member Running Image Version  : 1.1.1.0-003R
```

5. Verify redundancy status for the group:

```
RFS7000#sh redundancy-group

Redundancy Group Configuration Detail
Redundancy Feature                 : Enabled
Redundancy group ID                : 1
Redundancy Mode                    : Primary
Redundancy Interface IP            : 192.168.1.60
Number of configured peer(s)       : 1
Heartbeat-period                   : 5 Seconds
Hold-period                        : 15 Seconds
Discovery-period                   : 30 Seconds
Handle STP                         : Disabled
Switch Installed License           : 128
Switch running image version       : 1.1.0.0-038R
Auto-revert-period                 : 5 mins
Auto-revert Feature                : Disabled
DHCP-Server Redundancy             : Disabled

Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 256
Cluster AP Adoption Count            : 2
Switch AP Adoption Count             : 1
Redundancy State                     : Active
Radio Portals adopted by Group       : 4
Radio Portals adopted by this Switch : 2
Rogue APs detected in this Group     : 0
Rogue APs detected by this Switch    : 0
MUs associated in this Group         : 0
MUs associated in this Switch        : 0
Selfhealing APs in this Group        : 0
Selfhealing APs in this Switch       : 0
Group maximum AP adoption capacity   : 512
Switch Adoption capacity             : 256
Established Peer(s) Count            : 1
Redundancy Group Connectivity status : All members connected
DHCP Server in group                 : Unknown
```

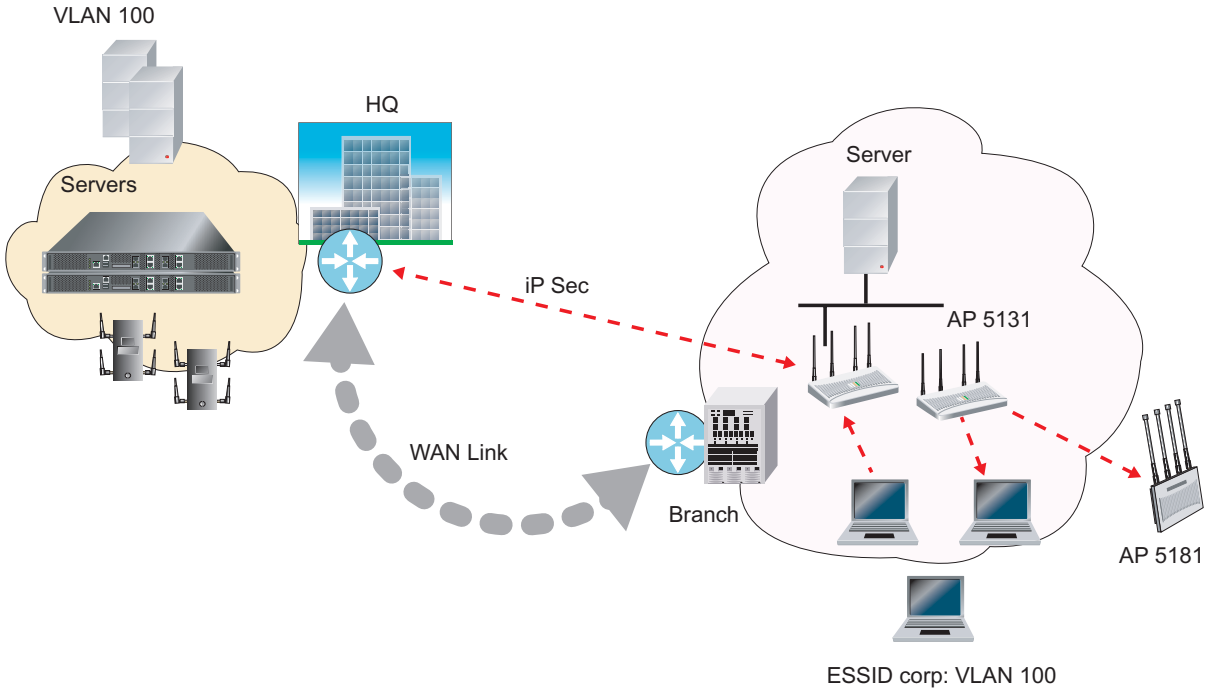
NOTE: Redundancy is not just created at the switch level, redundancy also must be established on different layers in the architecture. It all depends on how critical the data is to be transported over the WLAN and LAN.

8.5 Adaptive AP (AAP)

An *adaptive AP* (AAP) is an access point that can adopt like an AP300 (layer 3). The management of an AAP is conducted by the switch, once the access point connects to a switch and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- the tunneling of centralized traffic to the wireless switch



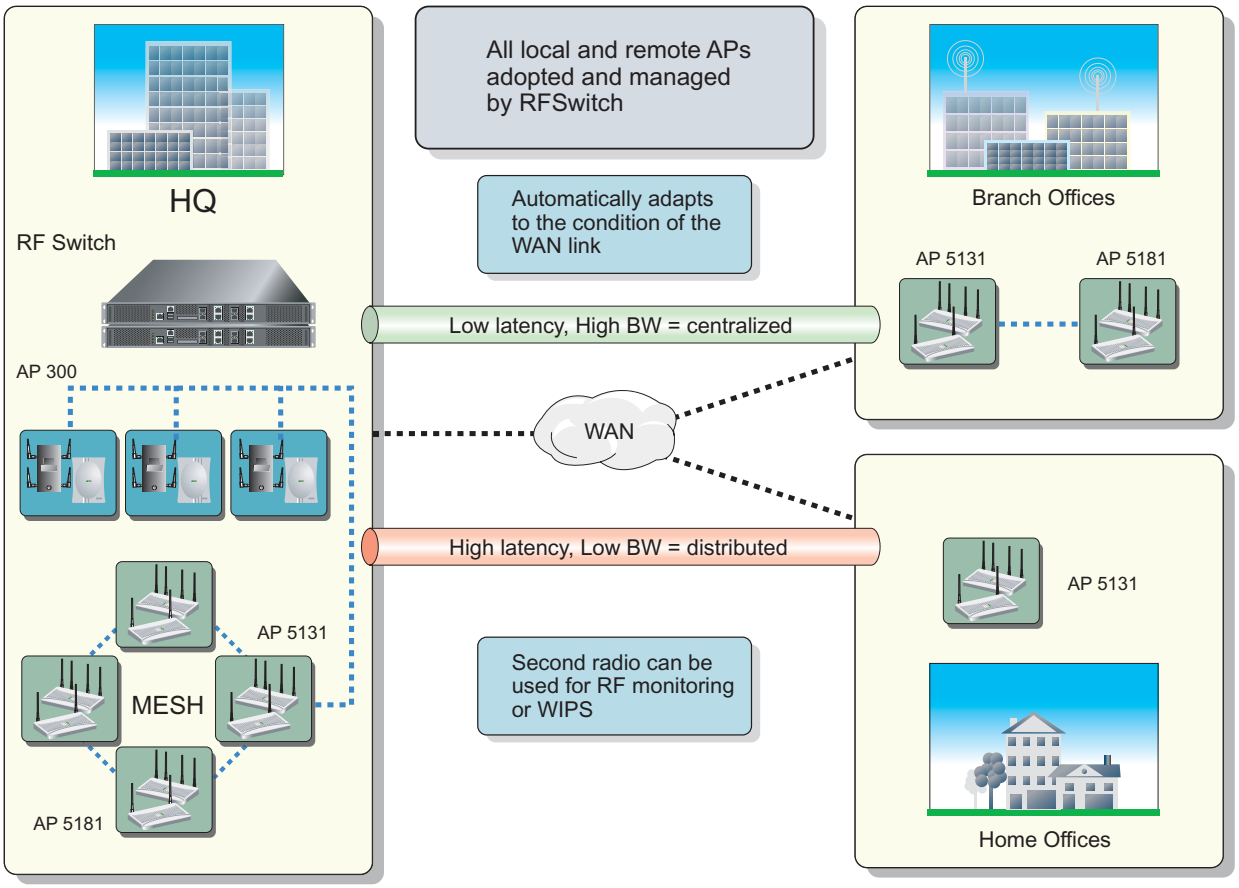
An AAP's switch connection can be secured using IP/UDP or IPSec depending on whether a secure WAN link from a remote site to the central site already exists.

The switch can be discovered using one of the following mechanisms:

- DHCP
- Switch *fully qualified domain name* (FQDN)
- Static IP addresses

The benefits of an AAP deployment include:

- *Centralized configuration management & compliance* - Wireless configurations across distributed sites can be centrally managed by the wireless switch or cluster
- *WAN survivability* - Local WLAN services at a remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLAN's to stores for corporate visitors* - Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location
- *Maintain local WLANs for in store applications* - WLANs created and supported locally can be concurrently supported with your existing infrastructure
- *Investment protection* - With adaptive AP you can support the adoption of 802.11n access points



8.5.1 The Elements of Adaptive AP

Refer to the following for an in-depth conceptual understanding of AAP as well as how to configure it.

- *Adaptive AP Management*
- *Types of Adaptive APs*
- *Licensing*
- *Switch Discovery*
- *Securing a Configuration Channel Between Switch and AP*
- *Adaptive AP WLAN Topology*
- *Configuration Updates*
- *Securing Data Tunnels between Switch and AAP*
- *Adaptive AP Switch Failure*
- *Remote Site Survivability (RSS)*
- *Adaptive Mesh Support*
- *Supported Adaptive Topologies*
- *How the AP Receives its Adaptive Configuration*
- *Establishing Basic Adaptive AP Connectivity*

- *Adaptive AP Deployment Considerations*
- *Adopting an Adaptive AP via a Switch Assisted Mesh*
- *Sample Swich Configuration for IPSec AAP and Independent WLAN*

8.5.1.1 Adaptive AP Management

An AAP can be adopted, configured and managed like a thin access port from the wireless switch.

NOTE: To support AAP functionality, a WS5100 model switch must be running firmware version 3.1 or higher, whereas a RFS6000 or RFS7000 model switch must be running firmware version 1.1 or higher. The access point must running firmware version 2.0 or higher to be converted into an AAP.

NOTE: An AAP cannot support a firmware download from the wireless switch

Once an access point connects to a switch and receives its AAP configuration, its WLAN and radio configuration is similar to a thin access port. An AAP's radio mesh configuration can also be configured from the switch. However, non-wireless features (DHCP, NAT, Firewall etc.) cannot be configured from the switch and must be defined using the access point's resident interfaces before its conversion to an AAP.

8.5.1.2 Types of Adaptive APs

Two low priced AP-5131 SKU configurations have been introduced allowing customers to take advantage of the adaptive AP architecture and to reduce deployment costs.

These dependent mode AP configurations are a software variant of the AP-5131 and are functional only after the access point is adopted by a wireless switch. After adoption, the dependent mode AP receives its configuration from the switch and starts functioning like other adaptive access points. For ongoing operation, the dependent mode AP-5131 needs to maintain connectivity with the switch. If switch connectivity is lost, the dependent mode AP-5131 continues operating as a stand-alone access point for a period of 3 days before resetting and executing the switch discovery algorithm again.

A dependent mode AP cannot be converted into a standalone access point through a firmware change.

Refer to *AP-51xx Hardware/ Software Compatibility Matrix* within the release notes bundled with the access point firmware.

- *AP-5131-13040-D-WR Dependent AP-5131 Dual Radio (Switch Required)*
- *AP-5131-40020-D-WR Dependent AP-5131 Single Radio (Switch Required)*

8.5.1.3 Licensing

An AAP uses the same licensing scheme as a thin access port. This implies an existing license purchased with a switch can be used for an AAP deployment. Regardless of how many AP300 and/or AAPs are deployed, you must ensure the license used by the switch supports the number of radio ports (both AP300s and AAPs) you intend to adopt.

8.5.1.4 Switch Discovery

For an access point to function as an AAP (regardless of mode), it needs to connect to a switch to receive its configuration. There are two methods of switch discovery:

- *Auto Discovery using DHCP*

- *Manual Adoption Configuration*

NOTE: To support switch discovery, a WS5100 model switch must be running firmware version 3.1 or higher, whereas a RFS6000 or RFS7000 model switch must be running firmware version 1.1 or higher. The access point must running firmware version 2.0 or higher.

Auto Discovery using DHCP

Extended Global Options 189, 190, 191, 192 can be used or Embedded Option 43 - Vendor Specific options can be embedded in Option 43 using the vendor class identifier: ***MotorolaAP.51xx-V2-0-0.***

	Code	***Data Type***
List of Switch IP addresses *(separate by comma, semi-colon, or space delimited)*	188	String
Switch FQDN	190	String
AP-7131 Encryption IPSec Passphrase (Hashed) **	191	String
AP-7131 switch discovery mode 1 = auto discovery enable 2 = auto discover enabled (using IPSec)	192	String

** The AP-7131 uses an encryption key to hash passphrases and security keys. To obtain the encryption passphrase, configure an AP-7131 with the passphrase and export the configuration file.

```
enc-admin-passwd d2
/
// System Configuration
/
system
set name AP-51xx
set loc \0
set email \0
set cc us
/
system
aap-setup
// Adaptive AP menu
set auto-discovery disable
set interface lan1
set name \0
set port 24576
delete all
set enc-passphrase bf0819993a702c39
set ac-keepalive 5
set tunnel-to-switch enable
/
// System-Access menu
system
access
set applet lan 1 enable
set applet slan 1 enable
set cli lan 1 enable
set ssh lan 1 enable
set snmp lan 1 enable
```

Encrypted Passphrase to be used in DHCP Option

Manual Adoption Configuration

A manual switch adoption of an AAP can be conducted using:

- *Static FQDN* - A switch fully qualified domain name can be specified to perform a DNS lookup and switch discovery.

- *Static IP addresses* - Up to 12 switch IP addresses can be manually specified in an ordered list the AP can choose from. When providing a list, the AAP tries to adopt based on the order in which they are listed (from 1-12).

8.5.1.5 *Securing a Configuration Channel Between Switch and AP*

Once an access point obtains a list of available switches, it begins connecting to each. The switch can be either on the LAN or WAN side of the access point to provide flexibility in the deployment of the network. If the switch is on the access point's LAN, ensure the LAN subnet is on a secure channel. The AP will connect to the switch and request a configuration.

8.5.1.6 Adaptive AP WLAN Topology

An AAP can be deployed in the following WLAN topologies:

- *Extended WLANs* - Extended WLANs are the centralized WLANs created on the switch
- *Independent WLANs* - Independent WLANs are local to an AAP and can be configured from the switch. You must specify a WLAN as independent to stop traffic from being forwarded to the switch. Independent WLANs behave like WLANs on a standalone access point.
- *Both* - Extended and independent WLANs are configured from the switch and operate simultaneously.

8.5.1.7 Configuration Updates

An AAP receives its configuration from the switch initially as part of its adoption sequence. Subsequent configuration changes on the switch are reflected on an AAP when applicable. An AAP applies the configuration changes it receives from the switch after 30 seconds from the last received switch configuration message. When the configuration is applied on the AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds) forcing associated MUs to be deauthenticated. MUs are quickly able to associate.

8.5.1.8 Securing Data Tunnels between Switch and AAP

If a secure link (site-to-site VPN) from a remote site to the central location already exists, the AAP does not require IPSec be configured for adoption. For sites with no secure link to the central location, an AAP can be configured to use an IPSec tunnel (with AES 256 encryption) for adoption. The tunnel configuration is automatic on the AAP side and requires no manual VPN policy be configured. On the switch side, configuration updates are required to adopt the AAP using an IPSec tunnel.

8.5.1.9 Adaptive AP Switch Failure

In the event of a switch failure, an AAP's independent WLAN continues to operate without disruption. The AAP attempts to connect to other switches (if available) in background. Extended WLANs are disabled once switch adoption is lost. When a new switch is discovered and a connection is secured, an extended WLAN can be enabled. If a new switch is located, the AAP synchronizes its configuration with the located switch once adopted. If *Remote Site Survivability* (RSS) is disabled, the independent WLAN is also disabled in the event of a switch failure.

8.5.1.10 Remote Site Survivability (RSS)

RSS can be used to turn off RF activity on an AAP if it loses adoption (connection) to the switch.

RSS State	***Independent WLAN***	***Extended WLAN***
RSS Enabled	WLAN	WLAN continues beaconing but AP does allow clients to associate on that WLAN
RSS Disabled	WLAN stops beaconing	WLAN stops beaconing

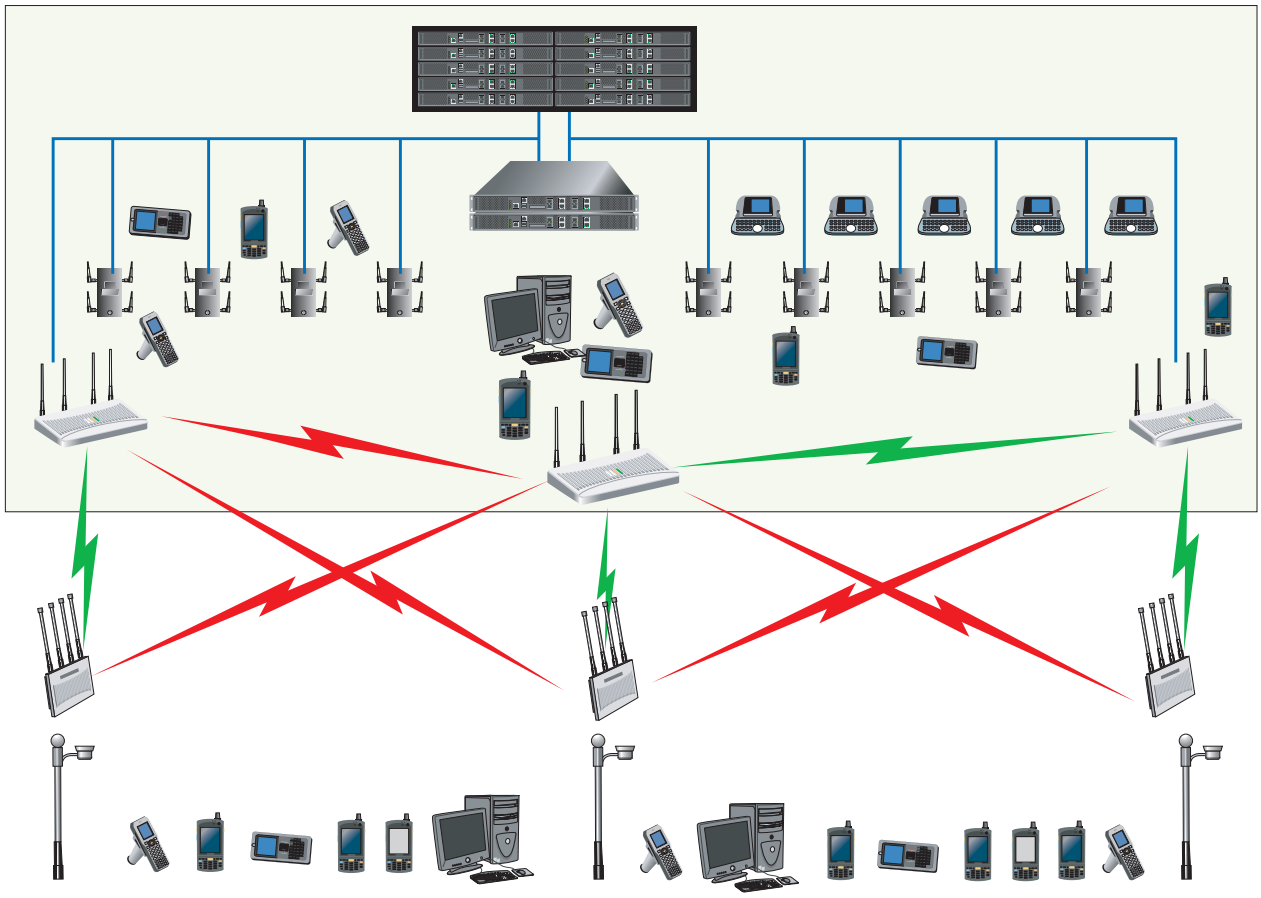
NOTE: For a dependant AAP, independent WLANs continue to beacon for three days in the absence of a switch.

8.5.1.11 Adaptive Mesh Support

An AAP can extend an AP51x1's existing mesh functionality to a switch managed network. All mesh APs are configured and managed through the wireless switch. APs without a wired connection form a mesh backhaul to a repeater or a wired mesh node and then get adopted to the switch. Mesh nodes with existing wired access get adopted to the switch like a wired AAP.

Mesh AAPs apply configuration changes 300 seconds after the last received switch configuration message. When the configuration is applied on the Mesh AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds), forcing associated MUs to be deauthenticated and the Mesh link will go down. MUs are able to quickly associate, but the Mesh link will need to be re-established before MUs can pass traffic. This typically takes about 90 to 180 seconds depending on the size of the mesh topology.

NOTE: When mesh is used with AAPs, the *ap-timeout* value needs to be set to a higher value (for example, 180 seconds) so Mesh AAPs remain adopted to the switch during the period when the configuration is applied and mesh links are re-established.



8.5.1.12 Supported Adaptive Topologies

The following AAP topologies are supported by the access point:

- *Extended WLANs Only*
- *Independent WLANs Only*
- *Extended WLANs with Independent WLANs*
- *Extended WLANs with MESH Configurations*

Deployment Considerations

When reviewing the AAP topologies describes in the section, be cognizant of the following considerations to optimize the effectiveness of the deployment:

- An AAP firmware upgrade will not be performed at the time of adoption from the wireless switch. Instead, the firmware is upgraded using the AP-51x1's firmware update procedure (manually or using the DHCP Auto Update feature)
- An AAP can use its LAN1 interface or WAN interface for adoption. The default gateway interface is set to LAN1. If the WAN Interface is used, explicitly configure WAN as the default gateway interface
- Motorola recommends using the LAN1 interface for adoption in multi-cell deployments

- If you have multiple independent WLANs mapped to different VLANs, the AAP's LAN1 interface requires trunking be enabled with the correct management and native VLAN IDs configured. Additionally, the AAP needs to be connected to a 802.1q trunk port on the wired switch
- Be aware IPSec Mode supports NAT Traversal (NAT-T)

Before deploying your switch/AAP configuration, refer to the following usage caveats to optimize its effectiveness:

- Extended WLANs are mapped to the AP's LAN2 interface and all independent WLANs are mapped to the AP's LAN1 Interface
- If deploying multiple independent WLANs mapped to different VLANs, ensure the AP's LAN1 interface is connected to a trunk port on the layer 2/3 switch and appropriate management and native VLANs are configured
- The WLAN used for mesh backhaul must always be an independent WLAN
- The switch configures an AAP. If manually changing wireless settings on the AP, they are not updated on the switch. It's a one way configuration, from the switch to the AP
- An AAP always requires a router between the AP and the switch
- An AAP can be used behind a NAT
- An AAP uses UDP port 24576 for control frames and UDP port 24577 for data frames. Multiple VLANs per WLAN, layer 3 mobility, dynamic VLAN assignment, NAC, self healing, rogue AP, MU locationing, hotspot on extended WLAN are some of the important wireless features not supported in an AAP supported deployment

Extended WLANs Only

An extended WLAN configuration forces all MU traffic through the switch. No wireless traffic is locally bridged by the AAP.

Each extended WLAN is mapped to the access point's virtual LAN2 subnet. By default, the access point's LAN2 is not enabled and the default configuration is set to static with IP addresses defined as all zeros. If the extended VLAN option is configured on the switch, the following configuration updates are made automatically:

- The AAP's LAN2 subnet becomes enabled
- All extended VLANs are mapped to LAN2

NOTE: MUs on the same WLAN associated to the AAP can communicate locally at the AP Level without going through the switch. If this scenario is undesirable, the access point's MU-to-MU disallow option should be enabled.

Independent WLANs Only

An independent WLAN configuration forces all MU traffic be bridged locally by the AAP. No wireless traffic is tunneled back to the switch. Each extended WLAN is mapped to the access point's LAN1 interface. The only traffic between the switch and the AAP are control messages (for example, heartbeats, statistics and configuration updates).

Extended WLANs with Independent WLANs

An AAP can have both extended WLANs and independent WLANs operating in conjunction. When used together, MU traffic from extended WLANs go back to the switch and traffic from independent WLANs is bridged locally by the AP.

All local WLANs are mapped to LAN1, and all extended WLANs are mapped to LAN2.

Extended WLANs with MESH Configurations

Mesh networking is an extension of the existing wired network. There is no special configuration required, with the exceptions of setting the mesh and using it within one of the two extended VLAN configurations and defining an access point radio as a preferred base bridge.

The mesh backhaul WLAN must be an independent WLAN mapped to LAN1. The switch enforces the WLAN be defined as an independent WLAN by automatically setting the WLAN to independent when backhaul is selected. The AP ensures the backhaul WLAN be put on LAN1.

8.5.1.13 How the AP Receives its Adaptive Configuration

An AAP does not require a separate *local* or *running* configuration. Once enabled as an AAP, the AP obtains its configuration from the switch. If the AP's WAN link fails, it continues to operate using the last valid configuration until its link is re-established and a new configuration is pushed down from the switch. There is no separate file-based configuration stored on the switch.

Only WLAN, VLAN extension and radio configuration items are defined for the AAP by its connected switch. None of the other access point configuration items (Radius, DHCP, NAT, Firewall etc.) are configurable from the connected switch.

After the AP downloads a configuration file from the switch, it obtains the version number of the image it should be running. The switch does not have the capacity to hold the access point's firmware image and configuration. The access point image must be downloaded using a means outside the switch. If there is still an image version mismatch between what the switch expects and what the AAP is running, the switch will deny adoption.

Adaptive AP Prerequisites

Converting an access point into an AAP requires:

- Version 2.0 or higher firmware running on the AP-5131 or AP-5181 model access point.
- A Motorola WS5100 (running firmware version 3.1 or later) or a RFS7000 (running firmware version 1.1 or later) model switch.
- The appropriate switch licenses providing AAP functionality on the switch.
- The correct password to authenticate and connect the adaptive to the switch.

Configuring an Adaptive AP for Switch Adoption

An AAP needs to find and connect to the switch. To ensure this connection:

- Configure the switch's IP address on the AAP
- Provide the switch IP address using DHCP option 189 on a DHCP server. The IP address is a comma delimited string of IP addresses. For example "157.235.94.91, 10.10.10.19". There can be a maximum of 12 IP addresses.
- Configure the switch's FQDN on the AAP. The AAP can use this to resolve the IP address of the switch.
- Use the switch's secret password on the AAP for the switch to authenticate it. To avoid a lengthy broken connection with the switch, Motorola recommends generating an SNMP trap when the AAP loses adoption with the switch

Configuring the Switch for Adaptive AP Adoption

To adopt an AAP on a switch:

- Ensure enough licenses are available on the switch to adopt the required number of AAPs.
- As soon as the AAP displays in the adopted list adjust each AAP's radio configuration as required. This includes WLAN-radio mappings and radio parameters. WLAN-VLAN mappings and WLAN parameters are global and cannot be defined on a per radio basis. WLANs can be assigned to a radio as done today for an AP300 model access port. Optionally, configure WLANs as independent and assign to AAPs as needed.
- Configure each VPN tunnel with the VLANs to be extended to it. If you do not attach the target VLAN, no data will be forwarded to the AAP, only control traffic required to adopt and configure the AP

8.5.1.14 Establishing Basic Adaptive AP Connectivity

This section defines the activities required to configure basic AAP connectivity with a WS5100 or RFS7000 model switch. In establishing a basic AAP connection, both the access point and switch require modifications to their respective default configurations. For more information, see:

Adaptive AP Configuration

Switch Configuration

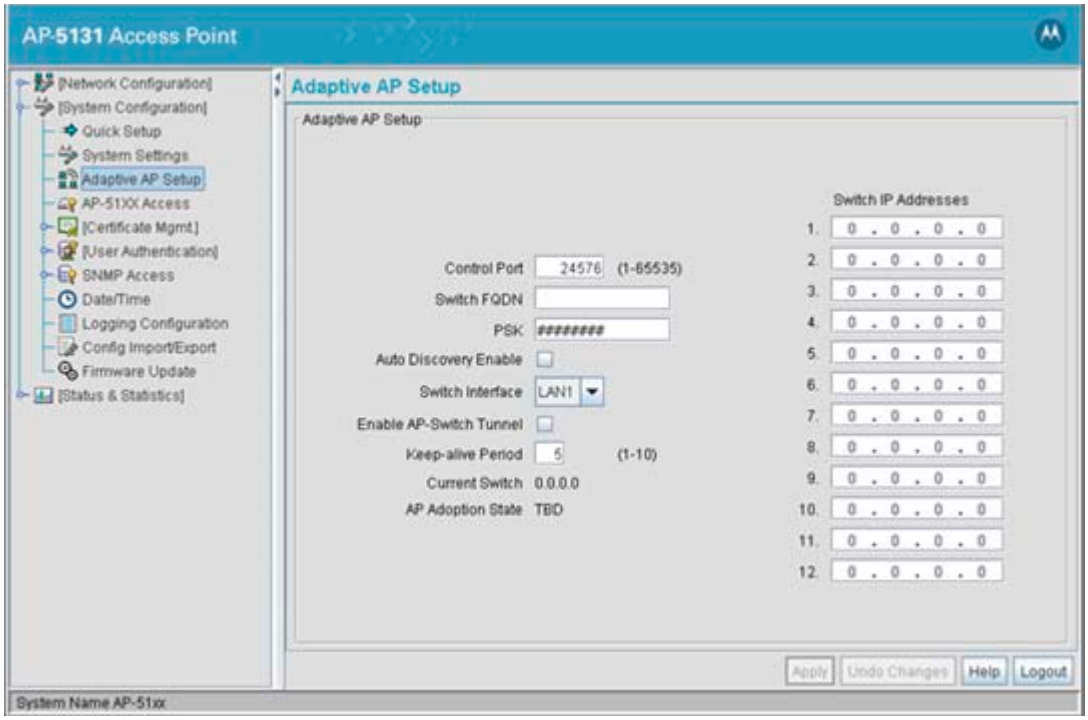
Adaptive AP Configuration

An AAP can be manually adopted by the switch, adopted using a configuration file (consisting of the adaptive parameters) pushed to the access point or adopted using DHCP options. Each of these adoption techniques is described in the sections that follow.

Manual Adoption

To manually enable the access point's switch discovery method and connection medium required for adoption:

1. Select **System Configuration** -> **Adaptive AP Setup** from the access point's menu tree.



2. Select the **Auto Discovery Enable** checkbox. Enabling auto discovery will allow the AAP to be detected by a switch once its connectivity medium has been configured (by completing steps 3-6)
3. Enter up to **12 Switch IP Addresses** constituting the target switches available for AAP connection.

   The AAP will begin establishing a connection with the first addresses in the list. If unsuccessful, the AP will continue down the list (in order) until a connection is established.
4. If a numerical IP address is unknown, but you know a switch's *Fully Qualified Domain Name* (FQDN), enter the name as the **Switch FQDN** value.
5. Select the **Enable AP-Switch Tunnel** option to allow AAP configuration data to reach a switch using a secure VPN tunnel.
6. If using IPSec as the tunnel resource, enter the **IPSec Passkey** to ensure IPSec connectivity.
7. Click **Apply** to save the changes to the AAP setup.

NOTE: The manual AAP adoption described above can also be conducted using the access point's CLI interface using the admin(system.aapsetup)> command.

Adopting an AP Using a Configuration File

To adopt an AAP using a configuration file:

1. Refer to Adopting an Adaptive AP Manually and define the AAP switch connection parameters.
2. Export the AAP's configuration to a secure location. Either import the configuration manually to other APs or the same AP later (if you elect to default its configuration). Use DHCP option 186 and 187 to force a download of the configuration file during startup (when it receives a DHCP offer).

Adopting an Adaptive AP Using DHCP Options

An AAP can be adopted to a wireless switch by providing the following options in the DHCP Offer:

Option	*Data Type*	*Value*
189	String	<Switch IP Address or Range of IP addresses separated by [, ; <space>]>
190	String	<Fully qualified Domain Name for the Wireless Switch>
191	String	<Hashed IPSec Passkey - configure on 1 AP and export to get hashed key>
192	String	<Value of "1" denotes Non-IPSec Mode and "2" denotes IPSec Mode>

NOTE: Options 189 and 192 are mandatory to trigger adoption using DHCP options. Unlike an AP300, option 189 alone won't work. These options can be embedded in Vendor Specific Option 43 and sent in the DHCP Offer.

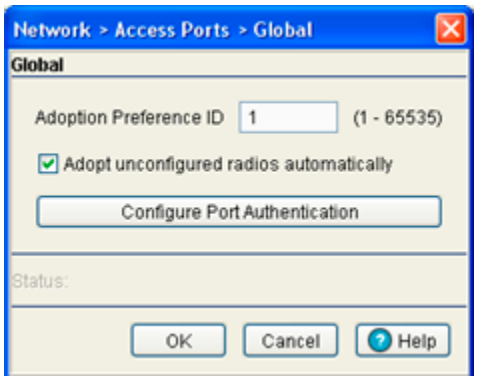
Switch Configuration

Both a WS5100 (running firmware version 3.1 or later) or a RFS6000/ RFS7000 (running firmware version 1.1 or later) require an explicit adaptive configuration to adopt an access point (if IPSec is not being used for adoption). The same licenses currently used for AP300 adoption can be used for an AAP.

Disable the switch's **Adopt unconfigured radios automatically** option and manually add AAPs requiring adoption, or leave as default. In default mode, any AAP adoption request is honored until the current switch license limit is reached.

To disable automatic adoption on the switch:

1. Select **Network** > **Access Port Radios** from the switch main menu tree.
2. Select the **Configuration** tab (should be displayed be default) and click the **Global Settings** button.



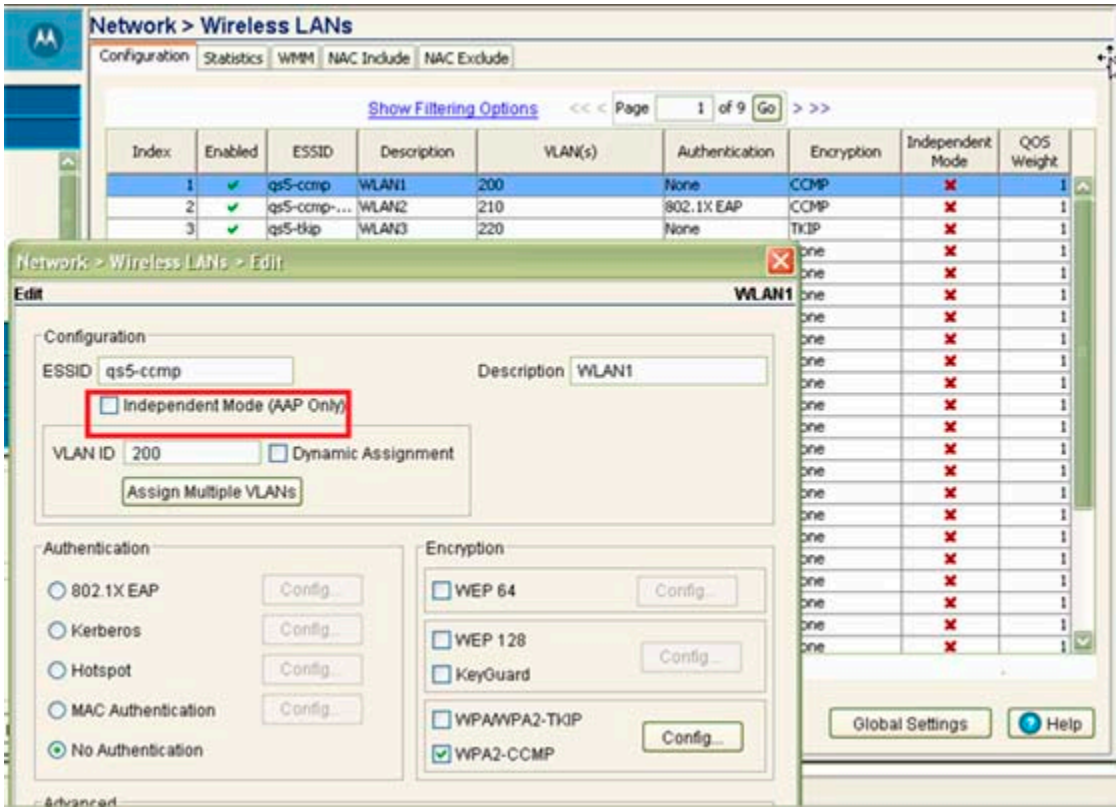
3. Ensure the **Adopt unconfigured radios automatically** option is NOT selected.

   When disabled, there is no automatic adoption of non-configured radios on the network. Additionally, default radio settings will NOT be applied to access ports when automatically adopted.

   Any WLAN configured on the switch becomes an extended WLAN by default for an AAP.
4. Select **Network** > **Wireless LANs** from the switch main menu tree.
5. Select the target WLAN you would like to use for AAP support from those displayed and click the **Edit** button.
6. Select the **Independent Mode (AAP Only)** checkbox.

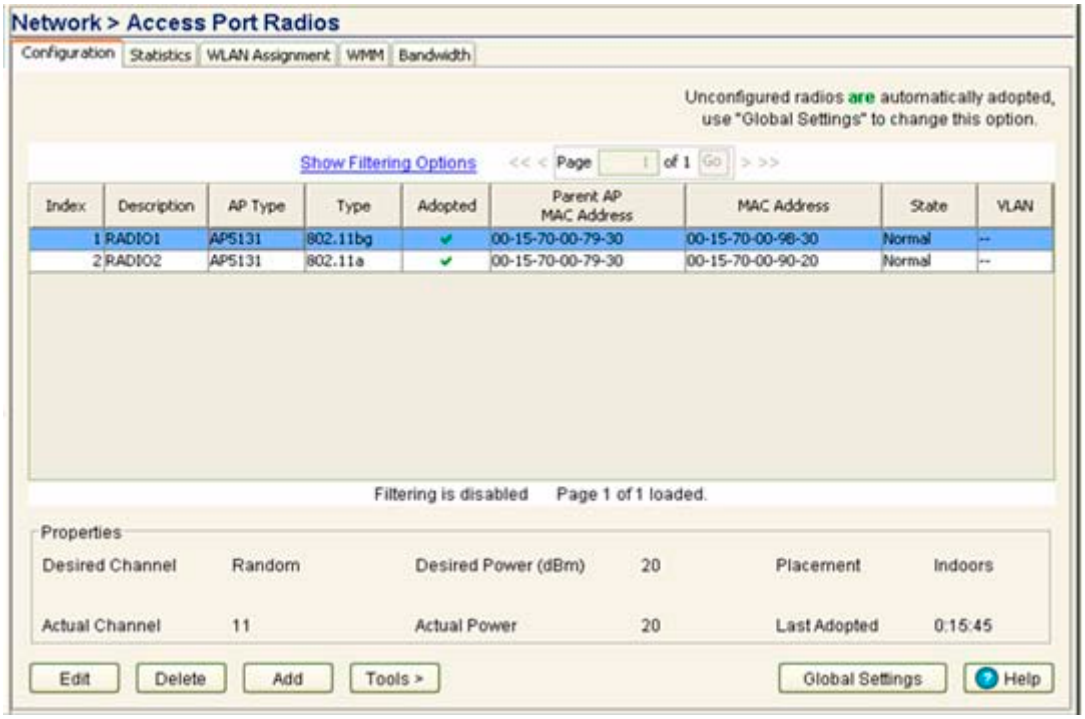
   Selecting the checkbox designates the WLAN as independent and prevents traffic from being forwarded to the switch. Independent WLANs behave like WLANs as used on a a standalone access point. Leave

this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the switch).



NOTE: Additionally, a WLAN can be defined as independent using the *wlan <index> independent* command from the config-wireless context.

Once an AAP is adopted by the switch, it displays within the switch **Access Port Radios** screen (under the Network parent menu item) as an AP-7131 within the **AP Type** column.



8.5.1.15 Adaptive AP Deployment Considerations

Before deploying your switch/AAP configuration, refer to the following usage caveats to optimize its effectiveness:

- Extended WLANs are mapped to the AP's LAN2 interface and all independent WLANs are mapped to the AP's LAN1 Interface.
- If deploying multiple independent WLANs mapped to different VLANs, ensure the AP's LAN1 interface is connected to a trunk port on the layer2/3 switch and appropriate management and native VLANs are configured.
- The WLAN used for mesh backhaul must always be an independent WLAN.
- The switch configures an AAP. If manually changing wireless settings on the AP, they are not updated on the switch. It's a one way configuration, from the switch to the AP.
- An AAP always requires a router between the AP and the switch.
- An AAP can be used behind a NAT.
- An AAP uses UDP port 24576 for control frames and UDP port 24577 for data frames.
- Multiple VLANs per WLAN, layer 3 mobility, dynamic VLAN assignment, NAC, self healing, rogue AP, MU locationing, hotspot on extended WLAN are some of the important wireless features not supported in an AAP supported deployment.

8.5.1.16 Adopting an Adaptive AP via a Switch Assisted Mesh

In a *Wireless Switch Assisted Mesh* (WAM) you must inform the switch which AP is the base bridge and which AP is the client bridge.

You must let the switch know which MAC addresses it can expect to be adopted by. In the switch, define which MAC address will be the base bridge and which MAC address will be the client bridge.

In the following example, the 802.11a radio is used for the mesh backhaul communication. AP 1 is for backhaul traffic, and AP2 is for backhaul and client connectivity.

NOTE: The radio MAC address is not the AP MAC address. The AP MAC address can be found on the back of the AP in text and in barcode.

```
 ! Here we add the 802.11b/g radio 1 of MAC of AP 1
 radio add 1 00-15-70-67-11-22 11bg aap5131
 ! Here we assign a number to the radio
 radio 1 radio-number 1
 ! Here we tell what BSSID will have what number of WLAN
 radio 1 bss 1 1
 radio 1 max-mobile-units 127
 !Here we enable the Remote Survivability Switch
 radio 1 rss enable
 !Here we add the 802.11a radio 2 of the MAC of the AP 1
 radio add 2 00-15-70-67-11-22 11a aap5131
 radio 2 radio-number 2
 !Here we tell what BSSID will have what number of WLAN. 1 = BSSID 1 of this
radio and 2 is the second WLAN
 radio 2 bss 1 2
 radio 2 max-mobile-units 127
 radio 2 rss enable
 !Here we configure that this radio is a base bridge
 radio 2 base-bridge max-clients 12
 radio 2 base-bridge enable
 radio add 3 00-15-70-67-12-54 11bg aap5131
 radio 3 bss 1 1
 radio 3 bss 2 3
 radio 3 max-mobile-units 127
 radio 3 rss enable
 radio add 4 00-15-70-67-12-54 11a aap5131
 !this WLAN assignment to the BSSID has to be the same WLAN then in the Base
bridge radio.
 radio 4 bss 1 2
 radio 4 max-mobile-units 127
 radio 4 rss enable
 !Since multiple WLAN can be on one BSSID, we have to configure what WLAN will
the Radio use to operate in mesh mode
 radio 4 client-bridge ssid mesh
 radio 4 client-bridge mesh-timeout 0
! Here we enable client bridge mode on the radio
 radio 4 client-bridge enable
```

Now that you have configured the switch, power up an out of box AP. As soon the switch detects the AP, the respective base bridge and client bridge configurations are applied to the respective APs.

8.5.1.17 Sample Swich Configuration for IPSec AAP and Independent WLAN

The following constitutes a sample RFS7000 switch configuration file supporting an AAP IPSec with Independent WLAN configuration. Please note new AAP specific CLI commands in red and relevant comments in blue.

The sample output is as follows:

```
!
! configuration of RFS7000 RFS7000-1 version 1.1.0.0-016D
!
version 1.0
!
!
aaa authentication login default none
service prompt crash-info
!
hostname RFS7000-1
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
To configure the ACL to be used in the CRYPTO MAP
!
ip access-list extended AAP-ACL permit ip host 10.10.10.250 any rule-precedence
20
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst config
name My Name
!
country-code us
logging buffered 4
logging console 7
logging host 157.235.92.97
logging syslog 7
snmp-server sysname RFS7000-1
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
!
To configure the passkey for a Remote VPN Peer - 255.255.255.255 denotes all
AAPs. 12345678 is the default passkey. If you change on the AAP, change here as
well.
!
crypto isakmp key 0 12345678 address 255.255.255.255
!
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
no service pm sys-restart
timezone America/Los_Angeles
license AP
xyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxy
xyxyxyxxyxyxyx
!
```

```
wireless
no adopt-unconf-radio enable
manual-wlan-mapping enable
wlan 1 enable
wlan 1 ssid qs5-ccmp
wlan 1 vlan 200
wlan 1 encryption-type ccmp
wlan 1 dot11i phrase 0 Symbol123
wlan 2 enable
wlan 2 ssid qs5-tkip
wlan 2 vlan 210
wlan 2 encryption-type tkip
wlan 2 dot11i phrase 0 Symbol123
wlan 3 enable
wlan 3 ssid qs5-wep128
wlan 3 vlan 220
wlan 3 encryption-type wep128
wlan 4 enable
wlan 4 ssid qs5-open
wlan 4 vlan 230
wlan 5 enable
wlan 5 ssid Mesh
wlan 5 vlan 111
wlan 5 encryption-type ccmp
wlan 5 dot11i phrase 0 Symbol123
!
To configure a WLAN as an independent WLAN
!
wlan 5 independent
wlan 5 client-bridge-backhaul enable
wlan 6 enable
wlan 6 ssid test-mesh
wlan 6 vlan 250
radio add 1 00-15-70-00-79-30 11bg aap7131
radio 1 bss 1 3
radio 1 bss 2 4
radio 1 bss 3 2
radio 1 channel-power indoor 11 8
radio 1 rss enable
radio add 2 00-15-70-00-79-30 11a aap7131
radio 2 bss 1 5
radio 2 bss 2 1
radio 2 bss 3 2
radio 2 channel-power indoor 48 8
radio 2 rss enable
radio 2 base-bridge max-clients 12
radio 2 base-bridge enable
radio add 3 00-15-70-00-79-12 11bg aap7131
radio 3 bss 1 3
radio 3 bss 2 4
radio 3 bss 3 2
radio 3 channel-power indoor 6 8
radio 3 rss enable
radio add 4 00-15-70-00-79-12 11a aap7131
radio 4 bss 1 5
radio 4 bss 2 6
radio 4 channel-power indoor 48 4
radio 4 rss enable
radio 4 client-bridge bridge-select-mode auto
```

```
radio 4 client-bridge ssid Mesh
radio 4 client-bridge mesh-timeout 0
radio 4 client-bridge enable
radio default-11a rss enable
radio default-11bg rss enable
radio default-11b rss enable
no ap-ip default-ap switch-ip
!
radius-server local
!
To create an IPSEC Transform Set
!
crypto ipsec transform-set AAP-TFSET esp-aes-256 esp-sha-hmac mode tunnel
!
To create a Crypto Map, add a remote peer, set the mode, add a ACL rule to match
and transform and set to the Crypto Map
!
crypto map AAP-CRYPTOMAP 10 ipsec-isakmp
set peer 255.255.255.255
set mode aggressive
match address AAP-ACL
set transform-set AAP-TFSET
!
interface ge1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge2
switchport access vlan 1
!
interface ge3
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge4
switchport access vlan 1
!
interface me1
ip address dhcp
!
interface sa1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
!
!
!
!
```

```
interface vlan1
ip address dhcp
!
To attach a Crypto Map to a VLAN Interface
!
crypto map AAP-CRYPTOMAP
!
sole
!
ip route 157.235.0.0/16 157.235.92.2
ip route 172.0.0.0/8 157.235.92.2
!
ntp server 10.10.10.100 prefer version 3
line con 0
line vty 0 24
!
end
```

8.6 QoS on Motorola EWLAN Products

Quality of Service (QoS) is required to support multimedia applications and advanced traffic management. WMM adds prioritized QoS capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources.

Using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network owners and Enterprise network managers to decide which data streams are most important and assign them a higher traffic priority. The Wi-Fi Alliance defined WMM as a profile of the upcoming IEEE 802.11e standard and started a certification program for WMM to satisfy the most urgent needs of the industry for a QoS solution supporting Wi-Fi networks.

WMM provides prioritized media access and is based on *Enhanced Distributed Channel Access* (EDCA). It defines four priority classes to manage traffic from different applications:

- *Voice*
- *Video*
- *Best effort*
- *Background*

Access Category	***Description***	***DSCP Tags***
WMM Voice (AC3)	Highest priority, allows concurrent voice calls	7, 6
WMM Video (AC2)	Prioritzes video traffic above all other	5, 4
WMM Best Effort (AC1)	Legacy device traffic transmission window supported	0, 3
WMM Background (AC0)	Low priority traffic without strict latency	2, 1

For additional information on QoS support on Motorola WLAN infrastructure, see:

- *WMM Operation*

- *WMM and Wi-NG*
- *VoIP*

8.6.1 WMM Operation

WMM's prioritization capabilities are based on the four access categories. The higher the AC, the higher the probability to transmit. ACs were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled switches/ APs coexist with legacy devices (devices not WMM-enabled).

Packets not assigned to a specific AC are categorized by default as having best effort priority. Applications assign each data packet to a given AC Packets are then added to one of four independent transmit queues (one per AC - voice, video, best effort, or background) in the client. The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client should be granted the *opportunity to transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each AC:

- The minimum interframe space, or *Arbitrary Inter-Frame Space Number* (AIFSN)
- The *contention window* (CW), sometimes referred to as the random backoff wait

Both values are smaller for high-priority traffic. For each AC, a backoff value is calculated as the sum of the AIFSN and a random value from zero to the CW. The value of the CW varies through time. Initially the CW is set to a value that depends on the AC.

After each collision the CW is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the CW is reset to its initial, AC dependant value.

The AC with the lowest backoff value gets the TXOP.

As frames with the highest AC tend to have the lowest backoff values, they are more likely to get a TXOP.

Once a client gains a TXOP, it is allowed to transmit for a given time that depends on the AC and the PHY rate. The TXOP limit ranges from 0.2 ms (background priority) to 3 ms (video priority) in an 802.11a/g network, and from 1.2 ms to 6 ms in an 802.11b network.

This bursting capability greatly enhances the efficiency for high data rate traffic, such as AV streaming. Also, the devices operating at higher PHY rates are not penalized when devices that support only lower PHY rates (because of the distance) contend for medium access.

Motorola infrastructure devices support WMM using:

- *WMM-UPSD (power save)*
  - Switches are WMM-UPSD capable
  - Unscheduled power save and delivery improves voice capacity and battery life for voice devices
  - SpectraLink phones support WMM-UPSD
- *MU based load balancing*
  - The switch ensures load indicators (Motorola proprietary as well as 802.11e standard specific) are sent to the MU. Motorola MUs make use of this information for load balancing
- *Admission control*

MUs are not allowed to send traffic on certain access categories (voice/video) unless they have requested the AP for permission first.

- MUs request permission using a TSPEC, which is a special 802.11 frame directed to the AP specifying the access category the MU wants to send/receive traffic in
- The switch has the choice of accepting or rejecting the TSPEC.
- The switch can be configured to allow a certain number of MUs access to each access category
- Any additional MUs that associate with that AP will not be allowed to send traffic in video or voice AC
- MUs can still use best-effort, so they don't lose service, but being a lower priority than the voice, they don't impact the performance of voice supported MUs

8.6.2 WMM and Wi-NG

WMM is supported on the Wi-NG architecture. If an application and device connect to Motorola infrastructure, it will take advantage of WMM. Implementing WMM on a particular WLAN is as simple as checking a box and specifying the QoS classification you want to associate to that device. Prioritizing voice is also a check box on the WLAN configuration page.

8.6.3 VoIP

Voice over wireless LAN (VoWLAN) technologies have been deployed by companies for little over a decade under evolving standards. For many users the early experience using *voice over IP* (VoIP) over a wireless LAN was less than optimal due to a lack of standards. Industry standards concerning VoIP have since evolved to raise the level of quality amongst vendors.

NOTE: VoIP should not be confused with voice recognition devices.

8.6.3.1 VoIP In General

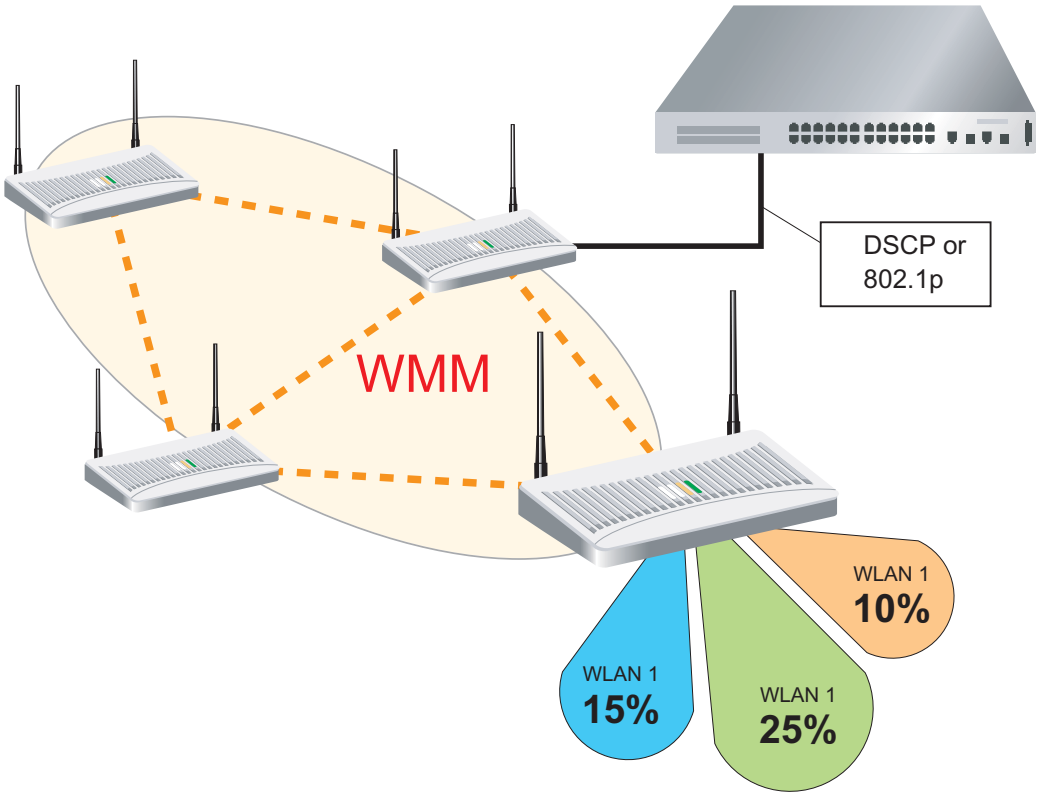
IP Telephony works by converting voice communications into data packets. Conveniently, it runs on the Ethernet LAN (or WLANs for wireless deployments), which currently supports over 96 percent of all company needs for LANs. IP Telephony enables voice communication over *Internet Protocol* (IP) networks. It unites an organization's many locations (including mobile workers) into a single converged network. It promises cost savings by combining voice and data on one network that can be centrally maintained. But more importantly, it brings advanced features and applications that enhance productivity throughout an organization.

A VoIP telephony system is built on a single, shared IP-based packet network. A packet-based network provides a foundation that can carry many types of information, including data, audio, and video. The challenge with such a network is separating and prioritizing the various types of traffic. A VoIP telephony system provides services and reliability comparable to traditional telephony systems. This converged network offers cost benefits, as you can install and administer a voice and data network together and use an existing IP network for voice traffic. Integrating voice and data on one network infrastructure makes it easier to deploy business applications that bring together voice, data, and video across the enterprise.

When networks are built on industry-standard operating systems and protocols, rather than on proprietary systems, it becomes simpler and less costly for network planners to integrate products from multiple vendors and reuse existing equipment. The convergence of wireless voice and data networks enables the implementation of voice-enabled WLANs.

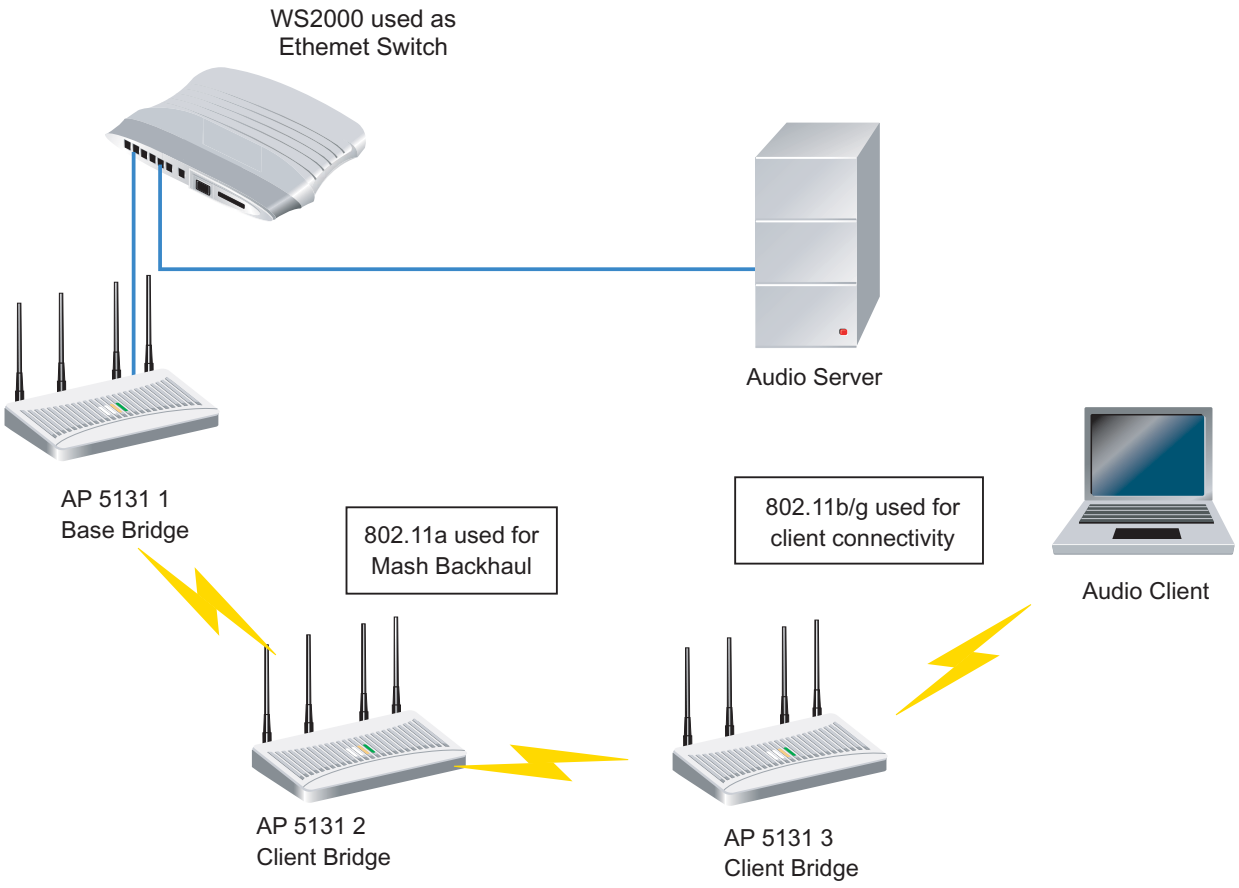
8.7 WMM over an AP-5131 Mesh Connection

Mesh nodes support WMM to ensure QoS for data traversing the mesh network. WLAN bandwidth management allows bandwidth partitioning between WLANs and the mesh network.



8.7.1 QoS over the AP51XX Mesh

The following (on the next page) shows the packet flow within a typical AP-5131 QoS deployment:



In the above example, an 802.11a radio as is used to ensure mesh backhaul connectivity and the 802.11b/g radio supports client connectivity.

NOTE: Even with 2 wireless hops, QoS is secured. This enables excellent VoIP conversations over a 2 hop mesh network.

The following is a list of used MAC addresses. This is provided to better analyze the traces used.

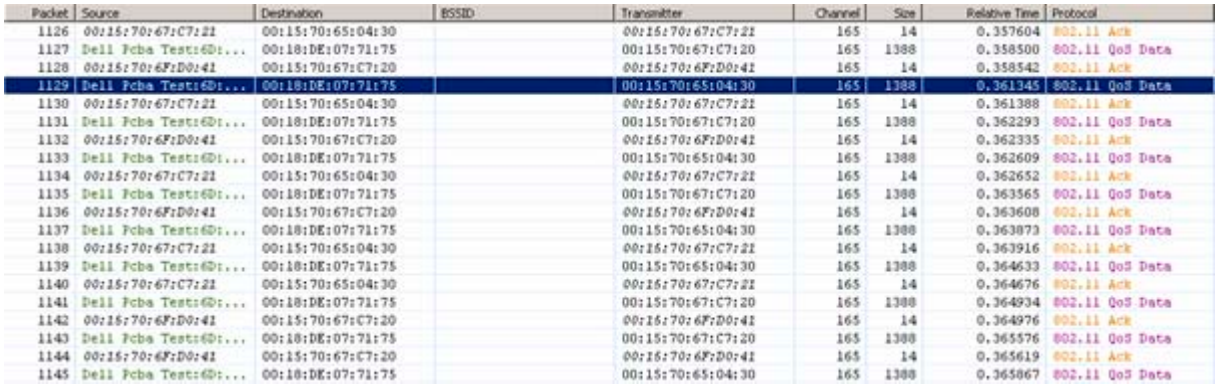
Device	***MAC***	***802.1a MAC***	***802.11bg MAC***	***ESSID***
AP5131_1	00:15:70:59:77:7C	00:15:70:65:04:30		mesh (802.11a)
AP5131_2	00:15:70:6D:1F:E8	00:15:70:67:C7:20		mesh (802.11a)
AP5131_3	00:15:70:68:41:DE	00:15:70:6F:D0:40	00:15:70:6F:C2:80	mesh (802.11a) client (802.11b/g)
Audio Server	00:0D:56:6D:3A:C5			
Audio Server	00:18:DE:07:71:75			

The 802.11a radio is set to use channel 165, and the 802.11b/g radio is set to use channel 6. WMM is set to use the default WMM settings.

By looking into an individual packet, you can see DSCP is set for voice:

```
P1

Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        1362
  Timestamp:            13:40:12.507377000 06/11/2008
Ethernet Header
  Destination:          00:18:DE:07:71:75
  Source:               00:0D:56:6D:3A:C5  Dell Pcba Test:6D:3A:C5
  Protocol Type:        0x0800  IP
IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5  (20 bytes)
  Differentiated Services:%11011000
                        .... ..00 Not-ECT

  Total Length:         1344
  Identifier:           60034
  Fragmentation Flags:  %010
                        0.. Reserved
                        .1. Do Not Fragment
                        ..0 Last Fragment

  Fragment Offset:      0  (0 bytes)
  Time To Live:         64
  Protocol:             17  UDP
  Header Checksum:      0xE02C
  Source IP Address:    181.1.0.5
  Dest. IP Address:     181.1.0.30
UDP - User Datagram Protocol
  Source Port:          46588
  Destination Port:     1234  search-agent
  Length:               1324
  UDP Checksum:         0x66ED
Application Layer
  Data Area:
  G.E..wp.:..-..8.  47 00 45 16 E4 77 70 17 3A BE 17 2D 9D 07 38 0D
  ....B...%g..:...  0F 90 E8 DD 42 C0 07 0F 25 67 81 DB 3A F6 D1 8E
  W9ly..c?X...jq..  57 39 6C 79 98 8D 63 3F 58 DE 80 E1 6A 71 F1 DD
  ....l3...}s...d.  F3 13 A0 D7 6C 33 01 FC 1C 7D 73 B0 A9 9D 64 1E
  ...C/'..z.9..\..  AB E9 18 43 2F 27 E3 9C 7A B9 39 B8 1C 5C 97 CE
  .:....8.....Gm..  C3 3A 02 D4 C2 F7 38 9F 06 F6 1E C1 47 6D 06 AF
  .e..0...S8...B..  BE 65 87 F6 30 CF 88 E7 53 38 1D 02 12 42 C3 AF
  m......z...G8\L&  6D 99 A1 1B A5 96 8E 7A D7 80 06 47 38 5C 4C 26
….

FCS - Frame Check Sequence
```

```
  FCS:                    0xBE4C6B6B
```



Packet	Source	Destination	BSSID	Transmitter	Channel	Size	Relative Time	Protocol
1126	00:15:70:67:C7:21	00:15:70:65:04:30		00:15:70:67:C7:21	165	14	0.357604	802.11 Ack
1127	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:67:C7:20	165	1388	0.358500	802.11 QoS Data
1128	00:15:70:6F:D0:41	00:15:70:67:C7:20		00:15:70:6F:D0:41	165	14	0.358542	802.11 Ack
1129	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:65:04:30	165	1388	0.361345	802.11 QoS Data
1130	00:15:70:67:C7:21	00:15:70:65:04:30		00:15:70:67:C7:21	165	14	0.361388	802.11 Ack
1131	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:67:C7:20	165	1388	0.362293	802.11 QoS Data
1132	00:15:70:6F:D0:41	00:15:70:67:C7:20		00:15:70:6F:D0:41	165	14	0.362335	802.11 Ack
1133	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:65:04:30	165	1388	0.362609	802.11 QoS Data
1134	00:15:70:67:C7:21	00:15:70:65:04:30		00:15:70:67:C7:21	165	14	0.362652	802.11 Ack
1135	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:67:C7:20	165	1388	0.363565	802.11 QoS Data
1136	00:15:70:6F:D0:41	00:15:70:67:C7:20		00:15:70:6F:D0:41	165	14	0.363608	802.11 Ack
1137	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:65:04:30	165	1388	0.363873	802.11 QoS Data
1138	00:15:70:67:C7:21	00:15:70:65:04:30		00:15:70:67:C7:21	165	14	0.363916	802.11 Ack
1139	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:65:04:30	165	1388	0.364633	802.11 QoS Data
1140	00:15:70:67:C7:21	00:15:70:65:04:30		00:15:70:67:C7:21	165	14	0.364676	802.11 Ack
1141	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:67:C7:20	165	1388	0.364934	802.11 QoS Data
1142	00:15:70:6F:D0:41	00:15:70:67:C7:20		00:15:70:6F:D0:41	165	14	0.364976	802.11 Ack
1143	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:67:C7:20	165	1388	0.365576	802.11 QoS Data
1144	00:15:70:6F:D0:41	00:15:70:67:C7:20		00:15:70:6F:D0:41	165	14	0.365619	802.11 Ack
1145	Dell Pcba Test:6D:...	00:18:DE:07:71:75		00:15:70:65:04:30	165	1388	0.365867	802.11 QoS Data

Observe the two transmitter MAC addresses. These MAC addresses are the BSSIDs from the two client bridges (AP5131_2 and AP5131_3).

When taking a closer look at the packet, observe the *wired* DSCP setting has been translated into the respective WMM access category for voice. Observe this in the packet between the base bridge (AP5131_1) and client bridge (AP5131_2); as well as between base bridge/client bridge (AP5131_2) and client bridge (AP5131_3).

Packets between the base bridge (AP5131_AP1) and client bridge (AP5131_2) appear as follows:

```
Packet Info
  Flags:                  0x00000000
  Status:                 0x00000000
  Packet Length:          1388
  Timestamp:              13:52:28.552066000 06/11/2008
  Data Rate:              108 54.0 Mbps
  Channel:                165  5825MHz  802.11a
  Signal Level:           54%
  Signal dBm:             -57
  Noise Level:            0%
  Noise dBm:              -104
802.11 MAC Header
  Version:                0
  Type:                   %10  Data
  Subtype:                %1000  QoS Data
Frame Control Flags:      %00000011
                          0... .... Non-strict order
                          .0.. .... Non-Protected Frame
                          ..0. .... No More Data
                          ...0 .... Power Management - active mode
                          .... 0... This is not a Re-Transmission
                          .... .0.. Last or Unfragmented Frame
                          .... ..1. Exit from the Distribution System
                          .... ...1 To the Distribution System


  Duration:               44  Microseconds
  Receiver:               00:15:70:67:C7:21
```

```
  Transmitter:          00:15:70:65:04:30
  Destination:          00:18:DE:07:71:75
  Seq Number:           2012
  Frag Number:          0
  Source:               00:0D:56:6D:3A:C5  Dell Pcba Test:6D:3A:C5
  QoS Control Field:    %0000000000000110
                        xxxxxxxx x.......  Reserved
                        ........ .00.....  Ack: Normal Acknowledge
                        ........ ...0....  EOSP: Not End of Triggered
  Service Period
                        ........ ....0...  Reserved
                        ........ .....110  UP: 6 - Voice

802.2 Logical Link Control (LLC) Header
  Dest. SAP:            0xAA  SNAP

  Source SAP:           0xAA  SNAP
  Command:              0x03  Unnumbered Information
  Vendor ID:            0x000000
  Protocol Type:        0x0800  IP


IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5  (20 bytes)
  Differentiated Services:%11011000
                        .... ..00  Not-ECT

  Total Length:         1344
  Identifier:           18755
  Fragmentation Flags:  %010
                        0..  Reserved
                        .1.  Do Not Fragment
                        ..0  Last Fragment

  Fragment Offset:      0  (0 bytes)
  Time To Live:         64
  Protocol:             17  UDP
  Header Checksum:      0x816C
  Source IP Address:    181.1.0.5
  Dest. IP Address:     181.1.0.30
UDP - User Datagram Protocol
  Source Port:          40039
  Destination Port:     1234  search-agent
  Length:               1324
  UDP Checksum:         0x7AF1
Application Layer
  Data Area:
  G.E........m....  47 00 45 1C 98 92 9C 8D 8A C8 EC 6D CE 03 A0 0D
  ........0.....Z@  00 19 E0 07 A0 0D 80 A9 30 02 E0 13 93 12 5A 40
```

```
  .A..)%.4.ax.....  A1 41 89 0D 29 25 A4 34 A2 61 78 A4 80 1F 92 CA
  A](...[.......T.  41 5D 28 18 AF F1 5B 15 91 D8 DB D1 F7 C2 54 BC
  .8...."...v.j..  B5 38 0C E9 F7 CB 22 2C 0E C7 B3 76 1C 6A 8D 1C
  CA 02……..
  0.>.....p...(...  30 D7 3E CD 98 8D C0 07 70 7F 85 07 28 07 C6 D3
  ..-j.c....;~.;^=  E4 EE 2D 6A DD 63 C4 1C C6 2E 3B 7E 00 3B 5E 3D
  ..p....;9.......  DD 9D 70 FD C0 E3 98 3B 39 1A 1B D9 C2 96 A0 0F
  9.%p}.y.+(x.%...  39 EC 25 70 7D D6 79 1B 2B 28 78 A2 25 10 8C C2
  ...,              07 A8 F1 2C
FCS - Frame Check Sequence
  FCS:                0x07AB5063
```

Packets between the base bridge/client bridge (AP5131_AP2) and the client bridge (AP5131_3) appear as follows:

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        1388
  Timestamp:            13:52:28.553014000 06/11/2008
  Data Rate:            108 54.0 Mbps
  Channel:              165  5825MHz  802.11a
  Signal Level:         72%
  Signal dBm:           -44
  Noise Level:          0%
  Noise dBm:            -104
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %1000  QoS Data
Frame Control Flags:    %00000011
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...1 To the Distribution System

  Duration:             44  Microseconds

  Receiver:             00:15:70:6F:D0:41
  Transmitter:          00:15:70:67:C7:20
  Destination:          00:18:DE:07:71:75
  Seq Number:           3373
  Frag Number:          0
  Source:               00:0D:56:6D:3A:C5  Dell Pcba Test:6D:3A:C5
  QoS Control Field:    %0000000000000110
                        xxxxxxxx x....... Reserved
                        ........ .00..... Ack: Normal Acknowledge
                        ........ ...0.... EOSP: Not End of Triggered Service
                        ........ ....0... Reserved
                        ........ .....110 UP: 6 - Voice

802.2 Logical Link Control (LLC) Header

  Dest. SAP:            0xAA  SNAP
  Source SAP:           0xAA  SNAP
  Command:              0x03  Unnumbered Information
  Vendor ID:            0x000000
  Protocol Type:        0x0800  IP
```

```
IP Header - Internet Protocol Datagram
  Version:                4
  Header Length:          5  (20 bytes)
  Differentiated Services:%11011000
                          .... ..00 Not-ECT

  Total Length:           1344
  Identifier:             18755
  Fragmentation Flags:    %010
                          0.. Reserved
                          .1. Do Not Fragment
                          ..0 Last Fragment

  Fragment Offset:        0  (0 bytes)
  Time To Live:           64
  Protocol:               17  UDP
  Header Checksum:        0x816C
  Source IP Address:      181.1.0.5
  Dest. IP Address:       181.1.0.30
UDP - User Datagram Protocol
  Source Port:            40039
  Destination Port:       1234  search-agent
  Length:                 1324
  UDP Checksum:           0x7AF1
Application Layer
  Data Area:
  G.E........m....  47 00 45 1C 98 92 9C 8D 8A C8 EC 6D CE 03 A0 0D
  ........0.....Z@  00 19 E0 07 A0 0D 80 A9 30 02 E0 13 93 12 5A 40
  .A..)%.4.ax.....  A1 41 89 0D 29 25 A4 34 A2 61 78 A4 80 1F 92 CA
  A](...[.......T.  41 5D 28 18 AF F1 5B 15 91 D8 DB D1 F7 C2 54 BC
  A6 7E DD..........................................................
  c.7.8.O..9...q..  63 CC 37 0F 38 8B 4F BE C6 39 E3 D5 D6 71 E6 8B
  '....uGa.\.n.O..  27 D3 ED CC E0 75 47 61 DD 5C F8 6E 8C 4F CA 02
  0.>.....p...(...  30 D7 3E CD 98 8D C0 07 70 7F 85 07 28 07 C6 D3
  ..-j.c....;~.;^=  E4 EE 2D 6A DD 63 C4 1C C6 2E 3B 7E 00 3B 5E 3D
  ..p....;9.......  DD 9D 70 FD C0 E3 98 3B 39 1A 1B D9 C2 96 A0 0F
  9.%p}.y.+(x.%...  39 EC 25 70 7D D6 79 1B 2B 28 78 A2 25 10 8C C2
  ...,              07 A8 F1 2C
FCS - Frame Check Sequence
  FCS:                    0x49398A63
```

Lastly, observe the packet sent to the audio client. Observe the QoS received over the mesh connection will be translated to the client access WLAN:

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000001
  Packet Length:        1382
  Timestamp:            14:24:29.218469000 06/11/2008
  Data Rate:            108 54.0 Mbps
  Channel:              6  2437MHz  802.11bg
  Signal Level:         84%
  Signal dBm:           -36
  Noise Level:          11%
  Noise dBm:            -89
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %1000  QoS Data
Frame Control Flags:    %00000010
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             44  Microseconds
  Destination:          00:18:DE:07:71:75
  BSSID:                00:15:70:6F:C2:80
  Source:               00:0D:56:6D:3A:C5  Dell Pcba Test:6D:3A:C5
  Seq Number:           2982
  Frag Number:          0
  QoS Control Field:    %0000000000000110
                        xxxxxxxx x....... Reserved
                        ........ .00..... Ack: Normal Acknowledge
                        ........ ...0.... EOSP: Not End of Triggered Service
                        ........ ....0... Reserved
                        ........ .....110 UP: 6 - Voice

802.2 Logical Link Control (LLC) Header
  Dest. SAP:            0xAA  SNAP
  Source SAP:           0xAA  SNAP
  Command:              0x03  Unnumbered Information
  Vendor ID:            0x000000
  Protocol Type:        0x0800  IP
IP Header - Internet Protocol Datagram
  Version:              4
```

```
  Header Length:        5  (20 bytes)
  Differentiated Services:%11011000
                        .... ..00 Not-ECT

  Total Length:         1344
  Identifier:           42758
  Fragmentation Flags:  %010
                        0.. Reserved
                        .1. Do Not Fragment
                        ..0 Last Fragment

  Fragment Offset:      0  (0 bytes)
  Time To Live:         64
  Protocol:             17  UDP
  Header Checksum:      0x23A9
  Source IP Address:    181.1.0.5
  Dest. IP Address:     181.1.0.30
UDP - User Datagram Protocol
  Source Port:          59633
  Destination Port:     1234  search-agent
  Length:               1324
  UDP Checksum:         0xBD42
Application Layer
  Data Area:
  G.E.............  47 00 45 1E 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  ....              00 00 00 00
FCS - Frame Check Sequence
  FCS:                  0x572B18A8
```

9

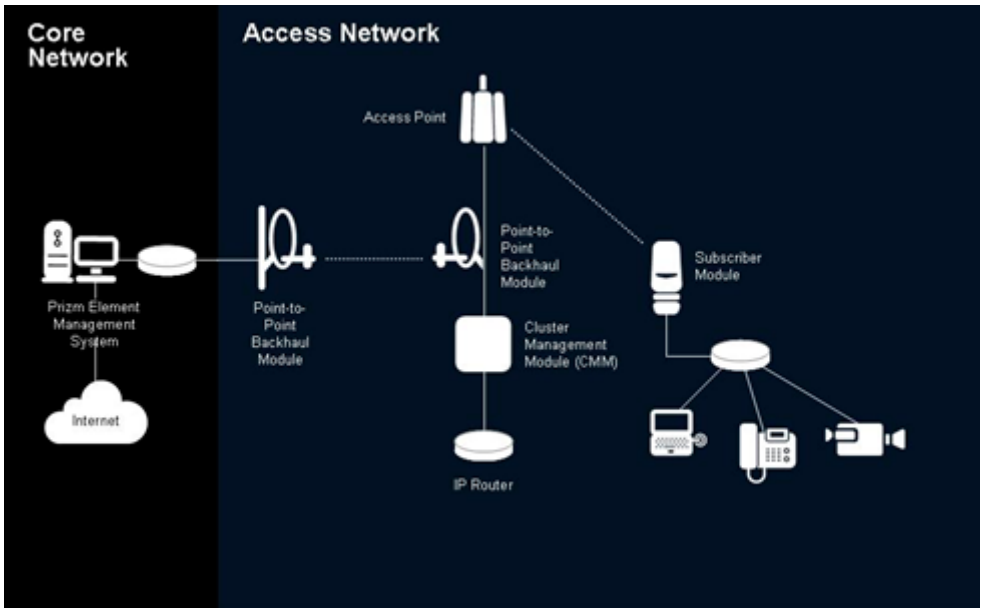
Canopy Systems

The *Canopy*® system, Motorola's innovative wireless broadband solution, is an ideal technology for developing, enhancing and extending advanced broadband networks and services. Canopy makes the delivery of high-demand technologies (like broadband Internet access, voice over IP, video services, security surveillance and E1/T1 capabilities) quicker and less expensive.

Canopy wireless broadband technology combines carrier-grade toughness with exceptional performance, security, ease-of-use and cost effectiveness. It significantly reduces the time to design and deploy new commercial and Enterprise broadband networks. It also seamlessly integrates with existing network systems and management tools to make extending and augmenting existing service simpler and less cost-intensive.

The Canopy platform offers one of lowest total costs of ownership in the industry, and can deliver proof of business case with ROIs in just six-to-twelve months.

The Canopy system leverages Motorola's more than 75 years of radio knowledge, experience and leadership. Motorola's dedication to creating and maintaining trusted relationships over the long-term means Canopy platform users are assured of high levels of worldwide service and support as their networks grow over the years.



The Motorola Canopy system is a *Broadband Wireless Access* (BWA) solution for extending an existing network to provide broadband services to new users. The system provides a wireless Ethernet connection which can be used to transport voice, video and data in channelized or unchannelized formats. Modules are

available to support *Line of Sight* (LOS) and *Non-Line of Sight* (NLOS) point-to-point links and point-to-multipoint last mile access solutions. With a broad array of backhaul (PTP module), access point (AP) and *subscriber modules* (SM), the system can be configured to meet the needs of business and residential network users.

For more information on the Motorola Canopy system, refer to:

- *Benefits of the Canopy System*
- *Applications*
- *Canopy's Key Attributes*

9.1 Benefits of the Canopy System

Service providers can enhance their customer base and revenues by extending the network to reach new business and residential subscribers beyond the reach of broadband offerings. Canopy systems can:

- Complement existing broadband networks to reach customers in new territories, whether adjacent to an existing network or in a completely new region
- Offer wireless broadband services to existing subscribers currently using dial-up; alternative to other equipment like DSL and cable
- Extend network geography into new, under served areas
- Rapidly mass-deployed, value-based broadband

Enterprises can establish cost-effective links to campus locations or remote branch offices at a fraction of the cost of leasing lines or deploying wireline broadband systems. Canopy systems enable:

- Rapid access to business information between locations
- Cost-effective; substantially less than cost of leased-line alternatives - no recurring monthly fee
- Wireless infrastructures to connect indoor WLANs, creating a completely wireless IP network and connecting inside to outside

Government network operators can establish cost-effective links for public safety, public service, and public access. Government Canopy deployments can:

- Rapidly deploy video surveillance and data connectivity for public safety
- Create a cost effective data network for public works
- Create and infrastructure for community wide public access

9.2 Applications

The Canopy system provides a wireless broadband connection for IP traffic. Canopy modules can be used to complement DSL, Cable, Fiber and other wireless networks or used in stand alone configurations.

- *Data Transfers* - The Canopy platform brings powerful radio technology to Enterprise communications applications, making deploying and delivering low-cost broadband access faster and easier than ever before. It provides the performance, versatility and ease-of-use that enable Enterprise environments-including corporate, municipal, health care, education and more-to improve communication, productivity, security and *return on investment (*ROI).
- *Video* - IP-based video surveillance is revolutionizing the way organizations, municipalities and institutions are protecting their property, personnel and proprietary assets. Motorola's proven Canopy

wireless technology helps you and your customers join the revolution. Compared to analog or hybrid systems, IP-based solutions provide a number of crucial advantages, including:

- Real-time situational awareness and response
- Remote monitoring and accessibility
- Faster, lower cost deployments
- Leveraging existing networks
- Maximizing the benefits of smart cameras and software
- Optimized ROI
- Digital image encryption for security

Voice - Canopy modules can be used to transport Voice over IP (VoIP) services as a PBX extension when IP phones and typical hubs are used at the customer premises.

9.3 Canopy's Key Attributes

In today's crowded broadband communications marketplace, no system can match the Canopy platform's combination of advanced technology, simplified configuration, rapid deployment and remarkable cost effectiveness. The system enables ISPs to differentiate themselves, create competitive advantages and attract residential and business customers, even in hard-to-reach geographic areas.

Some of the key attributes of the Canopy system include:

- *Simple Network Design*
- *Superior Performance*
- *Exceptional Security*
- *Incredible Speed*
- *Interference Tolerance*
- *Scalability*
- *Return on Investment*
- *Flexible Configuration Options*
- *Canopy Solution Elements*
- *Point-to-Multipoint Access*
- *Point to Point Links*
- *Deploying Canopy Networks*
- *Reference Architectures for Access Networks*
- *Reliable, Secure Network Extensions for Network Operators*
- *Facts and Fiction about Broadband Wireless Access*
- *Network Deployment*
- *Network Design Trade-offs*
- *Canopy System Reliability*

9.3.1 Simple Network Design

The Canopy system's intelligent protocols streamline deployment and operation. A simple network design allows the system to complement your existing network, and makes it easy to install. There is no need to run overhead or in-ground wire, install microwave or software. The equipment is intuitive and efficient, providing built-in installation and deployment assistance that makes it faster to get up and running, often in a matter of hours or days instead of weeks or months.

9.3.2 Superior Performance

The Canopy solution delivers superior performance using a modulation scheme that improves the quality of data delivery and mitigates interference from other systems. The system's wireless signals are highly effective in penetrating obstacles and avoiding obstructions, making it as efficient in dense urban environments as it is in suburban areas or rural locations. The platform provides last mile access in a variety of spectrum choices, ensuring exceptional broadband performance no matter which spectrum is best for your network.

9.3.3 Exceptional Security

The Canopy platform also offers security with over-the-air *Data Encryption Standar*d (DES) encryption and is also available with *Advanced Encryption Standard* (AES) capabilities, providing 128-bit encryption, to ensure secure data delivery and exceptional reliability.

9.3.4 Incredible Speed

The Canopy platform's upload and download speeds are as fast as or faster than virtually every other service available today. The point-to-multipoint Canopy system offers speeds from 512 Kbps to 21 Mbps (aggregate data rates) and the Motorola point-to-point bridges deliver from 7.5 to 300 Mbps (aggregate data rates) to your user now. Of course, upload and download speeds are affected by several factors so actual speeds may vary, but the potential to offer an incredible broadband experience is inherent in the Canopy system.

9.3.5 Interference Tolerance

Because of its unique signal synchronization, the Canopy system has a high level of tolerance to self-interference. The Canopy system provides reliable service even when the APs are placed close together.

9.3.6 Scalability

The Canopy system scales to meet network growth so that throughput remains consistent as new subscribers are added to the network.

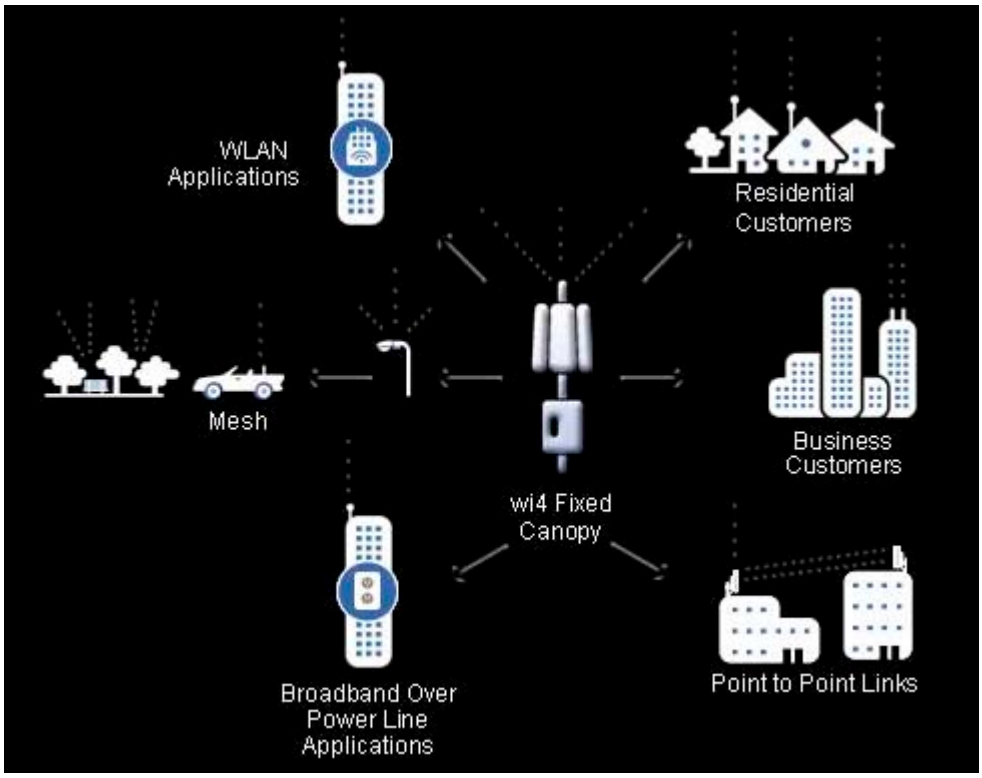
9.3.7 Return on Investment

Low infrastructure costs and wireless last mile connectivity yield a payback in terms of months. Motorola is glad to provide detailed case studies of customers who have successfully deployed the Canopy system in a variety of applications.

9.3.8 Flexible Configuration Options

The Canopy system’s configuration options meet and exceed both provider and customer expectations. The platform can be configured as a single-site point-to-multipoint system that supports subscribers for distances up to 15 miles (24 kilometers). The Motorola point-to-point series of wireless Ethernet bridges

increase delivery range up to 124 miles (200 kilometers). In addition, the system includes interfaces making it to easily integrate with standard network management tools and billing systems, as well as the diagnostic capabilities needed to remotely monitor the network.



Canopy solutions are used in unlicensed bands. Canopy products have been designed to optimize interference tolerance. With GPS synchronization, they provide superior performance in areas where there is noise in the spectrum. These solutions can be deployed as an access network, or as a capacity injection layer for other last mile solutions.

Canopy solutions are proven reliable, cost effective proprietary solutions. To date, these solutions comprise the largest deployment of MOTOwi4 modules.

For more information on MOTOwi4, see *MOTOwi4 Wireless Broadband Solutions on page 9-24* and *MOTOwi4 Fixed Solutions on page 9-24*.

9.3.9 Canopy Solution Elements

An access point module distributes network or Internet services in a 60° sector to up to 200 subscribers. The AP is configurable through a Web interface. The *subscriber module* (SM) is a *customer premises equipment* (CPE) device that extends network or Internet services by communication with an AP. The SM is configurable through a web interface.

9.3.9.1 Access Point and Subscriber Modules

Access point modules are available in a wide range of frequencies from 900 MHz to 5.9 GHz. These modules are available with integrated antennas for ease of installation, or are available with versions to enable network operators to configure their network to meet their specific requirements. AP's are also available with higher performance options to provide higher throughput.

Subscriber modules are CPE equipment that establish connectivity at the subscriber's location. These modules are simple to install and can provide connectivity for a single device or a downstream WLAN network. Subscriber modules are available in a wide range of frequencies from 900 MHz to 5.9 GHz. These modules are available with integrated antennas for ease of installation, or are available with versions to enable network operators to configure their network to meet their specific requirements. 900 MHz subscriber modules have an Indoor option. Subscriber modules can be equipped with passive range extenders to boost performance to establish connectivity to remote locations. Subscriber modules are also available with higher performance options to provide higher throughput and NLOS connectivity

9.3.9.2 Point to Point (PTP) Backhaul

PTP modules point-to-point connectivity in either:

- A standalone or wired link to another PTP
- A wired link through a cluster management module to an AP cluster

9.3.9.3 Element Management

Canopy Prizm software allows you to use:

- A primary server to distribute bandwidth resources per subscriber, requires subscriber modules to authenticate per AP, and deny service to unauthorized subscriber modules
- A secondary server to redundantly store identical subscriber module bandwidth, authentication data and govern if the primary server goes out of service
- An optional tertiary server to do the same if both the primary and secondary servers go down

9.3.9.4 Cluster Management Module (CMM)

The *Cluster Management Module* (CMM) 4 provides power, GPS timing, and networking connections for an AP cluster. If the CMM is also connected to a PTP module, the CMM is the central point of connectivity for the entire site. The CMM can connect as many modules and an Ethernet feed. The CMM requires two cables for each connected module:

- One cable provides Ethernet communications and power (this cable terminates in an RJ-45 connector)
- The other cable provides GPS synchronization (sync), GPS status, and time and date in a serial interface (this cable terminates in an RJ-11 connector)

9.3.9.5 Power Connection and Cables

A 110-V AC input Motorola ACPS110-03 power supply provides 24-V/400-mA power in Canopy networks in U.S.A., NOM, and Canada. The Canopy system is typically installed in outside infrastructure platforms, such as radio towers and roof tops. Motorola recommends shielded outdoor cables that adhere to Category 5 and 5e standards for the installation of Canopy AP and PTP modules.

9.3.9.6 Coverage Extender

A coverage extender provides simple, high performance expansion of a Canopy network to serve potential end-customers outside of the current wireless coverage range. A coverage extender enables service providers to deliver reliable VoIP and data service in areas previously not effectively covered.Potential customers could be located beyond the *line-of-sight* (LOS) of the AP or AP cluster, or in a dead-zone, blocked by obstructions.

9.3.9.7 Reflector

A 27RD passive reflector dish extends range and focuses the beam into a narrower angle. The internal patch antenna of the module illuminates the canopy passive reflector dish from an offset position. The module support tube provides the proper angle for this offset.

9.3.9.8 LENS

A canopy LENS antenna enables service providers to provide reliable data and VOIP services in areas that could not previously be reached due to range limitations. By increasing the range and focusing the antenna beam, a LENS allows service providers to reach more subscribers and results in a reduction of external RF noise. This compact yet durable product easily mounts directly onto existing Canopy radios and requires no additional mounting hardware.

Surge Suppressor

A 200SS, 300SS, or 600SS surge suppressor provides a path to ground (protective earth) that protects connected subscriber home equipment from near-miss lightning strikes.

9.3.10 Point-to-Multipoint Access

9.3.10.1 Throughput and Range

The Canopy BWA system (with its hundreds of engineering development years, more than 60 patents, and hundreds of commercially deployed networks in over 120 countries) delivers broadband wireless access for all applications. Designed to optimize consistent performance across the network, the Canopy provides reliable throughput to all network users in the following deployments:

- Small and large number network subscribers
- Subscribers located both near and far from an access point
- Networks supporting varying types of traffic

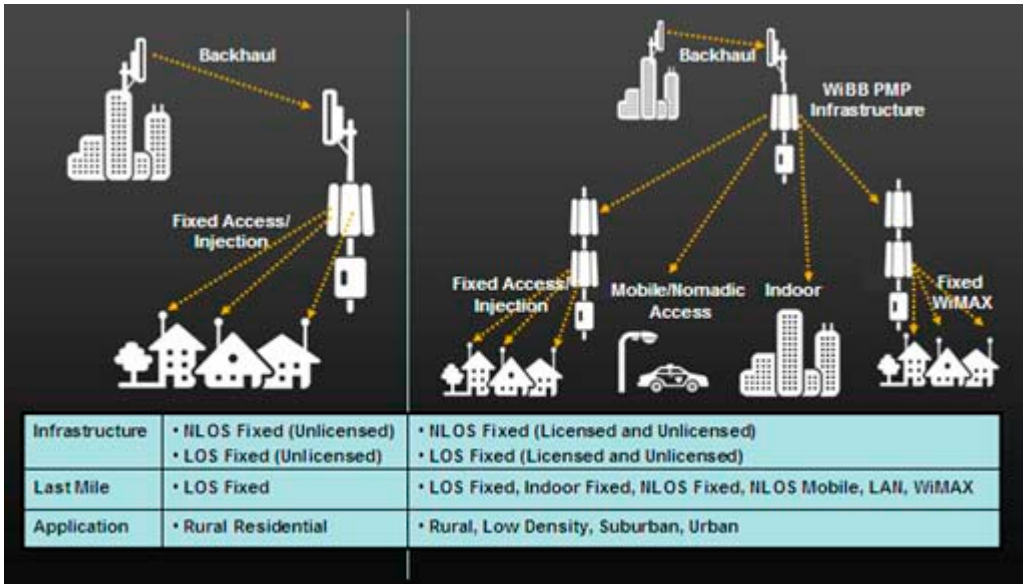
The operating range and data throughput of wireless systems is dependant on terrain, foliage and background RF energy, among other conditions. Canopy modules are designed to provide reliable communication with a minimal throughput disruption as distance increases and as subscribers are added. The Canopy system's unique signaling provides a consistent data rate and throughput across the entire service area.

9.3.10.2 Access Networks

Canopy system access points and subscriber modules comprise an access network. APs are the distribution head. Each AP can serve up to 200 subscribers in a 60 degree arc. APs can be clustered in groups of up to six providing, 360 degree *line of sight* (LOS) coverage for a community of up to 1,200 subscribers. Subscriber modules are installed at the subscriber location. With the new Canopy 400 series AP, subscriber modules products provide *near-line-of-sight* (nLOS) and *non-line-of-sight* (NLOS) performance through the use of OFDM technology, longer cyclic prefixes, and higher gain antenna solutions. The improvement is seen most in multi-path environments where the signal is reflected off other buildings and objects. Improvements in penetration of foliage are also possible. In general, OFDM technology improves performance in near- and non-line-of-sight environments. This makes it possible to provide connectivity in areas where trees or other items may be present. However, the power level limits specified in the standards (27dBm EIRP for 10MHz channel in 5.4GHz) and the fundamental physical propagation characteristics of 5 GHz prevent the use in high path loss applications.

9.3.10.3 Network Infrastructure

A Canopy network can be deployed to provide bandwidth to an access last mile application. Canopy networks can supply connectivity for WiMAX, WLAN, mesh and other networks.



Infrastructure	• NLOS Fixed (Unlicensed) • LOS Fixed (Unlicensed)	• NLOS Fixed (Licensed and Unlicensed) • LOS Fixed (Licensed and Unlicensed)
Last Mile	• LOS Fixed	• LOS Fixed, Indoor Fixed, NLOS Fixed, NLOS Mobile, LAN, WiMAX
Application	• Rural Residential	• Rural, Low Density, Suburban, Urban

In addition to standard AP configurations at the distribution head end, the Canopy system architecture supports remote AP configurations, where an AP is co-located with a subscriber module to account for remote distribution and increased network extensions. This technique is useful in two deployment situations:

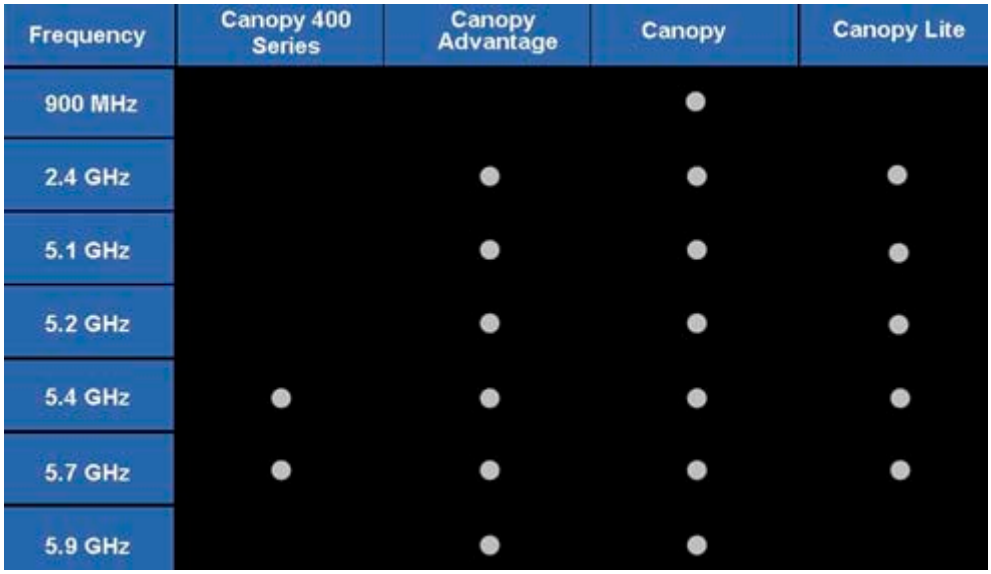
- Extended range and coverage when no tower is available in the area
- Getting under a tree line and distribute the signal to a customer clusters. A lower tower height reduces the coverage area.

Canopy system modules are available in different frequencies to provide network design flexibility and allow equipment options for the best solution for an individual service area. Passive reflectors are available for most subscriber modules to provide extended range capabilities to reach remote subscribers and reduce interference by creating a smaller beam pattern.

Motorola recommends a network be built using a backbone of 5.2 and 5.7 GHz equipment, as these frequencies are clean and less likely to have interference from 2.4 GHz or 900 MHz transmitters. 2.4 GHz modules can provide extended range. 900 MHz modules can then be used to reach subscribers in sparsely populated remote areas or in areas where increased *Non Line of Sight* (NLOS) performance is required to penetrate foliage.

Product	***Typical Application***	***Features***
Canopy CSM54400	Enterprise and/or residential broadband services	21 Mbps maximum throughput to a single user nLOS/NLOS Operator configurable cap on CIR
Canopy Advantage	Enterprise broadband services	14 Mbps maximum throughput to a single user Operator configurable Cap on CIR

Product	***Typical Application***	***Features***
Canopy	Residential and/or Enterprise broadband services	7 Mbps maximum throughput to a single user Operator configurable Cap on CIR Upgradeable to Advantage SM capabilities to offer more bandwidth as demand grows
Canopy Lite	Emerging markets or for residential broadband services	Entry level pricing for emerging markets 512 kbps maximum throughput to a single user 100 kbps cap on CIR Throughput upgrades to 1, 2, 4, 7 Mbps



9.3.10.4 Performance

A Canopy system gracefully scales to support large deployments. The system's unique synchronization allows network operators to re-use frequencies within a geographic area and add capacity while consistently ensuring QoS to customers. As a result, subscribers experience proven reliable service. The Canopy system's unique signal modulation technique yields an industry-leading nominal *Carrier to Interference* (C/I) ratio of less than 3 dB and ensures reliable communication when other transmitters are present.

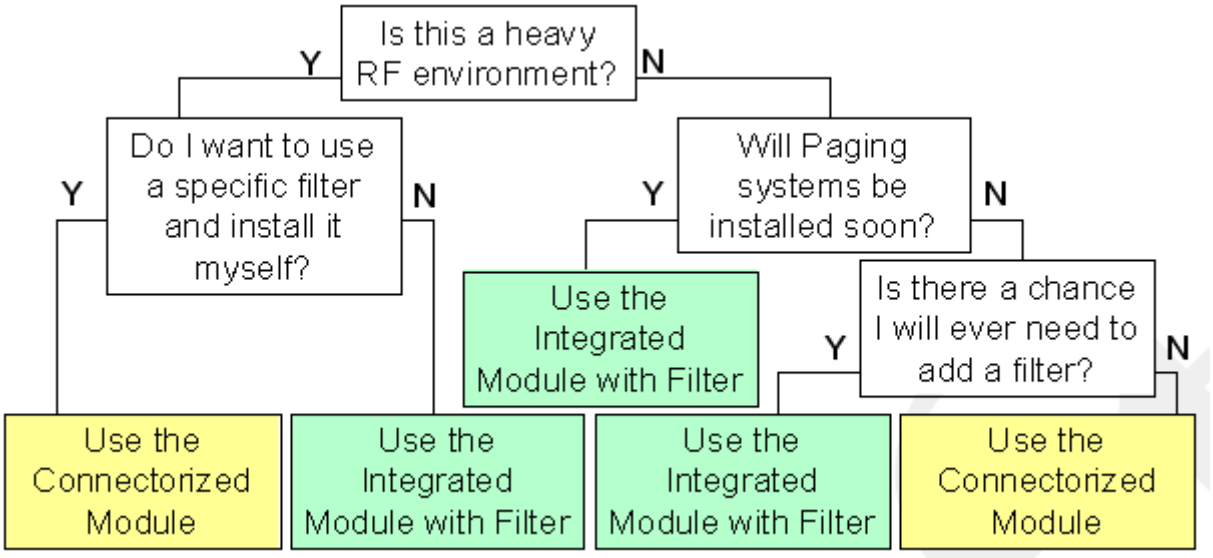
The following chart shows the differences in throughput, burst rates and CIR for each of the Canopy modules:

Product	Total Aggregate Throughput	Burst	CIR in Each Direction	VoIP Channels Supported	Typical Application
Canopy 400 Series SM	21 Mbps	21 Mb	No Cap	Multiple	Residential and/or Enterprise Broadband Services
Canopy Advantage SM	14 Mbps	14 Mb	No Cap	Multiple	Enterprise Broadband Services
Canopy SM	7 Mbps	14 Mb	No Cap	Multiple	Residential and/or Enterprise Broadband Services
Canopy Lite SM	512 Kbps 1 Mbps 2 Mbps 4 Mbps 7 Mbps	768 kb 1.5 Mb 3.0 Mb 7.0 Mb 7.0 Mb	100 kbps 100 kbps 100 kbps 200 kbps 200 kbps	1 1 1 2 2	Emerging Market or Residential Broadband Services

A Canopy Lite Upgraded to 7 Mbps of throughput does not have the same burst or QoS features as a Canopy SM

9.3.10.5 Noise Filters

900 MHz is a crowded frequency. Band pass filters are available to reduce the out of band noise received. The following chart can help determine whether to use a filter for 900 MHz installations:

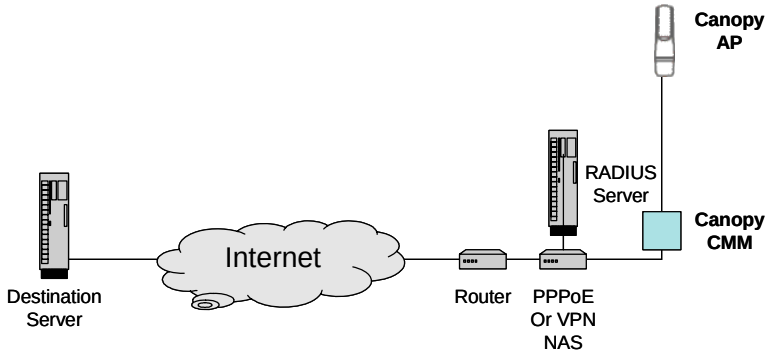


9.3.10.6 Connecting an AP to the Network

A Canopy system appears to a network like a layer 2 bridge and is transparent to layer 2 protocols. The AP is connected to the network via a UV rated CAT 5 cable approved for outdoor deployments. When more than one AP are installed in a cluster, a *Cluster Management Module* (CMM) distributes and synchronizes the signals of the AP cluster. Ideally, the IP network provides *Dynamic Host Configuration Protocol* (DHCP) to supply an IP address to the AP.

9.3.10.7 Cables

Proper cables and connections are critical to ensuring the planned performance of a Canopy system. A Canopy system is typically installed in an outside infrastructure such as radio a tower or roof top. Motorola recommends using shielded outdoor cables that adhere to Category 5 and 5e standards for the installation of Canopy AP and PTP modules.



9.3.11 Point to Point Links

Canopy system backhaul (PTP module) modules provide 10 Mbps, 20 Mbps, 45 Mbps, 150 and 300 Mbps wireless Ethernet links at a number of frequencies. Canopy backhaul modules are simple to install. Complete link installations can often be completed within a few hours, saving valuable time and expenses. There is no need to wait for costly network build-outs. Many backhaul modules are available with passive reflectors to extend range.

- *PTP 100 Series* - This series of radios makes use of Motorola's proprietary technology to deliver high-speed bandwidth up to 2 miles at consistent data rates. These modules can be equipped with a passive reflector to increase the range to up to 35 miles.
- *PTP 400 & 600 Series* - This series of radios achieves greater throughput at distances up to 124 miles, using wireless Ethernet bridges that can deliver 99.999 percent availability in even the most challenging environments. At short distances, speeds of up to 300 Mbps are possible.

9.3.12 Deploying Canopy Networks

Canopy system modules can be combined to tailor the network to meet current and emerging needs. As demand grows over time, new modules can be added to support network extensions or add capacity to backhaul links.

Since the Canopy system is scalable and easy to install, it can be rapidly deployed. Additionally, network operators do not have to incur large up-front investments in network property.

Step 1 - Perform Site Survey

A site survey includes both a physical and a radio frequency analysis of the area where the network is to be installed.

Physical Survey Issues:

- availability and height of tower locations
- estimate of coverage area
- type and density of foliage

- geographic conditions, including man made structures
- environmental conditions including seasonal changes

RF Survey Issues:

- spectrum analysis of the geographic area at desired frequency
- spectrum analysis at alternative frequencies
- polarization of signals
- anticipated changes in local RF conditions

Step 2 - Select Reference Architecture

After considering your goals and business strategy, select from the reference architectures in this document that best suit your business requirements. If the network includes diverse markets, a combination of reference architectures could be an appropriate solution.

The Canopy systems are deployed in more than 120 countries. Trained Motorola account managers, distributors and resellers can help design a network that best meets current and future requirements.

Step 3 - Plan Deployment

Detailed equipment requirements are developed from the network specific architecture. The network is engineered and module locations and their availability are verified. In addition, the network is designed in view of the existing traffic in the area by performing spectrum analysis.

The following aspects should be considered when deploying a Canopy network:

Aspect	***Explanation***
Bandwidth Distribution	The aggregate throughput requirement for each AP needs to be considered. This includes all downlink data to all subscriber modules and all uplink data from all subscriber modules that link to the particular AP. While a single AP can communicate with up to as many as 200 subscriber modules, keep in mind that the aggregate throughput is distributed across the subscriber modules that are actively getting data simultaneously. Where a PTP module is co-located with an AP cluster, the total throughput of the AP cluster should be used to determine the bandwidth requirement for the associated PTP module link. For PTP modules, the aggregate throughput on the channel also needs to be considered in network design. If a PTP module is set to a downlink ratio of 50%, then the bandwidth in each direction is half of the total PTP module link bandwidth.
RF Planning	Before diagramming network layouts: 1) Anticipate the correct amount of signal loss for your link budget calculation. Motorola provides the antenna gain, receiver sensitivity, EIRP power level and fade margin specifications for each module. Use this information to determine the range of the system in your specific network application. 2) Recognize all significant RF conditions. An RF signal in space is attenuated by atmospheric and other effects as a function of the distance from the initial transmission point. The further a reception point is placed from the transmission point, the weaker is the received RF signal. 3) Consider the specific site requirements, including tower rights, power availability and temperature control. 4) Evaluate potential sites by their fitness to address fade margin and ambient RF conditions. An essential element in RF network planning is the analysis of spectrum usage and the strength of the signals that occupy the spectrum you are planning to use.
IP Network Architecture	Canopy network elements are accessed through IP Version 4 (IPv4) addressing. Proper IP addressing is critical to the operation and security of the network. For security, either assign an non-routable IP address, or assign a routable IP address only if a firewall is present to protect the module. The Canopy system allows you to set *Maximum Information Rates* (MIR) to provide data rates that meet customer requirements.

There are many successful deployments of Canopy networks which apply the strengths of the different modules to meet the specific requirements of the particular environment in which they are used. These networks use combinations of 2.4 GHz, 5.1, 5.2, 5.4, 5.7 and 5.9 GHz APs, subscriber modules and backhauls, complemented with 900 MHz modules to fill in the holes or difficult to reach areas of the network.

Given the crowded bands in the unlicensed spectrum, there are things network operators can do to get the best advantage possible:

- Understand the spectrum, particularly 900 MHz, can be very congested with both in-band and out-of-band interference
- Perform a spectrum analysis of the area from the location where the APs are intended to be mounted and mount the AP as high as possible where there is a clean RF environment

- For 900 MHz, use horizontal polarization if possible. Statistically, most 900 MHz gear in the field is vertically polarized
- Use 5.2 GHz, 5.7 GHz and 2.4 GHz for the backbone of the network. Deploy the 900 MHz product as a *hole-filler*
- Use FCC certified sectorized antennas with the 900 MHz radio (Canopy has certified three 60 degree panel antennas for use with the radios)
- Ensure the equipment is configured properly with correct *max range* and *antenna gain* settings

There are some key activities to avoid, and avoiding these will also help you get the best advantage in operating the network successfully:

- *Don't* use omni antennas if it can be avoided. Omni antennas are exposed to interference from every direction
- If it can be avoided, *don't* use vertical polarization for 900 MHz. Simply using horizontal polarization at this frequency is likely to reduce the noise level
- *Don't* set the antenna gain parameter with anything except the actual gain of the antenna. Other numbers may violate FCC regulations for power output
- *Don't* increase the value of the antenna gain parameter expecting it to increase your power output. This will decrease your power output
- *Don't* expect the 900 MHz integrated module with filter to help with in-band interference because it won't. It specifically tackles out-of-band interference

Motorola and its distributors offer specific training for network operators to ensure a Canopy system is planned and implemented properly. This training includes a discussion of case studies and network deployments.

	Canopy Network Management Capabilities
Element Management	The element management system provides network operators bandwidth allocation control to assign maximum data rates per subscriber including: sustained uplink uplink burst allocation sustained downlink data rate downlink burst In addition, the EMS is the central point of authentication in the Canopy system. Complementing the Canopy system's data encryption, the element management system provides an additional layer of security to restrict access to system data. Radius authentication enables network operators to exchange information freely from the Canopy system and therefore, will not need to maintain separate databases. Support for a variety of databases ensures the EMS will work with more installed operations systems including Radius servers, or to a specific database through ODBC.
Security	*FIPS 197 certified encryption* - a 128-bit encryption standard that meets the security requirements of federal, municipal, financial and health care institutions *DES (Data Encryption Standard) encryption* - providing 56-bit encryption *BRAID Encryption* - The AES key is encrypted by Motorola's 128-bit Telecommunications Industry Association (TIA) standard BRAID algorithm making it more secure than others in the market. *Synchronization* - The Canopy system's unique synchronization technique provides higher security than 802.11 alternatives by requiring precise synchronization from all modules in the network *Authentication* - Canopy modules can be scheduled to periodically exchange a random number challenge to authenticate system users and keep out rogue modules *45, 150 and 300 Mbps backhaul units* - employ a built in proprietary signal with scrambling applied as an additional layer of security. In addition, this backhaul employs the following security levels: - Reed Solomon forward error correction - Scrambling code repeating every eight Reed-Solomon code words - Convolutional Encoding where the signal is scrambled into two streams and then sent serially with some bits not sent. - Encoding into BPSK, QPSK, 16QAM or 64QAM waveforms - Interleaving across a 1024 carrier OFDM wave form

Step 4 - Install and Verify Service

Properly planned, a Canopy deployment can be completed in a matter of hours. The Canopy system includes detailed user interfaces to provide required information to the field technician. When necessary, the system also provides detailed diagnostic information to assist field technicians in the troubleshooting and repair.

The Motorola Canopy training includes modules on installation and repair and a hands-on lab wherein attendees work with live systems to perform the installation and verification.

9.3.13 Reference Architectures for Access Networks

The following reference architectures illustrate some of the applications carriers have deployed using Canopy systems. Canopy systems are commonly used for:

- *Network Extensions*
- *Remote Locations*
- *Remote Area Service*
- *Extended IP Networks*
- *High Throughput Data Transfer*
- *Connecting over a "Right of Way"*

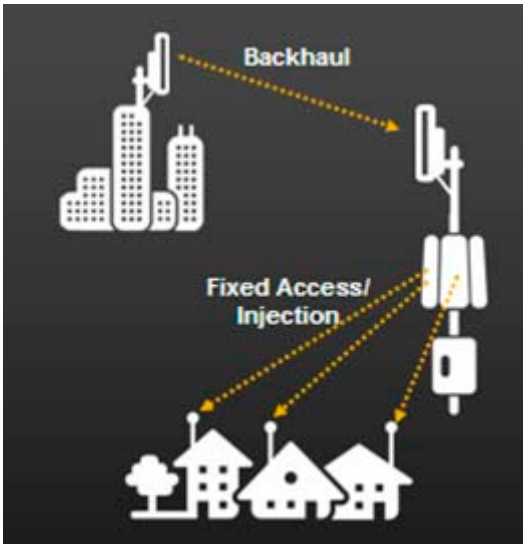
9.3.13.1 Network Extensions

Network extensions can be quickly deployed without the labor and material cost of laying cable and a DSLAM. Also, new broadband subscribers can be added without grooming the existing network for broadband services.

Application: An ILEC provides broadband service to a new construction, residential or business campuses. Residents have reliable service available faster than wireline alternatives.

A Canopy system complements an existing broadband network and allows service providers to build incremental extensions. In areas where existing DSL equipment is operating at capacity, it is difficult to justify capacity additions for incremental subscriber additions. Service providers have the opportunity to quickly provide broadband service to these customers.

Reference Architecture:



9.3.13.2 Remote Locations

Because of the low installation cost and ease of relocation, wireless access may be the only viable solution for remote live motion video surveillance, automation control, portable applications or temporary broadband link requirements.

Application: An International airport installs over 60 full motion cameras using Canopy links to relay sound and video to a center to monitor cameras, gates and phones. The network operator did not have to incur the cost and time to dig a trench or lease T1 services.

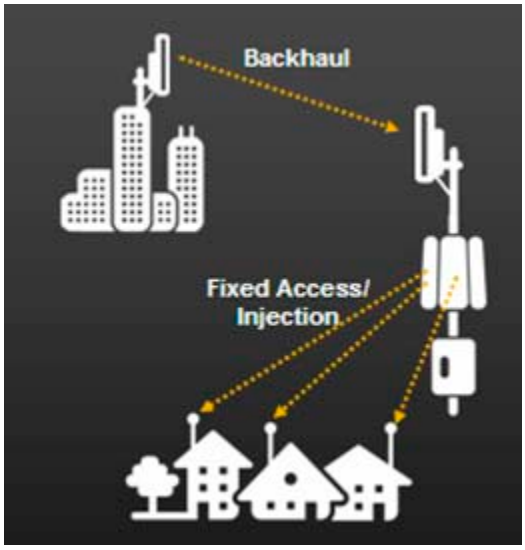
Reference Architecture:

9.3.13.3 Remote Area Service

Motorola's Canopy system allows service providers to reach into remote areas quickly without requiring expensive and time consuming network build-outs. The Canopy system can augment an existing network to reach remote dial-up users.

Application: A company adds broadband network services to an area previously serviced only by dial-up using 900 MHz subscriber modules.

Reference Architecture:

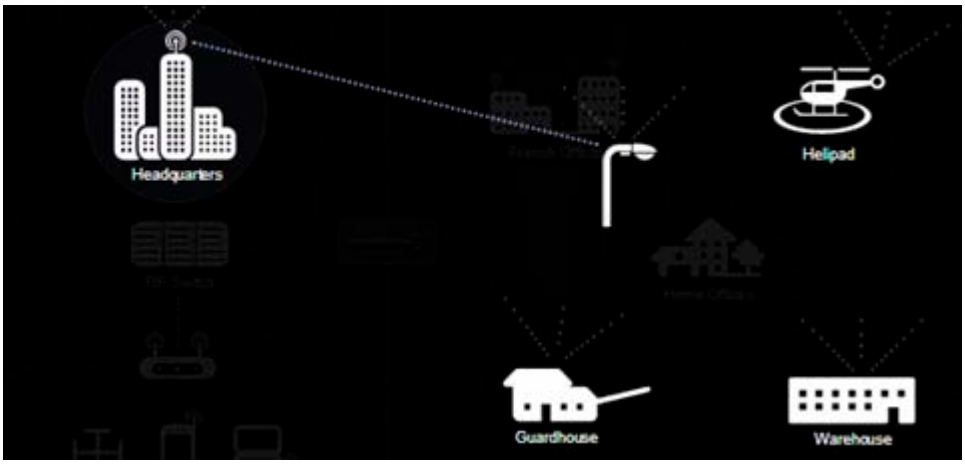


9.3.13.4 Extended IP Networks

Provide IP connectivity to buildings not served by broadband or fiber services. The Canopy system's fast installation time and lower initial and operating costs allow network owners to connect broadband service in a matter of hours.

Application: Business branch offices in remote locations use Canopy links to share data with the regional center.

Reference Architecture:

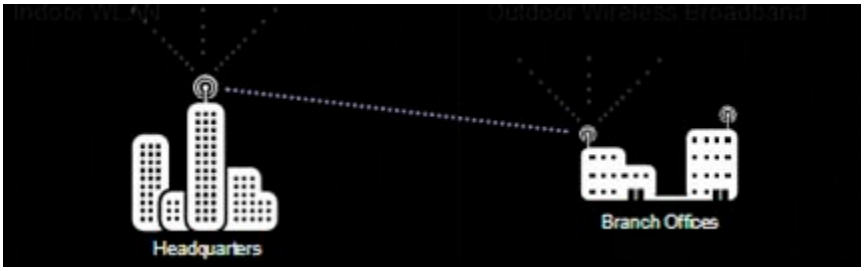


9.3.13.5 High Throughput Data Transfer

Provide additional network links to existing deployments by adding Canopy system backhaul modules to transfer information.

Application: Canopy links enable clinics to share information, images and x-rays for diagnostics and consultation.

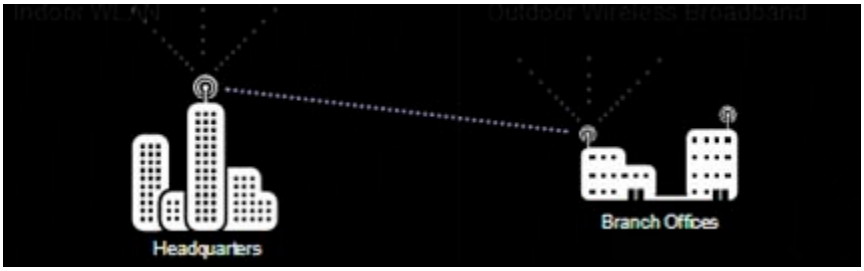
Reference Architecture:



9.3.13.6 Connecting over a "Right of Way"

Provide secure, reliable service on long-range, high-throughput LOS, nLOS and NLOS links with varying throughput levels.

Reference Architecture:



9.3.14 Reliable, Secure Network Extensions for Network Operators

Network owners need to deploy reliable broadband services to meet demand. Network extensions must provide data, voice and video services quickly and efficiently, providing capacity in a *just-in-time* manner. Motorola's Canopy system provides proven secure, reliable broadband service over a wireless connection. Network operators can extend existing networks at a fraction of the cost of wireline alternatives because there is no trenching or waiting to increase network coverage. The Canopy system is comprised of point-to-point links and point-to-multipoint access networks easily configured to meet specific performance and cost requirements.

Service providers require secure and reliable communications. Motorola's Canopy system, with patented signaling technology and military-level security, provides the reliability associated with wireline services with the cost advantage of wireless technology. Canopy provides an opportunity to efficiently extend the network in areas where the investment required to deploy wireline service is restricting growth.

Requirement	***Canopy System Performance***
Reliability	Because of its unique signal modulation technique, the Canopy system is the most interference tolerant system in the unlicensed spectrum. Data rate and throughput is consistent to all subscribers, even those at the outer edge of the network.
Installation and maintenance	Subscriber modules are fast to install. Built in alignment tools verify installation and minimize truck rolls. Technical training is available to shorten the learning curve for installs and support.
Security	FIPS 197 AES encryption meets HIPPA and military specifications. Multiple layers of encryption and authentication restrict access to data.
Return on investment	System payback is in terms of months. The system scales to deployment levels with low up front investment.

9.3.14.1 Key Points to Keep in Mind when Planning a Network

- *Quality of Service*: The Canopy system provides carrier grade reliable service because of its industry leading interference tolerance
- *Capacity*: The Canopy system provides a consistent data rate to all subscribers. The data rate is consistent for even the most distant subscribers in the network and does not degrade as more subscribers are added
- *Security*: The Canopy system has multiple layers of security with authentication and military-level data encryption to restrict access by unauthorized users
- *Network Management*: The Canopy system integrates into existing network management systems through open interfaces from an element manager

- *Scalability*: With an array of access network modules and a selection of point to point links, carriers can expand their customer base and associated revenue quickly
- *Reliability:* The Canopy system is field-proven. All of the configurations and reference architectures in this document are based on actual installations

9.3.15 Facts and Fiction about Broadband Wireless Access

Network operators who have built their business on reliable service are rightfully concerned about perceptions regarding wireless broadband technology. There are wireless broadband products on the market that do not adhere to the same stringent requirements as Canopy products and whose performance, reliability and security have led to negative perceptions of interference problems, excessive downtime and loose security.

Concern	***Canopy System Deployment Fact***
Wireless broadband systems are not secure against hackers and intruders.	The Canopy system has multiple security layers including signal modulation techniques, authentication and military-level AES encryption. It's certified FIPS 197 compliant by NIST and meets HIPPA requirements. Canopy provides a level of security equivalent to wireline services.
Wireless broadband systems do not provide the advertised data rate to the maximum range.	The Canopy system's unique signal modulation is different from 802.11 systems and allows subscribers to receive planned bandwidth regardless of the distance from the AP to the subscriber modules.
The number of subscribers will load down the system.	Canopy scales from an initial deployment to serving dense metropolitan area while maintaining a consistent throughput to all subscribers in the network. Adding new subscribers has no negative impact to the aggregate bandwidth provided to all subscribers.
Unlicensed wireless communication is not reliable for quality service.	The license-free spectrum is available for use at no charge and is open to many users. Network operators should check a frequency before they use it. The Canopy system is unique in that it was designed to be optimized for interference tolerance. The Canopy system's synchronization and signal modulation yield an industry leading interference tolerance.
I don't understand wireless technology enough to deploy it in my network with confidence.	Motorola has deployed wireless technology for decades. In the few years that the Canopy system has been available, it has been deployed to tens of thousands of subscribers in more than 120 countries. Motorola provides training, technical support and will introduce you to an enthusiastic community of users who have experienced the Canopy system for themselves.
Doesn't the weather have an impact on the quality of service I can expect?	Extreme weather can affect communications. Canopy modules operate at frequencies not affected by weather conditions. Canopy systems are field proven in hot, cold, humid and windy conditions.

9.3.16 Network Deployment

With many different Canopy system modules available, network operators can deploy in respect to demand when building the network and overlay different frequencies as required. Areas of access network coverage can be linked to the network by Canopy system backhaul connections.

By co-locating Canopy system AP's of different frequencies, operators can provide coverage in dense locations while providing service to remote locations.

Issue	***Canopy System Performance***	***Canopy Benefit***
Scalability	The Canopy system can scale from fewer than 200 subscribers in an area using a single AP to as dense as 4,800 subscribers in an urban area using multiple APs.	The Canopy system provides *just-in-time* scalability so the investment is made as subscribers are added, not up front where usage must be anticipated weeks, months or even years in advance. As subscribers are added to the network, data throughput to each subscriber remains consistent.
Traffic Type	The Canopy system supports legacy voice, video and data transmissions.	These services provide additional revenue streams.
Security	Canopy system products are available with either AES or DES encryption. All Canopy system modules have multiple layers of authentication to restrict access.	Service providers can meet the encryption requirements of municipalities, hospitals and corporate Enterprises.
Redundancy	Canopy system point to point links are cost effective redundant backhaul links where Ethernet connections are required.	Service providers can offer reliable redundant services at a fraction of the cost of building out the wireline network.
Options	Canopy system modules are designed to meet specific network requirements. Options for data encryption, passive reflectors and antennas make the system highly configurable.	Network investment is triggered by specific customer demand, lowering initial investment in network facilities.

9.3.17 Network Design Trade-offs

Canopy system AP's can communicate with up to 200 subscriber modules. AP's can have a 10, 20 or 35 Mbps signaling rates (depending upon the platform Lite, Canopy, Advantage, or 400 Series) divided evenly across the subscriber modules. As the network grows and new subscriber modules are added, network operators can add AP capacity by using an AP with a different frequency.

Performance Value	***Issue or Problem***	***Alternative Solution(s)***
Subscriber capacity	50 subscribers are connected to a single AP with 4 Mbps downstream capacity, yielding 80kbps downstream when all are active.	Add new subscribers on a different AP frequency to continue provide service at high data rates.
Subscriber range	Subscribers are too far from the AP to provide service.	Add a passive reflector dish at the SM location to extend the range. Install a new AP closer to the subscribers. Install a remote AP at a subscriber location. Add distant subscribers at a lower frequency.
Subscriber throughput	Individual subscribers require more bandwidth to transfer voice, video and data services efficiently.	Set the *Maximum Information Rate* (MIR) for subscribers to provide an upper transmission boundary for selected network users. Verify the IP network architecture is configured to match the flow of data and not a *flat* architecture. Verify backhaul links are providing sufficient throughput for associated AP's and not contributing to information bottlenecks. Check the number of subscriber modules associated with the AP and consider adding an additional AP on a different frequency. Consider whether a point-to-point link meets the needs of high bandwidth users.

9.3.18 Canopy System Reliability

With its patented signaling technique, the Canopy system provides consistent managed throughput to all subscribers and an industry-leading low Carrier to Interference (C/I) ratio. Canopy modules are robust and able to perform even in the most crowded license free frequency bands. Subscribers receive dependable carrier grade service - even those subscribers at the outer edge of the network.

Motorola provides product support coverage and backs all Canopy equipment with a one-year warranty.

9.3.19 Canopy System Security

All Canopy system modules are equipped with multiple layers of security to protect IP communication and provide a secure air interface. Canopy modules meet Health Insurance *Portability & Accountability Act* (HIPPA) compliance requirements. The Canopy system has point-to-point link and point-to-multipoint access network products with either 128-bit AES encryption or 56-bit DES encryption. AES encryption provides the highest level of security, as required for the following institutions:

- Banks
- Other financial institutions
- Health care organizations
- Government facilities
- High risk situations with specific security concerns

9.4 MOTOwi4 Wireless Broadband Solutions

The MOTOwi4™ portfolio of wireless broadband solutions combines speed and coverage to help capture the most demanding customers. It's clear what customers want. They want to share, connect and communicate from the heart of the city to the ends of the earth. In addition, they want more than voice! They want high-speed data. Whether its music video or gaming, the MOTOwi4 portfolio allows you to provide customers exactly what they want. MOTOwi4™ gives you a range of flexible, mix-and-match, cost-effective options to fit your network and business model (WiMAX, fixed broadband, Metro WiFi, mesh and *broadband over powerline* (BPL).

9.5 MOTOwi4 Fixed Solutions

The wi4 fixed portfolio combines point-to-point and point-to-multipoint solutions to enable cost-effective, reliable and secure connectivity in thousands of networks in over 120 countries. Serving a broad range of licensed and unlicensed spectrums (with solutions at 900 MHz through the 5 GHz frequencies), wi4 Fixed solutions are designed for even the harshest of outdoor environments to provide high-speed voice, access and data services for your wireless broadband needs.

10

Wireless Standards

10.1 802.11 Standards

IEEE 802.11 is a set of standards for *wireless local area network* (WLAN) computer communication, developed by the *IEEE LAN/MAN Standards Committee* (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.

Although the terms 802.11 and Wi-Fi are often used interchangeably, the Wi-Fi Alliance uses the term *Wi-FI* to define a slightly different set of overlapping standards. In some cases, market demand has led the Wi-Fi Alliance to begin certifying products before amendments to the 802.11 standard are completed.

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, and are amendments to the original standard. 802.11a was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments, and was later enhanced via the 802.11i amendment after governmental and legislative changes. 802.11n is a new multi-streaming modulation technique under draft development, but products based on its proprietary pre-draft versions are being sold. Other standards in the family (c-f, h, j) are service amendments and extensions or corrections to previous specifications

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this frequency band, 802.11b and 802.11g equipment can occasionally sustain interference from microwave ovens and cordless telephones. Bluetooth devices, while operating in the same band (in theory) do not interfere with 802.11b/g because they use a *frequency hopping spread spectrum signaling* method (FHSS) while 802.11b/g uses a *direct sequence spread spectrum signaling* method (DSSS). 802.11a uses the 5 GHz U-NII band, which offers 8 non-overlapping channels rather than the 3 offered in the 2.4GHz ISM frequency band.

The segment of the radio frequency spectrum used varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as explained in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six (802.11b) fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

For information on the unique 802.11 standards, refer to:

- *802.11a*
- *802.11b*
- *802.11c*
- *802.11d*

- *802.11e*
- *802.11f*
- *802.11g*
- *802.11h*
- *802.11i*
- *802.11j*
- *802.11k*
- *802.11m*
- *802.11n*
- *802.11p*
- *802.11r*
- *802.11s*
- *802.11T*
- *802.11u*
- *802.11v*
- *802.11w*
- *802.11y*

10.1.1 802.11a

802.11a is the IEEE 802.11 specification that defines the 54 Mbps data rate. Operating in the 5GHz band, 802.11a supports a maximum data rate up to 54 Mbps. 802.11a has four, eight, or more channels, depending on the country. Possible Data Rates for 802.11a include 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

Interference: 802.11g vs. 802.11a

- The range of 802.11g (higher rates) is much shorter than 802.11b
- 54 Mbps require 24 dB SNR as opposed to 11 Mbps which requires 8 dB
- Planning for full high rate coverage requires much denser AP placement
- The number of channels at 2.4 GHz is 3 (83.5 MHz total non-overlapping), at 5 GHz it is up to 12 (555 MHz total non-overlapping)
- The channel layout for dense AP environments is much better at 5 GHz
- With 802.11a (and a larger number of channels), co-channel interference decreases dramatically

10.1.2 802.11b

IEEE 802.11b-1999 or 802.11b (an amendment to the IEEE 802.11 specification) extends throughput up to 11 Mbit/s using the same 2.4 GHz band. This specification (under the marketing name of Wi-Fi) has been implemented all over the world. The amendment has been incorporated into the published IEEE 802.11-2007 standard.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today (in their 802.11a, 802.11b, and 802.11g versions) to provide wireless connectivity in the home, office and commercial establishments.

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, the maximum 802.11b throughput an application can achieve is about 5.9 Mbit/s using TCP and 7.1 Mbit/s using UDP.

802.11b products appeared on the market in early 2000, as 802.11b is a direct extension of the DSSS modulation technique defined in the original standard. Technically, the 802.11b standard uses *complementary code keying* (CCK) as its modulation technique. A dramatic increase in throughput (compared to the original standard), along with simultaneous substantial price reductions, led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones. Interference issues, and user density problems within the 2.4 GHz band, have become a major concern and frustration for users.

802.11b is used in a point-to-multipoint configuration, wherein an access point communicates via an omni-directional antenna with one or more nomadic or mobile clients located in a coverage area around the access point. Typical indoor range is 30 m (100 ft.) at 11 Mbit/s and 90 m (300 ft.) at 1 Mbit/s. The overall bandwidth is dynamically demand shared across all the users on a channel. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometers (5 miles), although some report success at ranges up to 80-120 km (50-75 miles) where line of sight can be established. This is usually done in place of costly leased lines or cumbersome microwave communications equipment. Designers (who wish to remain within the law) must be aware of the legal limitations on radiated power.

802.11b cards can operate at 11 Mbit/s, but can back to 5.5, then 2, then 1 Mbit/s if signal quality becomes an issue.

10.1.3 802.11c

IEEE 802.11c is an amendment to the IEEE 802.1D MAC bridging standard that incorporates bridging in wireless bridges or access points. This work is now part of IEEE 802.1D-2004.

802.11c was ratified in October of 1998 and is a supplement to IEEE 802.1D that adds requirements associated with bridging 802.11 wireless client devices. In particular, it adds a sub clause (under 2.5 Support of the Internal Sublayer Service) to cover bridge operations with 802.11 MACs.

10.1.4 802.11d

To support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory within additional countries. This is especially important for operation in 5GHz bands, since the use of these frequencies differs widely from one country to another. As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products.

The 802.11d standard (when ratified) will allow WLAN vendors to provide additional capabilities to customers who want to have a single radio that will work in every regulatory domain worldwide.

The PHY layer of a WLAN is subject to regulations that vary significantly from one geopolitical area to another. The proposed standard provides a mechanism allowing an implementation to be built that meets many different sets of regulations. This allows conforming equipment to operate in more than one regulatory

domain over time. The proposed standard describes the mechanism required to implement 802.11 FH and DS MUs that support cross-domain mobility and operation in multiple regulatory domains.

NOTE: This does not eliminate the need to obtain type acceptance in each of the regulatory domains in which the equipment will operate.

The standard provides a framework for WLAN developers to work from, but the actual method for configuring individual devices is outside the scope of the standard. The standard only discusses the IBSS (Infrastructure) mode of WLAN operation. No mention is made of AdHoc mode or backward compatibility between access points and MUs that may not support 802.11d. As is typical with IEEE standards, no mention of interoperability between WLAN vendors is made. It is left to WLAN vendors to manufacture systems acceptable to regulatory bodies in countries they wish to sell equipment into. International roaming is not a requirement for WiFi certification, but may become a WECA requirement for WiFi at some point in the future.

The new *WLAN Communication Elements* standard is relatively straightforward. It adds new elements to AP beacons and probe responses. These new elements may contain the following informational elements:

Element ID	Length
Country String	(Octets 1, 2)
Country String (Octet 3)	First Channel Number
Number of Channels	Maximum Transmit Power Level

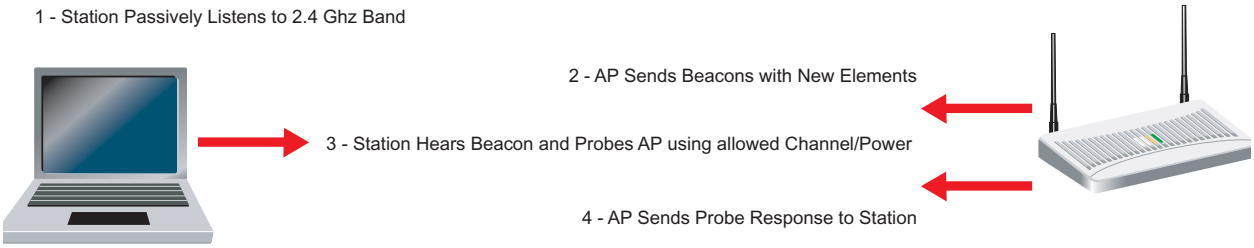
10.1.4.1 802.11d in Operation

An MU enabled for operation across regulatory domains will default to passive scanning when it has lost connectivity with its ESS or when first powered on. Passive scanning is performed using only the receive capabilities of the MU and is, thus, compatible with regulatory requirements. The timeout for determining the loss of connectivity is system dependent and beyond the scope of the standard.

When an MU enters a regulatory domain, it will passively scan to learn at least one valid channel (a channel upon which it detects 802.11 frames). The beacon frame contains information on the country code, the maximum allowable transmit powers and the channels used for the regulatory domain.

Optionally, the beacon frame can also include, on a periodic basis, the regulatory information returned in a probe response frame. Once the MU has acquired the information required to meet the transmit requirements of the regulatory domain, it transmits a probe request to an AP to gain additional regulatory domain information contained in the probe response frame (unless previously received in a beacon frame). The MU then has sufficient information available to configure its radio for operation in the regulatory domain.

A MU returns only information elements that it supports. An MU may ignore the first information element requested that is not ordered properly. In a probe response frame, the MU returns requested information elements in the same order requested in the request information element. The diagram below represents a typical message exchange between an AP supporting 802.11d*:*



10.1.5 802.11e

802.11e is an approved amendment to the IEEE 802.11 standard that defines a set of QoS enhancements for wireless LAN applications through modifications to the *Media Access Control* (MAC) layer. The standard is considered critical for delay-sensitive applications, such as Voice over Wireless IP and Streaming Multimedia. The amendment has been incorporated into the published IEEE802.11-2007 standard.

802.11 is an IEEE standard that allows devices such as laptop computers or cellular phones to join a wireless LAN widely used in the home, office and some commercial establishments.

10.1.5.1 Original 802.11 MAC

The basic 802.11 MAC layer uses the *Distributed Coordination Function* (DCF) to share the medium between multiple MUs. DCF relies on CSMA/CA and optional 802.11 RTS/CTS to share the medium between MUs. This has several limitations:

- When numerous MUs communicate at the same time, collisions will occur, which lowers the available bandwidth
- There is no notion of high or low priority traffic
- Once a MU *wins* access to the medium, it can keep the medium for as long as it chooses. If a MU has a low bit rate (1 Mbit/s, for example), it takes a long time to send a packet, and all other MUs will suffer
- There are no QoS guarantees.

The original 802.11 MAC defines another coordination function called the *Point Coordination Function* (PCF). It is available only in infrastructure mode, where MUs are connected to the network through an access point. This mode is optional, and very few APs or Wi-Fi adapters actually implement it. APs send beacon frames at regular intervals (usually every 0.1 second). Between these beacon frames, PCF defines two periods: the *Contention Free Period* (CFP) and the *Contention Period* (CP). In the CP, the DCF is used. In CFP, the AP sends *Contention Free-Poll* (CF-Poll) packets to each MU, one at a time, to grant them the right to send a packet. The AP is the coordinator. This allows for a better management of the QoS. Unfortunately, the PCF has limited support and a number of limitations (it does not define classes of traffic).

10.1.5.2 802.11e MAC Protocol Operation

802.11e enhances the DCF and the PCF, through a new coordination function, the *Hybrid Coordination Function* (HCF). Within the HCF, there are two methods of channel access, similar to those defined in the legacy 802.11 MAC: *HCF Controlled Channel Access* (HCCA) and *Enhanced Distributed Channel Access* (EDCA). Both EDCA and HCCA define *Traffic Classes* (TC). For example, emails could be assigned to a low priority class, and *Voice over Wireless LAN* (VoWLAN) could be assigned to a high priority class.

10.1.5.3 EDCA

With EDCA (*Enhanced Distributed Channel Access*), high priority traffic has a higher chance of being sent than low priority traffic, as a MU with high priority traffic waits a little less before it sends its packet (on average) than a MU with low priority traffic. Each priority level is assigned an *opportunity to transmit* (TXOP). A TXOP is a bounded time interval during which a MU can send as many frames as possible (as long as the duration of the transmissions does not extend beyond the maximum duration of the TXOP). If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames. The use of TXOPs reduces the problem of low rate MUs gaining an inordinate amount of channel time in the legacy 802.11 DCF MAC. A TXOP time interval of 0 means it is limited to a single MSDU or MMPDU.

The purpose of QoS is to protect high priority data from low priority data but there can be scenarios in which the data which belongs to same priority needs to be protected from data of same priority. For example, suppose a network can accommodate only 10 data calls & an eleventh call is made. Admission control in EDCA address the problem. The AP publishes the available bandwidth in beacons. The clients can check the available bandwidth before adding more traffic in the network that cannot be entertained.

Wi-Fi Multimedia (WMM) certified APs must be enabled for EDCA and TXOP. All other enhancements of the 802.11e amendment are optional.

10.1.5.4 HCCA

HCCA (*HCF (Hybrid Coordinator Function) Controlled Channel Access*) works a lot like the PCF. However, in contrast to PCF, in which the interval between two beacon frames is divided into two periods of CFP and CP, the HCCA allows for CFPs initiated at almost anytime during a CP. This kind of CFP is called a *Controlled Access Phase* (CAP) in 802.11e. A CAP is initiated by the AP, whenever it wants to send a frame to a MU, or receive a frame from a MU, in a contention free manner. In fact, the CFP is a CAP too. During a CAP, the *Hybrid Coordinator* (HC) controls access to the medium. During the CP, all MUs function in EDCA. The other difference with the PCF is that *Traffic Class* (TC) and *Traffic Streams* (TS) are defined. This means the HC is not limited to per-MU queuing and can provide a kind of per-session service. Also, the HC can coordinate these streams or sessions in any fashion it chooses (not just round-robin). Moreover, the MUs provide info about the lengths of their queues for each TC. The HC can use this info to give priority to one MU over another, or better adjust its scheduling mechanism. Another difference is MUs are assigned a TXOP, they may send multiple packets in a row, for a given time period selected by the HC. During the CP, the HC allows MUs to send data by sending CF-Poll frames.

HCCA is generally considered the most advanced (and complex) coordination function. With the HCCA, QoS can be configured with great precision. QoS-enabled MUs have the ability to request specific transmission parameters (data rate, jitter, etc.) which should allow advanced applications like VoIP and video streaming to work more effectively on a Wi-Fi network.

HCCA support is not mandatory for 802.11e APs. In fact, few (if any) APs currently available are enabled for HCCA. Nevertheless, implementing the HCCA does not require much overhead, as it basically uses the existing DCF mechanism for channel access (no change to DCF or EDCA operation is needed). In particular, the MU side implementation is very simple, as MUs only need to be able to respond to poll messages. On the AP side, however, a scheduler and queuing mechanism is needed. Given that APs are already equipped better than MU transceivers, this should not be a problem either.

10.1.5.5 APSD

Automatic Power Save Delivery (APSD) is a more efficient power management method than legacy 802.11 PSP. Most newer 802.11 MUs already support a power management mechanism similar to APSD. APSD is very useful for a VoIP phone traffic, as data rates are roughly the same in both directions. Whenever voice

data are sent to the access point, the access point is triggered to send the buffered voice data in the other direction. After that, the phone enters a doze state until the next voice data has to be sent to the access point.

10.1.6 802.11f

IEEE 802.11f is a recommendation describing an optional extension to IEEE 802.11providing wireless access-point communications among multi vendor systems. 802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in 802.11a, 802.11b, 802.11g and 802.11n versions to provide wireless connectivity at home, office and commercial establishments.

The IEEE 802.11 standard doesn't specify communications between access points to support roaming and load balancing. 802.11 purposely didn't define these elements to provide flexibility in working with different wired and wireless distribution systems (wired backbones that interconnect access points).

The protocol is designed for the enforcement of unique associations throughout an ESS and for a secure exchange of security data between a current AP and a new AP during a handoff. Based on the security level, session keys between APs are distributed by a Radius server. The server also provides a mapping service between an access point MAC and IP addresses.

10.1.7 802.11g

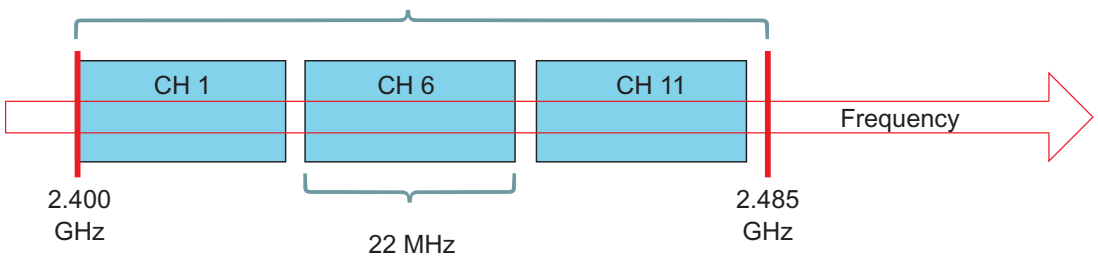
802.11g is the IEEE 802.11 specification that defines the use of higher data rates in the 2.4GHz band. 802.11g offers the throughput of 802.11a, coupled with the backward compatibility of 802.11b. 802.11g operates in the 2.4 GHz band, but delivers data rates from 6 Mbps to 54 Mbps. Like 802.11b, it supports up to three non-overlapping channels, but the range of 802.11g (higher rates) is much shorter than 802.11b.

- 54 Mbps require 24 dB SNR versus 11 Mbps which requires 8 dB
- Planning for full high rate coverage requires much denser AP placement
- The number of channels at 2.4 GHz is 3 (83.5 MHz total non-overlapping), at 5 GHz it is up to 12 (555 MHz total non-overlapping)
- Too much channel overlap exists for 802.11g to support a dense coverage topology.

10.1.7.1 802.11g and Motorola

Short slot time is a 802.11g feature that improves channel utilization. It is applicable only to 802.11g operation.

A WS2000 switch automatically enables short slot times in an 802.11g only portal until at least one 802.11g client (that cannot support short slots) associates with that portal. In a dual 802.11b/g environment, short slot times are implemented until the first 802.11b client associates or the first 802.11g client that does not support short slot times associates with the portal.



	802.11b	***802.11g***
Encoding	DSSS	DSS + OFDM
Modulation	BPSK, QPSK, CCK	BPSK, QPSK, CCK 16-QAM, 64-QAM
Data Rates (Mbps)	1, 2. 5.5, 11	1, 2. 5.5, 11, 12, 18, 24, 36, 48, 54
Total User Bandwidth	6 Mbps x 3 channels = *18 Mbps*	18 Mbps x 3 channels = *66 Mbps*

Wi-Fi Requirements:

- Although it is not explicitly required by the 802.11g spec, the Wi-Fi test plan requires an 802.11g AP detect legacy 802.11b APs co-located on the same channel.
- It also requires an 11g AP detect if legacy 11b MUs are connected to another 11g AP co-located on the same channel.
- A WS2000 and AP300 deployment does not currently implement this. However, Motorola plans on implementing this feature shortly to allow Wi-Fi certification.

Slot time has good and bad aspects to consider:

If a customer has legacy 11b MU, other APs on the same channel will detect the AP's presence and use protection mode appropriately. This will negatively impact system throughput, even on APs that do not have an 11b MU connected to it. On the other hand, it allows all of the systems to inter-operate.

In Motorola's current implementation, only the AP to which the MU is connected detects it and uses protection. However, if a customer only has 11g MUs and wants to achieve higher throughput by not allowing legacy systems to connect (and if he is next door to someone that has legacy systems), the Wi-Fi requirements state his 11g system needs to invoke protection. In this kind of environment, even someone who has selected a *g-only* configuration will have to deal with the throughput loss associated with invoking protection.

Motorola's current implementation invokes protection dynamically based on the current environment. Even if configured for b/g operation, protection is only invoked if the presence of a legacy MU is detected.

Therefore, if there are legacy MUs moving in and out of a given deployment, you would expect the protection to be invoked on those APs to which the 11b MU is connected and not on other APs on other channels. Once the 11b MU leaves an AP, the protection stays on for some time and then is turned off. This means over-all throughput will decrease and increase on a given AP as the 11b MU moves in and out of that BSS.

There certain MU implementations which use protection, even if the AP has not instructed them to do as *if* they hear a legacy 11b AP co-located on the same channel. This could occur, for example, if an AP300 is out of range of an 11b MU, but the MU connected to the AP 300 is between two APs and can hear them both.

10.1.7.2 802.11g Throughput Issues

Please keep the following considerations in mind when deploying an 802.11g network:

- 802.11g is significantly faster than 802.11b
- Once an 802.11b MU associates to an 802.11g AP, the throughput drops dramatically, because protection must be activated

- An 802.11b MU does not need to actively send data to cut throughput, it merely needs to be associated, so protection can be enabled
- Mixed 802.11b/g deployments are likely to be commonplace for the foreseeable future, especially in situations where there is no control over client adapters
- 802.11a networks can sustain much higher data rates than 802.11g networks with protection enabled. 802.11a offers the added advantage of more radio channels for easier layout in high-density deployments.
- 802.11g provides a significant speed advantage over 802.11b, but it does not achieve 802.11a's performance crown
- 802.11g has only 3 channels, cell layout causes significant co-channel interference (green circle overlap)

Exactly how many users can access a single AP-5131 or AP300 effectively before they get bogged down? For a hotel hotspot application where the deployment supports basic access only for the public areas of the hotel (no VoIP/Laptop roaming or heavy file transfer expectations).

54mb data rate = 18 to 22 mb of throughput. Thus, you should expect a mix of 802.11b and 802.11g clients which will invoke 802.11b/g compatibility.

If you want to provide a DSL type of connection speed per user (256k each = around 72 users), contention issues and RF characteristics will further take this number down. consequently, for every 45 users, add an additional access point. If you want to provide more throughput, add more APs.

10.1.8 802.11h

802.11h is an amendment added to the IEEE 802.1 standard for spectrum and Transmit Power Management Extensions. It solves problems like interference with satellites and radar using the same 5 GHz frequency band. It was originally designed to address European regulations but is now applicable in many other countries. The standard provides *Dynamic Frequency Selection* (DFS) and *Transmit Power Control* (TPC) to the 802.11a MAC. It has been integrated into the full IEEE 802.11-2007 standard.

IEEE 802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, and 802.11g versions to provide wireless connectivity in the home, office and commercial establishments.

DFS ensures channels containing radar are avoided by an AP and energy is spread across the band to reduce interference to satellites. TPC ensures the average power is less than the regulatory maximum to reduce interference.

10.1.9 802.11i

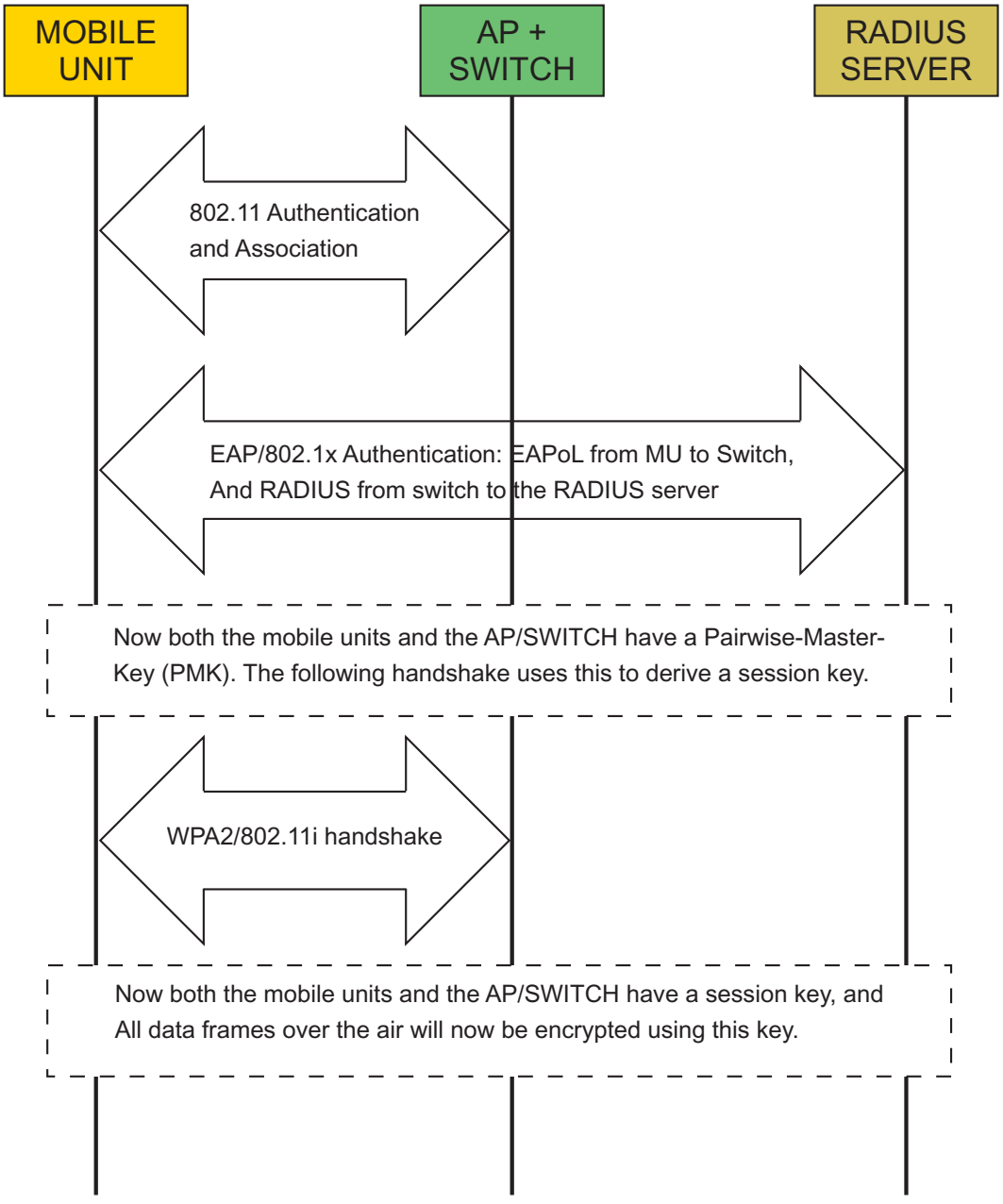
802.11i is the IEEE 802.11 specification that defines additional security services. It describes the encrypted transmission of data between systems. 802.11i defines encryption key protocols including the *Temporal Key Integrity Protocol* (TKIP) and the *Advanced Encryption Standard* (AES).

10.1.9.1 802.11i Fast Roaming Options

If the authentication on a WLAN is 802.1x, and the encryption is WPA2-TKIP or WPA2-CCMP, an exchange occurs upon a successful association and authentication.

- The 802.11 authentication and association could take around 10 ms
- The WPA2/802.11i handshake takes another 20 ms
- The EAP/802.1x authentication can typically take anywhere from 50 ms to 5 seconds

Roaming is the most time consuming operation a MU needs to perform before it can resume data traffic. Fast roaming options aim to avoid this 802.1x exchange on each association.

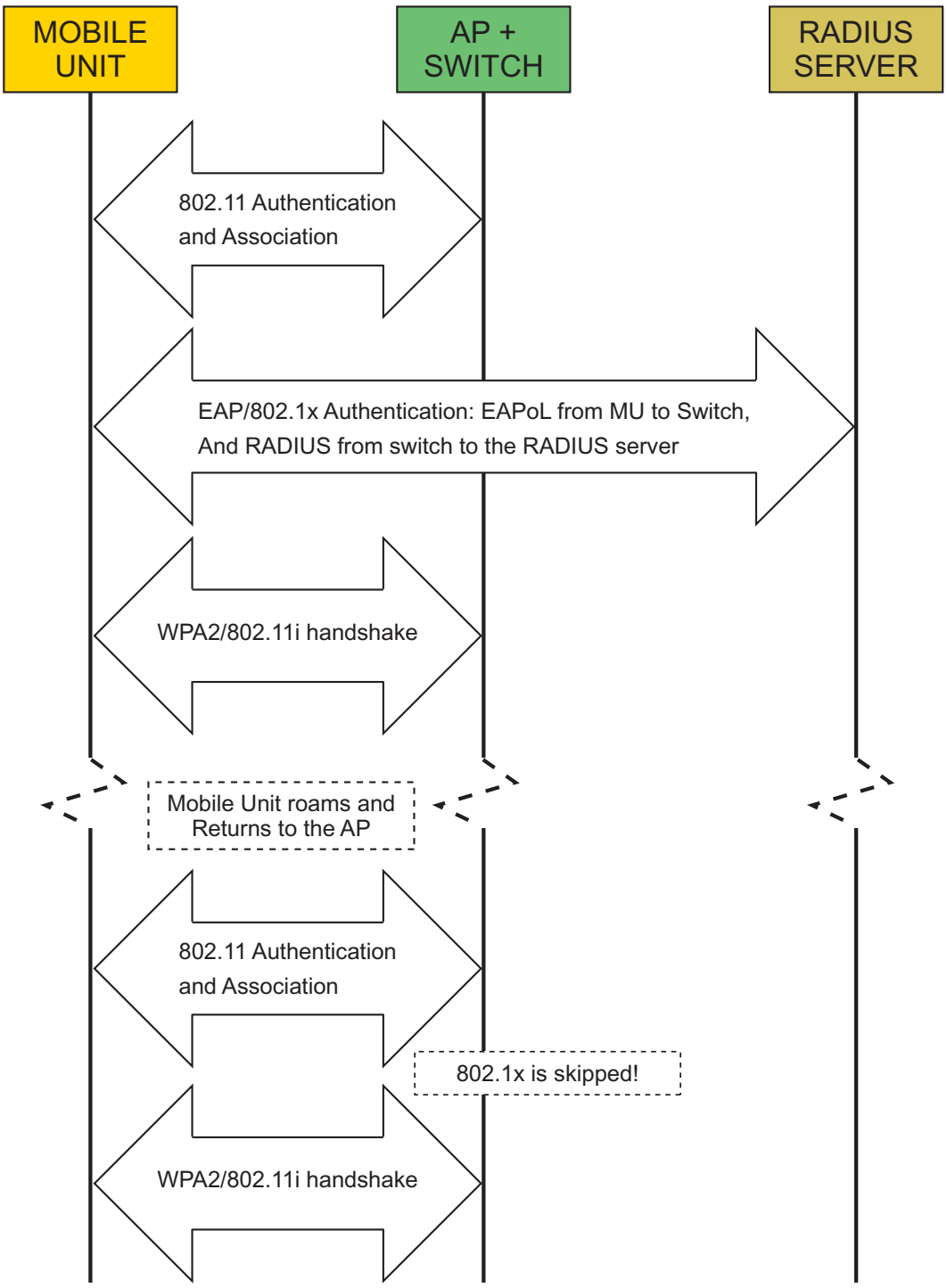


10.1.9.2 PMK Caching

An 802.11i handshake takes the PMK and derives a session key from it The handshake makes use of random numbers in the derivation, even if the same PMK is reused, the session keys are different. When a MU associates with an AP for the first time, it carries out an 802.1x exchange and derives a PMK. That PMK is used to derive session keys, and data traffic is subsequently encrypted with those keys. If a MU roams away from the AP, both the switch and the MU keep a copy of the PMK instead of deleting it.

If a MU roams back to the same AP, after 802.11 authentication and association, it can initiate a WPA2/802.11i handshake using the old PMK (this is known as PMK caching). The MU needs to do 802.1x only once with the AP. After that, it can used the cached PMK each time and roam quickly.

The MU informs the switch it has a PMK by adding a PMK signature (known as the PMKID in the association request. If the switch also has the PMK for that MU, then (instead of sending an EAP-request-identity) the switch begins the 802.11i handshake. If the switch had the PMK cached, but the association request from the MU did not include the PMKID, the cached PMK cannot be used, and a complete 802.1x exchange occurs.


MOBILE UNIT
AP + SWITCH
RADIUS SERVER
802.11 Authentication and Association
EAP/802.1x Authentication: EAPoL from MU to Switch, And RADIUS from switch to the RADIUS server
WPA2/802.11i handshake
Mobile Unit roams and Returns to the AP
802.11 Authentication and Association
802.1x is skipped!
WPA2/802.11i handshake

10.1.9.3 Opportunistic PMK Caching

PMK caching (as defined in 802.11i) is limited to one AP. However, in a wireless switch architecture, the switch can cache the PMK and re-use it across access points. This is known as *opportunistic PMK caching*.

When a MU associates with the switch for the first time it carries out the complete 802.1x exchange (with AP1). When it now roams to AP2, there is a possibility AP2 is managed by the same switch that controlled AP1, and has access to the older PMK. If this is the case, the MU can skip 802.1x and carry out the WPA2/802.11i exchange using the older PMK. The first cached PMK is now useful across all APs on the switch. Instead of doing 802.1x once per-AP, clients potentially need to do 802.1x only once per-switch.

Though opportunistic PMK caching is not defined in the 802.11i standard, the extension is supported by all major supplicant vendors including Microsoft, Funk and Meetinghouse.

10.1.9.4 Pre-Authentication

Pre-authentication is another fast roaming option specified in the 802.11i standard. When a MU is associated with AP1, and it discovers another access point/port AP2 (through beacons/probes) supports the same WLAN, the MU conducts an 802.1x exchange with AP2, thus deriving the PMK.

This exchange happens through AP1. If the MU roams to AP2, it can use this newly derived PMK to perform the handshake and skip the 802.1x phase. The 802.1x exchange through the second AP occurs while the MU is still associated with the first AP.

All the EAP frames are sent to the first AP, which forwards these frames to the second AP over the wire, which then can forward them to the Radius server.

Although pre-authentication is supported on Motorola switches, it is more useful in a standalone access point environment, or a mixed deployment of switches and access points since the PMK cannot be shared across standalone APs.

In a wireless switch architecture, opportunistic PMK caching provides the same functionality as pre-authentication without the additional load on the Radius serve and extra EAP messaging.

10.1.9.5 Support for 802.11i

The following Motorola Enterprise WLAN devices support 802.11i/WPA2:

- CB3000
- AP-5131
- AP-5181
- WS2000
- WS5100
- RFS6000
- RFS7000

10.1.10 802.11j

802.11j is an amendment to the IEEE 802.11 standard designed specially for the Japanese market. It allows WLAN operation in the 4.9 to 5 GHz band to conform to Japanese rules for radio operation for indoor, outdoor and mobile applications. The amendment has been incorporated into the published IEEE 802.11-2007 standard.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, and 802.11g versions to provide wireless connectivity in the home, office and commercial establishments.

10.1.10.1 Operation in Japan

The 802.11j standard *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: 4.9 to 5 GHz Operation in Japan* was finalized in 2004. The standard works in the 4.9 GHz to 5 GHz band to conform to the Japanese rules for radio operation for indoor, outdoor and mobile applications.

802.11j defines uniform methods that let APs move to new frequencies or change channel width for better performance or capacity, for example, to avoid interference with other wireless applications.

Public Safety

In the USA, the 4.9 GHz band is reserved for use by public safety wireless applications. The transmission mask is narrower for the public safety band than for consumer part 15 applications. Thus, one cannot simply operate 802.11j equipment in the public safety band and be FCC compliant. Public safety agencies are working with manufacturers and the FCC to leverage *Commercial Off The Shelf* (COTS) equipment. There are public safety groups working closely with the manufacturing community, federal interests, and standards bodies to create an 802.11 series standard for public safety.

10.1.11 802.11k

IEEE 802.11k is a proposed amendment to the IEEE 802.11-2007 standard for radio resource management. It defines and exposes radio and network information to facilitate the management and maintenance of a WLAN.

10.1.11.1 Radio Resource Management

IEEE 802.11k and 802.11r are the key industry standards now in development that enable seamless *Basic Service Set* (BSS) transitions in the WLAN environment. The 802.11k standard provides information to discover the best available access point.

802.11k is intended to improve the way traffic is distributed within a network. In a WLAN, each device normally connects to the AP that provides the strongest signal. Depending on the number and geographic locations of the subscribers, this arrangement can sometimes lead to excessive demand on one AP and an under utilization of others, resulting in degradation of overall network performance. In a network conforming to 802.11k, if the AP having the strongest signal is loaded to its full capacity, a wireless device is connected to one of the under utilized APs. Even though the signal may be weaker, the overall throughput is greater because more efficient use is made of the network resources

10.1.12 802.11m

IEEE 802.11m is an initiative to perform editorial maintenance, corrections, improvements, clarifications and interpretations relevant to documentation for the IEEE 802.11 family specifications. The term 802.11m also refers to the set of maintenance releases itself.

10.1.13 802.11n

IEEE 802.11n is a proposed amendment to the IEEE 802.11-2007 wireless networking standard to significantly improve network throughput over previous standards, such as 802.11b and 802.11g, with many experts claiming this wireless technology's potential 248 Mbit/s data rate will finally allow consumers to move beyond traditional wired ethernet LANs.

IEEE 802.11n builds on previous 802.11 standards by adding *multiple-input multiple-output* (MIMO) and 40 MHz operation to the physical layer. MIMO uses multiple transmitter and receiver antennas to improve system performance. 40 MHz operation uses wider bands (compared to 20 MHz bands) to support higher data rates. Wider bandwidth channels are cost effective and easily accomplished with moderate increases in digital signal processing.

If properly implemented, 40 MHz channels can provide greater than two times the usable channel bandwidth of two 802.11 legacy channels. Coupling MIMO architecture with wider bandwidth channels offers the opportunity to create powerful (yet cost-effective) approaches for increasing the physical transfer rate. MIMO is a technology which uses multiple antennas to coherently resolve more information than possible using a single antenna. The two important benefits it provides to 802.11n are antenna diversity and spatial multiplexing.

Multipath signals are reflected signals arriving at the receiver some time after a *line of sight* (LOS) signal transmission has been received. In legacy 802.11 deployments, multipath signals were perceived as interference degrading a receiver's ability to recover the message information in the signal. MIMO uses the multipath signal's diversity to increase a receiver's ability to recover the message information from the signal.

Another ability MIMO provides is *Spatial Division Multiplexing* (SDM). SDM spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth. MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires a discrete antenna at both the transmitter and the receiver. In addition, MIMO technology requires a separate radio frequency chain and analog-to-digital converter for each MIMO antenna which translates to higher implementation costs compared to non-MIMO systems.

Channel bonding is a second technology being incorporated to 802.11n which can simultaneously use two separate non-overlapping channels to transmit data. Channel bonding increases the amount of data that can be transmitted. Payload optimization (or packet aggregation) is a third technology utilized within 802.11n resulting in more data incorporated within each transmitted data packet.

10.1.13.1 Data Encoding

A transmitter and receiver use precoding and post coding techniques, respectively, to maintain a MIMO link. Precoding includes spatial beamforming and spatial coding, where spatial beamforming improves the received signal quality at the decoding stage. Spatial coding can increase data throughput via spatial multiplexing and increase range by exploiting the spatial diversity, through techniques such as Alamouti coding.

10.1.13.2 Number of antennas

The number of simultaneous data streams is limited by the minimum number of antennas in use on both sides of the link. However, individual radios often further limit the number of spatial streams carrying unique data. The moniker helps identify what a given radio is capable of. The first number *(a)* is the maximum number of transmit antennas or RF chains that can be used by the radio. The second number *(b)* is the maximum number of receive antennas or RF chains used by the radio. The third number *(c)* is the maximum number of data spatial streams the radio can use. For example, a radio transmitting on two antennas and receiving on three, but can only send or receive two data streams.

10.1.13.3 Frame Aggregation

Aggregation is the main *medium access controller* (MAC) feature providing performance improvement. Aggregation shows the performance of various 802.11n MAC features at the completed proposal stage. There are two types of aggregation:

- Aggregation of *MAC service data units* (MSDUs) at the top of the MAC (often referred to as A-MSDU aggregation)
- Aggregation of *MAC protocol data units* (MPDUs or frames) at the bottom of the MAC (commonly referred to as A-MPDU aggregation)

Aggregation in the MAC is necessary to make the best use of the properties of the 802.11n physical layer. A-MPDU aggregation requires the use of *Block Acknowledgement* (or BlockAck), which was introduced in 802.11e and has been optimized in 802.11n. Reverse direction is an optional feature that supports a bidirectional data flow given a single channel access.

10.1.13.4 Backward compatibility

When 802.11g was released, it had to ensure coexistence between legacy and new devices. 802.11n extends coexistence management to protect its transmissions from legacy devices, which include 802.11g, 802.11b and 802.11a.

802.11n has defined three differences in the type of protection it enables:

1. Wi-Fi Alliance 11n draft 2.0 devices often operate in *mixed mode*. In mixed mode, each 802.11n transmission is embedded in an 802.11a or 802.11g transmission. For 20 MHz transmissions, the embedding takes care of protection with 802.11a and 802.11g. However, 802.11b devices still need CTS protection.
2. Transmissions at 40 MHz (in the presence of 802.11a, 802.11b, or 802.11g clients) require protection with a CTS on both 20 MHz sides of the 40 MHz channel, to prevent interference with legacy devices.
3. An access point can advertise devices use CTS or RTS/CTS protection, even in mixed-mode transmissions.

Even with protection, large discrepancies can exist between the throughput an 802.11n device can achieve when alone compared to what it can get when legacy devices are present. This is an extension of the 802.11b/802.11g coexistence problem.

10.1.13.5 Status

Work on the 802.11n standard dates back to 2004. The draft is expected to be finalized in March 2009 with publication in December 2009. However, major manufacturers are now releasing *pre-n*, *draft n* or *MIMO - based* products based on early specs. These vendors anticipate the final version will not be significantly different from the draft, and in a bid to get an early mover advantage, are pushing ahead with the technology. Depending on the manufacturer, a firmware update may eventually be able to make current *draft n* hardware compatible with the final version.

10.1.13.6 Wi-Fi Alliance

As of mid-2007, the Wi-Fi Alliance has started certifying products based on IEEE 802.11n draft 2.0.This certification program established a set of features and a level of interoperability across vendors supporting those features, thus providing one definition of *draft n*. The certification covers both 20 MHz and 40 MHz channels (and up to two spatial streams), for maximum throughputs of 130 Mbit/s for 20 MHz and 300 Mbit/s for 40 MHz. A number of vendors, in both the consumer and Enterprise spaces, have built products that have achieved this certification. The Wi-Fi Alliance certification program subsumed the previous industry consortium efforts to define 802.11n, such as the now dormant *Enhanced Wireless Consortium* (EWC). The Wi-Fi Alliance is investigating further work on certification of additional features of 802.11n not covered by the draft 2.0 certification, including higher numbers of spatial streams (3 or 4), as well as extended range support through beamforming and Space-Time Block Coding.

10.1.13.7 Wi-Fi Alliance Time Line

January 2004

IEEE announced it had formed a new *802.11 task group* (TG) to develop a new amendment to the 802.11 standard for wireless local-area networks. The real data throughput will reach a theoretical 270 Mbit/s for the required dual stream MIMO device. (which may require an even higher raw data rate at the physical layer), and should be up to 20 times faster than 802.11b, up to 3 times faster than 802.11a, and up to 4 times faster than 802.11g.

19 January 2006

The IEEE 802.11n task group approved the joint proposal's specification, based on EWC's draft specification.

March 2006

The IEEE 802.11 working group sent the 802.11n draft to its first letter ballot, allowing the 500+ 802.11 voters to review the document and suggest bug fixes, changes and improvements.

2 May 2006

The IEEE 802.11 working group voted not to forward draft 1.0 of the proposed 802.11n standard. Only 46.6% voted to approve the ballot. To proceed to the next step in the IEEE standards process, a majority vote of 75% is required. This letter ballot also generated approximately 12,000 comments-much more than anticipated.

November 2006

The task group voted to accept draft version 1.06, incorporating all accepted technical and editorial comment resolutions prior to this meeting. An additional 800 comment resolutions were approved during the November session which will be incorporated into the next revision of the draft. As of this meeting, three of the 18 comment topic ad hoc groups chartered in May have had completed their work and 88% of the technical comments had been resolved with approximately 370 remaining.

19 January 2007

The IEEE 802.11 working group unanimously (100 yes, 0 no, 5 abstaining) approved a request by the 802.11n task group to issue a new draft 2.0 of the proposed standard. Draft 2.0 was based on the task group's working draft version 1.10. Draft 2.0 was the cumulative result of thousands of changes to the 11n document as based on all previous comments.

7 February 2007

The results of Letter Ballot 95, a 15-day procedural vote, passed with 97.99% approval and 2.01% disapproval. On the same day, the 802.11 working group announced the opening of Letter Ballot 97. It invited detailed technical comments to closed on 9 March 2007.

9 March 2007

Letter Ballot 97, the 30-day technical vote to approve draft 2.0, closed. They were announced by IEEE 802 leadership during the Orlando Plenary on 12 March 2007. The ballot passed with an 83.4% approval, above the 75% minimum approval threshold. There were still approximately 3,076 unique comments, which will be individually examined for incorporation into the next revision of draft 2.

25 June 2007

The Wi-Fi Alliance announces its official certification program for devices based on draft 2.0.

7 September 2007

Task group agrees on all outstanding issues for draft 2.07. draft 3.0 is authorized, which possibly may go to a sponsor ballot in November 2007.

November 2007

Draft 3.0 was approved (240 voted affirmative, 43 negative, and 27 abstained). The editor was authorized to produce draft 3.01.

January 2008

Draft 3.02 was approved. This version incorporates previously approved technical and editorial comments. There remain 127 unresolved technical comments. It is expected all remaining comments will be resolved and the task group and WG11 will subsequently release draft 4.0 for working group recirculation ballot following the March meeting.

10.1.14 802.11p

IEEE 802.11p is a draft amendment to the IEEE 802.11 standard to add wireless access in the *vehicular environment* (WAVE). It defines enhancements to 802.11 required to support *Intelligent Transportation Systems* (ITS) applications. This includes data exchange between high-speed vehicles and between vehicles and roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard on which IEEE 802.11p is based.

802.11p will be used as the groundwork for *Dedicated Short Range Communications* (DSRC), a U.S. Department of Transportation project based on European system CALM looking at vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services and commerce transactions via cars. The ultimate vision is a nationwide network that enables communications between vehicles and roadside access points or other vehicles. This work builds on its predecessor ASTM E2213-03.

The 802.11p task group is still active. Per the official IEEE 802.11 work plan, an approved 802.11p amendment is scheduled to be published in April 2009.

10.1.15 802.11r

802.11r is a standard supporting fast roaming. Fast roaming is something Motorola radios have supported for years.

Credential caching is the key to high speed roaming. Once a MU is authenticated, it is valid for all APs adopted to that switch. 802.11r was pushed along by the need for secure VoWLAN and other latency sensitive applications.

A IEEE 802.11r fast BSS transition minimizes the number of frames lost when an MU roams from one AP to another. To accomplish this, it provides three services:

- A key management framework for security that allows a MU and AP to pre-compute session keys
- An (optional) mechanism by which a MU can negotiate and request resources on an AP before it roams to it
- A mechanism for exchanging messages either directly to the target AP (over-the-air) or by relaying them through the currently associated AP (over-the-DS)

The decision of when and how a MU decides to roam, and what AP it picks is out of the scope of 802.11r.

802.11r describes a *Remote-Request-Broker* (RRB) which passes messages from one AP to another (over-the-DS). Within a Motorola switch managed network, there is no RRB. The ccsrvr coordinates and handles communications on behalf of the new AP. For inter-switch fast roams, RRB is part of the ccsrvr process. This involves forwarding messages received from a MU targeted for an AP on another switch (an 802.11r action frame where the destination is not a BSS on the current switch), and forwarding responses from that AP back to the MU. If the received frames has errors or unsupported/invalid fields, the RRB generates error frames and sends them back to the MU.

802.11r makes provisions for a *Mobility Domain Controller* (MDC). The MDC is a server/service that authenticates various devices on the network, and sets up secure channels so keying information can be securely exchanged. The MDC does not play a role while roaming within a switch (since the keys remain in the switch as the user roams from one AP to another). MDC message formats and protocol descriptions are out of the scope of 802.11r. Thus, Motorola's implementations are non-standard (since there is no standard).

As long as switches have layer 2 connectivity (in a cluster), pre-authentication provides the generation of keying material on the target AP, and 802.11r provides fast BSS transition. Motorola's MDC service pushes/pulls keying and state information across switches with layer 3 connectivity between them.

10.1.15.1 Enabling 802.11r Support

An administrator can enable or disable support for 802.11r on a per-WLAN basis. When enabled, a *Mobility-Domain Information Element* (MDIE) is included in the beacons and probes for the specified WLAN.

The WLAN's index is included in the mobility domain Identifier field of the MDIE. This allows the switch to identify the WLAN the MU is transitioning to, without relying on the BSSID. In Motorola's multi-ESS-multi-BSS architecture, there could be multiple fast-roaming enabled WLANs on one BSS, and the BSSID is not enough to get to a unique WLAN.

WISPE (the protocol used by Motorola for communications between the switch and the AP) contains an information element configurable on the switch to include/remove the MDIE from its beacons and probes.

10.1.15.2 Key Derivation Frames

802.11r achieves faster BSS transitions by using special action frames and overloading 802.11 authentication and association messages to carry out a four-way handshake. A new authentication algorithm has been specified enabling an AP to determine whether an authentication request is *legacy.* Additional information elements have been added to these messages (MIC extent, RSNIE, FTIE etc) allowing an AP and MU to ensure session keys are fresh and key confirmations (MICs) are part of a 4-way handshake.

Action-frames are used by an MU when it wants to fast-roam to another AP and use a DS method to initiate a roam to the AP. Modified authentication frames are used when a MU wants to use an over-the-air fast-roam. In both cases, the MU completes the fast roam using a new (re)association request, which confirms the newly derived keys.

Both fast transition action frames and overloaded authentication and association frames can carrying out a base fast transition for Motorola's wireless infrastructure devices. Support for action confirm frames is required only for resource reservation.

Unlike a 802.11i handshake, an 11r handshake also includes elements through which an AP can inform a MU about how long a session (or session keys) is going to be valid. A timeout interval information element has been added for this purpose.

Motorola's switch and infrastructure platform supports fast BSS transitions with both pre-shared keys as well as with 802.1x authentication.

10.1.15.3 Keying Hierarchy

IEEE 802.11i provides a simple (MSK/PSK)->PTK keying hierarchy. IEEE 802.11r extends this into a three tier hierarchy, where the MSK/PSK lead to a R0 level key. This, in turn, is used to derive an R1 level key. The R1 level key is used for PTK generation. The lifetime of the derived keys is same as the lifetime of the original key (so they all expire together), but a compromise of one key does not bring down the complete key hierarchy, just everything under it.

R1 level keys are meant to be securely transmitted across APs. When the APs are controlled by the same switch, the keys do not need to move. For layer 3 connected switches, Motorola supports a MDC.

Protocol Capability	***802.11r***	***Status***	***WiOS Support***
Fast BSS transition		Optional	Yes
Mobility domain	IE	Mandatory	Yes
Fast BSS transition	IE	Mandatory	Yes
MIC extent	IE	Mandatory	Yes
Timeout Interval IE	Mandatory	Yes	
EAPOL key	IE	Mandatory	Yes
FT authentication algorithm		Mandatory	Yes
FT action frames		Mandatory	Yes, except for resource reservation confirm/Ack
FT based on 802.1x		Mandatory	Yes
FT based on PSK		Mandatory	Yes
FT key hierarchy		Mandatory	Yes. The portion of getting the R1 keys from one holder to another is undefined by 802.11r, and Motorola only supports R1 keys within a switch
FT initial association		Mandatory	Yes
FT base mechanism		Mandatory	Yes
FT base mechanism in RSN		Mandatory	Yes
FT base mechanism without RSN		Mandatory	Yes
Reservation mechanism		Optional	No
Other capabilities related to reservation procedures		Mandatory, if Reservation supported	No

10.1.16 802.11s

The pre-802.11s standard is used extensively by Motorola. However, there are no Motorola Enterprise WLAN products that have an 802.11s radio embedded in them. 802.11s is supported by police and fire departments requiring unique and proprietary deployments.

A 802.11s approach fits layer 3 routing concepts into the MAC layer. Motorola's MEA product is pre-802.11s and is proprietary. No WiFi products will communicate directly to MEA.

IEEE 802.11s is a draft IEEE 802.11 amendment for mesh networking, defining how wireless devices can interconnect to create an ad-hoc network.

802.11s extends the IEEE 802.11 MAC standard by defining an architecture and protocol supporting both broadcast/multicast and unicast delivery using radio-aware metrics over self-configuring multi-hop topologies.

802.11s started as a study group of IEEE 802.11 in September 2003. It became a task group in July 2004. A call for proposals was issued in May 2005, which resulted in the submission of 15 proposals submitted to a vote in July 2005. After a series of eliminations and mergers, the proposals dwindled to two, which became a joint proposal in January 2006. This merged proposal was accepted as draft D0.01 after a unanimous confirmation vote in March 2006.

The draft evolved through informal comment resolutions until it was submitted for a letter ballot in November 2006 as draft D1.00. As of April 2008, the draft is at D2.00. Draft D2.00 failed to reach approval through a letter ballot on May 3 with approximately 61% approval. Letter ballots must reach the necessary 75% approval to pass.

The task group has scheduled an ad hoc meeting on June 23-25 in Munich, Germany, to work on comment resolution. The task group's stated goal for the July 2008 802.11 meeting is to continue to resolve comments and improve its draft.

10.1.16.1 Mesh Architecture

Devices in an 802.11s mesh network are often referred to as *Mesh Points* (MP). Mesh points form links with one another, over which mesh paths can be established using a routing protocol. 802.11s defines a default mandatory *Hybrid Wireless Mesh Protocol* (HWMP), yet allows vendors to operate using alternate protocols. HWMP is inspired by a combination of AODV (RFC 3561) and tree-based routing. An alternate protocol may be based on OLSR (RFC 3626).

MPs can be individual devices using mesh services to communicate with other devices in the network. They can also be 802.11 APs providing access to mobile clients, which have broad market availability. Also, MPs can take the role of a gateway and provide access to one or more 802.3 networks through a mesh portal. In both cases, 802.11s provides a proxy mechanism to provide addressing support for non-mesh 802 devices, allowing end-points to be cognizant of external addresses.

802.11s also includes mechanisms to provide deterministic network access, congestion control and power save.

10.1.17 802.11T

IEEE 802.11t is a proposed test specification to the IEEE 802.11 standard. IEEE 802.11T is also referred to as the *Wireless Performance Prediction* (WPP) - test methods and metrics recommendation. Given the complexity of the IEEE 802.11 family of protocols, a test specification is particularly important so product specifications and performance can be ascertained. The capital *T* in the title shows this is a recommended practice and not a standard.

The goal of the 802.11T is to provide a set of measurements, performance metrics, and test recommendations that enable manufacturers, independent test labs, service providers, and end users to measure the performance of IEEE 802.11 standard equipment and networks.

802.11T, scheduled for completion in January 2008, will have its PAR withdrawn in July 2008.

10.1.18 802.11u

IEEE 802.11u is a proposed amendment to the IEEE 802.11-2007 standard to add features that improve networking with external networks.

IEEE 802.11 makes the assumption a user is pre-authorized to use a network. IEEE 802.11u supports cases where a user is not pre-authorized. With 802.11u, a network is able to allow access based on a user's relationship with an external network (hotspot roaming agreements), indicate online enrollment is possible, or allow access to a limited set of services (such as emergency calls).

From a user's perspective, the aim is to improve the experience of a traveling user who turns on their laptop many miles from home. Instead of being presented with a long list of largely meaningless SSIDs, the traveling user could be presented with a list of networks, the services they provide, and the conditions under which the user can access them.

The IEEE 802.11u *Proposal Requirements Specification* contains requirements in the areas of enrollment, network selection, emergency call support, user traffic segmentation, and service advertisement.

The 802.11u standard is in its proposal evaluation stages. Per the official IEEE 802.11 work plan predictions, the formal 802.11u standard is scheduled to be published in May 2009.

10.1.19 802.11v

IEEE 802.11v is a proposed amendment to the IEEE 802.11 standard to allow the configuration of client devices connected to wireless networks.

802.11v is the *Wireless Network Management* standard for the IEEE 802.11 family of standards. An amendment to the 802.11 standard is in progress to allow the configuration of client devices while connected to IEEE 802.11 networks. The standard may include cellular-like management paradigms.

The 802.11v standard is still in its early proposal stages.

10.1.20 802.11w

IEEE 802.11w is a proposed amendment to the IEEE 802.11 standard to increase the security of management frames.

IEEE 802.11w is the *Protected Management Frames* standard for the IEEE 802.11 family of standards. 802.11w aims to improve the IEEE 802.11 *Medium Access Control* (MAC) layer to increase management frame security.

WLANs send system management information in unprotected frames, making them vulnerable. 802.11w will protect against network disruption caused by malicious systems that forge disassociation requests appearing to be sent by valid equipment.

802.11w extends IEEE 802.11i to apply to 802.11 management frames as well as data frames. These extensions will have interactions with IEEE 802.11r and IEEE 802.11u

The 802.11w standard is in its early proposal stages. The target for ratification is in 2008.

10.1.21 802.11y

IEEE 802.11y is an amendment to the IEEE 802.11 standard that enables high powered Wi-Fi equipment to operate on a co-primary basis (except when near a satellite earth station) in the 3650 to 3700 MHz band within the United States.

In June 2007 the FCC issued final rules for a novel lite licensing scheme in the 3650-3700 MHz band. Licensees pay a small fee for a nation wide, non-exclusive license. They then pay an additional nominal fee for each high powered base MU deployed. Neither client devices (fixed or mobile), or their operators require a license, but devices must receive an enabling signal from a licensed base station before transmitting. All stations must be identifiable in the event they cause interference to incumbent operators in the band. Further, multiple devices are provided an opportunity to transmit in the same area using a contention based protocol when possible. If interference between licensees, or the devices they have enabled, cannot be mediated by technical means, licensees are required to resolve the dispute between themselves.

US 3650 MHz rules allow registered stations to operate at much higher power than traditional Wi-Fi gear (up to 20 watts equivalent isotropically radiated power). The combination of higher power limits and enhancements to the MAC timing in 802.11-2007, allow the development of standards based 802.11 devices that can operate at distances of 5 km or more.

IEEE 802.11y adds three new concepts to 802.11-2007:

- *Contention based protocol* (CBP) - Enhancements have been made to 802.11 carrier sensing and energy detection mechanisms to meet FCC requirements for a contention based protocol.
- *Extended channel switch announcement* (ECSA) - Provides a mechanism for an access point to notify its connected MUs of its intention to change channels or channel bandwidth. This mechanism will allow a WLAN to continuously choose the least noisy channel and the channel least likely to cause interference. This mechanism will also be used in 802.11n, allowing devices to switch between 802.11y operation and 802.11n operation in the 2.4 and 5 GHz bands.
- *Dependent station enablement* (DSE)- Is the mechanism an operator uses to extend permission to license exempt devices (referred to as dependent STAs in 802.11y) to use a licensed radio spectrum. Fundamentally, this process satisfies a regulatory requirement that dictates dependent MU operation is contingent upon its ability to receive periodic messages from a licensee base station. However, DSE is extensible to other purposes in regards to channel management and coordination. Some benefits of DSE include:
    - The enabling device (the licensee's base station) may or may not be the access point that the dependent MU connects to. In fact, an enabling device may enable both an access point and its clients. Also, although the dependent devices are required (by regulatory) to receive information from the enabling device over the air, they are not required transmit over the air to complete the DSE process. A dependent device may connect to a nearby access point for a short period of time and use the internet or some other means to complete the channel permissioning process. This flexibility reduces the likelihood of a dependent device causes interference while attempting to connect to a remote device.
    - The personal privacy and security of end users are ensured while, at the same time, licensees have the information necessary to resolve disputes. 802.11y devices transmit a unique identifier for resolving interference. High powered fixed stations and enabling stations transmit the location they are operating is as their unique identifier. The location is also registered in an FCC database that will identify the licensee. Dependent stations broadcast the location of the device that enabled it plus a unique string supplied by the enabling device. This ensures the responsible part (the licensee) is contacted to resolve disputes. This mechanism also alleviates the problems associated with having the dependent devices broadcasting its location. Requiring all devices to have GPS or some other means of verifying their location would increase the cost and complexity of devices, and this solution may be inadequate indoors. This method also resolves fears MU that constantly beacon its location could be used inappropriately by third parties to track a user's location.

10.1.21.1 Beyond the US 3650 Band

While 802.11y's scope is limited to operation in the US 3650-3700 MHz band, care was taken so that, if the light licensing concept was well received, it would not be necessary to start the 3 year task group process for 802.11y devices to operate in other countries or in other frequency bands. As a result, lightly licensed 802.11 devices will be able to operate in any 5, 10, or 20 MHz channel that regulators make available by simply adding entries to the country and regulatory information tables in Annex I and J of 802.11.

Other potential bands for 802.11y include:

- *4.9 GHz* - The regulatory classes and channel sizing needed to support the US public safety allocation at 4.9 GHz were added to 802.11-2007[3]. DSE and ECSA will allow frequency coordinators to have dynamic control over channel access.
- *5 GHz* - Regulators and equipment manufactures continue to debate the effectiveness of *dynamic frequency selection* (DFS) as a mechanism to avoid incumbent users in the 5 GHz bands. For example, Canada is not currently certifying 802.11 equipment for use in the 5600-5650 MHz band used by certain types of weather radars. 802.11y may provide a solution that will allow WLANs access to these bands. Firstly, DSE can be used to create exclusion zones around incumbent users. Secondly, when combined with DSE, the 802.11y device identification mechanism allows devices that cause interference to be denied further access to a channel within seconds.
- *IMT-Advanced candidate bands- (450-862, 2300-2400, 2700-2900, 3400-4200, and 4400-5000 MHz* - Since 2003, *The International Telecommunications Union* (ITU) has been studying the potential for IMT-advanced services (aka systems beyond IMT-2000 or 4G) to use a number of frequencies between 450 and 5000 MHz for the next generation of cellular infrastructure. These systems will be capable of transmitting 100 Mb/s when mobile and 1000 Mb/s while stationary. Unfortunately, with the exception of a small amount of UHF spectrum available upon the completion of the transition from analogue to digital television, these bands are occupied on a piecemeal basis by incumbent users not easily relocated. Extensive studies have concluded that co-existence with legacy equipment over the same area is not feasible, so traditional mobile licensing approaches are not practical. Yet, academic studies have shown at any give time, even in dense urban environment, there is ample unused spectrum across the candidate bands. The problem is usage by the primary services in these bands may change over time (as is the case with some radar systems) or vary by sub-channel based on location (as is the case in the TV bands *white spaces*). 802.11y, along with the continued advances in multi-band radio technology, may provide a solution to this problem by granting channel access dynamically to users based on primary user avoidance techniques, location and time. The US has not been able to adopt a single position on the suitability of the 3650-3700 band for IMT-advanced, and neither of the proposed positions seem to recognize the FCC's rules, or the standardization work done to date.

10.1.21.2 802.11y Applications

Some 802.11y applications include:

- Back haul for municipal Wi-Fi networks
- Industrial automation and controls
- Campus and Enterprise networking
- Last mile wireless broadband access
- Fixed point to point links
- Fixed point to mobile links
- Public safety and security networks

10.1.21.3 802.11y Timeline

- In 1995, NTIA (as per an OMB report) suggests the *transfer* of the 3650 MHz to 3700 MHz frequency band to *mixed use* status
- Dec 1998: FCC's 3650 Allocation press release announces the primary to mixed use transition, Dec 17 1998 (Kennard's FCC.. see FCC 98-337) [7]
- Jan 1999: The spectrum from 3650 to 3700 is given *mixed-use status* and becomes available for non-federal use
- Apr 2004: Original NPRM dated 04/23/2004 (FCC-04-100) from Powell's FCC.. Titled *Unlicensed Operation in the Band 3650-3700 MHz et al*. These are the proposed rules to maximize the efficient use of the 3650-3700 band and foster the introduction of new and advanced services
- Mar 2005: FCC releases R&O (from EOT) dated 03/16/2005, (FCC-05-56) which describes in detail the use of the 3650 band and is titled *Wireless Operations in the 3650-3700 MHz Band; Rules for Wireless Broadband Services in the 3650-3700 MHz Band*
- Mar 2005: 802.11's WNG requests that a CBP study group be formed (CBP-SG) to examine the opportunities afforded by FCC's 3650 MHz Report and Order and Memorandum Opinion and Order (FCC 05-56).
- Nov 2005: The PAR and Five Criteria from the CBP-SG are approved by the 802 Executive Committee creating the 802.11y task group.
- Jan 2007: First letter ballot received greater than 75% approval from 802.11 WG
- Jun 2007: This is the FCC's MO&O dated 06/07/2007 from OET (FCC-07-99) in which the commission addresses the many petitions for reconsideration and other filings that resulted from FCC's 05-56 Report and Order
- Jun 2007: Draft 3.0 received 94% approval from 802.11 WG
- Jul 2007: Conditional approval was obtained from the 802.11 working group and granted by the Executive Committee to forward .11y to sponsor ballot
- Aug 2007: Last Ex-Parte comment filed on proceeding 04-151 in response to FCC's NPRM and R&O describing operations in the 3650 band. Almost 450 comments are filed
- Nov 2007: FCC begins providing the means, via FCC's Universal Licensing System, to allow non-Federal operators to purchase non-exclusive nationwide licenses to allow for licensed operations in the 3650 Band. Licensee call signs are assigned upon approval of application
- Dec 21, 2007: IEEE/ISO Sponsor Ballot begins for the 802.11 amendment y Standard using draft 7 of the amendment.
- Apr 16, 2008: After three IEEE/ISO Sponsor Ballot Recirculations--the last ending Apr 18th 2008--draft 10.0 of Amendment y, of the 802.11 Base Standard, is ready to be submitted to the IEEE RevCom in preparation for publication

10.2 Security Standards

This section describes the wireless security standards adopted by Motorola within our wireless infrastructure offerings. They include:

- *WPA*
- *WPA2*

- *EAP*

10.2.1 WPA

Wi-Fi Protected Access (WPA and WPA2) is a certification program administered by the Wi-Fi Alliance to indicate compliance with security protocols created to secure wireless computer networks. This protocol was created in response to several serious weaknesses researchers had found in the previous system, *Wired Equivalent Privacy* (WEP). The protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. The protocol is specifically designed to work with pre-WPA wireless network interface cards that pre-date the protocol (through firmware upgrades), but not necessarily with first generation wireless access points. The WPA2 certification mark indicates compliance with an advanced protocol that implements the full standard. This advanced protocol will not work with some older network cards.

10.2.1.1 WPA's History

WPA is a certification program created by the Wi-Fi Alliance, an industry trade group, which owns the Wi-Fi trademark and certifies devices that bear that mark.

A WPA certification mark indicates compliance with a security protocol designed to enhance the security of wireless networks. There are two versions of this protocol: Enterprise and personal. Enterprise is for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable *pre-shared key* (PSK) mode, where every allowed computer is given the same passphrase. With PSK, security depends on the strength and secrecy of the passphrase. The design of the protocol is based on a Draft 3 of the IEEE 802.11i standard.

The Wi-Fi Alliance created the protocol to introduce standard-based wireless network products prior to the IEEE 802.11i group finishing its work. The Wi-Fi Alliance (at the time) had already anticipated the WPA2 certification based on the final draft of the IEEE 802.11i standard. Therefore, they intentionally made the tags on the frame fields (also known as information elements, or IEs) different from 802.11i to avoid the confusion in unified implementations of both the original and advanced versions of the protocol.

Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in the protocol is *Temporal Key Integrity Protocol* (TKIP). TKIP dynamically changes keys as the system is used. When combined with the much larger initialization vector, TKIP provides improved protection against, and effectively defeats, well-known key recovery attacks on WEP.

In addition to authentication and encryption, WPA provides a vastly improved payload integrity. The *cyclic redundancy check* (CRC) used in WEP is inherently insecure. Consequently, it is possible to alter the payload and update the message CRC without knowing the WEP key. A more secure message authentication code (known as a MAC or MIC *message integrity code*) is used in the protocol, using an algorithm named *Michael*. The MIC used in WPA includes a frame counter, which prevents replay attacks being executed.

WPA makes breaking into a wireless LAN difficult by increasing the size of the keys and IVs, reducing the number of packets sent with related keys, and adding a secure message verification system. The algorithm was the strongest Wi-Fi Alliance designers could come up with that would work with most older network cards. TKIP will shut down the network for one minute if two frames are discovered that fail the MIC check (after passing all other integrity checks that would have caught noisy frames). It then requires the generation of new keys and reauthentication when the network restarts, forcing the attacker to start over.

10.2.2 WPA2

The WPA2 advanced protocol (certified through Wi-Fi Alliance's WPA2 program), implements mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm called CCMP, that is considered

fully secure. Beginning March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be certified by the Wi-Fi Alliance as *Wi-Fi CERTIFIED*.

10.2.2.1 Security in Pre-Shared Key Mode

Pre-shared key mode is designed for home and small office networks that don't require the complexity of an 802.1X authentication server. Each user must enter a passphrase to access the network. The passphrase can be from 8 to 63 printable ASCII characters or 64 hexadecimal digits (256 bits). If you choose to use the ASCII characters, a hash function reduces it from 504 bits (63 characters * 8 bits/character) to 256 bits (using also the SSID). The passphrase can be stored on the user's computer at their discretion under most operating systems to avoid re-entry. The passphrase must remain stored in the wireless access point.

Security is strengthened by employing a PBKDF2 key derivation function. However, weak passphrases are vulnerable to password attacks. To protect against a brute force attack, a truly random passphrase of at least 20 characters should be used, and 33 characters or more is recommended.

Some consumer chip manufacturers have attempted to bypass weak passphrases by automatically generating and distributing strong keys through a software or hardware interface that uses an external method of adding a new wireless adapter or appliance to a network. These methods include pushing a button (Broadcom SecureEasySetup and Buffalo AirStation One-Touch Secure System) and entering a short challenge phrase through software (Atheros JumpStart and ZyXEL OTIST). The Wi-Fi Alliance has standardized these methods and certifies compliance with these standards through a program called *Wi-Fi Protected Setup* (formerly Simple Config).

10.2.2.2 EAP Extensions Under WPA and WPA2 Enterprise

The Wi-Fi alliance has announced the inclusion of additional EAP types to its certification programs for WPA and WPA2. This ensures WPA-Enterprise certified products can interoperate with one another. Previously, only EAP-TLS (*Transport Layer Security*) was certified by the Wi-Fi alliance.

The EAP types now included in the certification program include

- EAP-TLS (previously tested)
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

Other EAP types can be supported by 802.1X clients and servers. Certification is an attempt for EAP types to interoperate. Their failure to do so is currently one of the major issues preventing the rollout of 802.1X on heterogeneous networks.

Hardware support

Most newer Wi-Fi certified devices support the security protocols discussed above, as compliance with this protocol has been required for Wi-Fi certification since September 2003.

The protocol certified through the Wi-Fi Alliance's WPA program (and to a lesser extent WPA2) was specifically designed to work with wireless hardware produced prior to the introduction of the protocol. Many of these devices support the security protocol after a firmware upgrade. However, firmware upgrades are not available for all legacy devices

10.2.3 EAP

Extensible Authentication Protocol (EAP) is a universal authentication framework frequently used in wireless networks and point-to-point connections. EAP is defined by RFC 3748. Although the EAP protocol is not limited to wireless LANs (and can be used for wired LAN authentication), it is most often used in wireless LAN deployments. Recently, the WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanisms.

EAP is an authentication framework, not a specific authentication mechanism. EAP provides some common functions and a negotiation of desired authentication mechanisms. Such mechanisms are called EAP methods, and there are currently about 40 different methods. Methods defined in IETF RFCs include; EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, and EAP-AKA. In addition, a number of vendor specific methods and new proposals exist. Commonly used modern methods capable of operating in wireless networks include; EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP and EAP-TTLS. Requirements for EAP methods used in wireless LAN authentication are described in RFC 4017.

Modern EAP methods can provide a secure authentication mechanism and negotiate a secure PMK between the client and NAS. The PMK can then be used for the wireless encryption session which uses TKIP or CCMP (based on AES) encryption.

EAP is not a wire protocol, instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages. In the case of 802.1X, this encapsulation is called *EAP over LANs* (EAPOL). For more information on the each types, see:

- *LEAP*
- *EAP-TLS*
- *EAP-MD5*
- *EAP-PSK*
- *EAP-TTLS*
- *EAP-IKEv2*
- *PEAP*
- *PEAPv0/EAP-MSCHAPv2*
- *PEAPv1/EAP-GTC*
- *EAP-FAST*

10.2.3.1 LEAP

The *Lightweight Extensible Authentication Protocol* (LEAP) is a proprietary EAP method developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard. Cisco distributed the protocol through the CCX (*Cisco Certified Extensions*) as part of getting 802.1X and dynamic WEP adoption into the industry in the absence of a standard. There is no native support for LEAP in any Windows operating system, but it is widely supported by third party client software included with WLAN devices. Due to the wide adoption of LEAP in the networking industry, many other WLAN vendors support LEAP.

LEAP uses a modified version of MS-CHAP, an authentication protocol in which user credentials are not strongly protected and easily compromised. Along these lines, an exploit tool called ASLEAP was released in early 2004 by Joshua Wright. Cisco recommends customers that absolutely must use LEAP do so only with sufficiently complex passwords, though complex passwords are difficult to administer and enforce. Cisco's current general recommendation is to use newer and stronger EAP protocols such as EAP-FAST, PEAP or EAP-TLS.

10.2.3.2 EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an IETF open standard. EAP-TLS is well supported among wireless vendors. TLS security (often called Secure Sockets Layer) is strong, as long as the user understands potential warnings about false credentials. It uses PKI to secure communication to a Radius authentication server or another type of authentication server. Even though EAP-TLS provides excellent security, the overhead of client-side certificates could be its achilles heel.

EAP-TLS is the original standard wireless LAN EAP authentication protocol. Although it is rarely deployed, it is still considered one of the most secure EAP standards available and is universally supported by all manufacturers of wireless LAN hardware and software including Microsoft. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience versus security trade-off. A compromised password is not enough to break into an EAP-TLS enabled system because a hacker still needs to have a client-side private key. The highest security available is when client-side keys are housed in smartcards, since there is no way to steal a certificate's corresponding private key from a smartcard without stealing the smartcard itself. It is significantly more likely the physical theft of a smartcard would be noticed (and the smartcard immediately revoked) than a (typical) password.

Up until April 2005, EAP-TLS was the only EAP type vendors needed to certify for a WPA or WPA2 logo. There are client and server implementations in Microsoft, Cisco, Apple, Linux, and open source. EAP-TLS is natively supported in Mac OS X 10.3 and above, Windows 2000 SP4, Windows XP, Windows Vista, Windows Server 2003, Windows Mobile 2003 and Windows CE 4.2.

10.2.3.3 EAP-MD5

EAP-MD5 (defined in RFC 3748) is the only IETF standards track based EAP method. It offers minimal security (the MD5 hash function is vulnerable to dictionary attacks), and does not support key generation. This makes it unsuitable for use with dynamic WEP or WPA/WPA2. EAP-MD5 differs from other EAP methods in that it only provides authentication of the EAP peer to the EAP server but not mutual authentication. By not providing EAP server authentication, EAP-MD5 is vulnerable to man-in-the-middle attacks.

10.2.3.4 EAP-PSK

EAP-PSK, defined in RFC 4764, is an EAP method for mutual authentication and session key derivation using a PSK. It provides a protected communication channel when mutual authentication is successful and is designed for authentication over insecure networks such as IEEE 802.11.

EAP-PSK is documented in an experimental RFC that provides a lightweight and extensible EAP method that does not require public-key cryptography. The EAP method protocol exchange is done in a minimum of four messages.

10.2.3.5 EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. It was co-developed by Funk Software and Certicom. It is widely supported across platforms, although there is no native OS support for this EAP protocol in Microsoft Windows, as it requires the installation of extra programs (such as SecureW2).

EAP-TTLS provides good security. The client does not need be authenticated via a CA-signed PKI certificate to the server, only the server to the client. This greatly simplifies the setup procedure, as the certificate does not need to be installed on every client.

After the server is securely authenticated to the client via its CA certificate, the server can then use the established secure connection (or *tunnel)* to authenticate the client. It can use an existing and widely

deployed authentication protocol and infrastructure (incorporating legacy password mechanisms and authentication databases) while the secure tunnel provides protection from eavesdropping and man-in-the-middle attack. A user's name is never transmitted in unencrypted cleartext, thus improving privacy.

10.2.3.6 EAP-IKEv2

EAP-IKEv2 is an EAP method based on the *Internet Key Exchange Protocol version 2* (IKEv2). It provides mutual authentication and session key establishment between an EAP peer and an EAP server. It supports authentication techniques based on the following types of credentials:

- *Asymmetric key pairs* - public/private key pairs where the public key is embedded into a digital certificate, and the corresponding private key is known only to a single party.
- *Passwords* - low-entropy bit strings that are known to both the server and the peer.
- *Symmetric keys* - high-entropy bit strings that are known to both the server and the peer.

It's possible to use a different authentication credential (and thereby technique) in each direction. For example, the EAP server authenticates itself using a public/private key pair and the EAP peer using a symmetric key. In particular, the following combinations are used in practice:

EAP Server	***EAP Peer***
Asymmetric key pair	Asymmetric key pair
Asymmetric key pair	Symmetric key
Asymmetric key pair	Password
Symmetric key	Symmetric key

EAP-IKEv2 is described in the Internet Draft (draft-tschofenig-eap-ikev2-15.txt). A prototype implementation can be found at *http://eap-ikev2.sourceforge.net*.

10.2.3.7 PEAP

PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.

The PEAP standard was created by Microsoft, Cisco, and RSA after EAP-TTLS had already come on the market. Even with its late start, Microsoft's and Cisco's size allowed them to quickly overtake EAP-TTLS in the market. PEAP is so successful in the market place that even Funk Software (the inventor and backer of EAP-TTLS), had no choice but to support PEAP in their server and client software for wireless networks.

As of May of 2005, there were two PEAP sub-types certified for the updated WPA and WPA2 standard. They are:

- *PEAPv0/EAP-MSCHAPv2*
- *PEAPv1/EAP-GTC*

The terms PEAPv0 and PEAPv1 refer to the outer authentication method, the mechanism that creates the secure TLS tunnel to protect subsequent authentication transactions. EAP-MSCHAPv2, EAP-GTC, and EAP-SIM refer to the inner authentication method which facilitates user or device authentication.

10.2.3.8 PEAPv0/EAP-MSCHAPv2

PEAPv0/EAP-MSCHAPv2 is the technical term for what people most commonly refer to as *PEAP*. Whenever the word PEAP is used, it almost always refers to this form of PEAP, since most people have no idea there

are so many flavors of PEAP. Behind EAP-TLS, PEAPv0/EAP-MSCHAPv2 is the second most widely supported EAP standard in the world.

There are client and server implementations of it in Microsoft, Cisco, Apple, Linux and open source. PEAPv0/EAP-MSCHAPv2 is natively supported in Mac OS X 10.3 and above, Windows 2000 SP4, Windows XP, Windows Server 2003 and Windows CE 4.2. The server side implementation of PEAPv0/EAP-MSCHAPv2, called IAS (*Internet Authentication Service*), is also included in Windows 2003 server. PEAPv0/EAP-MSCHAPv2 enjoys universal support and is known as the PEAP standard.

The support for inner EAP methods in PEAPv0 varies by vendor, while Cisco's implementation of PEAPv0 supports inner EAP methods EAP-MSCHAPv2 and EAP-SIM, Microsoft only supports PEAPv0/EAP-MSCHAPv2, but not the PEAPv0/EAP-SIM mode. Microsoft also only supports PEAPv0, and doesn't support PEAPv1. Thus, they simply call PEAPv0 *PEAP* without the v0 or v1 designator.

Microsoft supports another form of PEAPv0, which they call PEAP-EAP-TLS. Cisco and other third-party server and client software don't support this version. PEAP-EAP-TLS does require a client-side digital certificate located on the client's hard drive or a more secure smartcard. PEAP-EAP-TLS is very similar in operation to the original EAP-TLS, but provides slightly more protection due to the fact that portions of the client certificate that are unencrypted in EAP-TLS are encrypted in PEAP-EAP-TLS. Since few third-party clients and servers support PEAP-EAP-TLS, users should probably avoid it unless they only intend to use Microsoft desktop clients and servers.

10.2.3.9 PEAPv1/EAP-GTC

PEAPv1/EAP-GTC was created by Cisco as an alternative to PEAPv0/EAP-MSCHAPv2. It allows an inner authentication protocol other than Microsoft's MSCHAPv2. EAP-GTC (*Generic Token Card*) is defined in RFC 3748. It carries a text challenge from an authentication server, and a reply which is assumed to be generated by a security token. EAP-GTC does not protect authentication data in any way.

Even though Microsoft (along with RSA and Cisco) co-invented the PEAP standard, Microsoft never added support for PEAPv1 in general. Consequently, PEAPv1/EAP-GTC has no native Windows OS support. Since Cisco has always favored the use of its own less secure proprietary LEAP and EAP-FAST protocols over PEAP (and markets them as simpler certificate-less solutions), standardized PEAP is rarely promoted by Cisco.

With no interest from Microsoft to support PEAPv1 and little interest from Cisco to promote PEAP in general, PEAPv1 authentication is rarely used. There is no native OS support for this EAP protocol.

Though there is no in-built support for PEAP-GTC in MS Windows, it is supported by the Cisco CCX extensions program. CCX compatibility is enabled by default on many vendor-provided 802.11A/B/G clients.

This version of PEAP is defined through the IETF internet draft (draft-josefsson-pppext-eap-tls-eap-10). This is an individual submission and not standardized in the IETF.

Cisco's implementation of PEAPv1 also supports EAP-SIM as the inner EAP method, other than EAP-GTC.

10.2.3.10 EAP-FAST

EAP-FAST (*Flexible Authentication via Secure Tunneling*) is a protocol proposal by Cisco Systems as a replacement for LEAP. The protocol was designed to address the weaknesses of LEAP while preserving its *lightweight* implementation. Use of server certificates is optional in EAP-FAST. EAP-FAST uses a P*rotected Access Credential* (PAC) to establish a TLS tunnel in which client credentials are verified. EAP-FAST has three phases. Phase 0 is an optional phase, in which the PAC can be provisioned manually or dynamically, but is outside the scope of EAP-FAST as defined in RFC4851. PAC provisioning is still officially *work-in-progress*, even though there are many implementations. PAC provisioning only needs to be done once for a Radius server, client pair. In Phase 1, the client and the AAA server uses the PAC to establish TLS tunnel. In Phase 2, client credentials are exchanged inside the encrypted tunnel.

When automatic PAC provisioning is enabled, EAP-FAST has a slight vulnerability. An attacker can intercept the PAC and subsequently use it to compromise user credentials. This vulnerability is mitigated by manual PAC provisioning or by using server certificates for the PAC provisioning phase.

There is also a vulnerability where a hacker's AP can use the same SSID, reject the users PAC and supply a new one. Most supplicants can be set to prompt the user if he will accept it. If they do, they send their credentials using the inner method to the hacker, who will then get either a cleartext password (EAP-FAST w/ GTC) or a vulnerable to dictionary attack MSCHAPv2 hash.

The PAC file is issued on a per-user basis. This is a requirement in RFC 4851 sec 7.4.4. When a new user logs on the network from a device, they need a new PAC file provisioned first. This is one reason why it is difficult not to run EAP-FAST in insecure anonymous provisioning mode. The alternative is to use device passwords instead, but then it is not the user that is validated on the network.

- EAP-FAST can be used without PAC files, falling back to normal TLS
- EAP-FAST is natively supported in Apple OS X 10.4.8 and newer
- EAP-FAST is defined in RFC 4851

11

Motorola's Wireless LAN Products

This chapter provides a brief overview of the access points, wireless switches and RF management tools comprising the Motorola Enterprise Wireless LAN suite. For more information, refer to:

11.1 Access Ports/Points

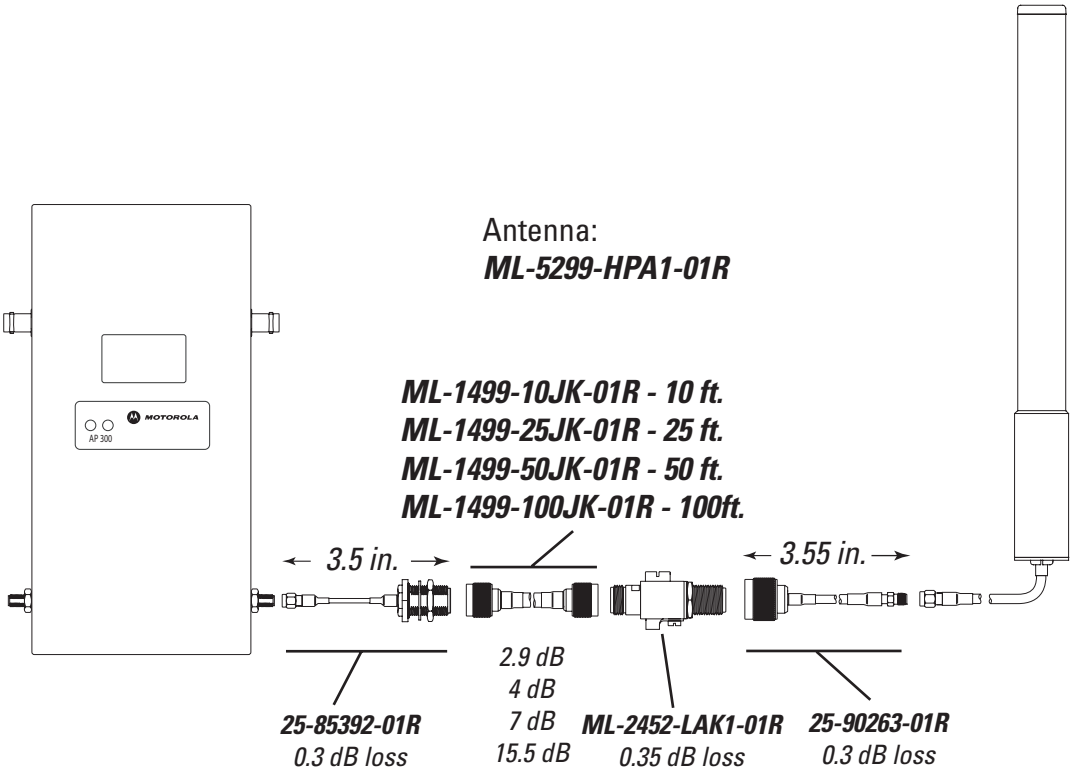
This sections describes the wireless thin access ports and fat access points supported by Motorola. They include:

11.1.1 AP300 Access Port

Motorola's AP300 delivers rich 802.11a/b/g connectivity, working in conjunction with Motorola's wireless switches as the point of connection between mobile devices and your wireless LAN.

A typical AP300 (external antenna) hardware deployment could appear as follows:

NOTE: For additional information on the detailed antenna and cabling options available to an AP300 model access port, refer to the *WLAN Antenna Specification Guide* available at http://support.symbol.com/support/product/manuals.do.



This thin next-generation access port is a low-cost device that is centrally and remotely managed through a Motorola wireless switch. Rapid configuration and the ability to quickly and easily upgrade the devices to support new functionality, features and security protocols substantially reduces the cost of deploying, implementing and managing your wireless LAN, while significantly increasing features, functionality and security of your wireless LAN infrastructure.

11.1.1.1 AP300 Features

Dual Form-Factors

The plastic internal-antenna housing allows for installation within the *carpeted-space* and provides cost-effective coverage via integrated 2.4 GHz and 5.2 GHz antennas.

Interoperability

Standards-based wireless, wired and security protocols ensure interoperability with third-party hardware.

802.1x supplicant

Allows authentication to a Radius server to enable an 802.1x-protected Ethernet port

802.11h

Enables worldwide operation through support for standards-based dynamic frequency selection and power control

802.11i

Support for IEEE standards-based security protocols for strong encryption (AES, TKIP), authentication and key management (802.1x-EAP)

802.3af

Simplifies and reduces total cost of installation through support of standards-based *Power-over-Ethernet* (PoE)

Load Balancing, Pre-Emptive Roaming and Rate Scaling

Increases reliability and resilience of the wireless network to support mission-critical applications

11.1.1.2 AP300 Specifications - Integrated Antenna Model

Technical Specifications

Operating Voltage	48VDC typical; 36-57VDC range
Operating Current	100mA to 165mA
Peak Current	250mA
Operating Temperature	0°C to 40°C (32°F to 104°F)
Operating Humidity	5% to 95% non-condensing
Operating Altitude (max)	2438m (8,000ft.)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Storage Humidity	85%
Storage Altitude (max.)	4572m (15,000ft.)
Drop	910mm (36in.) to concrete
Electrostatic Discharge	+/-15kV air; +/-8kV contact; +/-2kV pin

Dimensions & Weight

Length	241mm (9.5in.)
Width	178mm (7.0in.)
Height	51mm (2.0in.)
Weight	0.45kg (1.0lbs)

Radio Characteristics

The AP 300 Access Port is an IEEE 802.11-compliant device available in two models. The 802.11a/b/g model (WSAP-5100-100-WWR) contains one 802.11a radio and one 802.11b/g radio. The 802.11b/g model (WSAP-5100-050-WWR) contains one 802.11b/g radio. The following table lists radio characteristics for each radio's compliance. The three supported 802.11g modes are simultaneous CCK and OFDM, CCK only, or OFDM only.

Device	*Mbps Data Rate Support*	*Utilizing Diversity*	*GHz*
802.11a	6, 9, 12, 18, 24, 36, 48, 54 OFDM	Transmit and receive	4.9 to 5.875 range
802.11b/g	1, 2, 5.5, 11 CCK 6, 9, 12, 18, 24, 36, 48, 54 OFDM	Transmit and receive	2.4 to 2.5 ISM range

11.1.1.3 AP300 Specifications - External Antenna Model

Technical Specifications

Operating Voltage	48VDC typical; 36-57VDC range
Operating Current	100mA to 165mA
Peak Current	250mA
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Operating Humidity	5% to 95% non-condensing
Operating Altitude (max)	2438m (8,000ft.)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Storage Humidity	85%
Storage Altitude (max.)	4572m (15,000ft.)
Drop (without antennas)	910mm (36in.) to concrete
Electrostatic Discharge	+/-15kV air; +/-8kV contact; +/-2kV pin
Plenum Rated	UL 2043

Dimensions & Weight

Length	235mm (9.25in.)
Width	146mm (5.75in.)
Height	25.4mm (1.0in.)
Weight	0.73kg (1.6lbs)

Radio Characteristics

The AP 300 Access Port is an IEEE 802.11-compliant device available in two models. The 802.11a/b/g model (WSAP-5100-100-WWR) contains one 802.11a radio and one 802.11b/g radio. The 802.11b/g model (WSAP-5100-050-WWR) contains one 802.11b/g radio. The following table lists radio characteristics for each radio's compliance. The three supported 802.11g modes are simultaneous CCK and OFDM, CCK only, or OFDM only.

Device	***Mbps Data Rate Support***	***Utilizing Diversity***	***GHz***
802.11a	6, 9, 12, 18, 24, 36, 48, 54 OFDM	Transmit and receive	4.9 to 5.875 range
802.11b/g	1, 2, 5.5, 11 CCK 6, 9, 12, 18, 24, 36, 48, 54 OFDM	Transmit and receive	2.4 to 2.5 ISM range

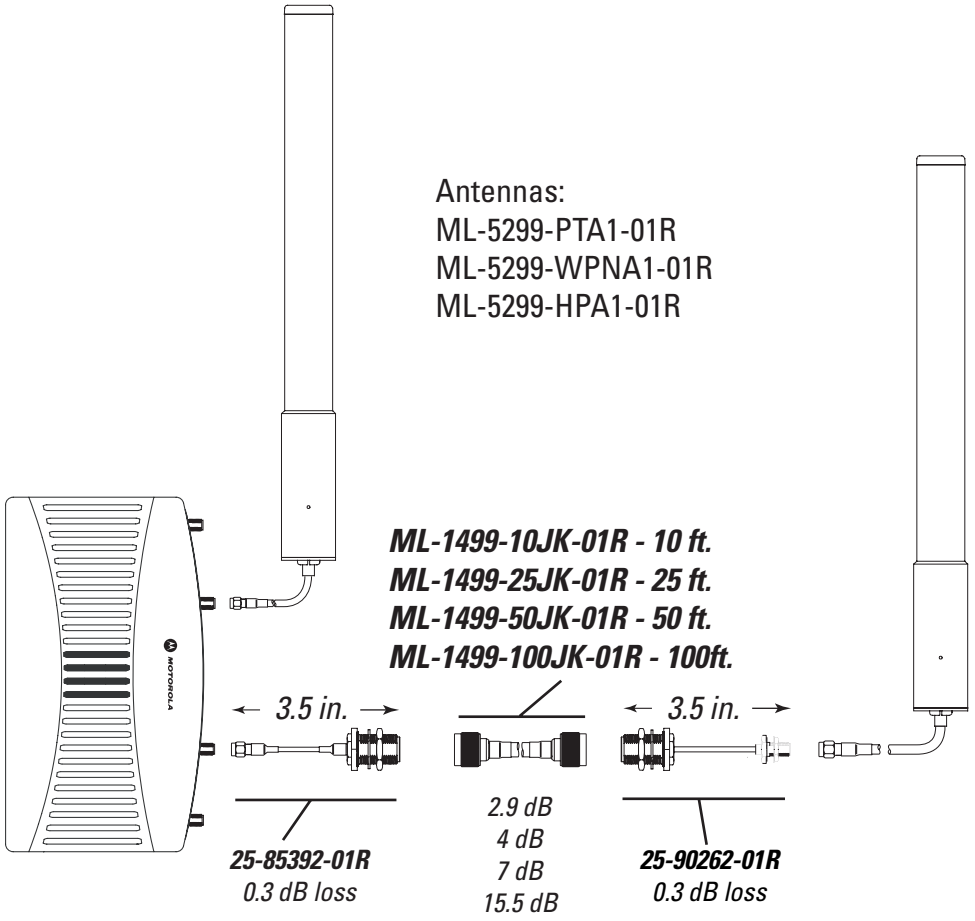
11.1.2 AP-5131 Access Point

An AP 5131 is an Enterprise-class 802.11a/b/g access point. Simple to deploy, an AP-5131 offers 802.11a/b/g wireless networking flexibility, the latest wired and wireless security standards and the speed required to support the most demanding applications, including voice and video.

Remote employees in branch offices, small businesses and telecommuters working from home enjoy secure connectivity to the Internet and corporate private networks from desktops, notebooks and other mobile devices. Enterprise users can take advantage of the AP-5131's mesh features to extend corporate networks to difficult-to-cable areas.

A typical AP-5131 hardware deployment could appear as follows:

NOTE: For additional information on the detailed antenna and cabling options available to an AP-5131 model access point, refer to the *WLAN Antenna Specification Guide* available at http://support.symbol.com/support/product/manuals.do.



11.1.2.1 AP-5131 Features

Cost-Effective, Secure, High-Performance Wired and Wireless Connectivity

Designed for small offices and retail locations, the AP-5131 delivers wired and wireless networking with Enterprise class performance and security in a single device. This easy-to-deploy solution offers the flexibility to connect securely to remote corporate private networks, the Internet and local network resources with the speed and reliability to support the most demanding applications, including real-time video and voice. The all-in-one AP-5131 delivers a new level of cost-efficiency and networking simplicity for employees in branch offices or telecommuters working at home. The AP-5131 boasts an integrated router, firewall, VPN, DHCP, AAA, hotspot gateway, and other services in one remotely manageable device, simplifying network set-up and management.

Enterprise-Class Security and Manageability

Support for today's standards-based security protocols ensures Enterprise-level protection for users on wireless laptops and other mobile devices, as well as wired computers. A wide variety of administration features provide powerful and secure control by either local, non-technical staff or remote IT professionals in the Network Operations Center

Dual-radio 802.11a/b/g Architecture

The dual-radio architecture offers the flexibility to best meet wireless LAN networking and security needs through either dual-band data services, or single-band data services and full-band rogue AP detection, which identifies and reports unauthorized entities on the network. A complete suite of dual and single-band antennas provides the versatility to customize radio coverage for even the most challenging environments, with a minimal number of access points.

Mesh Networking

To enable the extension of wireless network coverage to areas where ethernet or fiber cabling is cost-prohibitive or otherwise impractical, the AP-5131 can operate wirelessly, connecting to other access points for data backhaul, in a mesh topology. Enabling an array of applications, from simple point-to-point bridges connecting two wired networks, to complex multi-node, multi-link networks, this features offers a cost-effective way extend the network outdoors or in remote areas, relying on a highly resilient, self-configuring system. Taking advantage of the dual-radio architecture and the easy-to-use configuration interface, it becomes a simple task to deploy a wireless network of access points connected securely via 802.11a, providing Enterprise-class 802.11b/g service.

Wired Features

- *Router* - WAN-LAN-WLAN routing function
- *Firewall* - Isolation of LAN-WLAN from WAN
- *DHCP & NAT* - LAN IP address management
- *PPPoE* - Cable/DSL uplink support
- *802.1x wired*-authentication
- *802.1q Trunking* - VLAN support on LAN port
- *IPSec VPN client* - Secure backhaul to corporate network over WAN
- *Dual FE uplink* - (LAN + WAN)

Radio Features

- 4 BSSIDs per radio
- 16 WLANs, 8 BSSIDs total, 16 VLANs
- Supports 32 SSIDs. This means (for an AP300) 8 SSIDs are supported for the 802.11b/g radio and 8 SSIDs for the 802.11a radio.
- Wi-Fi certified
- WMM certified
- 802.11a DFS/TPC - Radar detection and avoidance
- Mesh networking with trunking
- Dual-radio 802.11a+b/g
- The 802.11 spec allows broadcasting a beacon for every BSSID (mac address) on the radio. Motorola radios have 4 BSSIDs (on AP5131). So on each radio 4 ESSIDs of the 16 can be selected as primary ESSIDs and can broadcast. The other 12 will only be reachable to mobile units via Probe-Responses.

Memory

- Volatile Memory is 64MB (Megabytes)

- Non-volatile Memory is 2MB and 64MB (Megabytes)

Management

- Web-based Java UI
- CLI
- SNMP v3
- SSL v3.1
- SSHv2
- Motorola Mobility Services Platform

Security

- Integrated VPN endpoint
- VPN terminations tested
- Cisco ASA
- Nortel
- Netscreen
- Cisco PIX

An AP-51x1 supports standard IPSec Modes. Thus, it will work with any VPN solution that conforms to the standard.

- AAA Server with hotspot gateway
- Supports 25 Radius entries that can be configured as the host or subnet
- Rogue AP detection
- Enterprise-class WPA2, 802.11i, KeyGuard, Kerberos security
- Enterprise-class management via MSP/SEMM
- Virtual AP technology for true broadcast domain separation in the air

MTBF

- AP5131 - ~245,000 hours

Port Adoption

The AP-5131 uses Adaptive AP to do it's port adoption. There is no *dumbing down* of the AP to adopt into the switch. AP-5131s and AP-5181s at remote branch offices or telecommuter sites can now be controlled from a wireless switch at a central site over a WAN connection. The adaptive access points remain operational even if they loose connection to the wireless switch. This also enables an adaptive mesh network where mesh access points can be centrally configured from the wireless switch.

11.1.2.2 AP-5131 Specifications

AP-5131 Physical Characteristics

The AP-5131 has the following physical characteristics:

Dimensions	5.32 inches long x 9.45 inches wide x 1.77 inches thick. 135 mm long x 240 mm wide x 45 mm thick.
Housing	Metal, Plenum Housing (UL2043)
Weight	1.95 lbs/0.88 Kg (single-radio model) 2.05 lbs/0.93 Kg (dual-radio model)
Operating Temperature	-20 to 50° Celsius
Storage Temperature	-40 to 70° Celsius
Altitude	8,000 feet/2438 m @ 28° Celsius (operating) 15,000 feet/4572 m @ 12° Celsius (storage)
Vibration	Vibration to withstand .02g^2/Hz, random, sine, 20-2k Hz
Humidity	5 to 95% (operating) 5 to 85% (storage)
Electrostatic Discharge	15kV (air) @ 50% rh 8kV (contact) @ 50% rh
Drop	Bench drop 36 inches to concrete (excluding side with connectors)

Electrical Characteristics

An AP-5131 access points has the following electrical characteristics:

Operating Voltage	48Vdc (Nom)
Operating Current	200mA (Peak) @ 48Vdc 170mA (Nom) @ 48Vdc

Radio Characteristics

An AP-5131 access point has the following radio characteristics:

Operating Channels

802.11a radio - Channels 34-161 (5170-5825 MHz)

802.11b/g radio - Channels 1-13 (2412-2472 MHz)
802.11b/g radio - Channel 14 (2484 MHz Japan only)

Actual operating frequencies depend on regulatory rules and certification agencies.

Receiver Sensitivity

802.11a Radio	802.11b/g Radio
6 Mbps -88	11 Mbps -84
9 Mbps -87	5.5 Mbps -88
12 Mbps -85	2 Mbps -90
18 Mbps -81	1 Mbps -94
24 Mbps -79	
36 Mbps -75	
48 Mbps -70	
54 Mbps -68	

** all values in dBm*

Radio Data Rates

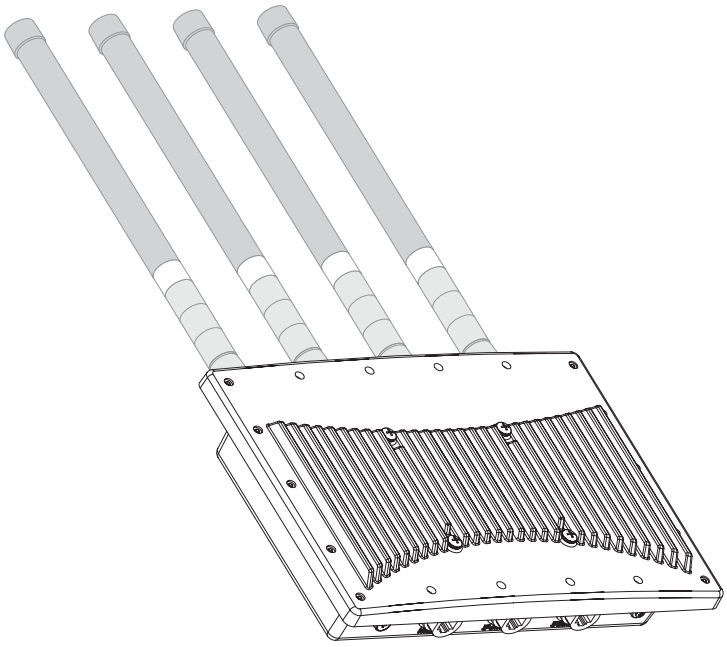
802.11a radio 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/Sec
802.11g radio 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/Sec
802.11b radio 1, 2, 5.5, 11 Mbps

Wireless Medium

Direct Sequence Spread Spectrum (DSSS)
Orthogonal Frequency Division Multiplexing (OFDM)

11.1.3 AP-5181 Access Point

Provide employees with network access (even in harsh environments) using Motorola's AP-5181 access point. Designed for outdoor use, the AP-5181 delivers Enterprise-class wireless networking to outdoor facilities, such as processing plants and ship yards.



NOTE: For additional information on the detailed antenna and cabling options available to an AP-5181 model access point, refer to the *WLAN Antenna Specification Guide* available at http://support.symbol.com/support/product/manuals.do.

Use the AP-5181's wireless mesh feature to connect two wired networks or create a complex multi-node, multi-link network. Either way, an AP-5181 offers a simple way to extend the network to outdoor or remote locations, without the expense of installing additional cable or fiber.

11.1.3.1 AP-5181 Features

NEMA 4X-modified, IP56 Weatherproof Housing

Equipment designed to withstand wind, rain, and extreme temperatures.

Extended Temperature Range

Operates in temperatures from -30° C to 55° C (-22° F to 131° F).

Mesh-Capable

Self-assembling, self-healing nodes automatically establish wireless links between APs; install nodes wherever there is power - no need to install cable or fiber.

Dual-Radio, Dual-Band Design; 802.11a/b/g in 2.4/5 GHz Bands

Simultaneous support of 802.11a/b/g; works with any standards-based IEEE WLAN device.

Integrated Router, Firewall and DHCP Server

No need to install extra hardware; easy to scale, upgrade and maintain.

AAA Server and Hotspot Gateway

Integrated services for authentication and public access management.

Wi-Fi Multimedia (WMM). Quality of Service (QoS) and Voice Prioritization

Superior performance for demanding mission-critical applications, including voice and video.

Adaptive AP

Can be controlled with a wireless switch to enable central management from the NOC, and in the event of loss of connectivity, resumes functionality as a standalone access point.

11.1.3.2 AP-5181 Specifications

AP-5181 Physical Characteristics

The AP-5181 has the following physical characteristics:

Dimensions	12 inches long x 8.25 inches wide x 3.5 inches thick.
Housing	Aluminum
Weight	4 lbs.
Operating Temperature	-30 to 55° Celsius
Storage Temperature	-40 to 85° Celsius
Altitude	8,000 feet/2438 m @ 28° Celsius (operating) 15,000 feet/4572 m @ 12° Celsius (storage)
Vibration	Vibration to withstand .02g²/Hz, random, sine, 20-2k Hz
Humidity	5 to 95% (operating) 5 to 95% (storage)
Electrostatic Discharge	15kV (air) @ 50% rh 8kV (contact) @ 50% rh
Drop	Bench drop 36 inches to concrete
Wind Blown Rain	40 MPH @ 0.1inch/minute, 15 minutes
Rain/Drip/Spill	IPX5 Spray @ 4L/minute, 10 minutes
Dust	IP6X 20mb vacuum max, 2 hours, stirred dust, .88g/m^3 concentration @ 35%RH

Electrical Characteristics

An AP-5181 access point has the following electrical characteristics:

Operating Voltage	48Vdc (Nom)
Operating Current	200mA (Peak) @ 48Vdc 170mA (Nom) @ 48Vdc

Radio Characteristics

An AP-5181 access point has the following radio characteristics:

Operating Channels

802.11a radio - Channels 34-161 (5170-5825 MHz)

802.11b/g radio - Channels 1-13 (2412-2472 MHz)
802.11b/g radio - Channel 14 (2484 MHz Japan only)

Actual operating frequencies depend on regulatory rules and certification agencies.

Receiver Sensitivity

802.11a Radio	802.11b/g Radio
6 Mbps -88	11 Mbps -84
9 Mbps -87	5.5 Mbps -88
12 Mbps -85	2 Mbps -90
18 Mbps -81	1 Mbps -94
24 Mbps -79	
36 Mbps -75	
48 Mbps -70	
54 Mbps -68	

** all values in dBm*

Radio Data Rates

802.11a radio 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/Sec
802.11g radio 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/Sec
802.11b radio 1, 2, 5.5, 11 Mbps

Wireless Medium

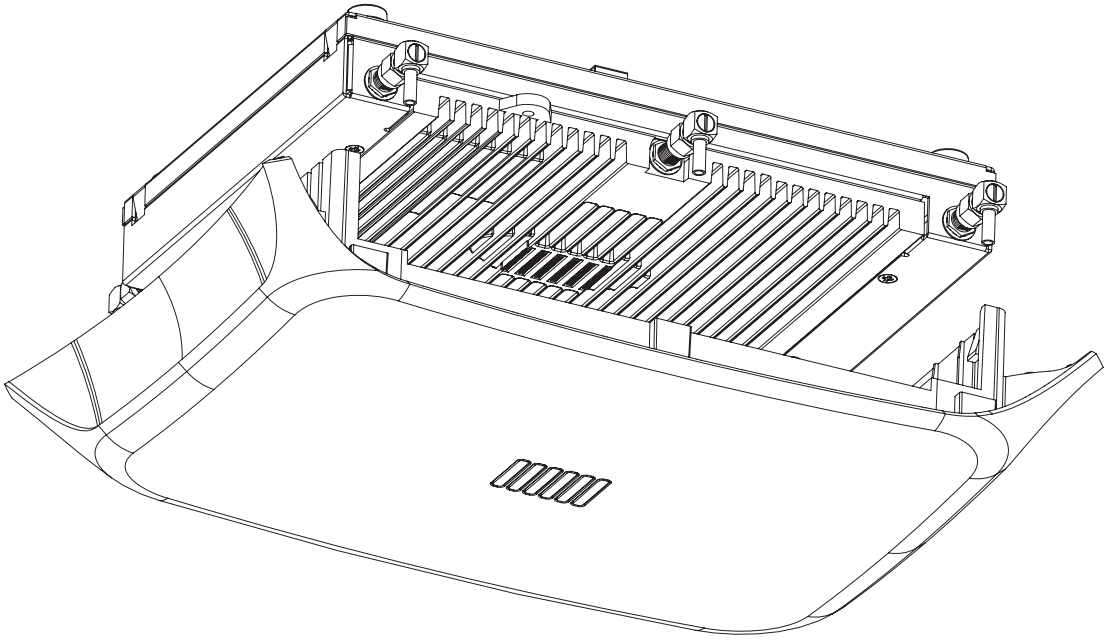
Direct Sequence Spread Spectrum (DSSS)
Orthogonal Frequency Division Multiplexing (OFDM)

11.1.4 AP-7131 Access Point

The AP-7131 802.11a/b/g/n access point delivers the throughput, coverage and resiliency required to build an all wireless Enterprise. The tri-radio modular design provides support for high-speed wireless voice and data services, mesh networking and non-data applications such as IPS. The fully DFS compliant 802.11n (Draft 2.0) AP-7131 offers speeds up to 600 Mbps (per AP), six times the bandwidth of an 802.11a/g access point. Its Adaptive AP architecture allows the AP to operation in either of two modes (without a firmware change). An AP-7131 can function as either as a stand-alone access point or as a wireless switch adopted access point for centralized management.

A typical AP-7131 deployment could appear as follows:

NOTE: For additional information on the detailed antenna and cabling options available to an AP-7131 model access point, refer to the *WLAN Antenna Specification Guide* available at http://support.symbol.com/support/product/manuals.do.



11.1.4.1 AP-7131 Features

Tri-Radio, Dual-Band Design; 802.11a/b/g/n in 2.4/5 GHz Bands

Works with any standards-based IEEE WLAN.

802.11n Support

Delivers maximum wireless network throughput to support virtually any Enterprise application, including voice and video.

- 3X3 MIMO
- 20/ 40 MHz channel width in both 2.4GHz & 5Ghz
- Frame aggregation (AMSDU/ AMPDU)
- Reduced interframe spacing
- 300 Mbps data rates per radio

Adaptive AP

Can be controlled with a wireless switch to enable central management from the NOC, and in the event of loss of connectivity, resumes functionality as a standalone access point

Integrated Router, DHCP Server, Firewall, AAA Radius, NAT, and Hot-Spot Gateway

Eliminates need to purchase and manage additional equipment; simplifies provisioning of network services and public access.

Mesh Networking

Allows wireless extension of existing wired or wireless networks in remote or outdoor locations.

802.11i, WPA2 and WPA; IPSec Encryption

End-to-end Enterprise class wired and wireless security.

Rogue AP Detection, On-board IDS, MU Assist Mode, Dedicated WIPS Sensor Radio

Around the clock network protection through instant identification and reporting of unauthorized users.

11.1.4.2 AP-7131 Specifications

AP-7131 Physical Characteristics

The AP-7131 has the following physical characteristics:

Dimensions	5.50 in. L x 8.00 in. W x 1.10 in. H 13.97 cm L x 20.32 cm W x 2.79 cm H
Housing	Metal, plenum-rated housing (UL2043)
Weight	2.22 lbs/9.98 kg
Operating Temperature	-4°F to 122°F/-20°C to 50°C
Storage Temperature	-40°F to 158°F/-40°C to 70°C
Altitude	8000 ft./2438 m @ 82°F/28°C (Operating) 15000 ft./4572 m @ 53°F/12°C (Storage)
Humidity	5 to 95% RH non-condensing
Electrostatic Discharge	15kV air, 8kV contact

Electrical Characteristics

The AP-7131 access point has the following electrical characteristics:

Operating Voltage	38-54V DC
Operating Current	Not to exceed 600mA @ 48VDC

Radio Characteristics

The AP-7131 access point has the following radio characteristics:

Operating Channels	All channels from 4920 MHz to 5825 MHz except channel 52 -64 Channels 1-13 (2412-2472 MHz) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory
Data Rates Supported	802.11g: 1,2,5.5,11,6,9,12,18,24,36,48, and 54Mbps 802.11a: 6,9,12,18,24,36,48, and 54Mbps 802.11n: MCS 0-15 up to 300Mbps

Wireless Medium	*Direct Sequence Spread Spectrum* (DSSS), *Orthogonal Frequency Division Multiplexing* (OFDM) *Spatial multiplexing* (MIMO)
Network Standards	802.11a, 802.11b, 802.11g, 802.3, 802.11n (Draft 2.0)
Maximum Available Transmit Power	20dBm
Transmit Power Adjustment	1dB increments
Antenna Configuration	3x3 MIMO (transmit and receive on all three antennas)

11.2 Wireless Switches

A wireless switch is an intelligent entity which maintains information about MU association, authentication and provides management and control plane services. In typical installations, it is connected to the thin access points indirectly through a 802.3af PoE capable layer 2 switch which provides power to the thin access points. Thin access points handle the real time 802.11 MAC layer functions of generating beacons, ACKs and responding to probes. Some wireless switches have built in PoE ports. It's possible for the controller and AP to be on different IP subnets, in which case there is a layer 3 switch or router between them. When an AP is powered on, it enter a discovery phase wherein it attempts to find a suitable controller. A controller has hardware and licensing limits that determine how many APs can connect. After a suitable controller responds, the AP receives its configuration (and optional firmware). The discovery and configuration phase lasts only a few seconds. The controller and AP exchange periodic heartbeat messages to indicate status.

11.2.1 The Wireless Switch and Motorola

Motorola introduced a new era in wireless LAN infrastructure technology with the introduction of the wireless switch system. This solution set features a wireless switch for media independent, switch-based wireless networking and access ports for wireless client communication. The switch includes a robust security suite to protect mobile data and applications through a wireless VLAN and other security measures. Ethernet-based power solutions reduce deployment and installation time and costs. Management software provides greater control, flexibility and enhanced services.

The concept of using a wireless switch to centralize management and aggregate subnets has quickly caught on within the networking world, with many new start-ups developing their own switch platforms.

However, Motorola's wireless switch system goes far beyond traditional dual-mode wireless LAN approaches, providing an architecture that can grow with a company's requirements. The switch's media-independence ensures the system is open, extensible, and expandable. This enables a seamless migration to new radio technologies without having to purchase a new switch, thus providing a continuous return on investment as the network evolves.

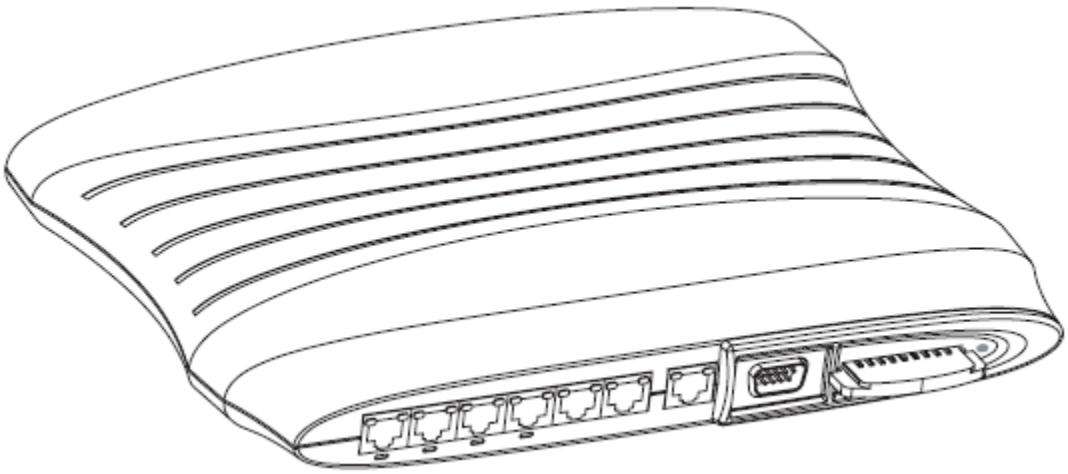
All data routing and forwarding is done by the switch software. The switch architecture supports a multi-core multi-processor design. This allows fast packet processing while simultaneously upgrading features (without having to upgrade switch hardware).

Refer to the following sections to review the Enterprise class switch offerings provided by Motorola:

- *WS2000*
- *WS5100*
- *RFS6000*
- *RFS7000*

11.2.2 WS2000

The WS2000 wireless switch is a market-leading powerful all-in-one solution that simplifies and reduces the costs of managing wired and wireless (802.11a/b/g) networks in Enterprise branch offices.



An integrated router, gateway, firewall and PoE eliminate the cost and the complexity of managing multiple pieces of equipment. A WS2000 can easily and cost-effectively scale to meet your growing deployment needs, as well as upgrade to support new security, and wireless standards needs as they are introduced.

11.2.2.1 WS2000 Features

Switch-Based Centralized Upgradeable Architecture

Enhanced performance and functionality; simplified deployment/management, investment protection; low total cost of ownership

802.11a/b/g Compatibility

Lower cost; broad, flexible radio support

Wi-Fi Multimedia (WMM) Extensions Support

Enables voice and video applications with wired QoS extension support

SIP Call Admission Control

Controls the number of active SIP sessions initiated by a wireless VoIP phone

Enterprise-Class security: 802.1X/EAP Kerberos, WPA2 (802.11i)

Enterprise-class authentication and encryption; ensures privacy of data during transmission

AAA Integrated Server: Verifies User Identify

Eliminates the cost/need for a separate Radius server

Integrated Gateway: Routing, DHCP, NAT, Firewall and WAN Uplink (with PPPoE)

Eliminates need to purchase and manage additional equipment; simplifies provisioning of network services

IP Filtering

Provides flexibility in defining access policies

Comprehensive Hot Spot Support

Provides secure public access (complimentary or service-based)

Rogue AP Detection

Identifies unauthorized access ports and points

IPSec VPN

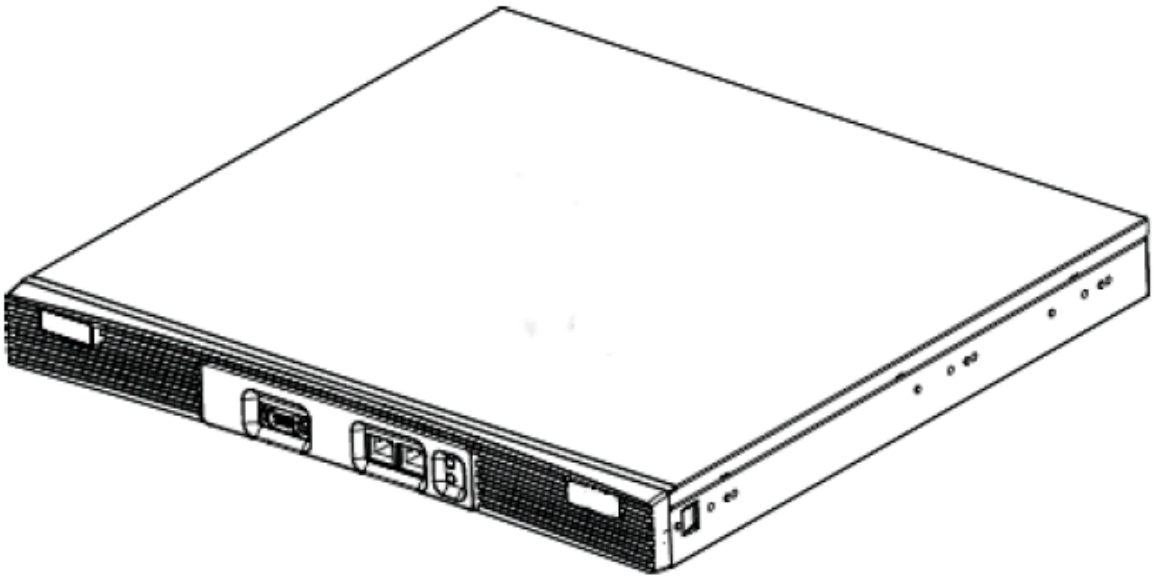
Cost-effective point-to-point communications

802.3af Power-over-Ethernet (PoE) support:

Eliminates the need and expense to power multiple access ports and points

11.2.3 WS5100

Enhance support for Enterprise mobility and multimedia applications in large health care, educational and retail organizations with the Motorola WS5100 wireless switch.



Enable campus-wide roaming across subnets without the need to re-authenticate, while extending mobile-client battery life and increasing voice capacity-with a wireless switch solution based on Motorola's *wireless next-generation architecture* (Wi-NG). Whether the demands on your wireless LAN are escalating due to an increase in employee count or from the bandwidth demands of new applications (or both), look no further than the WS5100.

11.2.3.1 WS5100 Features

Wi-Fi Multimedia Extension Support

Enables peak performance in demanding voice and video applications

Troubleshooting Tools

Automatic configuration and firmware updates, active/active failover and clustering support and built-in process monitors

Network Protection

Adherence to 802.11i and Motorola's unique mobility features for a superior level of data and network protection without sacrificing performance

Security Features

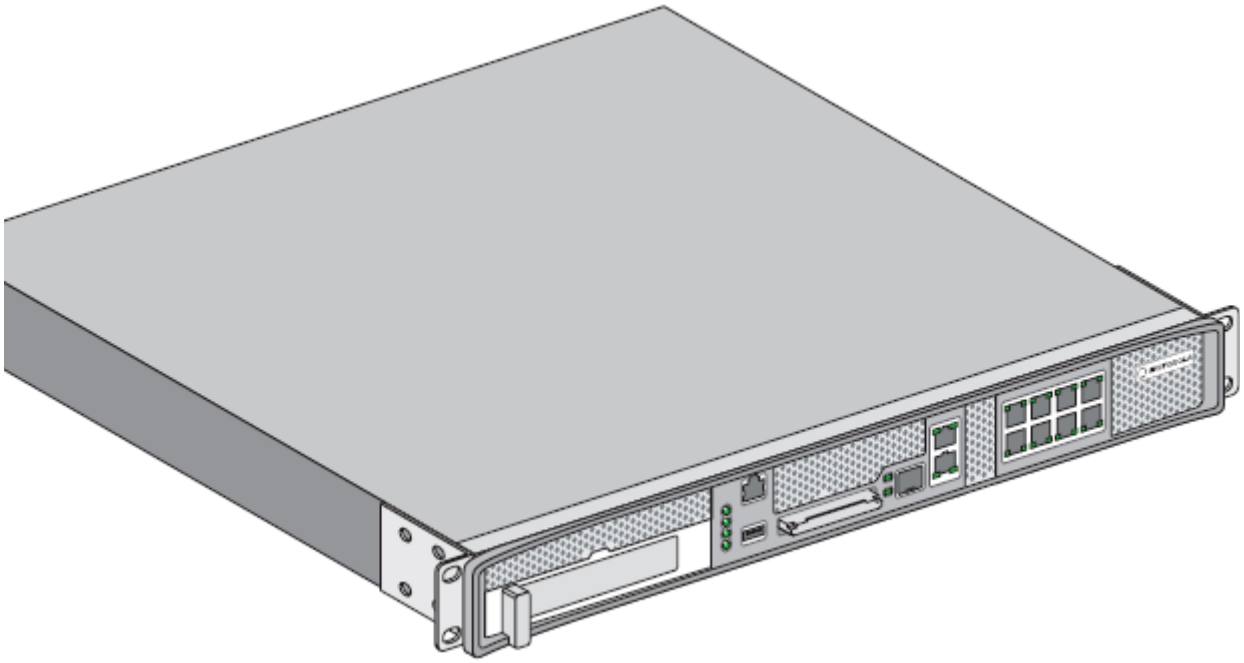
Intrusion detection, IPSec VPN gateway, secure guest access and protection against denial of service attacks

Adaptive AP

Enables centralized management of mesh access points at remote sites as well as site survivability of those remote locations

11.2.4 RFS6000

The RFS6000 provides an integrated wireless LAN communication platform that enables the delivery of highly secure mobile voice and data services inside and outside the Enterprise. Designed for medium to large Enterprises, the RFS6000 simplifies and reduces the cost associated with converged solutions through a comprehensive feature set that delivers the best in class performance, security, scalability and manageability required to meet the needs of your demanding mission critical business applications.



11.2.4.1 RFS6000 Features

Maximizes Benefits and Minimizes Costs

Motorola's Wi-NG architecture reduces installation and maintenance costs by providing a single infrastructure for mobile voice and data inside and outside the Enterprise.

Comprehensive and High Performance Voice Support

Support for VoWLAN provides cost-effective voice services throughout campus environments, enabling push-to-talk and more for employees inside the four walls as well as in outside areas such as the yard.

Enterprise Security for Voice and Data

Comprehensive network security features keep wireless transmissions secure and provide constant compliance with government regulations such as HIPAA and PCI.

Extensible and Scalable

A user accessible *ExpressCard™* slot allows the addition of a broadband card (3G/4G) for a redundant wireless WAN backhaul connection, increasing resilience for remote branch offices. The ability to cluster up to 12 switches provides the high level of scalability required for large Enterprise deployments.

Raises the Bar on Enterprise Class Performance

Designed to support large scale high bandwidth Enterprise deployments, the RFS6000 offers a multicore multithreaded CPU-based architecture that is capable of supporting 2,000 to 20,000 mobile devices and up to 48 dual radio 802.11 a/b/g access ports. In addition, the 802.11n ready device offers the failover capabilities and cluster management required to ensure high availability.

Cost Effective Centralized Management

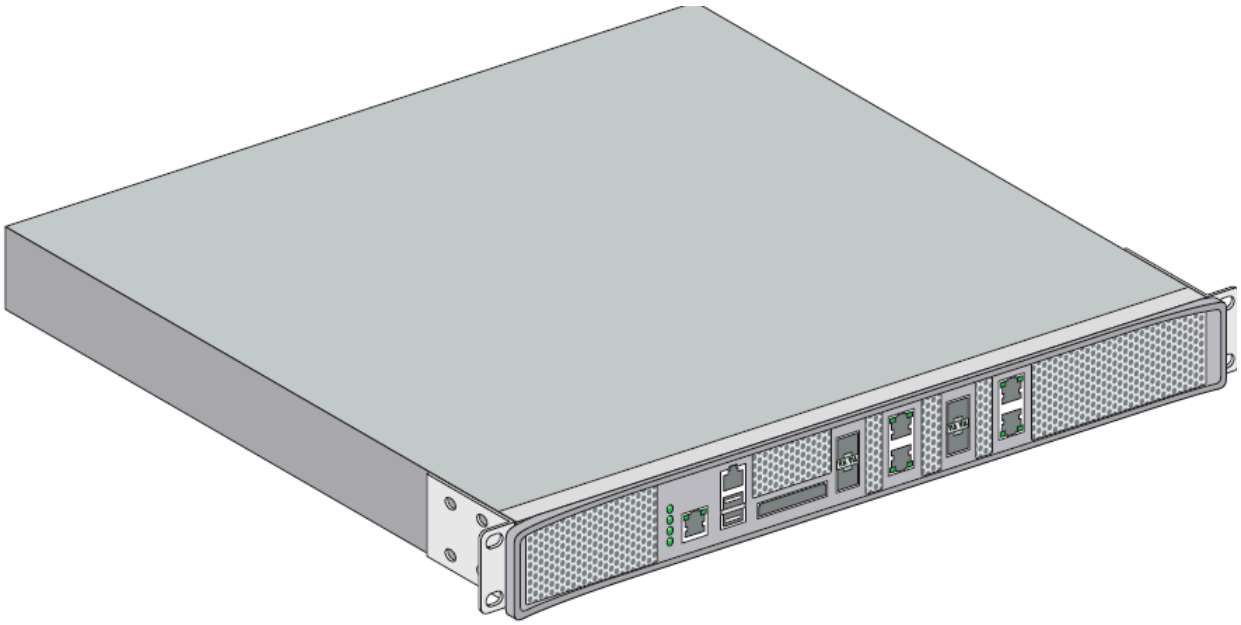
Motorola provides the tools you need to simplify and minimize the costs associated with day-to-day management of mobility solutions. The RFS6000 provides unified management of network hardware, software configuration, and network policies, complete with built-in process monitors and troubleshooting tools.

Adaptive AP

The RFS6000 delivers a new capability that simplifies and reduces the cost of extending mobility to remote, branch, small and home offices. Motorola's AP-51X1 access points can be deployed at remote locations yet centrally managed in the Network Operations Center (NOC) through the RFS6000.

11.2.5 RFS7000

Get the performance and scalability you need to propel your large, high-bandwidth wireless network. Built on Motorola's Wi-NG architecture, the RFS7000 enables campus-wide roaming across subnets with a wireless switch that improves failover capabilities, enhances quality of service, increases voice capacity and provides superior security.



11.2.5.1 RFS7000 Features

Centralized Multicore/Multithreaded Architecture

Security and high performance for bandwidth-heavy applications; a single point of management lowering the overall cost of network deployment and administration.

Unified RF Management

Improve business process flow and enable data sharing by managing multiple RF networks, such as wi-fi, RFID, 802.11n and Wi-MAX, on a single switch.

Layer 2/3 Roaming

Seamless roaming of mobile clients across even complex distributed networks.

Comprehensive Layered Security

Exceptional level of data and network protection without sacrificing fast roaming.

Clustering and Load Balancing

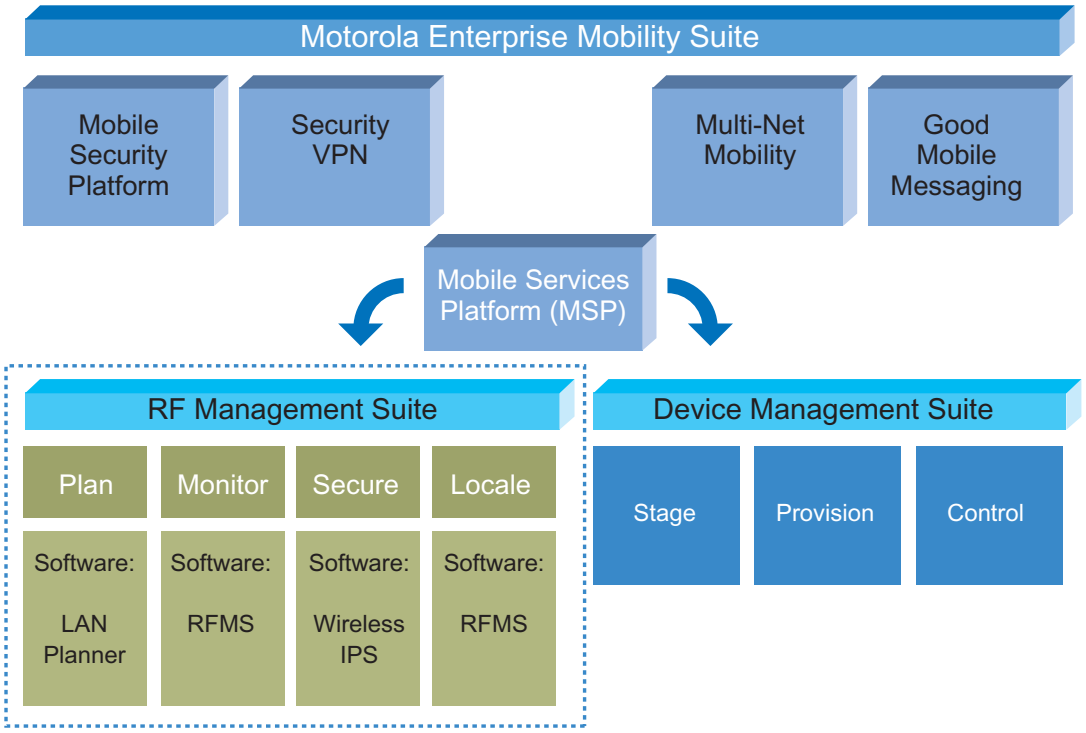
Ensures an *always-on* highly available network for superior performance; supports multiple levels of redundancy and failover capabilities.

Adaptive AP

Enables centralized management of mesh access points at remote sites as well as site survivability of those remote locations.

11.3 Motorola RF Management Suite (RFMS)

Motorola RF Management Suite (RFMS) is a high performance, flexible network management platform providing a framework for network planning, fault and performance management, configuration management (compliance, templates), security, reporting and location-based services. Tight integration with the Motorola LANPlanner solution allows data compiled during network design to be used for real-time wireless coverage maps, channel maps and RF related statistics. The scalable architecture allows for the management of thousands of devices for deploying configurations and firmware to devices. RFMS secures the Enterprise by managing multiple *Motorola Wireless IPS* (WIPS) servers and aggregating network and security related alerts into a single console.



RFMS is central for:

- *Planning*
- *Management and Troubleshooting*
- *Security*
- *Reporting*
- *Mobility Services Platform (MSP) Integration*

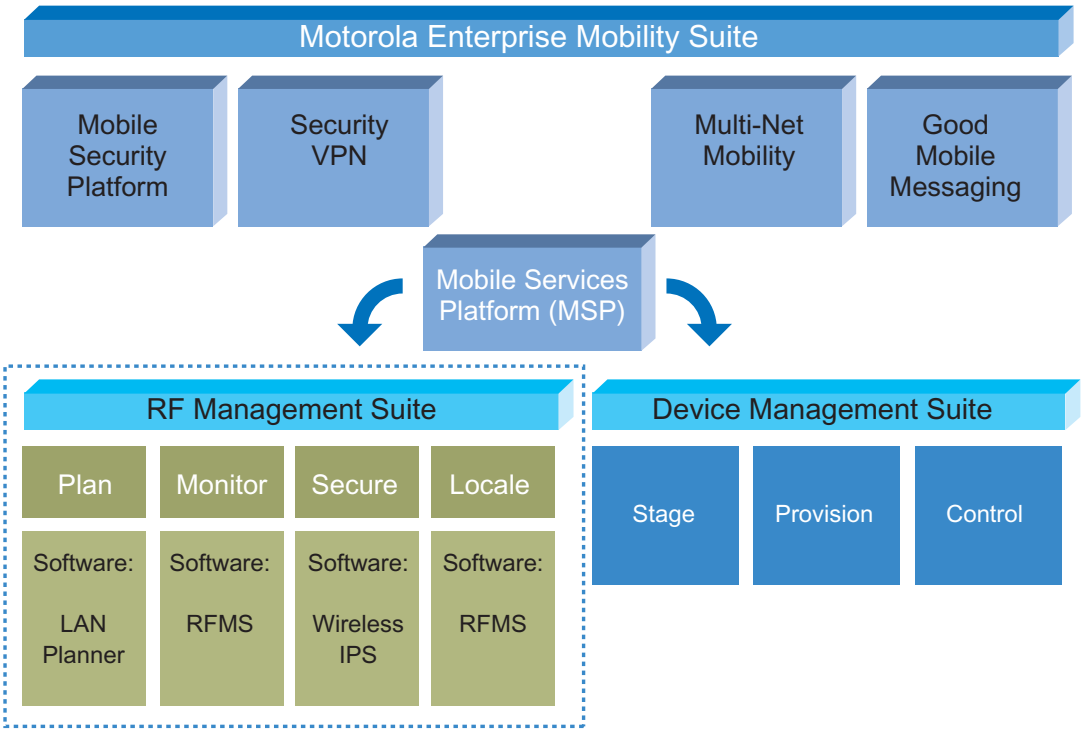
For information on the LANPlanner application (a powerful planning tool that can be invoked from RFMS), see *LANPlanner on page 11-23*.

For information on the *Wireless Intrusion Protection System* (WIPS) application (a robust threat detection tool that can be invoked from RFMS), see *Wireless Intrusion Protection System (WIPS) on page 11-23*.

Planning

The powerful Wi-Fi site planning tools in RFMS allow you the flexibility to create and modify Wi-Fi site coverage plans before you invest in wireless infrastructure equipment. Use RFMS to import floor plans, add

networking equipment, place barriers (walls or obstacles and define special zones for special coverage needs in a given area. RFMS even let's you customize barrier attenuation levels to see the effects of different materials on RF interference. When you've set up your virtual site, create a predicted heat map, export an AP installation plan and generated wireless switch/AP configuration data.



Management and Troubleshooting

RFMS provides a graphical view of over two hundred network statistics, enabling administrators to instantly assess the status of entire wireless infrastructure. It visualizes near real-time charts, graphs and time-trending of over 200 statistics such as AP utilization, MU utilization and WLAN utilization. This comprehensive reporting makes it easy to isolate network issues, so administrators can investigate and address them immediately. The *search* functionality (based on IP address, MAC address or user MU name) allows for checking any user (MU) and devices (such as AP). All statistical data can be exported to XML files for use in other applications.

Security

RFMS outputs information about security threats as detected by neighboring radios. RFMS reports rogue APs, excessive operations (excessive association/authentication requests, probes, ICV failures, retries, incorrect sequence numbers, authentication failures) and provides an anomaly analysis (illegal frame sizes, source multicast MAC and MAC spoofing).

Reporting

RFMS includes comprehensive reporting to enable planners to coordinate with installers, report the health and performance of their wireless infrastructure.

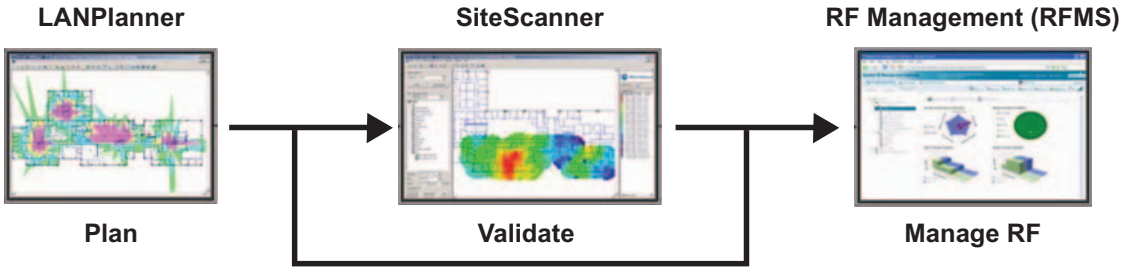
Mobility Services Platform (MSP) Integration

RFMS integrates with the *Mobility Services Platform* (MSP) 3.2 for mobile device management. The integration allows for a single sign-on, synchronization of sites, users, and relay servers. A Motorola mobile device in RFMS will have enhanced data points for identifying device model, operating system and version.

NOTE: For additional information on the detailed feature set and configuration options available to RFMS, refer to the *Motorola RFMS System Reference Guide* available at http://support.symbol.com/support/product/manuals.do.

11.3.1 LANPlanner

Motorola's LANPlanner application allows users to create design plans, simulate network traffic and perform site surveys for 802.11a/b/g networks, either as a standalone application or as invoked within RFMS.



WLAM Design
WiFi network design and simulation software for remote planning of coat effective, high performance 802.11a/b/g networks

Wi-Fi Site Survey
WiFi Site Survey
WiFi site survey software for testing, measurement and visual validation of deployed 802.11a/b/g networks

Monitoring and troubleshooting
WiFi monitoring and troubleshooting software for visualizing real-time network data, locating RF infrastructure/clients and identifying rogue APs

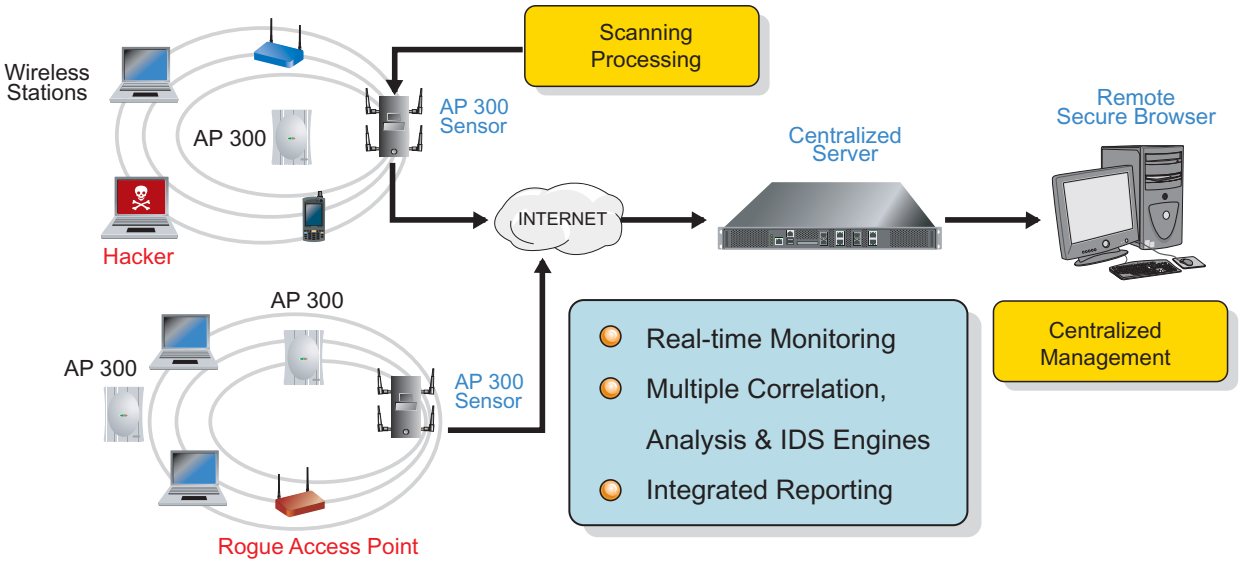
By inputting a specific number of users, their deployment environment and the applications in use (including wireless voice over IP), LANPlanner recommends the placement and density of equipment and provides site survey tools for network validation and troubleshooting once deployed.

NOTE: For additional information on the detailed feature set and configuration options available using LANPlanner, refer to the *LANPlanner Users Guide* available at http://support.symbol.com/support/product/manuals.do.

11.4 Wireless Intrusion Protection System (WIPS)

WIPS operatively protects your wireless network, mobile devices and traffic from attacks and unauthorized access.

With built-in forensic support and industry standard reporting WIPS provides powerful tools for standards compliance, as well as around-the-clock 802.11a/b/g wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices, and network vulnerabilities in real time and permits the wired and wireless lockdown of wireless device connections.



NOTE: For additional information on the detailed feature set and data protection options available using WIPS, refer to the *WIPS Operations Guide* available at http://support.symbol.com/support/product/manuals.do.

The Motorola Airdefense Solution offers a large variety of features to keep up and running. The main feature set includes:

- *Security*
- *Compliancy enforcement*
- *Advanced forensics*
- *Troubleshooting*

The central tasks in configuration you AirDefense solution include:

- *Alarm configuration*
- *Policy Management*

11.4.1 Alarm Configuration

Alarms and their criticality are dependent on your wireless environment. For example, an unauthorized station alarm would be considered critical and deserve immediate attention in a no-wireless zone, however, this could likely be ignored in a congested public area with many transient devices (such as a university campus). Each alarm can be enabled or disabled, and alarm criticality can be modified to fit the environment

AirDefense Alarms provide the user with 3 pre-defined security sensitivity modes that describe different environments, and the ability to define custom sensitivity settings. Before customizing a sensitivity mode, the user can select the pre-defined mode that best fits their organization, then proceed with its customization.

The pre-defined security sensitivity include:

- *Monitored WLAN* - Recommended for most WLAN deployments. It is very sensitive to adverse scenarios where active attacks, rogue devices, and policy compliance are considered critical events.

- *Monitored WLAN Security Only* - Recommended for WLAN deployments where performance monitoring is not a concern. It is sensitive to adverse scenarios where active attacks, rogue devices, and policy compliance are considered major events and emphasis is on security rather than performance alarms.
- *Monitored WLAN congested areas* - Recommended for wireless environments in congested areas with multiple neighbors and numerous transient devices. Alarms settings place emphasis on monitoring authorized infrastructure and devices interacting with that infrastructure.
- *Custom Sensitivity* - Allows users to selectively enable/disable alarms and set the priority of each alarm in the system.

NOTE: Alarms can be generated for stations and Access Points in a rogue, or unauthorized state.

The Alarms Engine in the Motorola Airdefence solution is divided in 8 sections, namely:

- *Behavior*
- *Exploits*
- *Performance*
- *Policy Compliance*
- *Reconnaissance*
- *Rogue Activity*
- *Vulnerabilities*

11.4.1.1 Behavior

Behavior alarms track atypical device behavior based on a calculated forensic baseline of that device. AirDefense utilizes a RF Rewind Engine to monitor and store detailed wireless forensic information about each device on a minute-by-minute basis. This information is then used to generate a normal behavior baseline for each device. Events are generated when a device operates outside of its normal behavior to alert the administrator of anomalous or suspicious behavior.

For example, consider a user device that has a wireless usage behavior baseline of basic Web and email access. A behavior event would be raised if this user suddenly downloads a significant amount of data after business hours, a time period when the station is not normally active. This anomalous behavior could be indicative of a stolen or spoofed identity, or a disgruntled employee that may be downloading significant amounts of confidential and/or proprietary information.

AP Behavior

Anomalous behavior specific to Access Points include:

- *Control frames received for AP exceeded thresholds*
- *Control frames sent for AP exceeded thresholds*
- *Control frames sent for AP exceeded thresholds*
- *Data frames sent for AP exceeded thresholds*
- *Management frames received for AP exceeded thresholds*
- *Management frames sent for AP exceeded thresholds*
- *Total bytes received for AP exceeded thresholds*

- *Total bytes sent for AP exceeded thresholds*

Station Behavior

Anomalous behavior specific to stations include:

- *Control frames received for station exceeded thresholds*
- *Control frames sent for station exceeded thresholds*
- *Control frames sent for station exceeded thresholds*
- *Data frames sent for station exceeded thresholds*
- *Management frames received for station exceeded thresholds*
- *Management frames sent for station exceeded thresholds*
- *Total bytes received for station exceeded thresholds*
- *Total bytes sent for station exceeded thresholds*

11.4.1.2 Exploits

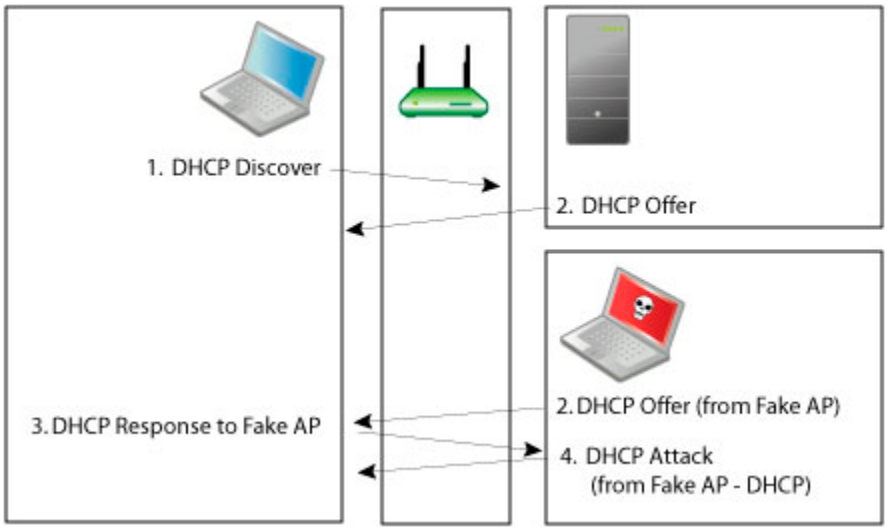
Exploits are events in which a user is actively interacting with the wireless network or wireless medium. By exploiting wireless vulnerabilities, a malicious user could cause wireless network disruptions or use the wireless medium to gain access to corporate resources and confidential data. The vulnerabilities may exist due to network configuration, corporate policy, or an inherent flaw in the 802.11 protocol. A malicious user with basic computer skills, a laptop and a CD drive can obtain various sets of open source tool kits which will transform the laptop into a fully configured wireless attack platform.

As time has progressed, these tools kits have become increasingly easier to use, while simultaneously offering an increasingly sophisticated toolset. Because exploits involve active interaction with the wireless network, AirDefense recommends timely action to understand and mitigate the threat to minimize security exposure. Exploits are divided into the following two sub-categories:

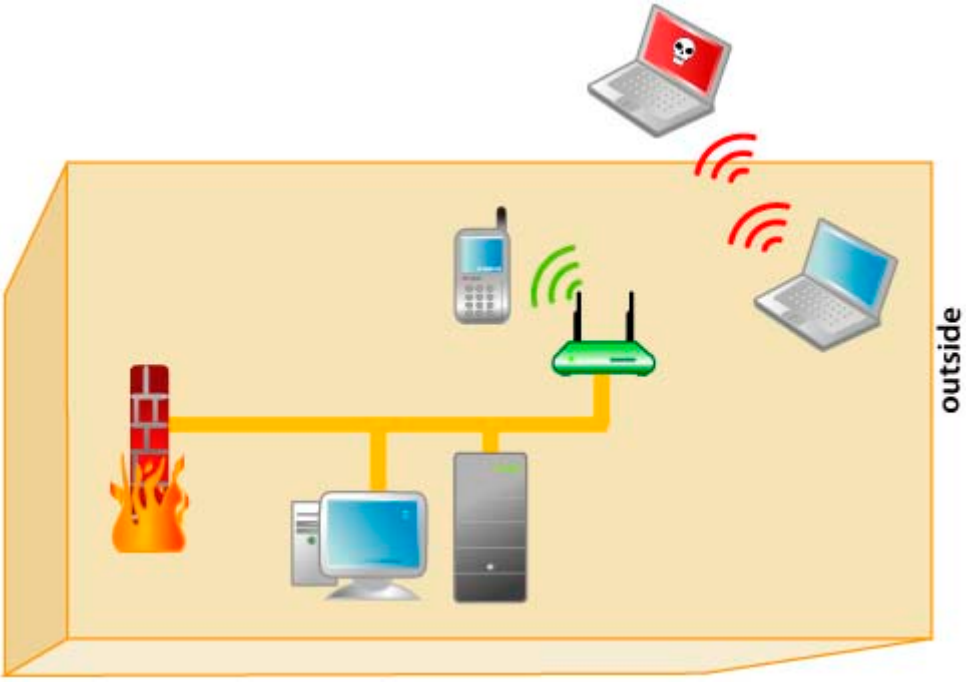
Active Attacks

Active attacks includes active malicious interaction with the wireless network. Active attacks are severe and present a high security risk and potential for significant exposure. Because these events are active in the wireless network, timely investigation is recommended to prevent the attack from continuing. These events can be mitigated wirelessly to minimize and prevent continued exposure; mitigation can be initiated manually by the administrator or automatically if the system has been configured for policy-based termination. Alarm attacks and their infestation scenarios can include:

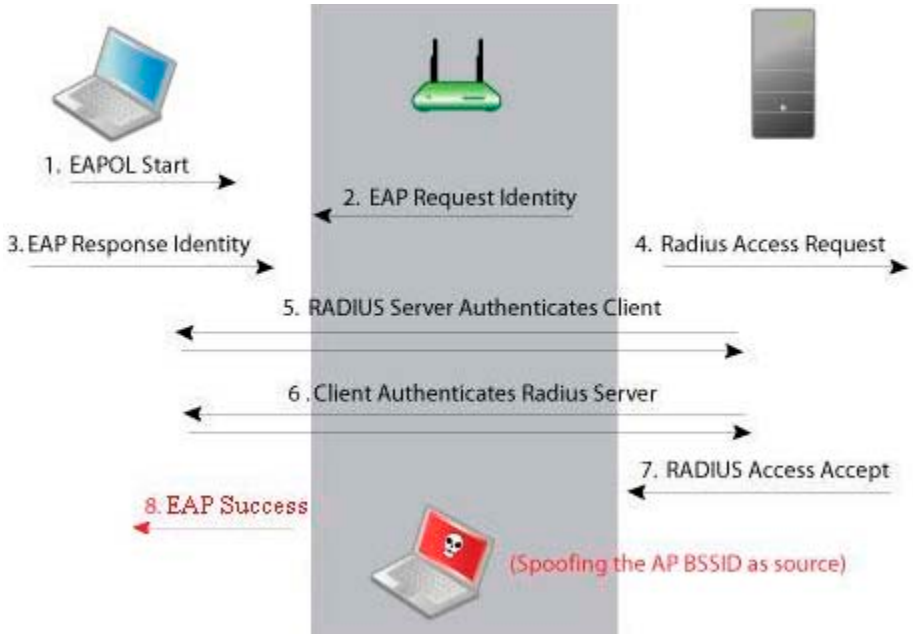
- *Airsnarf attack*
- *Asleap attack*
- *EAP dictionary attack*
- *EAP handshake flood*
- *Fake-AP flood attack*



- *Fake DHCP server detected*
- *Honeypot AP detected*
- *Hotspotter tool detected*



- *EAP spoofing (ID theft)*



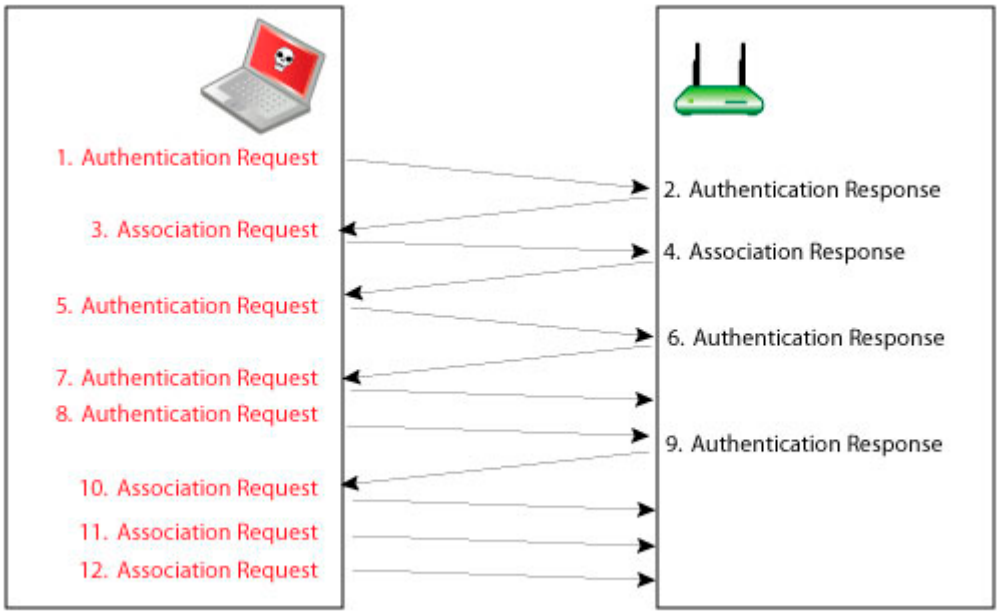
- *Out of Sequence (ID theft)*
- *Monkey-jack tool detected*

- *Multipot attack detected*
- *Replay injection attack*
- *Unauthorized AP using authorized SSID*

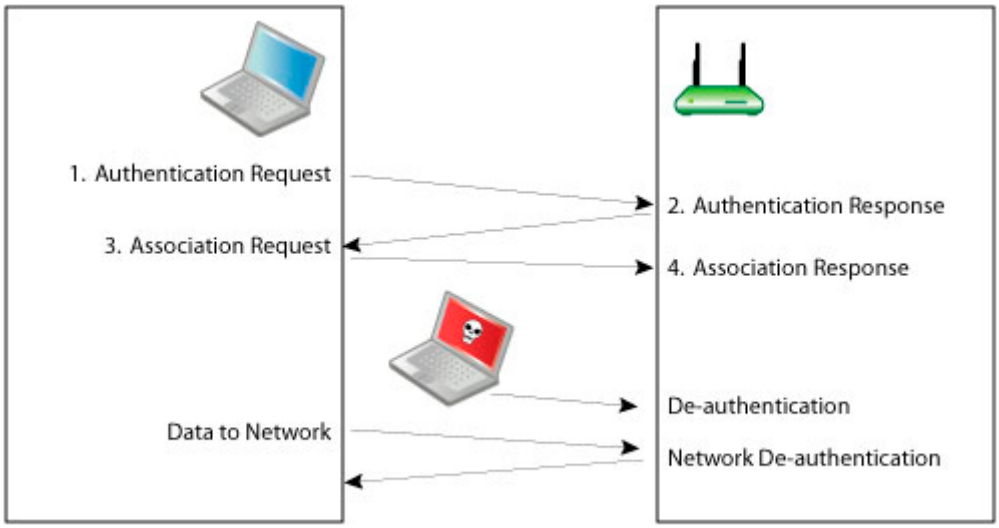
Denial of Services (DoS) Attacks

Denial of Service (DoS) events can cause significant disruption in wireless networks by preventing a user from accessing a wireless resources. DoS events can happen in two forms; the first form is a DoS attack directed at a specific device and the second form is a DoS attack directed at the wireless medium. Device

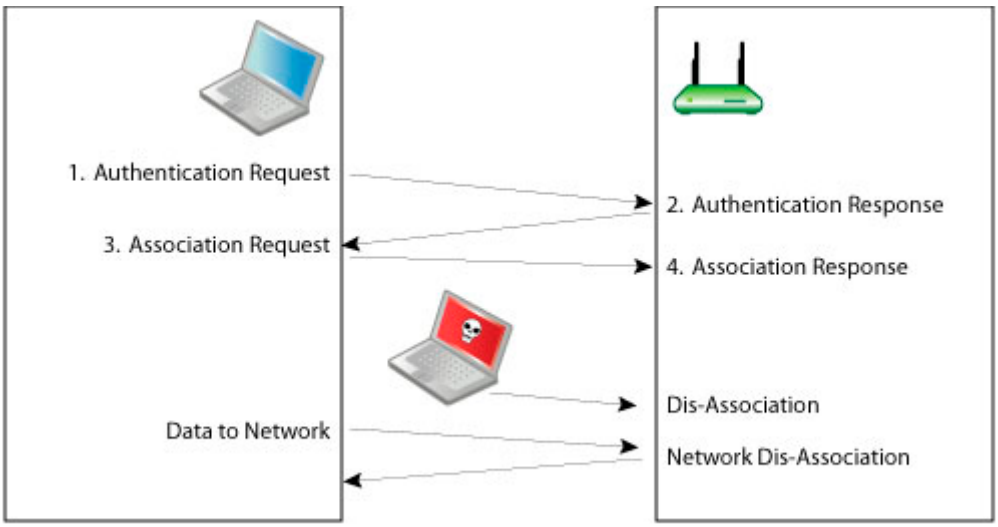
level attacks will affect one or more devices depending on the attack setup; broadcast attacks for example can impact all stations associated to an Access Point, whereas a more directed attack will only impact a single station leaving other stations connected to the Access Point. In either case DoS attacks of this nature consume wireless bandwidth. The second type of attacks directed at the medium exploit inherent flaws in the 802.11 protocol impacting all devices on the channel by making the medium temporarily unusable. DoS attacks by themselves are of little use to a hacker or malicious user, but they may serve as the foundation for other more significant exploits. DoS attacks and their infestation scenarios can include:



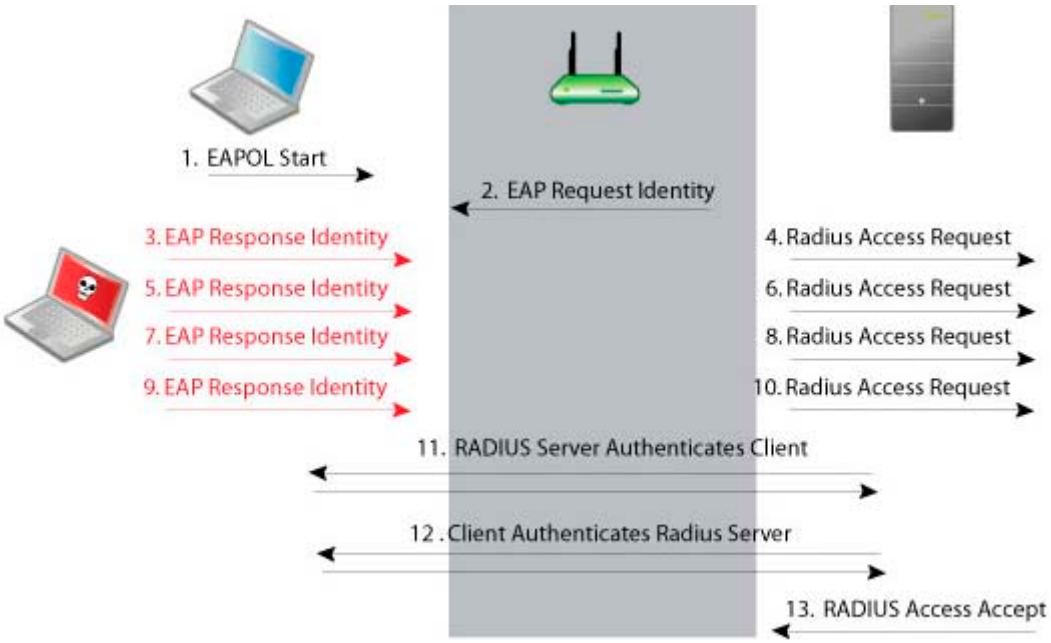
- *DoS assoc table overflow*
- *DoS CTS flood*



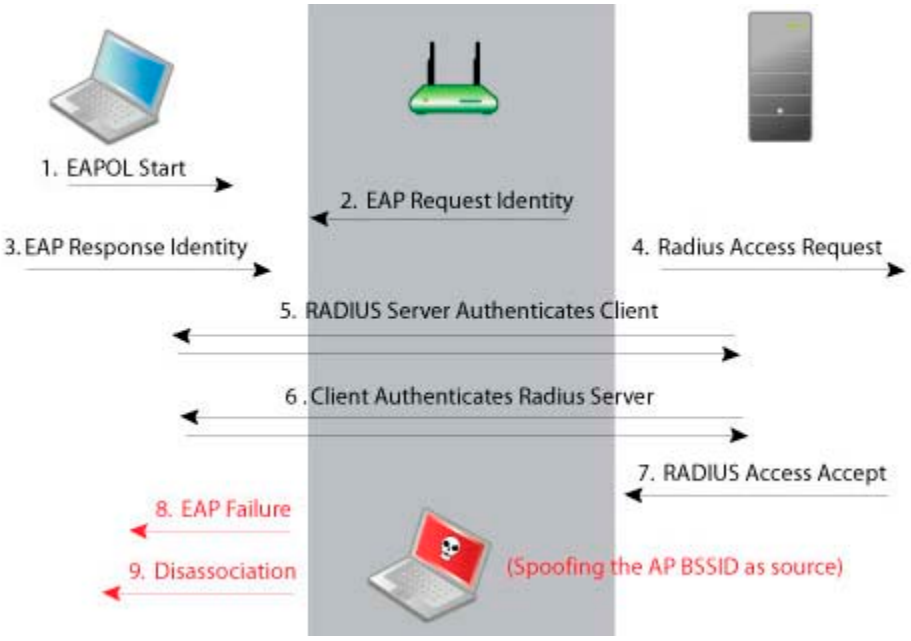
- *DoS deauthentication*



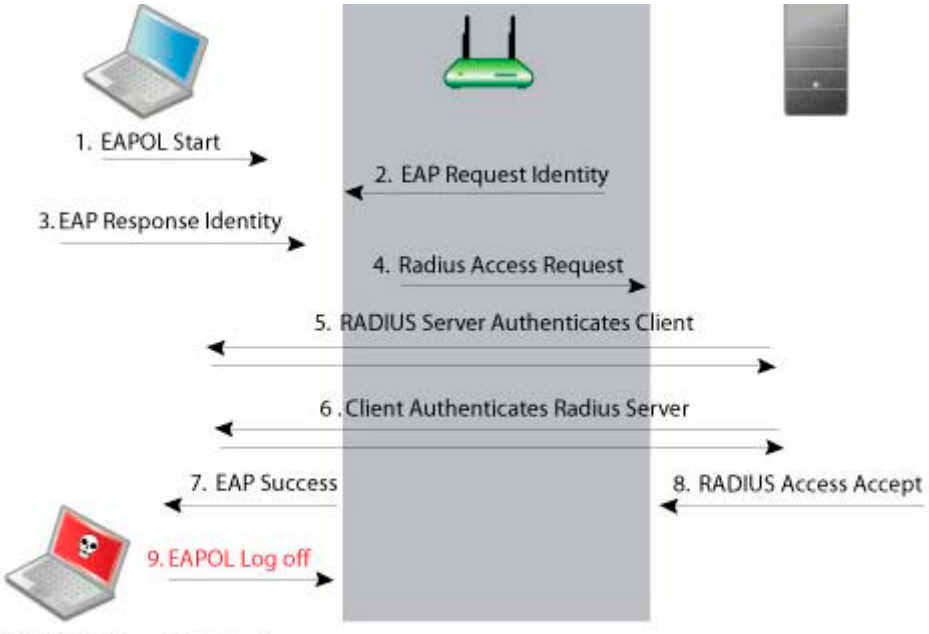
- *Dos disassociation*



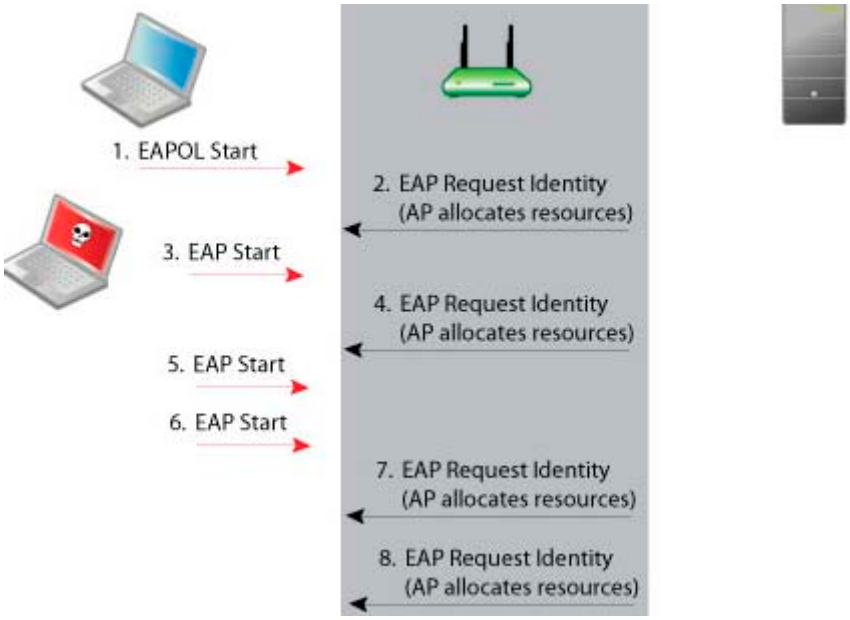
- *DoS EAP authentication flood*



- *DoS EAP failure*



- *DoS EAPOL logoff*



- *DoS EAPOL start storm attack*
- *DoS excessive AP MACs*
- *DoS excessive station MACs*
- *DoS PS poll flood*
- *DoS RF jamming*
- *DoS virtual carrier*

11.4.1.3 Performance

Performance alarm events provide critical information about the service levels of the wireless network. In a wireless environment, performance events can be an indication of problems related to configuration, compatibility, congestion, coverage, potential interference sources and utilization levels. Because 802.11 operates in a shared and unlicensed frequency spectrum, it's possible performance issues may be the result of non 802.11 devices, such as microwaves and cordless phones, or the result of a conflict with other 802.11 devices, including both valid and neighboring devices transmitting into the monitored airspace.

Performance alarms can be divided into the following sub-categories:

Configuration Compatibility

802.11 Wireless networks operate in unlicensed frequency ranges capable of operating in numerous different configurations. Monitoring the wireless devices operating configuration ensures maximum compatibility and network performance. Configuration compliance events can include:

- *AP missing PBCC option*
- *AP wrong protection mode*
- *Coordination function change*
- *Device streaming traffic*
- *PCF and DCF simultaneously used*
- *Station authentication failure*

- *Station data rate mismatch*
- *Station thrashing between 802.11b and 802.11g*

Congestion

802.11 Wireless network operate in a shared and uncontrolled medium. Congestion is inevitable as the number of wireless devices and bandwidth demands increase. AirDefense Enterprise proactively monitors for congestion problems to ensure maximum performance on the wireless network. Congestion events can include:

- *AP channel interference*
- *AP short slot time violations*
- *Channels with high noise levels*
- *CRC threshold exceeded*
- *Layer 3 traffic storm*
- *Station excessive roaming or reassociations*

Coverage

802.11 Wireless networks operate in unlicensed frequencies. However, the allowable power output by any single device has been regulated. This limits the range and coverage of an 802.11 capable wireless device. The main causes of coverage problems are related to deployments. AirDefense Enterprise provides detections of coverage problems to assist in troubleshooting specific areas of the wireless networks. Coverage events include:

- *AP excessive low speed transmissions*
- *AP rejected station association requests*
- *Excessive retransmissions*
- *Hidden station detected*

Potential Interference Sources

802.11 devices operate in unlicensed frequency ranges, 2.4GHz for 802.11b/g and 5GHz for 802.11a. Channels and are subject to interference from other devices utilizing the same frequency. Examples of these devices include: microwave ovens, Bluetooth devices, baby monitors, cordless telephones, Zigbee devices, non 802.11 wireless security cameras and wireless USB devices (wireless keyboard and mouse). Interference source events could include:

- *802.g device using non-standard data rate*
- *802.11n pre-standard device*
- *Turbocell in use*

RF Spectrum Analysis

802.11 Wireless networks operate in unlicensed frequencies; many non 802.11 transmitters such as cordless phones, and Bluetooth share the same spectrum with 802.11 wireless networks. A non 802.11 transmitter can impact the network by causing interference, identifying the source is difficult with standard 802.11 hardware as these it simply appear as noise. Spectrum Analysis can be used to identify the source of the interference and judge the impact the interferer will have on the wireless network.

- *BlueTooth interference detected*

- *Continuous wave interference detected*
- *Frequency hopping interface detected*
- *Microwave oven interface detected*

Utilization

802.11 Wireless networks operate in a medium where all devices share the available bandwidth. Any single device is capable of impacting performance by using all available wireless resources. AirDefense Enterprise monitors over 50 performance related utilization statistics for the authorized wireless devices, to ensure utilization related performance problems are discovered before causing significant wireless network performance degradation. Utilization events can include:

- *802.1x authentication frames sent threshold exceeded*
- *Association frames sent threshold exceeded*
- *Authentication frames sent threshold exceeded*
- *BSS: 802.11 authentication frames seen threshold exceeded*
- *BSS: 802.1x authentication frames seen threshold exceeded*
- *BSS: association frames seen threshold exceeded*
- *BSS: Control frames seen threshold exceeded*
- *BSS: Data frames seen threshold exceeded*
- *BSS: Deauthentication frames seen threshold exceeded*
- *BSS: Disassociation frames seen threshold exceeded*
- *BSS: Management frames seen threshold exceeded*
- *BSS: New associations threshold exceeded*
- *BSS: Probe request seen threshold exceeded*
- *BSS: Probe response threshold exceeded*
- *BSS: Total associations threshold exceeded*
- *BSS: Wired to wireless traffic threshold exceeded*
- *BSS: Wired traffic threshold exceeded for station*
- *BSS: Wireless station to station traffic threshold exceeded*
- *BSS: Wireless to wired traffic threshold exceeded*
- *Control frames received threshold exceeded*
- *Control frames sent threshold exceeded*
- *Data frames received threshold exceeded*
- *Data frames sent threshold exceeded*
- *Deauthentication frames sent threshold exceeded*
- *Disassociation frames sent threshold exceeded*
- *Fragment frames sent threshold exceeded*
- *Management frames received threshold exceeded*
- *Management frames sent threshold exceeded*

- *Minimum beacon frames to be sent Threshold Violated*
- *Probe requests sent threshold exceeded for station*
- *Probe response sent threshold exceeded for AP*
- *Traffic received threshold exceeded*
- *Traffic sent threshold exceeded*

11.4.1.4 Policy Compliance

Policy Compliance events provide information about an observed operational configuration, as compared to the configuration set in the AirDefense policy manager. Detected policy discrepancies allow configuration vulnerabilities to be corrected before they potentially exploited. Sanctioned Access Point configuration problems account for a significant percentage of security vulnerabilities in any organization. Policy configuration problems typically result in significant security issues and should be addressed in a timely manner.

Policy compliance events can be divided into the following sub-categories:

802.11 Encryption

802.11 Wireless networks operate in a shared medium, and all devices within the range of the transmission can passively hear the sender. Encryption is implemented in wireless networks to allow secure data transmissions, and prevent eavesdropping. AirDefense Enterprise monitors authorized Access Points to ensure defined encryption mechanisms are always used and the network operates in compliance with the enterprise policy. 802.11 encryption violations can include:

- *80211 encryption mode violation*
- *AP encryption mode violation*
- *Devices unprotected by TKIP*
- *WPA or 802.11i pre-shared key usage*

Advanced Key Generation

802.1x authentication provides a mechanism to authenticate a user and/or computer against a network and generate the keys necessary to encrypt data. If required, the keys can be changed dynamically. AirDefense Enterprise monitors authorized Access Points to ensure defined advanced key generation mechanisms are used and the network operates in compliance with the enterprise policy. Advanced key generation violations include:

- *Advanced key generation mode violation*
- *AP EAP-FAST violation*
- *AP EAP-TLS violation*
- *Device unprotected by 802.1x*
- *Device unprotected by EAP-FAST*
- *Device unprotected by PEAP*

AirDefense Personal Policy Violation

AirDefense Personal is a client product designed to monitor the network's edge. The edge of the network is defined by the mobile work force that travel throughout the world to airports, hotspots, hotels etc. As mobile workers travel, they use and access confidential and proprietary corporate data and can access the corporate

network through a VPN (Virtual Private Network). User stations typically present the weakest security link to a malicious users. AirDefense Personal ensures the enterprise policy is enforced anywhere, and any time the client is using mobile resources, even when it is outside of the range of AirDefense Enterprise monitoring sensors.

Authentication

AirDefense Enterprise monitors 802.11 authentication, as defined in a company policy, against what has been observed in the air, allowing for the notification of enterprise compliance policy violations. Authentication violations include:

- *AP authentication mode violations*
- *AP Symbol keyguard violations*
- *Basic authentication mode violations*
- *Extended authentication mode violations*

Environment

Environmental events allow for the monitoring of generic operation of wireless network activity. These events could have an impact on enterprise compliance, security and performance requirements. Environment events include:

- *Ad-Hoc network violations by authorized devices*
- *Ad-Hoc network violations by unauthorized devices*
- *AP PSPF violations*
- *Missing APs*
- *Missing stations*
- *RF regulatory violations*
- *Station usage time violations*
- *Station vendor violations*
- *Wireless bridging detected*

Global

Global events are generic informative events about observed behavior in the wireless network.

Incorrect AP Configurations

Access Points typically have static configurations set by an administrator. An Access Point which changes its configuration, or is not using its default configuration, could prevent authorized access or allow unauthorized access. Incorrect configuration events monitor the Access Point configuration as observed through the air against defined operational policies. Observed incorrect AP configuration events can include:

- *AP advertised data rate violations*
- *AP default configuration changes*
- *Incorrect AP channels*
- *An AP SSID is broadcast in the beacon*

11.4.1.5 Reconnaissance

Reconnaissance alarms track devices attempting to locate wireless networks. 802.11 wireless networking functions in a shared medium in which the wireless signals are not constrained by traditional physical boundaries. Signals can extend outside building boundaries into parking lots or neighboring faculties enabling valid client devices, attackers or malicious users to receive the signals and discover available wireless networks. Wireless behavior from supplicants such as such as *Windows XP zero configuration client* (WZC) is an example of normal reconnaissance behavior where the client continues to probe for configured networks (this is normal reconnaissance activity that allows clients to find networks not broadcasting SSIDs).

Alternatively, Reconnaissance can be used by a malicious user as a first step in an attack on a wireless network. Open source reconnaissance tools, such as Wellenreiter, Netstumbler, and Dstumbler, can be used to discover wireless networks. Some reconnaissance tools use active methods to detect wireless networks and are easily detected by AirDefense Enterprise, while other tools (such as Kismet) have transitioned to a passive, or listen only mode, and cannot be detected by a WIDS platform. For customers operating in no-wireless environments, reconnaissance events are of medium to high importance, and should be investigated. For deployments in urban multi-tenant areas, reconnaissance events are of minor importance, because of the increasing prevalence of wireless networks combined with the increasing sophistication of newer reconnaissance tools that operate in passive mode and cannot be detected.

Reconnaissance alarms can be divided into the following sub-categories:

Reconnaissance Tools

Reconnaissance tools enable a user to discover available wireless devices in the vicinity of the user running the tool. While early versions of these tools use active methods to find available wireless resources, newer versions are increasingly more sophisticated and have transitioned to passive (or listen only mode) and go undetected. Reconnaissance tools include:

- *AirMagnet handheld scanning*
- *Dstumbler scanning*
- *ESSID-jack*
- *NetStumbler scanning*
- *Wellenreiter scanning*

Client Activity

When in a wireless network, clients actively search for the wireless networks they have been configured to connect to, thus enabling clients to find wireless Access Points in their vicinity. Once a client connects to an Access Point, it continues to search for other resources, which may include different networks or resources with higher signal strength. Reconnaissance in environments with deployed wireless networks is considered typical and is an expected behavior (such as aggressive scanning).

Weakness

Access Points can be configured to make them more or less vulnerable to reconnaissance activity. Some of these options include broadcasting the SSID in the beacon, and options to respond to null probe requests. Configuring an Access Point to not respond to null probe requests and disable broadcasting the SSID in the beacon in the SSID are good practices to hide the wireless network from basic users, however it will do little to deter more advanced users attempting to discover the network.

11.4.1.6 Rogue Activity

Rogue activity alarms include events for devices participating in unauthorized communication in the airspace. Examples of this type of event included in this category are detection of a wireless device operating in the airspace to detection of the most sever risks unsanctioned wireless device communicating with the wired network. AirDefense Enterprise makes a clear distinction between an unauthorized device, which could be a neighboring device transmitting into the monitored airspace, and a rogue device, a device which is communicating with a device on the sanctioned wired network. This distinction is critical to understand and appropriately respond to each threat posed by an individual device. This advanced threat assessment capability allows an administrator to safely ignore neighboring Access Points while focusing attention to real threats.

Rogue activity alarms can be divided into the following sub-categories:

Access Violations

AirDefense Enterprise monitors all device communications in the airspace covered by the monitoring sensors. The system can distinguish between authorized and unauthorized communications. Access violations occur when authorized devices communicate to unauthorized devices. Access violations can result from:

- *Accidental associations*
- *Unauthorized bridging*
- *Unauthorized roaming*

Authorization Violations

AirDefense Enterprise monitors the airspace for all wireless devices. The authorization violation subcategory includes devices that have not been acknowledged as sanctioned, or ignored transient or neighboring devices. Authorized violations can result from:

- *Unauthorized APs*
- *Unauthorized stations*

Rogue Exploit

The *rogue exploit* subcategory contains alarms detecting genuine rogue activities by unsanctioned wireless devices communicating with the authorized devices on the wired infrastructure. Examples include: unauthorized Access Points physically attached to the wired network (Rogue AP) or unauthorized stations connected to an authorized AP (Rogue Station) on the wireless network. Rogue exploits can result from:

- *AirMagnet handheld scanning*
- *Dstumbler scanning*
- *ESSID-jack*
- *NetStumbler scanning*
- *Wellenreiter scanning*

11.4.1.7 Vulnerabilities

Vulnerabilities are weaknesses not actively exploited, but are weaknesses detected in the airspace. Weaknesses can potentially be exploited by both active and passive methods. For example, unencrypted wired side traffic leakage can be exploited passively by discovering wired-side device information, while rogue Access Points can be actively exploited by a station associating to it. Vulnerabilities provide an

inherent security risk to the enterprise and should be carefully evaluated to understand the potential exposure that could occur if a vulnerability was exploited. Once a vulnerability is discovered options should be considered to mediate the vulnerability to prevent it from being exploited.

Vulnerability Alarms can be divided into the following sub-categories:

Predictive Problems

Using passive wireless monitoring, AirDefense provides events indicating potential wireless security issues. Issues can be related to network or client configurations and may not currently be actively exploited, however the danger exists that they could be exploited. Predictive detection allows an administrator to take proactive measures to resolve security issues before a malicious user has the potential to exploit it. Predictive problems can result from:

- *Fuzzing: Invalid channel advertisement*
- *Fuzzing: Invalid management frame*
- *Station using a LEAP user*
- *Station vulnerable to hotspotter attack*
- *Transmitting device using invalid MAC*
- *Unassociated station detected*
- *Windows zero config memory leak*

Suspect Activity

Suspect activity captures wireless events or activity, though not a direct attack on the wireless network, suggest a potential exploit. Suspect activity should be scrutinized as it occurs. Suspect activity is often accompanied by other exploit events, as it may be only one facet of a larger threat. Suspect activity can result from:

- *Ad-Hoc advertisement of authorized SSID*
- *AP channel changes*
- *AP default SSID in use*
- *AP ESSID changes*
- *AP rate changes*
- *Conversation loops*
- *Crackable WEP IV key used*
- *Random MAC address detected*
- *Soft AP*
- *Watched station active*

Wired Leakage

In wireless networks, unencrypted *wired side traffic leakage* is a result of basic Access Point functionality. An Access Point, at its most simplistic form, is a bridge between the wired medium and the wireless medium, allowing wireless devices to communicate with devices on the bounded wired network. An Access Point typically works the same for traffic in the reverse direction, traffic from the wired network can be transmitted into the air, to specific devices as well as broadcast addresses. The security concern entails the broadcast or multi-cast wired traffic which the Access Point bridges into the air in clear text. All devices within range of the AP can passively listen to traffic and obtain information about network configurations, routing, and

the devices on the wired network. This is compounded when the Access Point is placed on a VLAN which has NetBios traffic that can reveal a great deal about networked devices. It is best to place the Access Points on a dedicated subnet which limits the network's broadcast domain to minimize wired side leakage. Wired linkage can result from:

- *HSRP multicast traffic*
- *IGMP multicast traffic*
- *IGRP multicast traffic*
- *IPX traffic*
- *Multicast all routers on this subnet*
- *Multicast all systems on this subnet*
- *Multicast DHCP server/relay agent*
- *NetBIOS traffic*
- *OSPF all routers multicast traffic*
- *OSPF designated routers multicast traffic*
- *RIP2 multicast traffic*
- *STP traffic*
- *Unencrypted broadcast or multicast traffic detected in encrypted environment*
- *VRRP multicast traffic*

12

802.11n

IEEE 802.11n is a next generation wireless technology that delivers spectacular improvements in the reliability, speed and range of 802.11 communications. Delivering about 6 times the throughput of 802.11ag with substantial improvements in network coverage and connection quality, 802.11n is projected to replace wired Ethernet as the dominant local area network technology of the future.

For additional information, refer to the following 802.11n subjects:

- *802.11n's Current State*
- *802.11n Overview*
- *Understanding RF Multipath and MIMO*
- *802.11n and Mixed Mode Operation*
- *Frequency Bands and Channel Availability*
- *Adopting 802.11n*
- *802.11n Site Surveys using LANPlanner*

Once you have thoroughly reviewed the content of this *Enterprise WLAN Design Guide* and applied it theoretically to the new 802.11n standard (as described within this chapter), you will have all the pre-requisite knowledge required to plan the replacement of an existing wired network and deploy an Enterprise-class wireless network supporting the latest wireless standards and performance strategies available.

12.1 802.11n's Current State

The IEEE 802.11n working group, called Task Group N (TGn), is working on publishing the 802.11n standard. In March 2007 TGn approved the 802.11n Draft 2.0 which has become the early standard for several 802.11n products available in the market today. Availability and adoption of 802.11n Draft 2.0 products has been aided to a large extent by the Wi-Fi Alliance's announcement of a Draft 2.0 interoperability certification program. The Wi-Fi alliance is an industry organization that certifies the interoperability of 802.11 devices from different vendors. Meanwhile TGn is continuing to work on refining the 802.11n standard based on comments received from various experts. Based on current time lines 802.11n is expected to achieve final IEEE Standards Board approval by November 2009.

12.2 802.11n Overview

802.11n introduces several enhancements to the 802.11 PHY (radio) & MAC layers that significantly improve the throughput and reliability of wireless communication. These enhancements include:

- *Spatial OFDM* - A new more efficient OFDM (Orthogonal Frequency Division Multiplexing) modulation technique that provides wider bandwidth and higher data rates.
- *40 MHz Channels* - 802.11n doubles data rates by doubling the transmission channel width from the 20MHz (used in 802.11abg) to 40 MHz.
- *Multiple-Input/Multiple-Output (MIMO)* - A radio system (transceiver) with multiple inputs into the receiver and multiple outputs from the transmitter capable of sending or receiving multiple spatial streams of data. (current 802.11 radios can transmit and receive a single data stream on a single best antenna used in a Primary/ Secondary diversity configuration).
- *Frame Aggregation* - 802.11n enhances the MAC layer and reduces the transmission overhead by allowing multiple data frames to be sent as part of a single transmission. Further reducing the inter frame spacing between the frames allows for transmissions to be completed in a shorter time making the medium available for other transmissions increasing overall throughput.

802.11n Draft 2.0 systems combine all of the above techniques to deliver connection speeds of 300 Mbps with improved communication range and more consistent coverage. While a majority of 802.11n benefits can only be availed in a Greenfield environment (comprising of 802.11n access points and 802.11n clients), Draft 2.0 does establish mechanisms for backwards compatibility with 802.11abg devices and offers several benefits even for existing 802.11abg devices.

802.11n has 2 modes of operation, a 2.4GHz 802.11b/g/n mode and a 5GHz 802.11a/n mode. A *Phased Co-existence Operation* (PCO) mode allows 802.11n to dynamically switch between 20MHz and 40MHz channels while communicating with 802.11abg and 802.11n devices allowing for backwards compatibility in both frequency bands.

12.3 Understanding RF Multipath and MIMO

In indoor environments, RF signals typically cross several barriers (walls, doors, partitions etc.) in their communication path towards the receiver. These barriers either reflect or absorb the original RF signal creating multiple reflected or secondary waveforms. Multipath results when multiple copies of the original RF signals travel different paths to arrive at the receiver.

Multipath traditionally has been considered the enemy of RF communication. Multiple reflected signals arriving at varying delays make it difficult for the receiver to separate a good signal from poor quality signals. Weaker signals may not be deciphered accurately resulting in data corruption and retries. Furthermore coverage holes can occur if reflected signals are out of phase but are received at the same time.

The higher the multipath in an environment the more the likelihood of poor RF performance resulting from weaker *received signal strength* (RSSI) increased retries and dead spots. Conventional RF system design has addressed the problem of multipath through the use of antenna diversity using two antennas for each radio in an access point. Antennas in a diversity configuration function almost like redundant antennas. A good signal from only one antenna is used at any time. Diversity switching logic implemented on the access point decides when to switch between a primary and a secondary (diversity) antenna for receiving the best signal.

MIMO introduces a new paradigm in RF systems design. MIMO capable radios actually perform better within a multipath rich environment. A MIMO system has multiple inputs into the receiver and multiple outputs from its transmitters allowing the system to receive or transmit multiple radio signal from its antennas. A MIMO radio can then apply several techniques to enhance signal quality and deliver more throughput. It is this

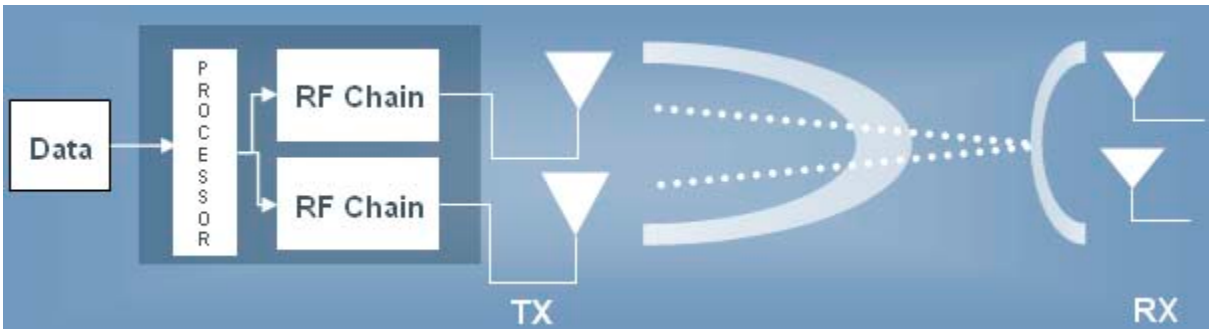
ability to add signal components from multiple antennas that differentiates MIMO access points from traditional access points that use antennas in a diversity configuration. An access point with antenna diversity selects signal components from one antenna that provides the best signal performance and ignores the other antenna.

A MIMO system has multiple *Radio Frequency* (RF) chains implemented in the radio allowing the processing of multiple RF signals from multiple antennas. Depending on the number of transmit/receive antennas and the number of spatial streams a MIMO system is often classified as a TXR:S system. Under this nomenclature *T* refers to the number of transmit antennas, *R* refers to the number of receive antennas and *S* refers to the number of spatial streams (data streams) the system can process.

A MIMO enabled access point (radio supporting multiple RF chains and multiple antennas) employs one or more MIMO techniques:

12.3.1 Maximal Ratio Combining (MRC)

To understand MRC consider a traditional access point that implements diversity antennas. Depending on the multipath in the environment, multiple RF signals will arrive on the antennas. The access point samples its antennas and selects the preferred signal from either one of its antennas ignoring the other signal. Diversity, in a sense, wastes RF energy using signal from any one antenna for a transmission. MRC is a receive side MIMO technique that takes RF signals from multiple receive antennas and combines them within the radio to effectively boost the signal strength. This MIMO technique is fully compatible with 802.11abg devices and significantly improves receiver sensitivity/overall gain for the access point radio especially in multipath environments.

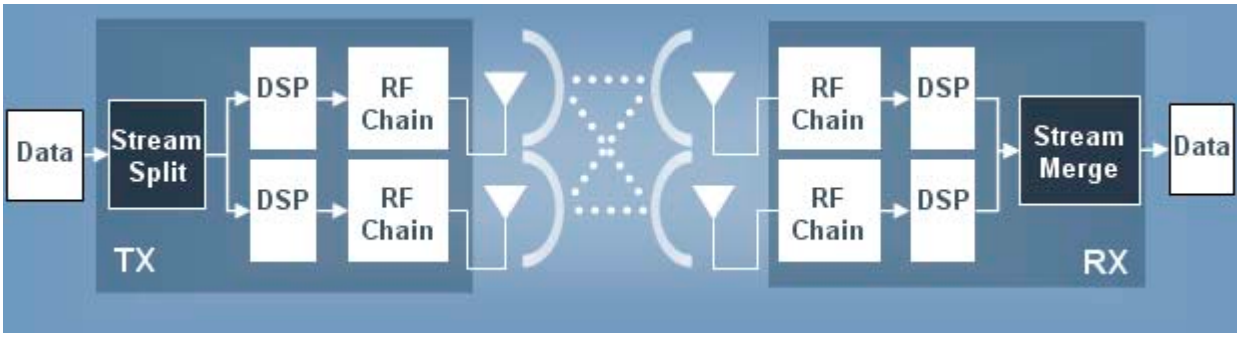


12.3.2 Beamforming

Transmit beamforming uses multiple transmitters (multiple RF chains + multiple antennas) and focuses RF energy towards the target receiver. An antenna array focuses energy towards the intended receiver in a way that less energy is wasted in other directions. As discussed previously, a single RF waveform arrives at the receiver as multiple waveforms and typically out of phase. The difference in phase can result in either an attenuated or an amplified waveform at the receiver. Transmit beamforming adjusts the phase of the RF signal at the transmitter such that the receiver signal is an amplified waveform. Standards based transmit beamforming is only supported for 11n clients. It requires the client to participate in the beamforming process by sending special frequency characteristics and channel response information to the access point. This information is used by the AP in calculating the phase adjustment for its next transmission. However, any changes in the multipath environment (movement of device, changes in obstructions) will nullify the beamforming phase optimization. Thus, this MIMO technique is unlikely to see widespread implementation in 11n access points.

12.3.3 Spatial Multiplexing

Spatial multiplexing is the fullest and most powerful application of MIMO and involves the transmission of spatial streams using N (or more) antennas. Spatial multiplexing requires a compatible MIMO client capable of receiving and de-multiplexing N spatial streams. Each spatial stream carries a unique data stream allowing the system to dramatically improve data rates and range. Spatially multiplexing MIMO systems are represented as TxR:N, where *T* represents the number of transmit antennas, *R* the number of receive antennas and *N* the number of data/spatial streams. Therefore, a 3x3:2 MIMO access point can transmit 2 spatial streams across 3 Transmit antennas, but is capable of receiving up to 3 spatial streams. The majority of 11n clients available in the marketplace can transmit and receive 2 spatial streams.



12.4 802.11 PHY

Although MIMO is the core building block for 802.11n, MIMO alone cannot deliver high throughput. The 802.11n physical layer (radio) implements wider channel width along with improved modulation techniques that provide a high bandwidth medium for multiple MIMO data streams. As an analogy, if MIMO delivers 2 trains, the 11n PHY provides 2 separate tracks to run the 2 trains, thereby doubling the transport of packets or increasing throughput.

12.4.1 Improved OFDM and Channel Bonding

802.11b radios used DSSS and CCK spreading methods with PSK modulation on a channel that was 22Mhz wide to deliver data rates between 1 Mbps to 11 Mbps. 802.11a and 802.11g both use 20Mhz channels, with OFDM spreading and PSK or QAM modulation to deliver data rates between 6 Mbps to 54 Mbps.

One of the reasons 802.11a and 802.11g offer higher data rates than 802.11b is they use OFDM modulation techniques.

802.11n uses a more efficient OFDM modulation and uses 2 bonded 20MHz channels to create a wider 40MHz channel. This doubles the data rate for 802.11n. When operating within a traditional 20MHz channel, OFDM further slices the channel into 48 sub-carriers. However when 802.11n applies OFDM on a 40MHz channel the number of sub-carriers do not simply double to 96 sub-carriers, they actually more than double to 104 sub-carriers. This allows 802.11n to deliver a 65 Mbps data rate (instead of 54 Mbps) per 20MHz channel for a total of 135 Mbps on a bonded 40Mhz channel - when transmitting a single spatial data stream. When transmitting in a MIMO mode with 2 spatial streams this data rate again doubles to 135 Mbps x 2 = 270 Mbps.

Under 802.11, every bit transmitted over the air is represented as a symbol. 802.11b transmits 1 symbol per microsecond for its 1 Mbps data, 2 symbols per microsecond for its 2 Mbps data rate and so on. An 802.11 a/g symbol is transmitted for 4 microseconds and packs many more bits - up to 256 bits for the 54 Mbps data rate. OFDM symbols are separated by a guard interval to reduce inter symbol interference.

Since no bits or data is transmitted during this time, the guard interval is typically an overhead to the communication process. The longer the guard interval between symbols, the lesser the throughput. 802.11a and 802.11g symbols are separated by an 800ns guard interval.802.11n introduces the concept of a short guard interval (400ns). In a high multipath environment, a long guard setting will typically improve overall RF performance, whereas in low multipath environments, a short guard setting can be more advantageous.

As noted earlier, when transmitting in MIMO mode with 2 spatial streams, 802.11n doubles data rates to 270 Mbps. However, when operating with a short guard interval 802.11n further improves data rates to deliver its top speed of 300 Mbps.

12.4.2 Frame Aggregation Techniques

802.11 communication uses a shared medium that has a significant amount of overhead associated it. Unlike wired Ethernet, there is no collision detection mechanism available in the wireless medium. Every wireless frame requires a positive *Acknowledgement* (ACK). This requirement for transmitting an ACK frame for every control/data frame has a huge performance penalty and significantly reduces throughput of 802.11 communication systems. 802.11 devices are also required to use a random wait interval (backoff period) after transmitting a frame and before getting access to the medium to transmit the next one. This further reduces aggregate system throughput.

802.11n introduces 3 key enhancements which address the inefficiencies of the traditional 802.11 MAC layer. Two of these techniques rely on frame aggregation; the third technique reduces interframe spacing between transmissions.

12.4.3 MSDU Aggregation

MSDU refers to an Ethernet frame. When MUs communicate with an access point, they first generate an Ethernet frame which gets wrapped in an 802.11 header for transmission to the access point. Even when the MU is communicating with multiple devices with different destination addresses, from an MU's standpoint it transmits all its 802.11 wrapped traffic to a single destination (the access point). The access point then unwraps these 802.11 frames, inspects each destination MAC address and forwards the traffic appropriately. The MSDU aggregation technique exploits this behavior and wraps multiple Ethernet frames within a single 802.11 wrapper and transmits a large 802.11 frame. Since the MU has a single security association with the access point, this large 802.11 frame only incurs the overhead of encryption once.

The main benefit of MSDU aggregation is that the aggregated frame has to be acknowledged as a single 802.11 frame, resulting in a single ACK being transmitted. This significantly reduces the acknowledgement overhead associated with 802.11 communications and improves overall throughput. The maximum MSDU size allowed by 802.11n is 7935 bytes.

12.4.4 MPDU Aggregation with Block ACK

MPDU aggregation gathers 802.11 frames which already have the 802.11 header(s) for the same destination and transmits them. Since this involves transmitting multiple 802.11 frames together, each frame requires it own ACK. However, instead of transmitting each ACK individually, 802.11n introduces a Block ACK frame which compiles all the individual acknowledgements into a single frame which gets transmitted from the receiver to the sender.

One of the disadvantages of MPDU aggregation, is each 802.11 frame needs to be encrypted separately adding encryption overhead. On the other hand, MPDU aggregation allows for the selective retransmission of those frames not acknowledged within the Block ACK. This can be very useful in environments which have a high number of collision or transmission errors. The maximum MPDU size allowed (by 802.11n) is 64K bytes.

12.4.5 Reduced Interframe Spacing

Normal 802.11 transmissions are required to implement a random backoff between transmissions. DCF (*Distributed co-coordinated Function*) is a contention based service widely implemented in infrastructure networks that defines the backoff period for devices. The interframe spacing in DCF is referred to *DCF Interframe Spacing* (DIFS).

DIFS is the minimum idle time for transmissions if the medium is idle for longer than the DIFS interval. WMM based QOS allows frame bursting for certain devices without requiring a random backoff. These WMM devices typically separate their ACK receipt and subsequent transmissions with a shorter interframe spacing, referred to as *Short Interframe Spacing* (SIFS). 802.11n introduces an even shorter interframe spacing called *Reduced Interframe Spacing* (RIFS). While MSDU and MPDU aggregation both provide mechanisms to reduce 802.11 overhead for transmissions to the same destination, RIFS provides a way to reduce overhead when transmitting a data stream to different destinations.

12.5 802.11n and Mixed Mode Operation

802.11n beacons are sent on a regular 20MHz channel using a low rate modulation. Beacons in the 2.4GHz frequency are fully understood by 802.11bg devices and 5GHz beacons are fully understood by 802.11a devices. An 11n beacon contains additional *High Throughput* (HT) mode information about an access point including channel width (20/40 MHz), guard interval (short/ long) and number of spatial streams (usually 2). An11n beacon also contains frame aggregation information, such as the maximum MSDU and maximum MPDU size. Due to all this extra information carried with the 11n beacon, the size of the 11n beacon frame is much larger than the conventional 802.11abg beacon size.

NOTE: 802.11n is fully backwards compatible to support mixed mode operation with 802.11abg devices.

The backwards compatibility 11n provides is similar to the protection mechanism 802.11g provides for 802.11b devices. 802.11n provides this protection mechanism in both bands, 2.4Ghz (for 11b/g devices) and 5GHz (for 11a devices). As with 802.11g, the protection mechanisms kick in as soon as an access point hears a legacy device transmitting on the same channel. The legacy device does not have to be associated to the 11n access point, the access point just needs to hear it on the same channel. However, mixed mode operation reduces the overall throughput for 802.11n. Keeping legacy clients on a different channel and dedicating separate channels for 11n devices can help resolve this problem.

12.6 Frequency Bands and Channel Availability

As noted previously, 802.11n can operate in both the 2.4GHz and 5GHz frequency bands and is fully backwards compliant for current generation devices in each band. 802.11g and 802.11a use channels that are 20MHz wide, while 802.11n uses 40Mhz channels (bonding 2 channels) when communicating with other 11n devices. The 2.4GHz frequency band has a total of 3 non-overlapping 20MHz channels, while the 5GHz band has a total of 23 non-overlapping 20MHz channels (for most countries). For 802.11n communications (that bond two 20MHz channels to create a 40MHz wide channel), this means the 2.4GHz band offers only a single 40MHz non-overlapping channel, while the 5GHz band offers up to 11 non-overlapping 40MHz channels. At a connection speed of 300 Mbps, a 2.4GHz deployment can deliver up to 450 Mbps (a single 40MHz 11n channel with 300 Mbps and a single 20MHz 11n channel with 150 Mbps), whereas the 5GHz deployment can deliver 3.45 Gbps (11 high throughput 40MHz 11n channels with 300 Mbps each and a single 20MHz 11n channel at 150 Mbps).

Clearly, the 5Ghz UNII band is better suited for multi-cell RF deployments. However, there are 2 issues that need to be considered with the 5Ghz frequency band. The 5Ghz band's range is a little less than 2.4Ghz, and there are radar detection requirements within this band. The range issue can be easily overcome with the proper antenna selection and transmit power adjustment. The second issue requires the 11n radio chip set provide radar detection and *dynamic frequency selection* (DFS) capabilities. Many early 802.11n access points (even those that are WiFi Draft N certified) use radio chipsets that cannot detect some newly introduced radar pulses. The operation of these access points is limited to only those bands that do not require radar detection, significantly reducing the number of available channels and overall system throughput.

12.7 Adopting 802.11n

12.7.1 RF Network Planning

RF network design typically involves determining the number of access points, their placement, channel assignment and power settings to deliver the required coverage and throughput for a given physical environment. Traditionally, RF network design has been evolved from a series of physical site surveys, in some cases, combining site surveys with planning tools offering RF prediction capabilities.

The RSSI based RF planning tools of the past are of little use in predicting and characterizing RF coverage for an 11n network. New planning tools must take into account the multi-path characteristics of a wide variety building construction material like concrete, glass, dry-wall, office cubicles, warehouse racks etc. Accurately characterizing multi-path is extremely important for optimal MIMO performance. Multi-path characterization includes the ability to automatically detect multiple partition types within a large site and assign attenuation and material reflectivity values based on site drawings representing the actual physical dimensions of the intended radio coverage area.

However, automatic construction profiling is only the first step. 802.11n uses MIMO transmissions with multiple data streams of varying modulation. Thus, merely predicting RSSI at any given point is of little or no value. 802.11n requires a system capable of combining the effects of MIMO with multiple spatial streams and the underlying data modulation. When supporting existing 11bg clients and simultaneously deploying 802.11n in the 5GHz band, there is no easy way to insert new 802.11n access points without causing harmful co-channel interference. Even with a *rip and replace* migration, a one-to-one replacement of legacy access points with an 802.11n AP (without transmit power adjustment) is likely to cause interference issues given the improved receiver sensitivity of the new radio technology.

802.11n planning can be simplified by using planning tools designed specifically for 802.11n and offer legacy deployment support. Customers should look for tools that drive RF heat-map algorithms based on the detailed RF characterization of the specific access point radio deployed. Predictions and coverage maps generated for generic access point models based can provide mis-leading results, delivering inconsistent coverage and poor performance when deployed.

12.7.2 802.11n Security Issues

The high throughput and reliability benefits of 802.11n will likely drive a greater proportion of new LAN deployments to be completely wireless networks. However, the need for security becomes even greater as businesses move mission critical applications to wireless and make it a primary network. A comprehensive WLAN security policy enforced by a dedicated IPS system provides the foundation for wired to wireless network transitions.

Time slicing IPS systems utilize the same infrastructure for providing WLAN and rogue detection services. These systems use specialized access points that can service WLAN clients on a BSS channel, and perform

off-channel scanning to detect rogue devices and capture threats for analysis. The access point forwards these frames to a backend system that compares them against a database of well known attack signatures to identify patterns and generate events or alarms.

Time slicing based IPS solutions may not work very well for 802.11n. The throughput of a typical 11n access point is expected to be about 6 times that of a traditional 802.11abg access point. With improvements in hardware (faster CPUs, increased memory), most access points can handle both data and IPS functions. However, time slicing radio resources for performing off channel scanning is likely to have a serious impact on latency sensitive and bandwidth intensive applications like voice and video. Optimizing the radio's configuration to spend more time servicing WLAN clients, with fewer off channel scans, can improve WLAN performance but leave more channels unmonitored and open for attack for longer periods of time. The time slicing problem becomes more acute with 802.11n, because each WLAN channel must now be monitored for attacks at both the 20MHz and 40Mhz modes. This effectively doubles the number of channels the sensor has to monitor. Access points optimized for high throughput 11n performance spend fewer cycles monitoring. The number of channels monitored exposes the wireless network to serious threats.

However, a dedicated sensor radio that does not serve WLAN clients (or perform wireless bridging) is able to spend all its time scanning for rogues and thus provides a much higher level of protection against potential attacks. A dedicated sensor can also spend more time on channels populated with authorized devices. These are more important channels and deserve a dedicated threat protection resource.

12.7.3 Indoor 802.11n Mesh

Mesh technology enables access points to wirelessly connect to each other and transmit data. Mesh provides a great way to extend network coverage, typically within hard-to-wire outdoor deployments. A dual radio access point design allows deploying one radio for WLAN client access, while leaving the second radio for a mesh backhaul. In 802.11abg access points, the 802.11a radio was typically used for mesh backhaul and provided a 54 Mbps connection to the network. With 802.11n, the capacity of this backhaul link increases to 300 Mbps, making mesh a higher speed network than fast Ethernet for inter connecting access points.

However, bandwidth alone is not sufficient to replace wired connections to multiple access points with wireless mesh connections. Typically, local area networks are segmented using *Virtual LAN* (VLANs), each with its own quality of service and security requirements. To replace a wired connection with a wireless link, the mesh access point should support intelligent backhauls that are VLAN and QOS aware supporting WPA2 security on the wireless link.

Mesh resiliency is another important consideration. Any changes in the physical environment can significantly change RF performance. The movement of goods within a warehouse could temporarily downgrade the RF link between two access points to unusable levels. Consequently, mesh AP's must maintain multiple redundant backhaul connections to other access points and dynamically self-heal based on changing RF conditions.

With the correct set of access point configurations, 802.11n based mesh provides a great opportunity to reduce the number of wired access points in an indoor WLAN and replace them with a mesh design that saves cabling costs and delivers a higher performance network.

12.8 802.11n and the Wireless Enterprise

802.11n offers many benefits to an Enterprise customer. In addition high speed connectivity and better range for 802.11n clients, the new standard also delivers significant improvements in WLAN reliability and

coverage for existing 802.11abg deployments. The following are some examples of high bandwidth applications that can take advantage of 802.11n:

- *Education* - Wireless access in high density areas, like classrooms and auditoriums with fewer access points
- *Health care* - Bedside access to medical imaging and patient records
- *Manufacturing* - Wireless sensor networks and video surveillance
- *Retail* - Store of the future applications, like smart carts with location based advertisement streaming, wireless digital signage and video surveillance

In high multipath environments (manufacturing, warehouses etc.), 802.11n will also deliver a more reliable wireless network with better coverage and fewer RF dead spots. All things being equal, 802.11n is expected to deliver a significantly better wireless experience compared to the existing WLAN technologies and standards. With 802.11n, wireless networking catches up with wired networking in the area of predictability and reliability and exceeds fast Ethernet in speeds and throughput.

The high bandwidth and improved reliability of 802.11n (when combined with the roaming benefits of wireless connectivity) will fundamentally transform the end-user mobility experience, impacting end-user behavior and business processes within the Enterprise. With 802.11n, wireless will no longer be the network of convenience, and in many cases, be the primary network running the most critical applications. For the Enterprise CIO, 802.11n lowers the cost of ownership for deploying, supporting and managing a LAN. In addition, business applications now can be defined for a single mobile device platform without the need for developing and porting to multiple platforms. Employees have reliable anytime, anywhere access to all business applications. Customers are better served by employees with seamless access to business information systems, regardless of location or device type. Traditional wireless networking enabled Enterprise mobility in select verticals, allowing key applications to be wireless enabled. 802.11n can unwire almost any business application used in the Enterprise today and support seamless, location independent information access for the workforce reducing infrastructure/platform costs while enhancing productivity levels and improving customer satisfaction.

802.11n enables the wireless Enterprise. The wireless Enterprise is an IT enabled business strategy that leverages wireless systems and applications to drive dramatic improvements in workforce productivity and customer satisfaction. From package delivery to warehouse and store operations, wireless technology has already improved business processes for verticals and retail. In the next 3 -5 years high speed, reliable and user friendly wireless technology will revolutionize the way businesses communicate, collaborate and service customers. The future of the network is wireless. Its time to cut the wire and become a smarter, more efficient wireless Enterprise.

12.9 802.11n Site Surveys using LANPlanner

LANPlanner is an efficient and effective tool which makes a perfect trade-off between simplicity and accuracy for 802.11n site surveys. Specifically, it can record measurement data about 802.11n network performance, and annotate the data directly to the building's drawing files. This section describes the best practices for conducting 802.11n surveys using LANPlanner.

For more information, refer to the following:

- *Pre-Survey*
- *LANPlanner Survey*

12.9.1 Pre-Survey

The following issues need to be resolved before conducting an 802.11n survey with LANPlanner:

- Model building floors and facilities using the *Building Wizard* utility from within the *Format Building* menu (see *Chapter 4 - Modeling Buildings and Facilities* in the LANPlanner User's Manual available at http://support.symbol.com/support/product/manuals.do.).
- Measure the current status of the RF environment by using the RF Monitoring Mode measurement feature of LANPlanner (see *RF Monitoring Mode* in the LANPlanner User's Manual available at http://support.symbol.com/support/product/manuals.do).
  - Determine which channels are being used by any AP in the environment. To obtain maximum reliability, the test AP should be set to a channel in which traffic from other clients is minimized.

    For 2.4GHz, only 3 non-overlapping channels (Channels 1, 6 and 11) are available. The test AP is recommended to use one of the above non-overlapping channels.

    For 5GHz, many more non-overlapping channels are available, so finding a channel with minimal interference is much less difficult.
  - If the noise value within the Access Point Information window is high, consider performing a spectrum analyzer survey to determine if there are any large noise sources in the environment which can degrade performance. The test AP should be positioned to minimize the effect of these noise sources.
  - Consider the mobility of objects in the measurement environment. If measuring an office with heavy foot traffic, consider measuring performance after typical business hours to increase measurement reliability.
- Plan measurement locations and routes ahead of time. If necessary consider additional test AP placement locations.
  - The inclusion of MIMO technology in the 802.11n standard means the performance of a wireless link can no longer be reliably predicted by RSSI values alone. The structure of walls surrounding the test AP can dramatically affect the structure of the signal multipath, and therefore dramatically affect 802.11n performance. A thorough survey should include measurements which represent the diversity of multipath environments (small offices, long hallways, tall ceilings, etc.).
  - In addition to best practices for WLAN surveys (which require measurements distributed throughout the full diversity of the RF environment), the following two scenarios should be always included in any complete 802.11n survey:

    1) Measurements in areas with poor MIMO performance characterized by long LOS links (greater than 10m of the test AP).

    2) Measurements in areas with good/standard MIMO performance characterized by NLOS links with high SNR or short LOS links (within 10m of the test AP).
- Prepare related survey equipment.
  - If necessary, deploy and configure the 802.11n AP in a suitable test location.
  - Connect a supported 802.11n wireless network adapter.
  - Configure the test network.

    If necessary, define a static IP address for the WLAN card which allows access to the same LAN as the 802.11n AP.

    Associate the WLAN card to the 802.11n AP.

- Extra batteries for the laptop (if available) & charger.

- Choose a method for data transfer. Due to the inclusion of MIMO technology in the 802.11n standard, 802.11n system performance can only be measured when data packets are sent from a specific AP to a specific client. LANPlanner provides three options for enforcing data transfers between the test AP and the client.
  - For local SiteSpy operation:

    Only one PC is required.

    Local SiteSpy operation is run from within the AP Performance mode measurement panel of LANPlanner and can be configured based on the instructions provided in the LANPlanner User's Manual available at *http://support.symbol.com/support/product/manuals.do.*
  - For remote SiteSpy operation:

    Two computers are required, one as the SiteSpy server and one as the SiteSpy client.

    The SiteSpy server can be run using the SiteSpy application or from within LANPlanner and can be configured based on the instructions provided in the LANPlanner User's Manual available at *http://support.symbol.com/support/product/manuals.do.*

    The SiteSpy client is run from within the *AP Performance* mode measurement panel of LANPlanner and can be configured based on the instructions provided in the LANPlanner User's Manual available at *http://support.symbol.com/support/product/manuals.do.*
  - For operation in other modes:

    Any network application can be used (such as a file transfer, VOIP, video streaming, iPerf, etc.) as long as data is consistently transferred between the test AP and the client.
  - Test connectivity between the server and the client. Common causes of network disconnect include:

    Improperly assigned IP addresses on the test AP, client, or remote server.

    A firewall on the test AP, client, or remote server is prohibiting connectivity between the SiteSpy server and client. In such cases, the firewall will need to be either disabled or configured to allow all traffic from the client.

12.9.2 LANPlanner Survey

By using a point-and-click measurement method, LANPlanner can obtain measurement data by simply roaming throughout the building environment and clicking on the associated position within the LANPlanner drawing. However, the validity and completeness of the measurement scenarios and the accuracy of measurement results should be guaranteed.

The following tasks and activities need to be carefully performed when conducting an 802.11n survey:

Choose an appropriate method for site data collection

Single marker and track run measurement modes are available for 802.11n surveys. The specifics of these two measurement methods is outlined in the LANPlanner User's Manual available at *http://support.symbol.com/support/product/manuals.do.* however an important distinction needs to be made between their operations during 802.11n surveys.

In both modes (when the user clicks to record a measurement), the software records the latest data available from the WLAN card. In single marker mode (if insufficient data is available when the software initially requests measurement data), the software waits up to 1 second to determine if a more reliable estimation of the RF performance can be obtained before recording the data. The 1 second timeout is not available in

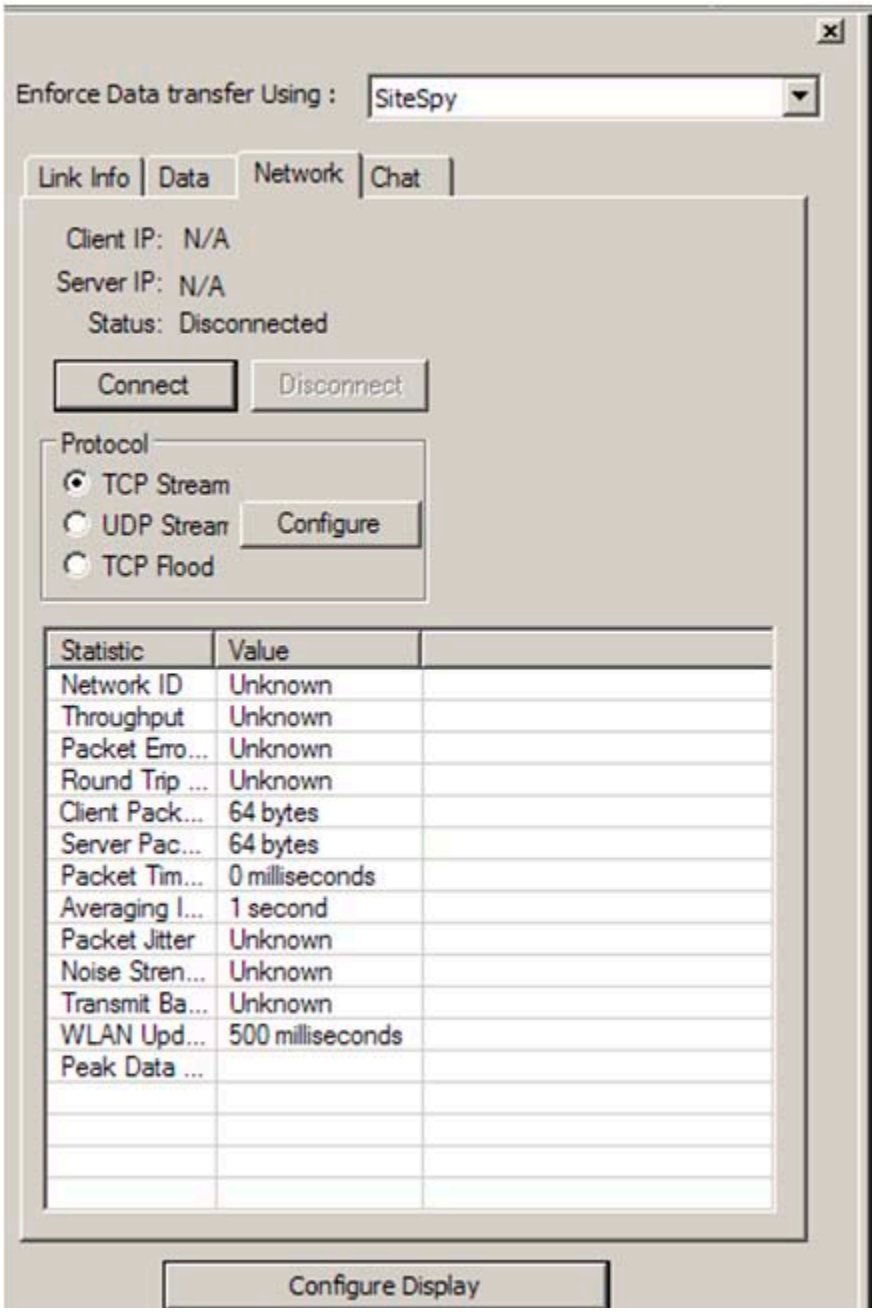
track run mode since the precise timing of the measurements is required for interpolating the position between the start and end points of the track run mode.

Maximize the reliability of the data collected at each measurement location

If using SiteSpy for enforced data transfer, guarantee the connection between the SiteSpy server and the SiteSpy client when taking measurements

A disconnect from the SiteSpy server can be determined when:

1. The status of the *Network* tab is Disconnected. The following shows the Network tab in a disconnected state.

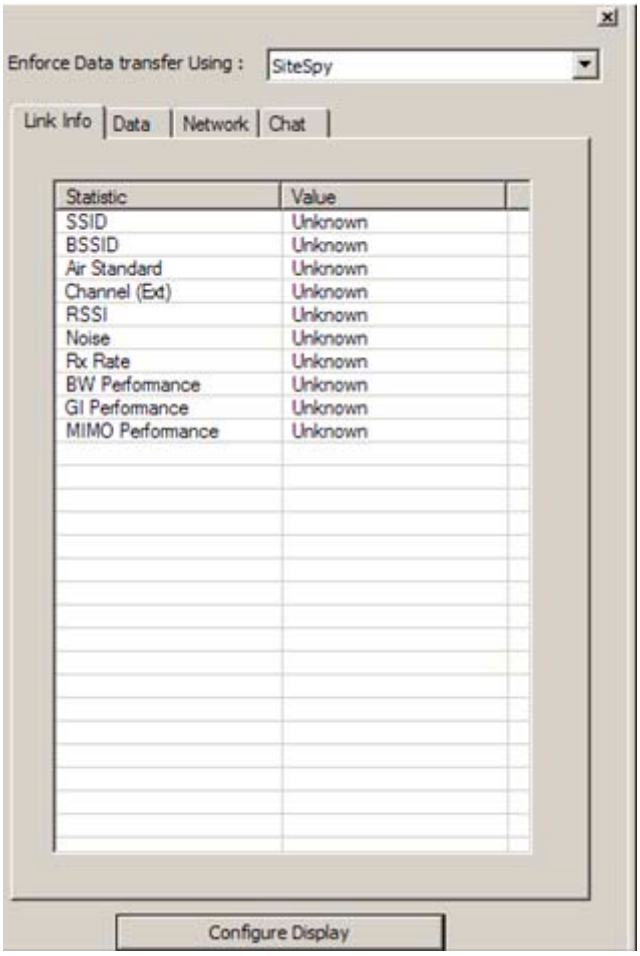


2. No associated AP is in the Access Point Information window. If an associated AP was present, a green circle would appear to the left of the MAC address.

   Click the *Connect* button in the *Network* tab to reestablish network connection.

   If the network connection cannot be reestablished because the receiver has left the coverage area of the test AP, the measurement run should be stopped.

   Monitor the link information in real-time to ensure data is being transferred from the test AP to the client. This data is available in the *Link Info* tab within the AP Performance mode's measurement panel.



   In single marker mode, it is best to initiate measurements (by clicking on the measurement location in the drawing) when the *Link Info* tab is populated with valid data.

   If Link Info data is always *Unknown*, check the connection to the SiteSpy server in the Network tab.

   When link information is not consistently available (valid values are only present ~20% of the time), valid measurement data cannot be always obtained. Even if the client is connected to the SiteSpy server the measurement run should be stopped, and the measurement setup will need troubleshooting to correct the problem.

   Common causes of this problem include packets being too large. A small packet (64KB) is recommended for 802.11n measurements since it maximizes the number of packets that can be sampled for

measurement data (in a short distance, even the largest packet can get 90% of the info). Another common cause is the receiver leaving the coverage area of the test AP.

To eliminate these problematic conditions:

- Take multiple measurements at each location, especially in single marker mode. Rotate the client to obtain one measurement at each rotation so collected data averages the effects of antenna orientation and body loss.
- In single marker mode, maximize accuracy of the marker location by referring to visual cues captured in both the formatted building in software and in the actual environment. Door frames, hallways, and cubicles all serve as excellent visual cues to help maximize measurement location accuracy.
- Define the measurement speed. In single marker mode, wait at least 2 seconds between each measurement. In track run mode, walk at a slow pace (~0.8m/s) during the survey.

Perform a complete survey of the 802.11n performance

- Take measurements which fully capture the diversity of the RF environment. This includes:

  NLOS measurements

  LOS measurements

  Longer LOS measurements in hallways or *canyons* (LOS measurements at distances of 10m or more in a hallway). This scenario is particularly important to measure since it represents areas of usually poor MIMO performance and so every effort should be made to measure the full length of a hallway link (when the test AP and client are both in the hallway).

  Measurement locations that separate the test AP and the client with a diversity of obstructions. For example, the LOS path from the test AP to the client should be obstructed by drywall partitions, cubicles, inventory racks, or any other obstructions which characterize the measurement environment.

- Cover enough RSSI range.

  Every effort should be made to measure the full range of signal strengths from the test AP (RSSI). This will help to obtain a full picture of the test AP performance in both good and bad environments. As an example, a typical range of RSSI values would cover all values from -40dBm to -90dBm.

  A full range of RSSI values should be gathered for both LOS and NLOS paths. Obviously, LOS paths may not receive RSSI values as low as NLOS paths, but every effort should be made to obtain as full of a RSSI range as possible.

  A good rule of thumb is to leave the coverage area of the test AP. This usually will guarantee that you have measured the lower end of the RSSI range.

- Guarantee the number of the measurements.

  Take measurements in at least 75 different measurement locations per survey.

  Balance the measurement number between LOS and NLOS scenarios. A 50-50 distribution is a good method.

  Take at least 20 measurements per 10dBm RSSI range.

  Take multiple measurements at each location. A good rule of thumb is to take 3 or 4 measurements per location when rotating the receiver about its azimuth plane to include the effects of orientation and body loss.

Organize the measurement results

- Use measurement filenames which adequately describe the type of survey conducted.
- Save the measurement results (*.wvc file) and the layout with markers locations (*.dwg file). By keeping a separate drawing file which includes all information regarding the test AP placement and configuration it is less likely that the relevant network model for the measured data will be lost.

NOTE: Measurement duration is based on the building scale and number of measurements. A typical survey of 100 measurement locations should take approximately 1 hour.

NOTE: Laptop recharging can be problematic. Make sure your laptop is fully charged before starting a measurement survey, and if possible bring extra batteries.

Appendix A Customer Support

Motorola's Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support for your region. Contact information is available by visiting http://www.motorola.com/customersupport and after selecting your region, click on the appropriate link under Support for Business

When contacting Enterprise Mobility support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Motorola responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola business partner, contact that business partner for support.

Customer Support Web Site

Motorola's Support Central Web site, accessed via the Symbol-branded products link under Support for Business, provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-122902-01
Revision A March 2009