Wi-Fi: The Importance of Mobility

SUMMIT DATA COMMUNICATIONS

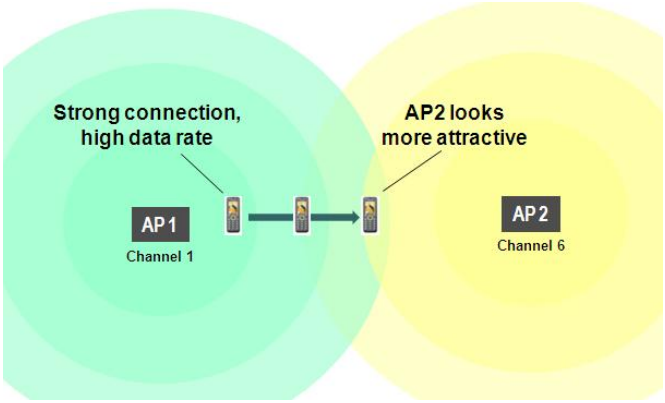
A Summit Data Communications White Paper
Originally Published: November 2009

Executive Summary

*Mobile computers require **persistent** network connections.*

- A momentary loss of network connectivity can disrupt applications running on the device.
- The result is lost data and lost productivity.

*As a Datalogic Mobile Computer moves, it **roams**.*



- The Wi-Fi® radio in the device initially connects to one access point (AP1).
- As the device moves away from AP1, AP2 offers a better connection.
- The process of switching from one AP to another while maintaining an active network connection is called roaming between two APs.
- A client performs four tasks to roam:
  1. Evaluate the current connection.
  2. Scan the vicinity for other APs.
  3. Select the AP that offers the best connection.
  4. Roam to it by establishing a connection and reauthenticating to the network.

*Many client devices do a **poor** job of roaming.*

- Wi-Fi client software usually is designed for consumer devices, which don't roam.
- Wi-Fi clients often select the wrong AP or take too long to roam from one AP to another.
- With robust security such as WPA2®-Enterprise, network reauthentication may take too long, disrupting applications on the device.

***Infrastructure-directed** roaming can cause bigger problems than it solves.*

- Wi-Fi infrastructure vendors argue that the infrastructure can select the best AP for each client.
- When the infrastructure does not allow a client to roam to its preferred AP, roaming can take too long, with applications disrupted.
- When the infrastructure forces a client to roam, applications can be disrupted.

With **Summit** Wi-Fi inside, a mobile computer provides **industrial-strength mobility**, including:

- Configurable active scanning for minimal disruption to application operation
- Robust algorithms for selecting the best target AP for roaming
- Fast EAP reauthentication for fast roaming with WPA2-Enterprise and WPA®-Enterprise
- Industry leadership in mobility, with solutions proven on hundreds of thousands of business-critical devices operating in the most challenging environments on the planet

Wi-Fi®, WPA®, and WPA2® are registered trademarks of the Wi-Fi Alliance.

DATALOGIC™

DATALOGIC MOBILE

Wi-Fi: The Importance of Mobility

SUMMIT DATA COMMUNICATIONS

A Summit Data Communications White Paper
Originally Published: November 2009

Summit inside!

SUMMIT DATA COMMUNICATIONS

A Summit Data Communications White Paper
Originally Published: November 2009

Wi-Fi in the Business World

Today's mobile workers need to connect to corporate data networks without having to "plug in" to wired, or Ethernet, network ports. One popular technology for wireless network connections is Wi-Fi® technology. Wi-Fi involves relatively short-range communication between radios, where one radio operates in a client device and the other operates in a network infrastructure endpoint device such as an access point (AP) or router. Most on-the-job computing devices include Wi-Fi radios as standard equipment.

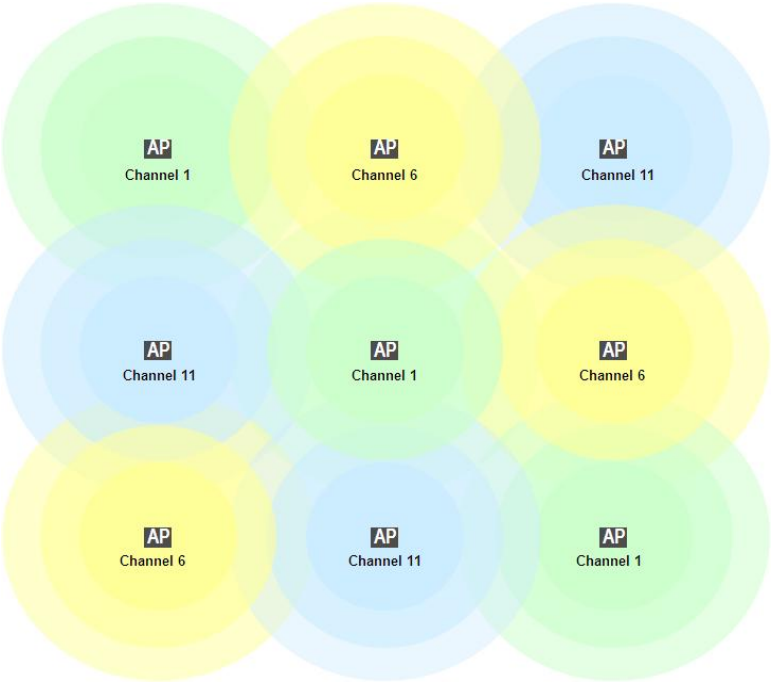
One reason Wi-Fi technology is so popular is because Wi-Fi products from different vendors interoperate, or work together. The Wi-Fi Alliance®, a non-profit industry association of more than 300 member companies, tests how well a product implements standards in areas such as interoperability and security. Since the introduction of the Alliance's testing programs in March 2000, more than 6,000 products have passed all tests required to earn the Wi-Fi CERTIFIED™ logo.

The Wi-Fi Alliance, however, does not test for mobility, which is the ability of a device to stay connected to a network as that device moves throughout the area for which Wi-Fi access is provided. For business-critical mobile devices such as mobile computers, mobility is essential. Roaming is a key part of mobility.

Why Roaming Occurs

In a typical Wi-Fi deployment, a large area is covered by the radio signals of many APs, with each AP offering a "cell" of coverage on a particular frequency channel. To minimize co-channel interference – collisions of signals from APs on the same channel – APs with adjacent or overlapping cells operate on different channels.

When a client device is associated to a nearby AP, the Wi-Fi radio in the client receives a strong signal from the AP. This signal enables the connection between the AP and the client to support a high data rate. As the client moves away from the AP, the strength of the signal decreases and the relative impact of interference sources in the area increases.



A typical Wi-Fi deployment is a set of overlapping "cells" of coverage.

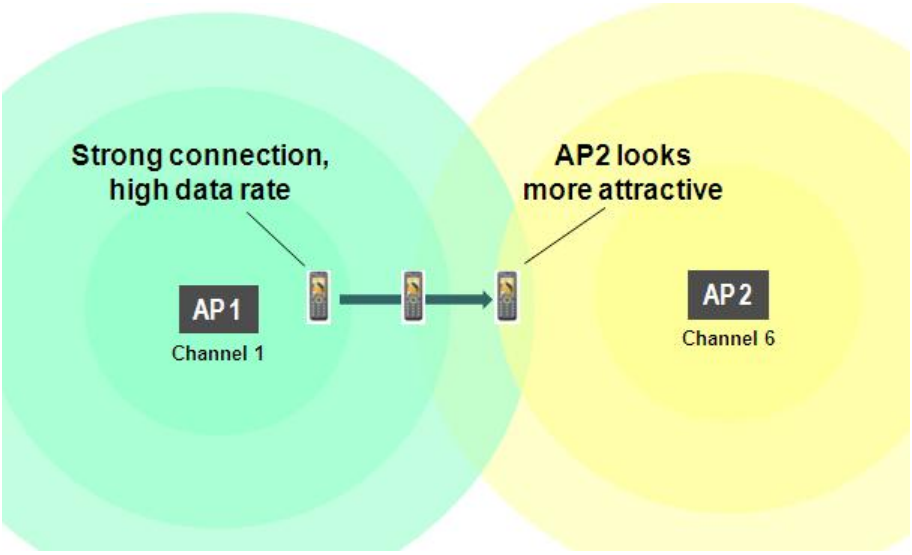
SUMMIT DATA COMMUNICATIONS

A Summit Data Communications White Paper
Originally Published: November 2009

Some transmitted data packets are not received, forcing the sender to retry the transmission. To maintain the reliability of data transfer over the connection, the client and AP negotiate a lower data rate.

If it continues to move away from the AP, then the client eventually reaches the edge of coverage for that AP, where a connection can be maintained only at the lowest data rate supported by that AP. Beyond the edge of coverage, the client is out of range for that AP, and the connection with the AP is lost.

Fortunately, a typical Wi-Fi deployment provides more than one AP, and the coverage areas of the APs overlap. When a client's connection to its current AP becomes tenuous (or simply less than optimal), the radio in that client can switch from the current AP to one that provides better connectivity. The process of switching from one AP to another while maintaining an active network connection is called roaming between two APs.



As a client moves away from the AP to which it is associated, the client's connection becomes weaker, and the client may look for an AP that offers a better connection.

While the movement of a client is the most common trigger for roaming, it is possible for a stationary device to roam. Suppose that a stationary device is within range of two APs but on the edge of the coverage area of each. A source of radio frequency (RF) interference could make the connection between the device's radio and the current AP tenuous enough so that the client needs to roam to the second AP to avoid losing its connection. Roaming by a stationary device, while possible, should occur rarely, especially when the Wi-Fi radio in the device has software that minimizes unnecessary roaming.

While clients typically initiate roaming, it is possible for the infrastructure to force a client to roam by severing that client's connection to its current AP and preventing the client from reconnecting to that AP. Reasons that the infrastructure may force a client to roam include:

- The infrastructure perceives that another AP in the client's vicinity will offer that client a better connection than the client's current AP.
- The infrastructure wants to balance the load across APs, and the client's current AP is handling many clients while a nearby AP has few or no clients associated to it.

Infrastructure-directed roaming is covered in more detail in the section "*Other Roaming Topics*".

SUMMIT DATA COMMUNICATIONS

A Summit Data Communications White Paper
Originally Published: November 2009

The Importance of Roaming

We define effective roaming as roaming that minimizes disruptions to network connectivity, thereby providing applications with the near equivalent of a persistent network connection. How important effective roaming is to a Wi-Fi device depends on how the device is used.

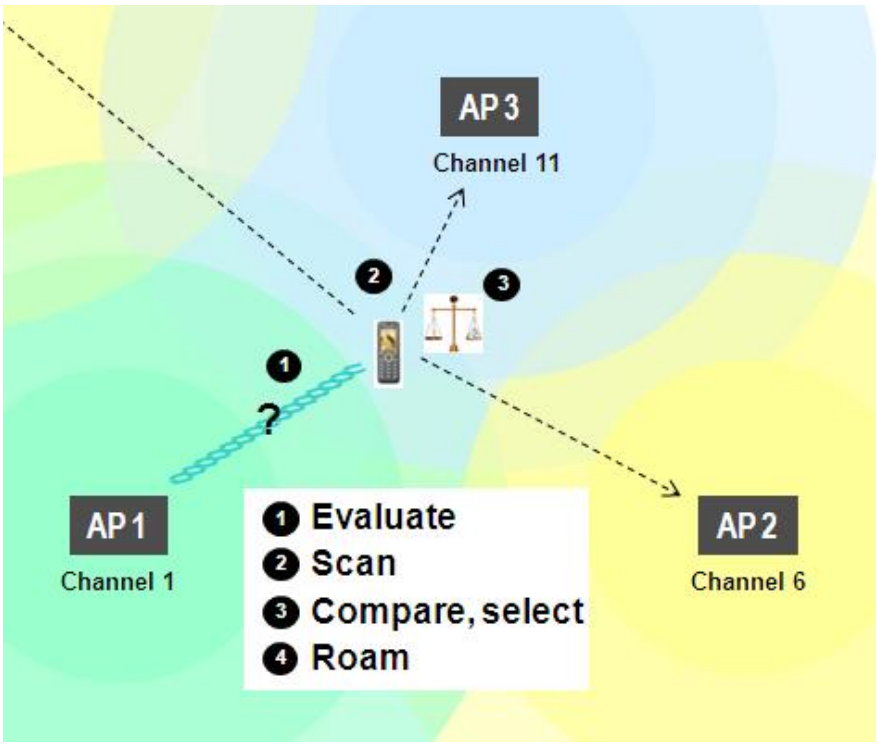
Nomadic computing devices tend to be used when the user is stationary. Consider a laptop computer. A laptop user tends to use the device when he or she is stationary in a conference room, at a desk, on a couch, or somewhere else. When the user is in motion with his or her laptop, the laptop's lid is closed and the user is not interacting with the laptop. Most applications that operate on the laptop do not depend on a persistent network connection. If an application has an error or fails because the network connection is lost while the user is in motion, then the user restarts the application when the network connection is re-established.

Mobile computing devices, in contrast, often are used while the user moves from one place to the next. Two examples of such devices are mobile phones and mobile computers. Many applications that operate on mobile computing devices depend on a persistent network connection, and even a momentary loss of that connection can disrupt such applications, resulting in a significant negative impact on the user's productivity. In short, effective roaming is essential for a mobile computing device.

How Roaming Works

Roaming is more complex than just switching from one AP to another. The roaming process has four steps:

1. Evaluate: Determine if the connection with the current AP is less than optimal.
2. Scan: If the connection is less than optimal, then scan the vicinity for other APs.
3. Select: Determine if any AP within range is likely to provide a better connection than the current AP.
4. Roam or Repeat: Roam from the current AP to the best candidate in the vicinity, or determine when to repeat the process beginning at step one.



Roaming involves four steps.

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

Note: *This white paper assumes that all APs to which a client may roam are a part of the same Internet Protocol (IP) subnet, so that all roams are roams within a subnet or a Layer 2 (L2) domain.*

Let's examine each of the steps of the roaming process.

1. Evaluate the Current Connection

The most common way to evaluate the current connection is to examine the strength of the RF signal from the current AP. The signal strength is represented by a received signal strength indication (RSSI) that typically is measured in dBm, or decibels (dB) referenced to one milliwatt (mW or m). The RSSI value is negative, and a stronger signal has a value closer to zero. For example, a signal with an RSSI of -40 dBm is stronger than a signal with an RSSI of -60 dBm. If the RSSI for the current AP is stronger than a threshold value, then the current signal is considered strong enough, and the client will not scan for an AP with a stronger signal.

Some Wi-Fi client radios incorporate metrics other than RSSI into the decision on whether or not to scan for APs. Metrics employed by a client may include:

- Signal-to-noise ratio
- Number of data retries in a specified time period
- Number of expected AP beacons not received in a specified time period
- Current data rate, especially if that data rate is the lowest supported rate
- Elapsed time since the last scan

2. Scan for a "Better" AP

To determine if another AP offers a better connection than the current AP, a client radio first must determine what other APs are within range. The customary way to identify APs within range is to perform an active scan* by issuing a probe request on every frequency channel on which an AP may be operating. When the client receives a probe response from an AP, the client knows that that AP is within range.

An AP that supports 802.11b, 802.11g, or 802.11n in the 2.4 GHz frequency band can operate on:

- One of 11 channels in the United States and other parts of the world where the 2.4 GHz frequency spectrum is governed by the Federal Communications Commission (FCC)
- One of 13 channels in Europe as well and other parts of the world where the 2.4 GHz frequency spectrum is governed by the European Telecommunications Standards Institute (ETSI)
- One of 14 channels in Japan, where the 2.4 GHz frequency spectrum is governed by the Telecom Engineering Center (TELEC)

An AP that supports 802.11a or 802.11n in the 5 GHz frequency band, including support for Dynamic Frequency Selection (DFS) channels, can operate on:

- One of 24 channels in the FCC domain
- One of 19 channels in the ETSI domain
- One of 12 channels in the TELEC domain

While a client radio is scanning, it cannot interact with the AP with which it is associated.

* An alternative to an active scan is a passive scan, whereby the client listens on each channel for beacons, which APs send out periodically. The risk with a passive scan is that, if the client does not wait long enough on a channel, then the client may miss an AP's beacon.

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

3. Select the "Best" AP

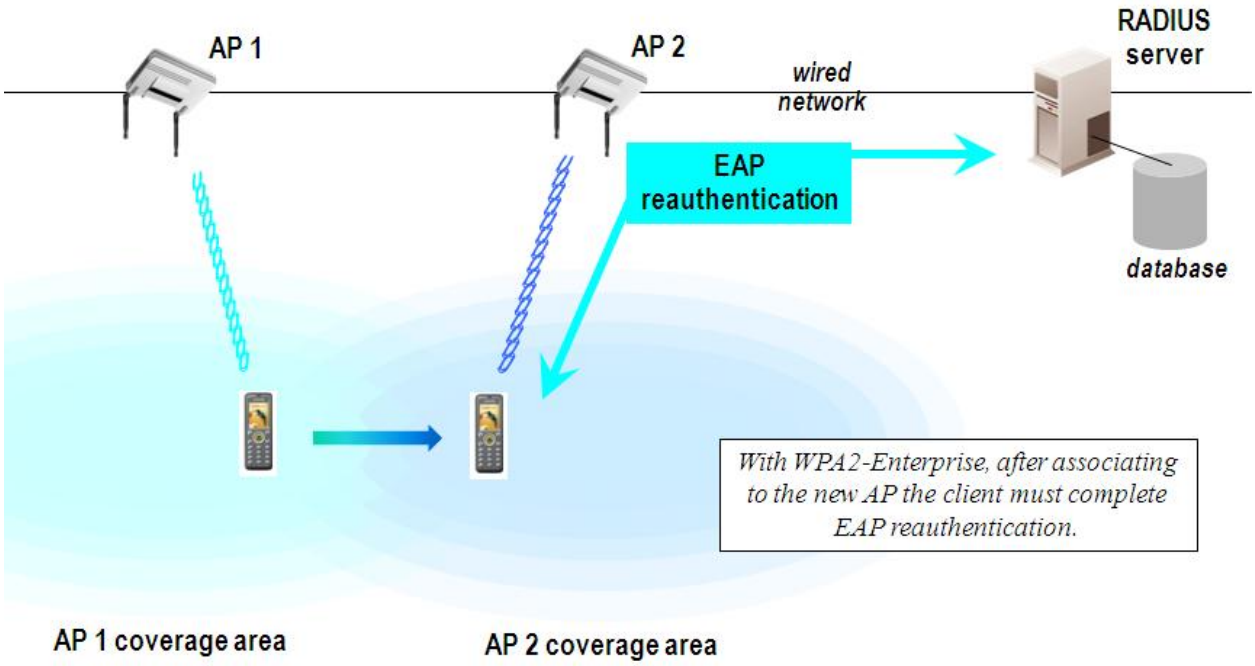
Once it creates a list of APs that are within range, a client radio must determine which AP is likely to offer the most reliable connection. Making this determination can be difficult, because the only relevant information that a client can glean from a typical AP's probe response is RSSI. Some APs supply additional information, such as the number of clients associated to the AP, but that information is in a proprietary format that the client must recognize and decipher.

4. Roam to the "Best" AP

A client radio cannot be associated, or connected, to two APs at the same time. Once it decides that it will roam to a new AP, the client must disassociate from its current AP and associate to the new AP.

When associating to the new AP, the client must reauthenticate to the network of which the AP is a part. When the Enterprise version of Wi-Fi Protected Access® (WPA®) or WPA2® is used for Wi-Fi security, reauthentication is 802.1X reauthentication using an Extensible Authentication Protocol (EAP) type that may involve communication with an authentication server on the network. The reauthentication process can be lengthened by congestion or distance on the network between the AP and the authentication server.

If the client is unable to associate to the new AP and reauthenticate to the network, then the client will attempt to return to the AP to which it was associated previously.



Standard EAP reauthentication requires interaction with an authentication server on the wired network.

Once the client completes the roam, the two APs must interact to ensure that the infrastructure is aware that the client has moved from one AP to another. APs communicate using an inter-AP protocol that:

- Is supported by APs designed for use in multi-AP settings such as businesses but may not be supported by consumer-grade APs that are used primarily in single-AP settings such as homes

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

- Varies by AP vendor, which means that APs from one vendor may not communicate with APs from another vendor

Optimizing Roaming

A persistent network connection minimizes disruptions to the client's ability to send data to the network and receive data from the network. When applications that require a persistent connection operate on a mobile device, that device must minimize connectivity disruptions, even when the device is in motion.

Two activities in the roaming process – active scanning and the actual roam – are disruptive to network connectivity:

- Active scanning: When a client radio is performing an active scan, it cannot send data to or receive data from the AP to which it is associated. The longer active scanning takes, the greater the potential for disruption to an application that is sending and receiving data.
- Roaming: When a client initiates a roam by disassociating from the current AP, that client cannot send or receive data until it successfully associates to a new AP and reauthenticates to the network. The longer it takes a client to associate to a new AP and complete the reauthentication process, the greater the potential for disruption to an application that is sending and receiving data.

Mobile computers require fast and reliable roaming but tend to operate in environments that present challenges to such roaming. To succeed on mobile computers, a Wi-Fi radio must support ways to optimize active scanning and roaming. This section provides some techniques for optimizing these critical activities.

Active Scanning

Active scanning typically is triggered when the RSSI value for the current AP drops below a threshold. When that threshold can be configured by a network administrator, that administrator can tune active scanning for a particular environment. In some situations, an administrator wants clients to be "sticky", or to have a tendency to stay with the current AP and roam only when absolutely necessary. While every situation is different, here are some general guidelines on when to make client radios more or less sticky:

Factor	More "Sticky"	Less "Sticky"
Number of APs for size of facility	Few	More
Mobility of client devices	Low	High
Amount of data transferred	Small	Large
Application's need for persistence	High	Low

Here are some ways to control how often a client performs an active scan and attempts to roam:

- Threshold: The higher the absolute value of the RSSI threshold, the weaker the current AP's RSSI value must be before the client does an active scan.
- Delta: The greater the RSSI advantage of a candidate AP over the current AP, the less often the radio attempts to roam to that candidate AP.
- Period: The greater the period of time that must elapse between one active scan and the next, the less often the radio performs active scans.

When a client is scanning, it cannot send or receive data. Scanning all 2.4 GHz channels typically takes a client several hundred milliseconds. In a typical Wi-Fi deployment, however, APs operate

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

on only three channels. To reduce the disruption of scanning, Wi-Fi radio software should support a way to scan only those channels on which APs operate. Two methods of reducing the number of channels scanned are:

1. On the client, configure a limited channel set to scan.
2. Leverage a Cisco Compatible Extensions (CCX) facility called the AP neighbor list. With this facility, the Cisco AP to which a client is associated provides that client with a list of channels of nearby APs, enabling the client to scan only those channels.

In certain situations, it is necessary to override the configured or standard approach to roaming. For example, when a client suddenly begins to miss an inordinately high percentage of beacons from the current AP, the client is at risk of losing its connection. To prevent a loss of connection, the client should temporarily employ a more aggressive scheme for scanning and roaming, where scans are performed frequently across all channels and the delta is a fairly low value. As soon as the client roams, it then can return to its standard approach to scanning and roaming.

Fast EAP Reauthentications

Once a client selects the AP to which it will roam, it must disassociate from its current AP, associate to the target AP, and reauthenticate to the network on which the APs reside. The process of disassociating from one AP and reassociating to another AP takes only a few milliseconds. The process of reauthenticating to the network, however, can take hundreds of milliseconds when EAP authentication is used, as it is with WPA-Enterprise and WPA2-Enterprise. That is because standard EAP authentication includes several interactions between the client and an authentication server on the network, where the AP acts as the intermediary between the client and server.

If there is network congestion, or if the authentication server is on a network that is remote from the AP, then reauthentication may be slowed to the point where it causes problems for applications that require a persistent connection. There are three methods for accelerating EAP reauthentications:

1. Cisco Centralized Key Management, or CCKM, which is supported by Wi-Fi infrastructure products from Cisco and by clients that are certified for CCX
2. Opportunistic Pairwise Master Key (OPMK) caching, which is supported with WPA2, but not with WPA, by some controller-based Wi-Fi infrastructures and by some clients
3. IEEE 802.11r pre-authentication, which may not be widely supported until 2011

CCKM, which is supported with WPA and WPA2, relies on a Cisco Wireless Domain Services (WDS) infrastructure device, typically an AP or a controller. The WDS device acts as a local resource to a set of APs. When a CCKM client associates to an AP for the first time and completes its initial EAP authentication, the AP caches some authentication information on the WDS device. When the CCKM client roams to another AP served by the same WDS device, then EAP reauthentication uses the cached information, and there is no need for communication with the authentication server. The entire reauthentication process is reduced from hundreds of milliseconds to a few dozen milliseconds.

WPA2 defines two alternatives to CCKM: PMK caching and OPMK caching. Both are supported by infrastructures from a variety of vendors. As with CCKM, the goal of PMK caching and OPMK caching is to speed up roaming between APs by accomplishing EAP reauthentications without communicating with the authentication server.

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

When a client does an initial EAP authentication to the WLAN infrastructure, both the client and the infrastructure derive the information needed for reauthentications. If there are no controllers in the infrastructure, then standard PMK caching is used and reauthentication information is cached only on the initial AP. When the client tries to reauthenticate to that AP, the client and the AP use the cached information to do the four-way handshake to exchange keys. If there are controllers, then OPMK caching is used and reauthentication information is cached on the controllers. When the client tries to reauthenticate, the client and the controller behind the AP use the cached information to do the four-way handshake to exchange keys.

Other Roaming Topics

Infrastructure-Directed Roaming

While some client devices support fast and effective Wi-Fi roaming, many do not. That is because the Wi-Fi software on many devices is designed for consumer devices that function as stationary or nomadic computing devices. Accommodating clients with widely varying roaming capabilities can be a challenge for a network administrator.

Recognizing that administrators need help with managing a broad range of clients, some vendors of Wi-Fi infrastructure promote capabilities that they term infrastructure-assisted roaming or infrastructure-directed roaming. Infrastructure products with these capabilities play a proactive role in roaming by performing tasks such as:

- Sending each client a list of nearby APs and a recommendation on which AP the client should select when that client roams
- Preventing a client from roaming to a particular AP that has reached a load threshold
- Severing a client's connection to its current AP, thereby forcing the client to roam

Reasons that a Wi-Fi infrastructure may force a client to roam away from its current AP include:

- The infrastructure perceives that another AP in the client's vicinity offers that client a better connection than the client's current AP.
- The infrastructure wants to balance the load across APs, and the client's current AP is handling many clients while a nearby AP has few or no clients associated to it.

Infrastructure providers argue that infrastructure-directed roaming is a smart approach because the infrastructure can monitor the entire RF environment on a regular basis, whereas a client captures irregular snapshots of only a small part of that environment. In addition, the infrastructure has insight into the status of every AP, including the client load on that AP and all of its neighbors. Some infrastructure providers claim that infrastructure-directed roaming results in an improved experience for all clients.

When clients run applications that require a persistent connection, however, infrastructure-directed roaming can be disruptive. When the infrastructure forces a client to roam from AP 1 to AP 2, the infrastructure must disassociate the client from AP 1 and reject any attempt by the client to associate to an AP other than AP 2. Potential issues with this approach include:

- The client chose AP 1 because the client determined that AP 1 was the best AP for that client, probably because AP 1 offered the client the most reliable connection.
- By disassociating a client from AP 1, the infrastructure forces that client to initiate a roam unexpectedly and puts at risk the client's ability to maintain a persistent network connection.

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

- If AP 3 is more attractive to the client than AP 2 is, then the client will make at least one attempt to associate to AP 3. By the time the infrastructure rejects that attempt and the client decides to associate to AP 2, applications that require a persistent connection are likely to fail.
- When a client is moving quickly, it may move out of range of AP 2 before it is able to associate to AP 2.

When a client is responsible for initiating and directing its own roaming, that client can take the actions necessary to ensure that it maintains a reliable connection with the network.

Single-Channel Infrastructures

As discussed earlier, most Wi-Fi deployments use a micro-cellular architecture. Each AP offers a cell of coverage on a particular frequency channel, and APs with adjacent or overlapping cells operate on different channels. When a client roams from one AP to another, the client typically changes its channel.

In the past few years, a few Wi-Fi infrastructure vendors have introduced products that use an alternative to the standard micro-cellular architecture. In the alternative architecture, every AP is on the same channel and a controller behind the APs manages all AP cells as a single virtual cell. Vendors that offer this single-channel architecture claim that a client sees the entire network as a single AP and never has to roam between APs. The controller reportedly handles all client connectivity decisions and ensures that each client is connected to the right AP.

Because single-channel infrastructures are relatively new, it is unclear how well various clients interoperate with these infrastructures. Typically, a client's roaming algorithm assumes that the channels of neighboring APs are different than that of the current AP. When a client decides that its current connection is becoming tenuous and decides to roam, the client may become confused when all APs within range are on the same channel.

Another potential issue involves broadcast network identifiers, or BSSIDs. Some single-channel infrastructures support a single BSSID across all APs. At least one single-channel infrastructure, however, replaces BSSIDs with a unique beacon for each client. Because per-client unicast beacons are outside the 802.11 specification, some clients may not know how to interpret and respond to these beacons, leading to unanticipated interoperability issues.

Multi-channel Wi-Fi systems have been predominant for 15 years, since before the first Wi-Fi standards were finalized. Micro-cellular architectures were introduced in the mid-1990s to avoid two sets of issues with single-channel architectures: co-channel interference and insufficient capacity. Today, Wi-Fi infrastructure and client products designed for enterprise use support IEEE standards such as 802.11e and other facilities that optimize operation in a multi-channel environment.

Before choosing an infrastructure where all APs are on the same channel, it is prudent to conduct "real world" tests with that infrastructure, including tests with a large number of business-critical mobile devices operating simultaneously.

Roaming between Frequency Bands

802.11b and 802.11g operate in the 2.4 GHz frequency band. 802.11a operates in the 5 GHz band. When a Wi-Fi client radio supports both 802.11b/g and 802.11a, it usually does it by using a common media access controller (MAC) with two different physical interfaces, one for 802.11b/g

SUMMIT DATA COMMUNICATIONS
A Summit Data Communications White Paper
Originally Published: November 2009

and the other for 802.11a. Because there are not two full radios in the design, the radio cannot operate on both bands at the same time. The radio, however, may be able to roam between bands.

Active scanning on two bands can take a long time. The 5 GHz band includes eight non-overlapping channels in the UNII-1 and UNII-3 bands plus additional channels in the intermediate bands. Scanning all 2.4 GHz channels and all 5 GHz channels may take several seconds, and while it is scanning a radio cannot send and receive data.

To limit the amount of time required for scans, a dual-band radio should scan both bands only when absolutely necessary. The radio also should enable an administrator to specify which band has preference for selecting a target AP. Wi-Fi infrastructure from one leading vendor includes a facility that encourages clients to connect in the 5 GHz band, because that band usually is less "crowded" than the 2.4 GHz band.

Losing Connectivity

When a client moves completely out of the coverage area for all APs, it loses its network connection. All applications that are dependent on a network connection fail.

Once it recognizes that it is not associated to an AP, the client radio begins the process of establishing a Wi-Fi network connection, just as it does when it is initialized. The connection process involves scanning for available APs, selecting one, associating to it, and authenticating to the network behind it.

How aggressively should the client attempt to establish a connection? If it was taken outside all Wi-Fi coverage areas inadvertently, then the client should be aggressive in re-establishing a connection. If it is taken outside all Wi-Fi coverage areas on purpose, however, then a client should minimize its active scanning so that it does not consume battery life unnecessarily. Wi-Fi radio software should enable an administrator to control how aggressively a client attempts to connect to a network.

Meeting the Mobility Challenge

A business-critical mobile device is used while in motion and must maintain a persistent network connection while its Wi-Fi radio is roaming between APs. The decision to roam and the execution of the roam are handled by the software for that Wi-Fi radio.

Silicon providers, which make the chips in Wi-Fi radios, also provide reference-design software for those radios. That software provides sufficient functionality for the highest-volume devices, which are consumer-grade devices that function as stationary or nomadic computing devices. As a result, reference-design software does not support fast and reliable roaming and is insufficient for business-critical mobile devices.

Wi-Fi solutions from Summit Data Communications provide the industrial-strength mobility required by mobile computers and other business-critical mobile devices. The secure and reliable mobility of Summit solutions has been proven on hundreds of thousands of devices, many of which operate in the most challenging environments on the planet.

DATALOGIC™

DATALOGIC MOBILE

Wi-Fi: The Importance of Mobility

A Summit Data Communications White Paper
Originally Published: November 2009

Summit Data Communications is the ***mobile*** in today's mobile computers and other business-critical mobile devices. Summit's embedded Wi-Fi solutions provide secure, reliable connections in the challenging environments in which business-critical mobile devices operate, including factories, warehouses, ports, hospitals, and retail stores.