Labortestbericht
DR100409C

Cisco CleanAir Vergleichstest

April 2010

Miercom
www.miercom.com

Inhalt

Zusammenfassung

Unsere unabhängige Untersuchung hat ergeben, dass die Cisco CleanAir-Technologie eine umfassende und zweckmäßige Lösung für die Behebung von Interferenzproblemen in Wireless-Netzwerken darstellt, die auf andere Störquellen als auf Wi-Fi-Geräte zurückzuführen sind.

Übliche Nicht-Wi-Fi-Geräte, die im gleichen Funkfrequenzbereich wie Wireless-Netzwerke betrieben werden, können zu einer deutlichen Minderung der Verbindungsqualität, hoher Latenz und in einigen Fallen zu einer vollständigen Unterbrechung des Wireless-Netzwerks führen. Dies liegt an der Funktionsweise von 802.11 als „Polite-Protokoll“, das einen „Listen-before-Talk“-Algorithmus verwendet. Diese Funktionsweise kann dazu führen, dass ein Kanal vollständig von einem Interferenzsignal gestört wird, sodass es zur Trennung von Clients kommt. Die Möglichkeit, derartige Interferenzen zu erkennen und zu vermeiden, ist für Netzwerkadministratoren von großer Wichtigkeit.

Die Cisco CleanAir-Technologie verwendet einen angepassten Funk-ASIC (Application Specific Integrated Circuit, anwendungsspezifischen Schaltkreis) im Access Point, um erstklassige Tools für die Frequenzanalyse und die Störungsbeseitigung bereitzustellen, die in herkömmlichen Wi-Fi-Chipsets nicht verfügbar sind. Mit diesen Tools wird die Abtastauflösung verfeinert, schlechte Kanalbedingungen vermieden und die Netzqualität verbessert.

Uns hat die Geschwindigkeit und Genauigkeit überzeugt, mit der die unterschiedlichen Ursachen von Interferenzen erkannt werden, die nicht auf Wi-Fi-Geräte zurückzuführen sind. Besonders beindruckend ist dabei der Umfang an nützlichen Informationen, die zur Vermeidung von Interferenzen bereitgestellt werden. Mit Cisco CleanAir wird jede Störungsquelle eindeutig identifiziert, der Schweregrad der Interferenz und die Funkqualität angezeigt, der Gerätetyp richtig klassifiziert sowie der physische Standort der Störungsquelle auf einer Karte dargestellt. Die Fähigkeit der Technologie, mehrere Störungsquellen gleichzeitig zu erkennen und zu lokalisieren, war beeindruckend.

Mit seiner „Selbstheilungsfähigkeit“ konnte CleanAir zudem einen einzigartigen Vorteil gegenüber den Konkurrenzlösungen demonstrieren: So wechselte es in weniger als einer Minute auf einen sauberen Kanal und vermied somit Interferenzen durch Quellen, die sich bis zu 30 Meter entfernt befanden. Ein weiterer starker Aspekt war darüber hinaus die Erkennung unberechtigter Access Points, die auf Nebenfrequenzen senden und so eine Gefahr für das Netzwerk darstellen könnten.

Anbieter anderer Produkte haben nicht aktiv an den in diesem Bericht beschriebenen Tests teilgenommen. Es erhalten jedoch alle Anbieter die Gelegenheit, ihre Produkte in unseren Labors testen zu lassen, wenn sie mit den von uns präsentierten Ergebnissen nicht einverstanden sind.

Miercom freut sich, die Cisco CleanAir-Technologie für die unter Beweis gestellte Leistungsfähigkeit und die Integration von Funktionen zur Minderung von Interferenzen mit der „Performance Verified Certification“ auszeichnen zu können.

Rob Smithers
CEO
Miercom

Wichtigste Ergebnisse

- Interferenzen, die auf andere Ursachen als auf Wi-Fi-Geräte zurückzuführen sind, können den Durchsatz zwischen Access Points und Clients auf 2,4-GHz- und 5-GHz-Frequenzbändern beeinträchtigen.
- Mit der Cisco CleanAir-Technologie können die Standorte von Störquellen erkannt, klassifiziert und auf einer Karte dargestellt werden, was eine schnelle Problemlösung ermöglicht.
- Ein spezieller CleanAir-ASIC im Cisco Aironet Access Point der Serie 3500 bietet Abtast- und Erkennungsressourcen, die mit anderen Wi-Fi-Chipsets nicht verfügbar sind.
- Mit Cisco CleanAir können unberechtigte Geräte erkannt werden, die unübliche Funkfrequenzen benutzen, womit Backdoor-Angriffe vermieden werden können.
- Schnelle Selbstheilungsfähigkeiten durch die Vermeidung von Interferenzen ermöglichen ein verbessertes Endbenutzererlebnis sowie eine schnelle Wiederherstellung bei Kanalstörungen.
- Eine Vergleichsanalyse des Motorola Produkts AirDefense ergab eine Zuverlässigkeit in weniger als 25 % der Testfälle. (Irrtümliche Identifizierung 15 %, unregelmäßige Erkennung 23 %, fehlende oder unvollständige Klassifizierung 38 %).

Überblick

Miercom hat die Cisco CleanAir-Technologie auf Störungsklassifizierung, -beseitigung und -vermeidung überprüft und diese den Produkten anderer Anbieter gegenüber gestellt. Die Leistung der neuesten Wireless-Controller und Access Points von Cisco, Aruba, Motorola, Trapeze, HP und Meru wurden in Bezug auf diese Aspekte verglichen.

Wir haben die Auswirkung von Interferenzen durch zahlreiche Nicht-Wi-Fi-Geräte auf den Durchsatz getestet, darunter kontinuierliche Wellensignale von Videoüberwachungskameras, zwischen 2,4 GHz und 5 GHz wechselnden Telefonen und Bluetooth-Geräten sowie zyklische Störungen von Mikrowellenherden. Getestet wurde die Fähigkeit, alle Interferenztypen von einzelnen Quellen zu erkennen und zu klassifizieren sowie die Fähigkeit, mehrere Störungsquellen zuverlässig zu klassifizieren. Wir haben auch die Selbstheilungseigenschaften untersucht, d. h. die Fähigkeiten, größere Störungsquellen zu erkennen und zu einem anderen Kanal zu wechseln, um diese zu vermeiden. Es wurde auch die Fähigkeit untersucht, unberechtigte Access Points zu erkennen, die nicht standardmäßige Frequenzen verwenden und sich zwischen Standard-Wi-Fi-Kanälen verbergen, womit sie sich „quasi durch die Hintertür“ Zugriff auf das drahtgestützte Netzwerk verschaffen könnten.

Mit der Cisco CleanAir-Technologie konnten Störungsquellen erkannt und identifiziert sowie deren Standort auf einer Karte dargestellt werden, sodass entprechende Abhilfemaßnahmen ergriffen werden konnten.

Verwendete WLAN-Geräte:

Cisco Wireless LAN Controller 5508 (7.0.93.110)
- Cisco Access Point der Serie 3500, 802.11n

Cisco Wireless Control System (7.0.130)

Cisco Mobiltiy Services Engine 3350 (7.0.99)

Aruba 6000 Controller mit (3.4.2.2)
- Aruba Access Point AP125, 802.11n
- Aruba Access Point AP105, 802.11n

HP Controller MSM760 mit Software (5.3.3)
- HP Access Point MSM422, 802.11n

Motorola RFS7000 Controller mit Software (4.2.1)

Motorola Access Point AP-7131N, 802.11n mit neuester Software (4.0.3)

Motorola AirDefense 1250 Services Console mit neuster Software (8.0.0.15)

Motorola AirDefense M520 Sensor mit neuester Firmware (5.2.0.11)

Trapeze Controller MX-200R (7.0.13.3)
- Trapeze Access Point MP-432, 802.11n

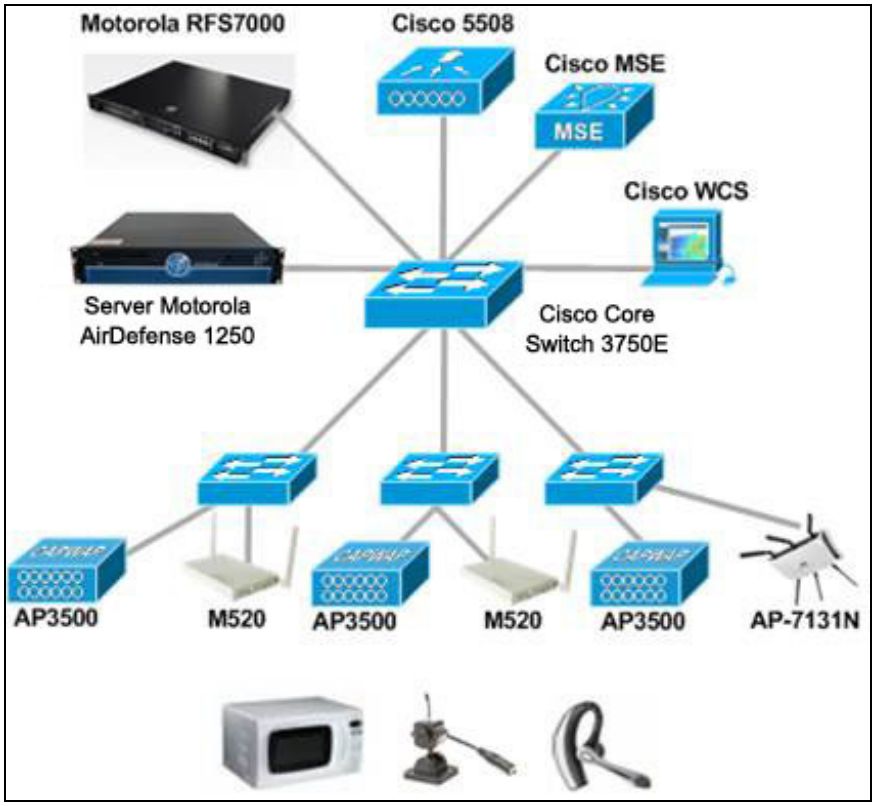
Meru Controller MC4100 mit Software (3.6.1)
- Meru Access Point AP320, 802.11n

802.11n-Clients (Intel 5300AGN - Treiber 13.1.1.1)

Störquellen:

Mikrowellenherd
Schnurloses Plantronics Bluetooth-Headset
Schnurloses DECT-Telefon 2,4 GHz
Schnurloses DECT-Telefon 5,8 GHz
Q-See drahtlose Videoüberwachungskamera 2,4 GHz
Drahtlose Videoüberwachungskamera 5,8 GHz (Modell: W5803W1)

Diagramm der Testumgebung



So haben wir getestet

Klassifizierungstest:

Für Cisco wurde eine Umgebung aus drei Aironet Access Points der Serie 3500, dem Wireless Controller 5508, dem Cisco Wireless Control System (WCS) und der Cisco Mobility Services Engine (MSE) verwendet. Für Motorola wurden zwei Sensoren M520, ein Access Point AP7131N, ein Server Motorola AirDefense 1250 und ein Motorola RFS7000 WLAN-Controller verwendet. Der Sensorstandort war für beide Anbieter der gleiche. Zwei Sensoren wurden in einem Abstand von ca. 15 m platziert, wobei sich die Störungsquelle im gleichen Abstand zwischen diesen befand. Der dritte Sensor wurde in einem Abstand von ca. 21 m platziert. Als Störungsquelle wurde ein herkömmlicher Mikrowellenherd verwendet, der während des Tests auf 2 Minuten und hohe Leistung eingestellt wurde. Außerdem wurden schnurlose Telefongeräte mit Handgeräten und Basisstation (2,4 GHz und 5 GHz), Videoüberwachungskameras (2,4 GHz und 5 GHz), ein Bluetooth-Headset mit Ladestation sowie ein Funkstörsender eingesetzt.

Selbstheilungstest:

Fünf Clients wurden in einer Entfernung von ca. 3 bis 10 m vom Access Point aus platziert. Jeder Client empfing einen geschleiften Videostream mit niedriger Bandbreite. Da die Anwendung zur Videowiedergabe den Stream pufferte, wurde ein Befehlszeilenfenster verwendet, das regelmäßige Ping-Anfragen an den Access Point sendete, um den Moment zu ermitteln, in dem die Kommunikation unterbrochen wurde. Die Zeitmessung erfolgte mit einer Stoppuhr. Es wurden drei Positionen für die Störquellen festgelegt: Position A befand sich im Abstand von ca. 3 m vom Access Point, Position B ca. 15 m und Position C ca. 30 m. Wir erwarteten, dass jeder Client in Abhängigkeit von seinem Abstand zur Störquelle und der Nähe der Störquelle zum Access Point in unterschiedlichem Umfang beeinträchtigt würde. An Position C erwarteten wir, dass der Client mit dem Abstand von ca. 30 m vom Access Point und dem geringsten Abstand zur Störquelle ausfallen, die anderen jedoch ihre Kommunikation unbeeinträchtigt fortsetzen würden. Als Störquelle wurde die 2,4-GHz-Videoüberwachungskamera verwendet, da diese die stärkste negative Auswirkung aufwies. Der erste getestete Zugriffspunkt war der Cisco Access Point der Serie 3500.

Testergebnisse

Auswirkung der Interferenz

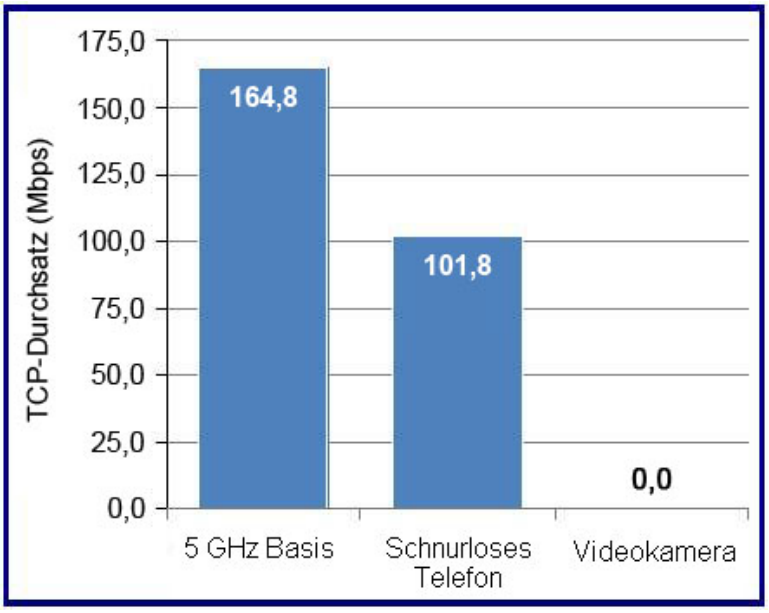
Es wurde getestet, welche Leistungsauswirkung unterschiedliche Arten von Signalen hatten, die nicht von Wi-Fi-Geräten stammten. Der Client war ein 802.11n-konformer Laptop, und ein Cisco 3500 fungierte als Access Point. Der Basisdurchsatz wurde im ungestörten Spektrum auf einem 40-MHz-Kanal im 5-GHz-Band gemessen. Es wurden einzelne Störsignale aktiviert und der Durchsatz gemessen. Es wurden mehrere Durchgänge ausgeführt, um einen Durchschnitt zu erhalten. Der Basisdurchsatz im ungestörten Spektrum betrug 164,8 Mbps.

Als eine drahtlose 5-GHz-Videoüberwachungskamera eingeschaltet wurde, wurde Kanal 153 mit kontinuierlichen Welleninterferenzen gestört, und die Netzverbindung des Client wurde unterbrochen. Während des Kamerabetriebs lag der Netzwerkdurchsatz bei 0 %.

Es wurde 5 GHz DECT verwendet, um die Signalauswirkung von Frequenzsprüngen zu erfassen. Es wurden drei Telefone verwendet. Zwei wurden in einer Konferenzschaltung verbunden, eines diente als an das Festnetz angeschlossene Basisstation. Bei Verwendung von drei Telefonen sank der Netzwerkdurchsatz auf 102 Mbps, und der Access Point maß eine Funkqualität von 86 % von möglichen 100 % für 5 GHz DECT.

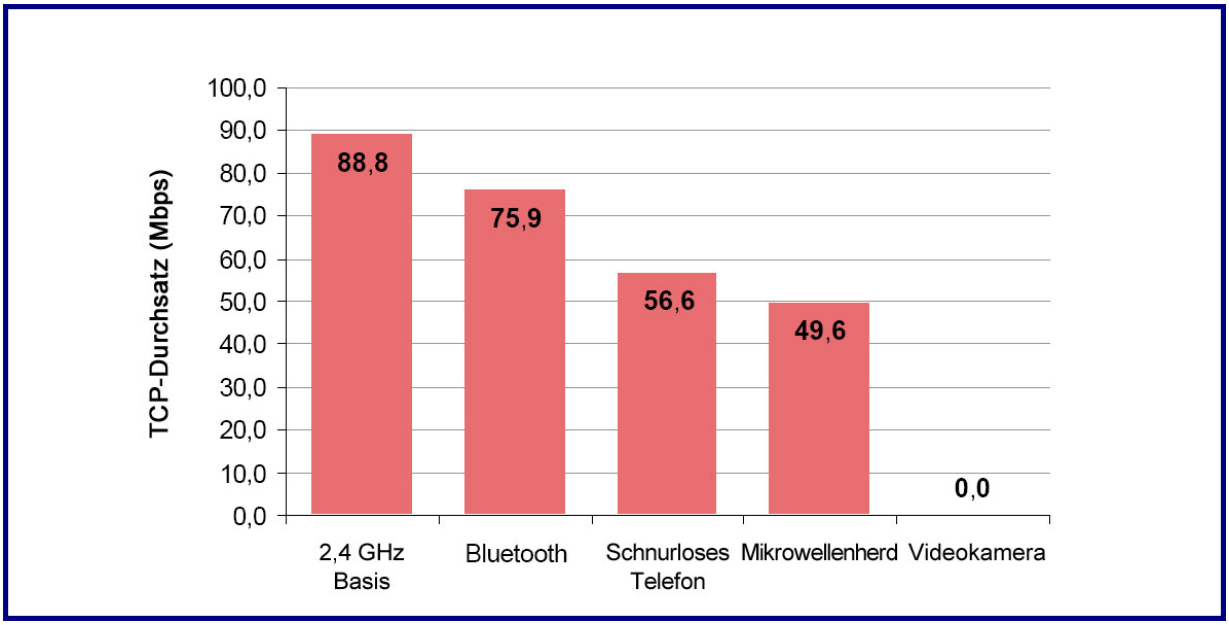
Die 5.0-GHz-Basiswerte finden Sie in *Abbildung 1*.

Abbildung 1: 5,0-GHz-Basismessungen mit Auswirkung der Interferenz auf den Durchsatz



Vergleich der Basismessungen mit Messungen bei Betrieb von schnurlosen Telefonen und Videokamera

Abbildung 2: 2,4-GHz-Basismessungen mit Auswirkung der Interferenz auf den Durchsatz



Vergleich der Basismessung mit den Interferenzen durch Bluetooth, schnurlose Telefone, Mikrowelle und Videokamera. Jede Nicht-Wi-Fi-Störquelle hat unterschiedliche Auswirkungen. Diese wurden daher einzeln getestet und mit der Basismessung verglichen.

Im Anschluss wurde die Interferenz im 2,4-GHz-Band getestet. Dieses Band umfasst die Kanäle 1, 6 und 11. Der Basisdurchsatz im ungestörten Spektrum betrug 88,849 Mbps. Wenn ein Bluetooth-Headset aktiv war und Sprache übertrug, fiel der Durchsatz auf 76 Mbps. Bluetooth führt zudem zu einer Interferenz durch Frequenzsprünge.

Es wurden schnurlose 2,4-GHz-Telefone verwendet, um die Signalauswirkung von Frequenzsprüngen zu erfassen. Es wurden drei Telefone verwendet. Zwei wurden in einer Konferenzschaltung verbunden, eines diente als an das Festnetz angeschlossene Basisstation. Bei Verwendung von drei Telefonen fiel der Netzwerkdurchsatz auf 57 Mbps.

Mikrowellenherde erzeugen zyklische Interferenzen, die sich auf Kanäle im oberen Bereich des 2,4-GHz-Bands auswirken, beispielsweise die Kanäle 6 bis 11, in Abhängigkeit vom Modell. Wenn der Herd für 2 Minuten mit hoher Leistung betrieben wurde, sank der Durchsatz auf 50 Mbps. Die 2,4-GHz-Basiswerte finden Sie in *Abbildung 2*.

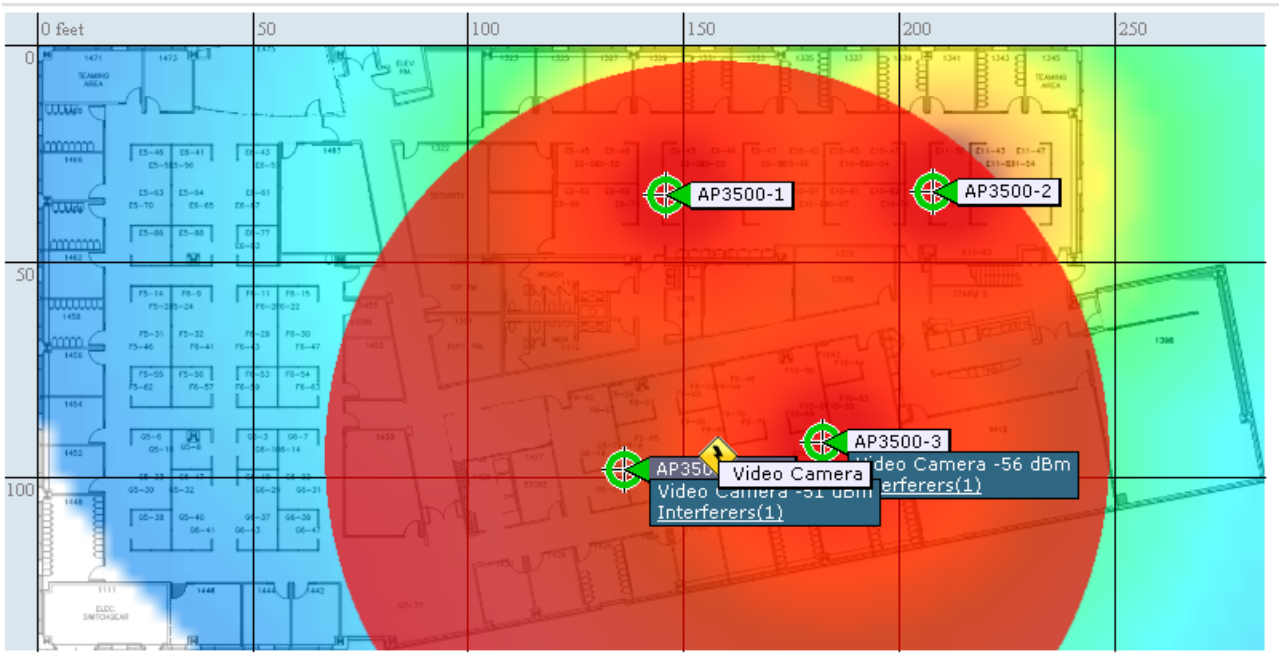
Wenn eine drahtlose Videoüberwachungskamera im 2,4-GHz-Band eingeschaltet wurde, sank der Durchsatz auf 0 Mbps.

Störungsklassifizierung

Es ist nicht nur wichtig, die Auswirkungen anderer Signaleinrichtungen auf ein Netzwerk zu kennen, es muss auch der Standort und die Quelle ermittelt werden, um das Problem beheben zu können. Wir haben die Cisco CleanAir-Technologie mit dem Aironet Access Point der Serie 3500 und die Motorola AirDefense-Lösung mit dem Access Point AP-7131N und dem Sensor M520 getestet. Beide Lösungen sind in der Lage, Störungsquellen zu klassifizieren, während die getesteten Lösungen anderer Anbieter keine Funktionen zur Störungsklassifizierung enthielten.

Der Cisco Aironet Access Point der Serie 3500 verfügt über einen integrierten Spektrumanalysator eines neuen CleanAir-ASIC im Access Point, der eine Netzwerküberwachung in Echtzeit sowie die Bereitstellung von WLAN-Diensten für die Clients ermöglicht. Auch mit dem Motorola AP-7131N kann das Frequenzband bzw. oder Spektrum analysiert werden. Der Motorola Access Point kann entweder WLAN-Services bereitstellen oder das Spektrum überwachen, jedoch nicht beides gleichzeitig. Die Deaktivierung eines Access Point für die Ausführung der Störungsüberwachung kann zu einer höheren Auslastung anderer Access Points führen, wodurch die Netzwerkleistung abnimmt. Da es sich um ein herkömmliches Wi-Fi-Chipset handelt, ist der Detailgrad der Analyse begrenzt. Wir haben für Cisco CleanAir eine Abtastauflösung von 78 KHz und für die Motorola Lösung eine Abtastauflösung von 5 MHz ermittelt. Dies ist im Vergleich zu Motorola eine 64 mal bessere Abtastauflösung.

Über die WCS-Benutzeroberfläche ist es mit Cisco CleanAir zudem möglich, die physische Position eines Interferenzsignals auf einer Karte darzustellen.



Dies ist ein Screenshot von Cisco WCS, der den physischen Standort einer Videokamera als Störquelle anzeigt. Der rote Kreis um das Gerät kennzeichnet die Wirkungszone der Störquelle.

Wir testeten einzelne und mehrere Störquellen im 2,4-GHz-Band sowie einzelne Störquellen im 5-GHz-Band.

Screenshot des Cisco Systems

Worst 802.11b/g/n Interferers *

Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle (%)	Discovered	Last Updated	Floor
a8:09:7e:00:00:1b	Video Camera	Active	97	1..5	100	Tue Mar 30 13:49:44 PDT 2010	Tue Mar 30 13:51:35 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:20	Microwave Oven	Active	27	6..11	17	Tue Mar 30 13:51:22 PDT 2010	Tue Mar 30 13:52:13 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1d	DECT Like Phone	Active	4	4..11	8	Tue Mar 30 13:50:15 PDT 2010	Tue Mar 30 13:51:21 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1e	Bluetooth Link	Active	3	3..11	6	Tue Mar 30 13:50:16 PDT 2010	Tue Mar 30 13:51:01 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1c	DECT Like Phone	Active	2	2..11	2	Tue Mar 30 13:50:06 PDT 2010	Tue Mar 30 13:51:15 PDT 2010	System Campus > MR-1 > MR1-Floor1

Diese Abbildung zeigt die erfolgreiche Klassifizierung mehrerer gleichzeitiger Störquellen.

Zunächst verwendeten wir eine einzelne 2,4-GHz-Videoüberwachungskamera als Störquelle. Das Motorola System löste einen Alarm für eine „kontinuierliche Welle“ aus, konnte das Gerät jedoch nicht identifizieren. Das Cisco WCS identifizierte das Gerät als Videokamera, lokalisierte es und gab einen Störungsschweregrad von 98 an. Auf der Benutzeroberfläche des Cisco Wireless Controller wurde außerdem die Ausnutzung des Wi-Fi-Kanals angezeigt, und die Funkqualität wurde als schlecht bewertet.

Im Mikrowellenherd-Test gab das Motorola System zwei Alarme aus, einen am Access Point und einen am Sensor. Die Quelle wurde richtig identifiziert. Der Access Point erkannte die Störung bei 2437 MHz und der Sensor bei 2462 MHz. Das Motorola System stellt keine Korrelation her, daher wurde das gleiche Gerät im AirDefense-System mit zwei Alarmen angezeigt.

Das Cisco System erkannte die Interferenz an drei Access Points als Mikrowellenherd und meldete ein einziges Ereignis. Es wurde erkannt, welche Kanäle betroffen waren, und der Herd wurde lokalisiert. Nach aufgetretener Interferenz bleiben diese Informationen weiterhin verfügbar, sodass bei periodischen Interferenzen entsprechende Abhilfemaßnahmen ergriffen werden können.

Eine Basisstation eines schnurlosen DECT-Telefons wurde der Umgebung hinzugefügt. Die Basisstation verursacht Interferenzen, wenn sie versucht, mit den Handgeräten zu kommunizieren. Dies geschieht jedoch in einem geringeren Arbeitszyklus als bei einem aktiven Anruf. Motorola zeigte die Interferenz auf der Benutzeroberfläche an, konnte die Quelle jedoch nicht identifizieren. Der geringe Arbeitszyklus reichte für die Identifizierung nicht aus. Das Cisco System klassifizierte die Quelle als DECT-ähnliches Telefon und stellte den physischen Standort fest.

Der Arbeitszyklus wurde erhöht, indem der Basisstation ein aktives Handgerät hinzugefügt wurde. Jetzt erkannte Motorola die Interferenz am Access Point sowie an zwei Sensoren und klassifizierte die Quelle als Frequenzsprunggerät. Die Erkennung war unregelmäßig. Das Cisco System erkannte und klassifizierte das Telefon und die Basisstation als „DECT Like Phone“ (DECT-ähnliches Telefon) und stellte wiederum den physischen Standort fest.

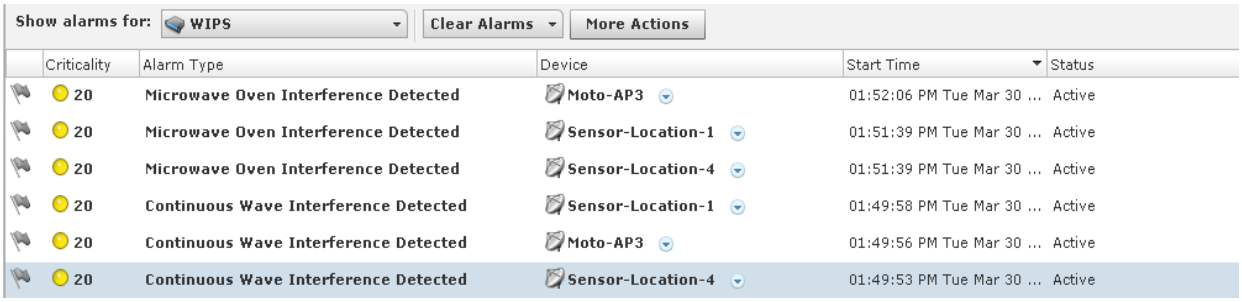
Es wurden zwei weitere aktive Handgeräte hinzugefügt. Das Motorola System klassifizierte die Störungsquelle als Frequenzsprunggerät. Die Erkennung blieb unregelmäßig. Wir testeten die Motorola Lösung sowohl im „Full Scan“-Modus (vollständiger Abtastmodus) als auch im „Interference Scan“-Modus (Interferenz-Abtastmodus). Die Erkennung war in beiden Modi unregelmäßig. Im „Interference Scan“-Modus erkannte der Access Point, der sich am nächsten an der Störquelle befand, nichts, und die beiden Sensoren klassifizierten die Störungsquelle falsch als Bluetooth.

Das Cisco System klassifizierte alle Telefone richtig und ordnete den physischen Standort in Bezug auf die Access Points richtig zu.

Bluetooth besitzt im Erkennungsmodus einen niedrigen Arbeitszyklus mit 1 % Interferenz. Ein Bluetooth-Headset wurde der Testumgebung hinzugefügt, um zu ermitteln, ob dieses von einem der beiden Systeme ermittelt würde. Weder das System von Cisco noch das von Motorola war in der Lage, das Gerät zu erkennen, da die Bluetooth-Erkennung nur während einer sehr kurzen Zeit erfolgt. Bei aktivem Bluetooth-Headset betrug der Arbeitszyklus 15 %. Das Motorola System erkannte die Interferenz unregelmäßig auf einem Sensor, jedoch nicht auf dem Access Point, der sich am nächsten an der Störungsquelle befand. Da das Motorola System den einzelnen Störungsquellen keine eindeutige ID zuweist, wurde die Interferenz als das falsch klassifizierte Bluetooth aus dem vorherigen Test des schnurlosen Telefons aufgeführt. Der Alarm übernahm die Startzeit vom vorherigen Test, zeigte jedoch keine Endzeit an. Dem Bluetooth-Alarm wurde auch der gleiche Schweregrad „Continuous Wave“ (kontinuierliche Welle) zugewiesen, obwohl sich die Auswirkungen dieser beiden Interferenzen in der Realität unterscheiden.

Das Cisco System erkannte und klassifizierte dieses Bluetooth-Gerät korrekt als einzelne Störungsquelle, zeigte seinen Standort auf einem Grundriss der Umgebung sowie seinen Schweregrad an.

Screenshot des Motorola Systems



Unter den Testbedingungen mit mehreren gleichzeitigen Störungsquellen erkannte das Motorola System den Mikrowellenherd und die Videokamera, jedoch nicht das DECT-Telefon und die Bluetooth-Quellen, bei denen es sich jeweils um Frequenzsprunggeräte handelte. Zu beachten ist, dass mehrere Alarme ausgelöst wurden, obwohl nur ein Mikrowellenherd eingeschaltet war.

Mehrere Störquellen - 2,4-GHz-Band

Wir wollten feststellen, ob CleanAir und AirDefense mehrere gleichzeitig vorhandene Störungsquellen richtig klassifizieren können.

Zu diesem Zweck verwendeten wir zwei Videoüberwachungssysteme, eines auf Kanal 1 und eines auf Kanal 2. Das Cisco System klassifizierte beide Störungsquellen korrekt als Videokameras und meldete, dass die eine die Kanäle 1-4 und die zweite die Kanäle 9-11 beeinträchtigt. Darüber hinaus wurde der physische Standort auf dem Grundriss angezeigt.

Das Motorola System verursachte auf beiden Sensoren und auf dem Access Point einen Alarm, war jedoch nicht in der Lage festzustellen, ob die Alarme von einem Gerät oder mehreren Geräten verursacht wurden. Jeder Sensor und der Access Point zeigten einen einzelnen Interferenzalarm.

Später wurden weitere Störungsquellen hinzugefügt. Diese bestanden aus einem 2,4-GHz-DECT-Telefon, einer 2,4-GHz-Videokamera, einem Bluetooth-Headset und einem Mikrowellenherd.

Das Cisco System erkannte, klassifizierte und lokalisierte alle Geräte richtig. Das Symbol für den Standort des Mikrowellenherds wurde zunächst vom Symbol für den Standort der Videokamera verdeckt.

Das Motorola System erkannte ein Gerät mit kontinuierlicher Wellenform (die Videokamera) bei 2462 MHz und löste einen Alarm aus und klassifizierte auch den Mikrowellenherd richtig. Es erkannte jedoch das DECT-Telefon und das Bluetooth-Headset nicht als Frequenzsprunggeräte.

Einzelne Störungsquellen - 5-GHz-Band

Wir untersuchten auch die Fähigkeit der einzelnen Produkte zur Klassifizierung einzelner Störungsquellen im 5-GHz-Band.

Beginnend mit dem schnurlosen DECT-Telefon war das Cisco System in der Lage, das Gerät korrekt als DECT-ähnliches Telefon zu erkennen und zu klassifizieren.

Wie bereits im 2,4-GHz-Test verhinderte der geringe Arbeitszyklus, dass das Motorola System das Gerät erkannte und einen Alarm auslöste.

Um den Arbeitszyklus der Interferenz zu erhöhen wurde ein aktives Handgerät hinzugefügt. Das Cisco System klassifizierte das Telefon wiederum richtig und ordnete den Standort des Telefons korrekt zu. Das Motorola System gab unregelmäßig einen Alarm für ein Frequenzsprunggerät auf nur einem Sensor aus, jedoch nicht auf dem Access Point.

Bei drei aktiven Telefonen gaben der Motorola Access Point und beide Sensoren einen Alarm für ein Frequenzsprunggerät aus. Das Cisco System klassifizierte und lokalisierte alle drei Telefone richtig.

Im Anschluss wurde der Umgebung eine 5-GHz-Videokamera hinzugefügt. Das Motorola System war nicht in der Lage, die Interferenz zu erkennen oder zu identifizieren, vermutlich weil der Arbeitszyklus der Interferenz nicht ausreichte, um den Schwellenwert für die Auslösung eines Alarms zu überschreiten. Das Cisco System konnte die Videokamera richtig klassifizieren und lokalisieren.

Eine Zusammenfassung der Störungsquellen und wie diese erkannt und klassifiziert wurden, ist in *Abbildung 3* auf Seite 15 zu finden.

Abbildung 3: Klassifizierung und Informationen zu Störungsquellen von Cisco CleanAir und Motorola AirDefense

Störungsquelle		Klassifiziert?		Hinweise zu Motorola AirDefense
Frequenzband	Typ	Cisco Clean Air	Motorola AirDefense	
2,4 GHz	Videokamera	Ja	Ja	Allgemein klassifiziert als „Continuous Wave“ (Kontinuierliche Welle).
	Mikrowellenherd	Ja	Ja	Es wurden zwei Alarme angezeigt, einer für jeden Sensor, keine Korrelation.
	Nur DECT-Basisstation	Ja	Nein	Das Motorola System benötigt für die Klassifizierung einen hohen Arbeitszyklus.
	DECT-Basisstation und ein Telefon	Ja	Unregelmäßig	Das Motorola System klassifiziert das Gerät, jedoch unregelmäßig.
	DECT-Basisstation und drei Telefone	Ja	Falsch klassifiziert	Ein Sensor erkannte das Gerät nicht. Die anderen Sensoren lösten sowohl einen Bluetooth- als auch einen Frequenzsprunggerät-Alarm aus.
	Bluetooth	Ja	Unregelmäßig	Unregelmäßig und Erkennung nur auf einem Sensor.
	Störsender	Ja	Falsch klassifiziert	Das Motorola System klassifizierte das Gerät für 1 Sekunde fälschlicherweise als einen Mikrowellenherd.
Mehrere 2,4-GHz-Geräte	Videokamera (Kanal 1) Videokamera (Kanal 11)	Ja	Nein	Das Motorola System gab einen Alarm für eine „Continuous Wave“ (Kontinuierliche Welle) auf allen Sensoren aus, führte jedoch nicht zwei Geräte als Ursache auf.
	DECT-Telefon, Videokamera, Bluetooth, Mikrowellenherd	Ja	Nein	Nur Mikrowellenherd und Videokamera wurden identifiziert.
5 GHz	DECT-Basisstation	Ja	Nein	Das Motorola System benötigt für die Klassifizierung einen höheren Arbeitszyklus.
	DECT-Basisstation und ein Telefon	Ja	Unregelmäßig	Unregelmäßig und Erkennung nur auf einem Sensor.
	DECT-Basisstation und drei Telefone	Ja	Ja	
	Videokamera	Ja	Nein	

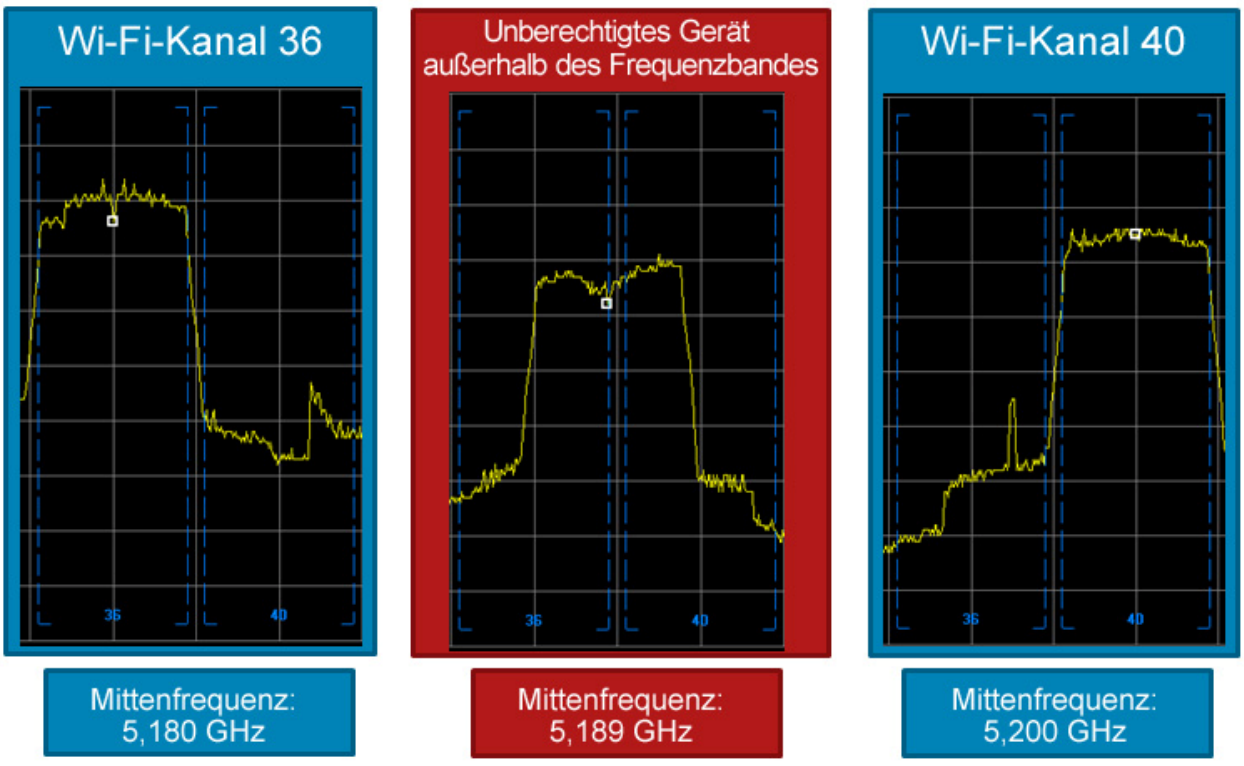
Unberechtigte Geräte auf Nicht-Standard-Kanälen

Da unberechtigte Geräte das kabelgebundene Netzwerk durch die Gewährung von „Backdoor“-Zugriffen gefährden können, wurde überprüft, ob die Access Points derartige Gefahren erkennen können.

Wir konfigurierten einen Cisco Access Point als Workgroup Bridge und platzierten diesen auf Kanal 36. Diese Bridge erhielt die SSID „Stealth“ (Verborgen), und im Anschluss wurde überprüft, ob sie erkannt wurde.

Das Cisco System identifizierte die Bridge richtig als unberechtigten Access Point. Das Trapeze System identifizierte das unberechtigte Gerät ebenfalls richtig. Das Motorola System erkannte es als „Unsanctioned BSS“ (Nicht zugelassenes BSS). Das HP System erkannte es als unberechtigtes Gerät, und das Aruba System erkannte die SSID als „Stealth“. Das Meru System erkannte das unberechtigte Gerät nicht.

Nahezu alle Access Points waren in der Lage, ein in das Netzwerk eingebundenes unberechtigtes Gerät zu erkennen. Anschließend testeten wir, was passiert, wenn ein unberechtigtes Gerät auf einem nicht standardmäßigen Kanal (Off-Channel) konfiguriert wird. Es sind Produkte erhältlich, mit denen Benutzer die Mittenfrequenz von Atheros-basierten Chipsets ändern können, die von den meisten Wireless Access Points verwendet werden, und die auf diese Weise dem Netzwerk verborgen bleiben. Um festzustellen, ob diese unberechtigten Geräte erkannt werden, setzten wir die Mittenfrequenz unseres unberechtigten Geräts auf 5,189 GHz. Wir wiederholten den Test, nachdem wir es zwischen den Kanälen 36 und 40 eingefügt hatten.



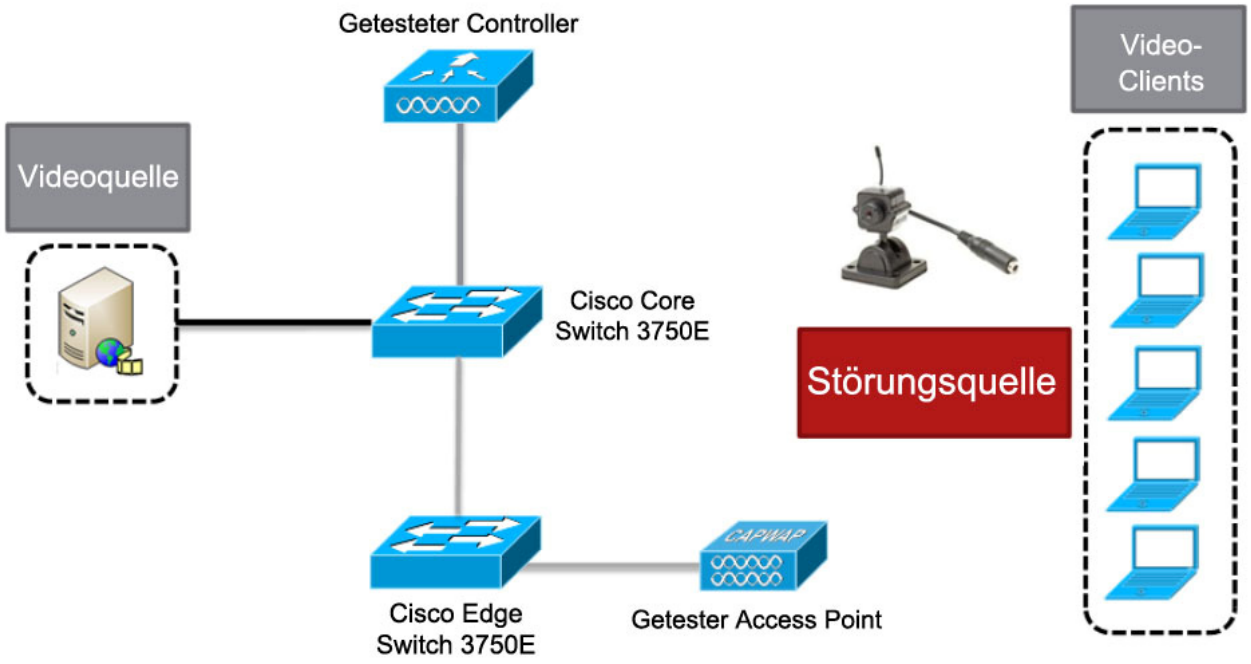
Das Cisco System erkannte das unberechtigte Gerät richtig als „Wi-Fi invalid channel“ (Ungültiger Wi-Fi-Kanal) und stellte seinen Standort dar. Die Systeme der übrigen Anbieter suchten nach Geräten, die „Off-Channel“ sendeten, nicht jedoch nach solchen, die „Off-Freqency“ sendeten. Das Aruba System erkannte das unberechtigte Gerät auf seiner neuen Frequenz nicht, ebenso wenig die Systeme von Trapeze, Motorola, HP und Meru.

Selbstheilung

In Anbetracht der negativen Auswirkungen auf Wireless-Netzwerke von Inteferenzen, die nicht von Wi-Fi-Geräten verursacht werden, müssen Access Points in der Lage sein, diese Störungen zu vermeiden, um die Netzqualität für Endbenutzer aufrechtzuerhalten. Wir führten diesen Test im 2,4-GHz-Band aus.

Cisco Geräte:

Wenn die Kamera an Position A aktiviert wurde, verloren alle fünf Clients sofort die Ping-Verbindung. Der Access Point wechselte von Kanal 1 zu Kanal 6, und die Clients stellten ihre Ping-Verbindung innerhalb von 49 Sekunden wieder her. Wenn die Kamera an Position B aktiviert wurde, benötigte der Access Point 39 Sekunden, um den Kanal zu wechseln und die Ping-Verbindung für die Clients wiederherzustellen. Wenn die Kamera an Position C aktiviert wurde, benötigte der Access Point 1 Minute und 4 Sekunden, um den Kanal zu wechseln und die Ping-Verbindung wiederherzustellen. Da der Cisco Access Point Interferenzgeräte konstant vermeidet, wurde er zwischen den Tests zurückgesetzt, damit alternative Kanäle nicht durch diese Funktion gesperrt blieben. Im Normalbetrieb kennzeichnet die konstante Vermeidung von Interferenz-Geräten die Störungsquelle automatisch als veraltet, damit der Kanal für das System wieder verfügbar ist. Ein zweiter Durchlauf dauerte an Position A 30 Sekunden, an Position B 41 Sekunden und an Position C 48 Sekunden. Wie erwartet, verlor an der 30-Meter-Position nur der am weitesten entfernte Client die Ping-Verbindung. Auch wenn die Videoqualität auf allen Clients beeinträchtigt war, erkannte der Access Point die Interferenz und wechselte den Kanal.



Aruba Gerät:

Der gleiche Test wurde mit dem Aruba AP125 ausgeführt. Bei der Kamera an Position A meldete das Aruba Gerät einen Störpegel von -87 dBm, während ein Spektrumanalysator einen Störpegel von -52 dBm meldete. Da der Kanal vollständig durch ein Interferenzsignal blockiert war, wurden keine Fehler gemeldet. Da der Rauschpegel die Fehlerschwellenwerte nicht überschritt, wechselte der Access Point den Kanal nicht, und alle Clients wurden abgetrennt.

Bei der Kamera an Position B wurden Clients in größerer Entfernung vom Access Point beeinträchtigt, während Clients in geringerer Entfernung aufgrund des Signal-Rausch-Verhältnisses nicht betroffen waren. Der Rauschpegel-Schwellenwert wurde überschritten, und der Access Point wechselte den Kanal innerhalb von 2:01 Minuten.

Bei der 30-Meter-Position wurden Rauschpegelwerte von -75 bis -77 dBm angezeigt, was für die Auslösung nicht ausreichend war. Clients mit einem größeren Abstand vom Access Point waren am stärksten beeinträchtigt, und für die gesamte Zelle ließ sich eine hohe Latenz und eine verminderte Bandbreite feststellen. Bei einem zweiten Testlauf wurde der Kanal bei ca. 3 Metern niemals gewechselt, während der Kanalwechsel bei ca. 15 Metern erst nach 2:10 Minuten und bei ca. 30 Metern erst nach 2:22 Minuten erfolgte, wenn der Rauschpegel von -70 dBm den Schwellenwert überschritt.

Auch die Selbstheilungsfähigkeiten des Aruba AP105 wurden untersucht. Der Basisrauschpegel betrug -105 dBm. Dieser Wert war zu niedrig und entsprach nicht dem vom AP125 in der gleichen Umgebung gemessenen Wert von -87 dBm. In einer Netzwerkumgebung mit dem AP105 und dem AP125 machte diese Abweichung im Grund-Rauschpegelwert die Anpassung des für den Kanalwechsel erforderlichen Rauschschwellenwerts schwierig. Der Rauschpegel muss sich für 120 Sekunden oberhalb des Schwellenwerts befinden, damit ein Kanalwechsel ausgelöst wird. Nachdem Clients in der 3-Meter-Position aufgrund der von der Videokamera verursachten Interferenz während 30 Minuten abgetrennt worden waren, konnte anhand der festgestellten Ungenauigkeit belegt werden, dass der Rauschpegel den Schwellenwert niemals lange genug für eine Auslösung überschritten hatte. Über die Befehlszeilenschnittstelle konnte zudem festgestellt werden, dass der Access Point den Funksender immer wieder zurücksetzte.

An der 15-Meter-Position verloren alle Clients die Ping-Verbindung, sobald die Kamera eingeschaltet wurde. Das AP105 meldete einen Rauschpegel von -74 bis -80 dBm, nahm jedoch während der 30-minütigen Testzeit keinen Kanalwechsel vor.

An der 30-Meter-Position verloren alle Clients die Ping-Verbindung, sobald die Videokamera eingeschaltet wurde. Der vom Access Point gemessene Rauschpegel betrug -100 dBM, und nachdem die Clients während 30 Minuten getrennt worden waren, konnte kein Kanalwechsel beobachtet werden. Wir versuchten, die Einstellung für „Non 802.11 Interference Immunity“ (Störungsimmunität für Nicht-802.11) von der Standardeinstellung „Stufe 2“ zu „Stufe 5“ zu ändern, alle fünf Clients konnten jedoch weiterhin keine Ping-Verbindung mit dem Access Point herstellen.

HP Gerät:

Beim HP Access Point beträgt das kleinste Intervall zum Wechsel des Kanals eine Stunde. Wenn die Videokamera an der 3-Meter-Position eingeschaltet wurde, verlor der Access Point die Verbindung mit allen Clients. Nach über einer Stunde hatte der Access Point noch keinen Kanalwechsel vorgenommen und noch kein Ereignis in einem Ereignisprotokoll erfasst. An der 15-Meter-Position blieb nur die Verbindung des Client erhalten, der sich am nächsten zum Access Point befand, nachdem die Kamera eingeschaltet wurde. Nach über einer Stunde hatte das HP Gerät noch keinen Kanalwechsel vorgenommen oder irgendwelche Ereignisse protokolliert. An der 30-Meter-Position behielten vier Clients die Verbindung, und wie erwartet wurde nur der am weitesten entfernte Client gestört. Nach über einer Stunde hatte der Access Point noch keinen Kanalwechsel vorgenommen.

Trapeze Gerät:

Das Trapeze Gerät besitzt ein Standard-Abtastintervall von 3600 Sekunden, und die minimale Abtastzeit kann auf 900 Sekunden festgelegt werden. Bei einem Abstand von ca. 3 Metern zur Videokamera gingen alle Client-Verbindungen verloren, und das Trapeze Gerät wechselte den Kanal nach 47 Minuten. Bei einem Abstand von ca. 15 Metern blieb die Verbindung eines Client erhalten. Nach über einer Stunde hatte das Trapeze Gerät noch keinen Kanalwechsel vorgenommen. Wir stellten fest, dass immer ein Rauschpegel von -96 dBm gemeldet wurde, unabhängig vom Standort oder dem Abstand zur Videokamera, die die Interferenz verursachte. Bei einem Abstand von ca. 30 Metern war nur der am weitesten entfernte Client beeinträchtigt. Nach über einer Stunde hatte das Trapeze Gerät noch keinen Kanalwechsel vorgenommen.

Motorola Gerät:

Das Motorola AP-7131N verfügt über Legacy-Selbstheilungsfunktionen sowie über die Funktion „Smart-RF“. Wir aktivierten „Auto Channel Select“ (Automatische Kanalauswahl) und änderten die Datenrateneinstellung auf dem Access Point, um die verfügbare Bandbreite zu erhöhen und die Kanalauslastung zu reduzieren, sodass der für unseren Test verwendete Video-Stream unterstützt werden konnte.

Die Legacy-Selbstheilungsfunktion bewirkt, dass der Access Point die durchschittliche Anzahl erneuter Versuche als Auslöseschwellwert für einen Kanalwechsel verwendet. Bei einem Abstand der Videokamera von ca. 3 Metern meldete das Motorola System 0 erneute Versuche. Es konnte keine Interferenzen feststellen. Der Client-Durchsatz war niedrig genug, um in wissenschaftlicher Notation wiedergegeben zu werden. Nach einer halben Stunde hatte der Access Point noch keinen Kanalwechsel vorgenommen. Die Tests wurden nach der Aktivierung der Smart-RF-Funktion wiederholt, die Ergebnisse blieben jedoch die gleichen. Es fanden keine erneuten Versuche statt, und es wurde kein Rauschpegel gemeldet. Alle Statistiken zeigten Nullen an. Das Netzwerk war vollständig blockiert, der Access Point konnte dies jedoch nicht erkennen und nahm keinen Kanalwechsel vor.

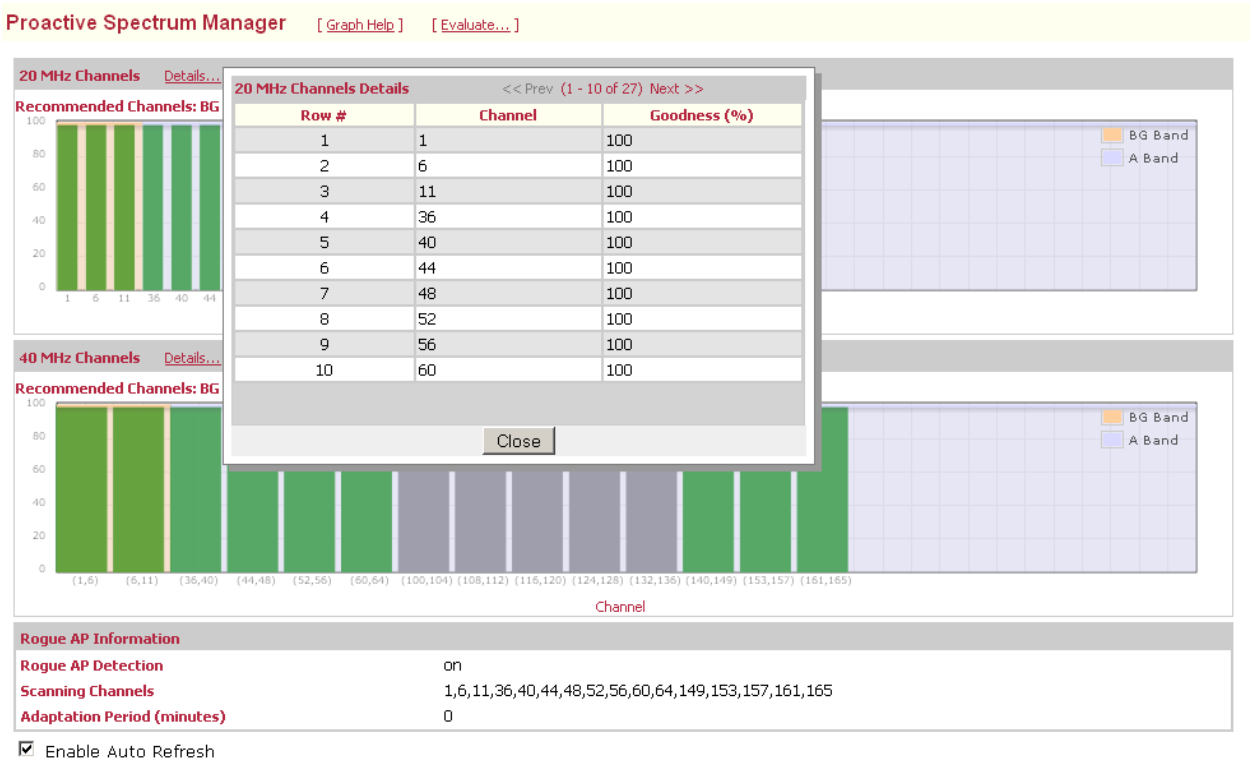
Bei einem Abstand von ca. 15 Metern lag die durchschnittliche Anzahl der erneuten Versuche zwischen 1 und 2, diese überschritten jedoch nicht den Schwellenwert. Nach 20 Minuten hatte der Kanal nicht gewechselt, und wir versuchten, ACS zu einem Kanalwechsel zu zwingen, dieser fand jedoch nicht statt.

Bei einem Abstand von ca. 30 Metern vom Access Point war nur der entfernteste Client beeinträchtigt. Der Rauschpegel betrug -66 dBm. Nach einer halben Stunde hatte der Access Point noch keinen Kanalwechsel vorgenommen. Unser Versuch, ACS manuell zu einem Kanalwechsel zu zwingen, war erfolglos.

Meru Gerät:

Der Meru AP320 verwendet die Funktion „Proactive Spectrum Manager“. Diese zeigt den „Gütegrad“ eines jeden Kanals an. Wenn wir Video-Streams über einen störungsfreien Kanal sendeten, meldete PSM diesen Kanal aufgrund der starken Ausnutzung als „schlecht“. Als die Kanäle jedoch durch die Videokamera blockiert waren, sodass keine Nutzung möglich war, meldete PSM für den Kanal einen „Gütegrad“ von 100 %.

Dieser 802.11n-konforme Access Point unterstützt „Auto Channel“ nicht wie die 802.11 a/b/g-konformen Modelle. Auch unterstützt er offensichtlich keine Selbstheilungsfunktionen. PSM überprüft jedoch den Kanal in dem vom Benutzer festgelegten Sekundenintervall und verschiebt die Stationen dann zu einem ungestörten Kanal. Der einzige Schwellenwert für die Auslösung dieses Wechsels ist das Vorhandensein von unberechtigten Geräten.



Dieser Screenshot wurde erstellt, als der Kanal durch das von der Videokamera stammende Interferenzsignal vollständig blockiert war. Das Meru Stystem meldet einen Gütegrad von 100 % für den Kanal, da die blockierende Interferenz bedeutet, dass seine Wi-Fi-Ausnutzung gemäß der Meru Qualitätsbewertung 0 % beträgt. Das Meru System nahm auch keinen Kanalwechsel vor, als der Kanal vollständig blockiert und für Wi-Fi nicht mehr verwendbar war.

Wir überprüften die relativen Rauschpegel auf dem Meru Access Point, um deren Genauigkeit zu ermitteln. Das Meru System ermittelte einen Rauschpegel von -82 dBm als Basiswert für einen ungestörten Kanal. Bei einem Abstand der Videokamera von ca. 15 Metern betrug der Messwert -85 dBm. Bei einem Abstand der Videokamera von ca. 30 Metern betrug der Messwert -71 dBm. Eine Zusammenfassung der Ergebnisse finden Sie in *Abbildung 4* auf Seite 22.

Abbildung 4: Zusammenfassung der Selbstheilungstests von Cisco CleanAir und Produkten von Mitbewerbern

	Zeit bis zur Selbstheilung						
Abstand der Störquelle vom Access Point	**Cisco**	**Aruba AP125**	**Aruba AP105**	**Motorola**	**HP**	**Trapeze**	**Meru**
Nah (ca. 3 m)	30 Sek.	Nie	Nie	Nie	Nie	47 Min.	Nie
Mittel (ca. 15 m)	41 Sek.	2:10 Min.	Nie	Nie	Nie	Nie	Nie
Weit (ca. 30 m)	48 Sek.	2:22 Min.	Nie	Nie	Nie	Nie	Nie
Hinweise:		Bei geringem Abstand blieb der Rauschpegel bei -87 dBm.	Der Rauschpegel variierte an jedem Standort, blieb aber niemals oberhalb des Schwellenwerts.	Die Anzahl der erneuten Versuche überschritt den Schwellenwert nicht und löste keinen Kanalwechsel aus.	Das HP System stellte bei einem Abstand von der Kamera von 15 m einen Rauschpegel von -70 dBm fest.	Der Rauschpegel blieb bei -96 dBm.	Der Gütegrad des Kanals blieb immer bei 100 %.