Cisco CleanAir-Technologie: Angewandte Intelligenz

Dieses Whitepaper beschäftigt sich mit den Herausforderungen durch Interferenzen, die sich aus der intensiven Nutzung eines gemeinsam Frequenzbereichs ergeben. Es werden die Einschränkungen von herkömmlichen Wi-Fi-Chip-Designs erläutert und wie sich diese auf die Fähigkeit einer IT-Abteilung auswirken, aussagefähige und praxisnahe Daten über das verwendete Frequenzband zu erfassen, die für eine effektive Fehlerbehebung erforderlich sind. Schließlich wird die Cisco® CleanAir-Technologie vorgestellt und erläutert, wie Benutzer durch die Integration von Funkintelligenz in das Netzwerk einen umfassenden Einblick in die tatsächliche Nutzung des für drahtlose Übertragungen verwendeten Frequenzbereichs erhalten. Dieser Einblick ist entscheidend für eine proaktive Verwaltung von Wi-Fi-Netzwerken, die unternehmenswichtige und latenzempfindliche Anwendungen unterstützen, wie sie heute in Krankenhäusern, verzweigten Unternehmen, Fertigungsanlagen, Einzelhandelsgeschäften und Büros zur Anwendung kommen.

Wi-Fi wird unternehmenswichtig

Die ersten Wi-Fi-Netzwerke in Unternehmen dienten ausschließlich der Bequemlichkeit, etwa für den Internetzugriff im Empfangsbereich oder in Konferenzräumen. Für diese Anwendungen war eine bestmögliche Leistung ausreichend.

Heute hat sich Wi-Fi soweit entwickelt, dass es für zahlreiche unternehmenswichtige Anwendungen verwendet wird. Krankenhäuser verwenden Wi-Fi für den mobilen Zugriff auf Patientendaten und für die entfernte Überwachung von sekundären Systemen am Patientenbett. Im Handel und in der Fertigung wird Wi-Fi für die Logistik und für Geschäftstransaktionen verwendet. Kleinere Zweigniederlassungen gehen dazu über, Wi-Fi als ausschließliche Methode für den Netzwerkzugriff zu verwenden und verzichten dabei auf drahtgestützte Verbindungen. Darüber hinaus wird Wi-Fi in zunehmendem Maße für Sprache und Video verwendet, die besonders empfindlich auf Störungen reagieren.

In all diesen Beispielen wird eine besonders hohe Zuverlässigkeit erwartet. Es ist nicht mehr akzeptabel, dass Wi-Fi-Netzwerke aufgrund von Interferenzen unerwartet ausfallen.

Definieren der Lösung

Spektrumintelligenz (SI) bezeichnet Daten über Aktivitäten im Funkspektrum, die von fortschrittlichen Algorithmen zur Identifizierung von Interferenzen abgerufen werden, wie sie in ähnlicher Weise auch vom Militär verwendet werden. SI ermöglicht einen Überblick über alle Benutzer im gemeinsam genutzten Frequenzband, als auch von Störquellen, die auf andere Ursachen als Wi-Fi-Geräte zurückzuführen sind. Zu jedem Gerät, das im unlizenzierten Band betriebenen wird, kann die SI feststellen, worum es sich handelt, wo es sich befindet, und wie es sich auf das Wi-Fi-Netzwerk auswirkt.

Spektrum-Management bezeichnet die aktive Nutzung von Spektrumintelligenzdaten zur Verbesserung der Leistung und zur Reduzierung der Betriebskosten von Wi-Fi-Netzwerken. Informationen über den Schweregrad und die Dauer von Interferenzen können verwendet werden, um die Auswirkung auf das Netzwerk zu berechnen und um Probleme zu beheben. Diese Informationen können auch zur Analyse zurückliegender Zeiträume und für die Ermittlung von Trends verwendet werden. In Kombination mit Kontextdaten wie dem physischen Standort und systemweiten Wechselbeziehungen ist das Spektrum-Management ein leistungsfähiges und proaktives Werkzeug zur Erhöhung der Zuverlässigkeit, der Leistung und der Sicherheit des WLAN.

Externe oder eigenständige SI-Tools sind zwar seit einiger Zeit verfügbar, Cisco hat jedoch den entscheidenden Schritt unternommen, SI direkt in das Chipset neuer Access Points zu integrieren. Cisco CleanAir ist eine revolutionäre Technologie und die erste in der Branche, die IT-Managern den Zugriff auf umfangreiche Spektruminformationen ermöglicht, die automatisch für alle Interferenzen erfasst werden, die auf andere Ursachen als auf 802.11-konforme Geräte zurückzuführen sind. Die von der CleanAir-Technologie bereitgestellte Spektrumintelligenz ermöglicht eine neue Stufe des Spektrum-Managements. Im Unterschied zu bisherigen Spektrum-Management-Tools, die lediglich zusammen mit anderen Wi-Fi-Geräten verwendet werden konnten und in der Regel unabhängig vom Wireless-Netzwerk waren, ist das neue integrierte Spektrum-Management Bestandteil der Struktur des Wireless-Netzwerks. Das Spektrum-Management der zweiten Generation erkennt alle Benutzer des drahtlosen Frequenzbands und ist in der Lage, durch die Behebung und Vermeidung von Interferenzen Maßnahmen zur Optimierung der Netzwerkleistung zu ergreifen.

Leistung und Zuverlässigkeit

Außer der Erkennung von Interferenzen verlangen IT-Verantwortliche auch, dass das Netzwerk Interferenzen nach Möglichkeit automatisch umgeht - sowohl zur Senkung der Betriebskosten als auch zur Reduzierung der Netzwerkausfallzeiten. Diese automatische Abstimmung ist die Aufgabe der Funkressourcenverwaltung (Radio Resource Management, RRM), einer Softwareschicht in der Infrastruktur, die Netzwerkparameter automatisch anpasst, um die Funkleistung aufrechtzuerhalten. Ältere Generationen von RRM waren größtenteils blind gegenüber Interferenzen, die über ein unbestimmtes „Rauschen“ hinausgingen. Mit der Einführung von integrierter SI ist eine neue Generation von RRM in der Lage, detaillierte Informationen über Störungsquellen zu verwenden, um wirklich intelligente Entscheidungen zu treffen und so die Zuverlässigkeit wesentlich zu erhöhen.

Zusätzlich zu automatisiertem RRM kann die integrierte Spektrumintelligenz systemweit für umfangreichere Spektrum-Management-Aufgaben verwendet werden. Diese sind möglicherweise neu im Wi-Fi-Bereich, für die Manager von drahtgestützten Netzwerken sind sie jedoch vertraut:

- Behebung von Leistungsproblemen in Echtzeit
- Ausführung von forensischen Analysen für zeitweilig auftretende oder vergangene Probleme
- Berichte zu Nutzungs- und Störungstrends
- Herstellung von Wechselbeziehungen zwischen Interferenzen auf mehreren Access Points, um die Auswirkungen zu ermitteln und übermäßige Alarme zu verringern

Wireless Security (Wireless-Sicherheit)

Schließlich ist festzustellen, dass sich die Herausforderungen der drahtlosen Übertragung nicht nur auf die Leistung, sondern auch auf die Sicherheit erstrecken. Es wurden zahlreiche Anstrengungen unternommen festzustellen, wie unberechtigte Access Points Sicherheitslücken in Unternehmensnetzwerken ausnutzen können. Wireless Intrusion Detection Systems und Intrusion Prevention Systems (wIDS/wIPS) wurden zur Behebung dieses Problems entwickelt. Aktuelle IDS- und IPS-Lösungen besitzen jedoch deutliche Schwächen, die nicht ohne die Ergänzung durch Spektrumintelligenz behoben werden können.

Aktuelle IDS/IPS-Systeme erkennen keine Access Points, die mit proprietären Erweiterungen wie Super G (von Atheros) betrieben werden. Diese betriebsbereit erhältlichen Geräte bleiben unerkannt. Darüber hinaus können Hacker herkömmliche Wi-Fi-Geräte verwenden (beispielsweise unter Linux) und diese so verändern, dass sie auf nichtstandardmäßigen Kanälen oder mit anderen nicht genormten Modulierungsverfahren betrieben werden. Diese erweiterten oder modifizierten Geräte können nur erkannt werden, indem die physikalische Funkschicht analysiert wird.

Neben Wi-Fi-Geräten können auch andere Arten von Nicht-Wi-Fi-Geräten wie Bluetooth-Access Points, Access Points unter älteren Standards wie 802.11FH und proprietäre drahtlose Brücken dazu verwendet werden, Lücken im Netzwerk zu öffnen. Im Fall von Brücken können diese Geräte Daten an einen Angreifer senden, der sich viele Kilometer von Ihrem Gebäude entfernt befindet. Noch einmal: diese Arten von Geräten können nur erkannt werden, wenn Sie alle in Ihrem Frequenzband vorhandenen Geräte analysieren.

Außer der Gefahr von unberechtigten Geräten besteht die Gefahr, dass eine böswillige Person versucht, Ihr Wi-Fi-Netzwerk mit einem DoS-Angriff (Denial-of-Service) zu deaktivieren. Obwohl IDS/IPS-Systeme zahlreiche DoS-Angriffe auf der „Protokollebene“ überwachen, überwachen sie keine DoS-Angriffe auf der Funkebene, die durch Störsender oder Wi-Fi-Geräte erfolgen können, die sich in einem diagnostischen Störmodus befinden.

Neben zielgerichteten Angriffen können auch einige einfache Geräte wie drahtlose Videokameras oder analoge schnurlose Telefone zu einer vollständigen Verstopfung Ihres Netzwerks führen. Integrierte Spektrumintelligenz und Spektrum-Management sind ausgesprochen effektiv bei der Identifizierung dieser Arten von DoS-Gefahren auf der Funkebene.

Wie wird das integrierte Spektrum-Management implementiert?

Einschränkungen bei herkömmlicher Wi-Fi-Hardware

Grundsätzlich eignet sich ein herkömmliches Wi-Fi-Chipset nur eingeschränkt zur Implementierung von Spektrumintelligenz. Dies liegt daran, dass Wi-Fi-Chipsets speziell dafür entwickelt wurden, nur Wi-Fi-Signale zu empfangen. Sie erkennen keine anderen Arten von Signalen (mit der Ausnahme von DFS-Radar (Dynamic Frequency Selection)). Herkömmliche Chipsets wurden nicht einmal dafür entwickelt, ausreichende Informationen weiterzuleiten, damit SI auf einer höheren Softwareebene ausgeführt werden kann.

Dies bedeutet, wenn ein herkömmliches Wi-Fi-Chipset einen Übertragungsstoß (Burst) feststellt, der nicht einzuordnen ist, kann es normalerweise nur einige Informationen melden: 1) dass ein nicht einzuordnender Burst stattgefunden hat, 2) den Stärkegrad des Burst und 3) die Start- und Endzeit des Burst. Beachten Sie, dass der Burst von einem Wi-Fi-Gerät auf einem anderen Kanal ausgegangen sein kann oder auf dem gleichen Kanal, jedoch in zu großer Entfernung, um richtig empfangen zu werden. Oder der Burst ist von einem Nicht-Wi-Fi-Gerät ausgegangen. Detaillierte Informationen über den Modulierungstyp des Burst, wo im Kanal er stattgefunden hat usw. sind in der Regel nicht verfügbar. Und es besteht keine Möglichkeit für Software, zur Analyse auf die tatsächlich von dem Burst empfangenen Daten zuzugreifen.

Trotz dieser Einschränkungen besteht die Möglichkeit, mithilfe eines Wi-Fi-Chips die nicht identifizierten Bursts zu summieren und eine Gesamtsumme der Interferenzen zu berechnen sowie die durchschnittliche Stärke der Interferenzen. Leider stellt dieses Konzept nicht die erforderlichen Informationen bereit, um das Problem auch zu lösen. Das Konzept der „totalen Interferenz“ liefert beispielsweise keine Informationen über die spezifische Art der Interferenz (z. B. handelt es sich nur um eine Wi-Fi-Interferenz auf einem Zweitkanal oder um etwas anderes?), ob die Interferenz von einer Quelle ausgeht oder von mehreren, wo sich die Störquelle befindet usw. Aus dieser Liste wird deutlich, dass der Umfang der SI, die mit einem herkömmlichen Wi-Fi-Chipset erfasst werden kann, relativ begrenzt ist.

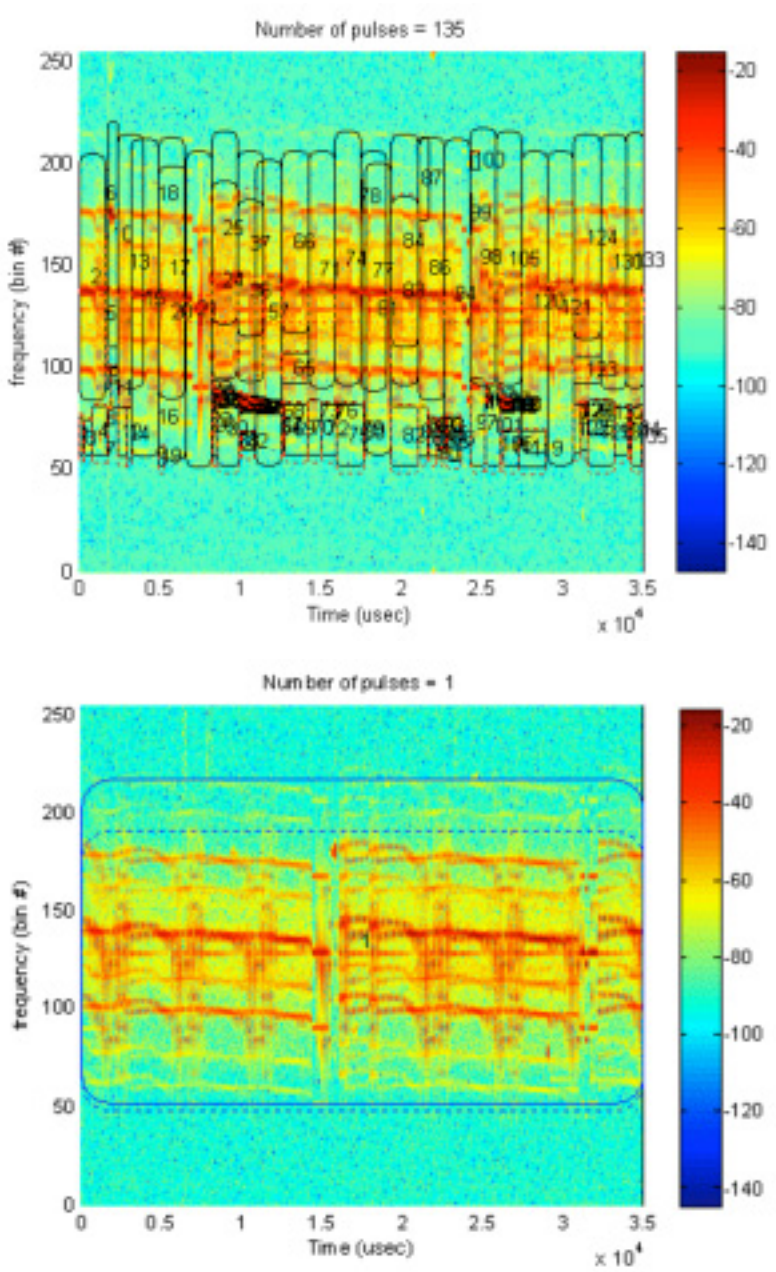
Cisco CleanAir Technology: Eine angepasste Hardware-/Softwarelösung

Um die offensichtlichen Einschränkungen herkömmlicher Wi-Fi-Chipsets zu umgehen, hat Cisco eine integrierte Lösung aus patentierten Chips und Software geschaffen, die speziell für die Analyse sämtlicher Funkaktivitäten entwickelt wurde. (Bis heute wurden für diese Technologie über 25 Patente eingetragen.) Im Wesentlichen hat Cisco die dem Analysetool Cisco Spectrum Expert zugrundeliegende Technologie verwendet und diese direkt in die Infrastruktur integriert, einschließlich einer weitgehenden Integration in das Chipset. Dies ist ein bedeutender Fortschritt, der deutlich macht, dass Wireless-Netzwerke nicht mehr nur der Bequemlichkeit dienen, sondern geschäftswichtige Funktionen im Unternehmen besitzen. Wi-Fi-Chipsets in Verbraucherqualität sind nicht mehr ausreichend.

Die angepasste Lösung beginnt mit der Hardware-Kerntechnologie der Cisco Spectrum Analysis Engine (SAgE), die unmittelbar in das Wi-Fi-Chipset der neuen Cisco Aironet® Access Points der Serie 3500 integriert wurde. Die SAgE-Kerntechnologie verarbeitet sehr rechenintensive Operationen wie schnelle Fouriertransformation (Fast Fourier Transform, FFT) und Impulserkennungsoperationen. (Ein Impuls ist ein Stoß von Funkenergie in Frequenz und Zeit.) Die SAgE-Kerntechnologie verarbeitet grundlegende Spektrumanalyseoperationen, die so verarbeitungsintensiv sind, dass ihre Verarbeitung in Echtzeit nicht möglich wäre.

Abbildung 1 veranschaulicht die Identifizierung von Energieimpulsen durch SAgE grafisch. Die erste Abbildung zeigt die Daten vom Hardware-Impulserkennungsblock, und die zweite Abbildung zeigt die Daten, nachdem die Software Impulse zusammengefasst hat, die so viele Übereinstimmungen aufweisen, dass sie als einziger Impuls betrachtet werden.

Abbildung 1. Erkannte Funkenergieimpulse vor und nach dem Filtern



Nachdem die SAgE-Verarbeitung abgeschlossen ist, werden die Funkmuster der zu untersuchenden Impulse zur detaillierten Charakteristikanalyse an die Softwareebene übergeben. Wenn diese Verarbeitung auf der Hauptfunk-CPU ausgeführt würde, würde sich dies negativ auf die Wi-Fi-Leistung auswirken. Um diese Beeinträchtigung zu vermeiden, verfügt die Cisco Hardwarelösung über einen angepassten Verarbeitungskern mit dem Namen DSP Vector Accelerator (DAvE), der direkt in das Wi-Fi-Chipset des Access Point integriert ist. Die DAvE-Kerntechnologie kann intensive Signalverarbeitungsoperationen ausführen, die als „Davelets“ bezeichnet werden, diese umfassen Filterung, Dezimierung, Drehung, Synchronworterkennung sowie Modulationserkennung, ohne die Haupt-CPU zu belasten. Der DAvE verarbeitet CPU-Intensive Signalverarbeitungsoperationen, die anderenfalls die Haupt-CPU überlasten würde.

Die abschließende Verarbeitungsstufe erfolgt in einem auf der Haupt-CPU ausgeführten Softwaremodul, das als „Sensord“ bezeichnet wird. Beachten Sie, dass die Auslastung der CPU aufgrund der umfassenden Unterstützung durch SAgE und DAvE jetzt sehr gering ist. Die Sensord-Software überwacht die Zeit und die Frequenz von Interferenz-Bursts sowie die festgestellten Attribute der Bursts wie den Modulationstyp und identifizierte Synchronwörter. Diese allgemeinen Informationen werden anschließend verwendet, um die abschließende Identifizierung und Separierung der einzelnen Geräte auszuführen. Dieser letzte Klassifizierungsschritt stellt die leistungsstarken Funktionen der SI bereit: Informationen über die spezifische Störungsquelle, ihren Standort sowie die mögliche Lösung.

Leistungsaspekte der SI-Implementierung

Anzahl der Klassifizierungen

Die CleanAir-Technologie verfügt über einen leistungsstarken Satz von 20 Nicht-Wi-Fi-Klassifizierungen. Da die Analyse in der Software stattfindet, kann die Liste der Klassifizierungen erweitert werden, sobald neue Störungsquellen auf dem Markt relevant werden. In anderen Worten: Die zugrundeliegende Hardwarelösung kann jede Art von zukünftig auftretenden Interferenzen erkennen, es ist lediglich eine Aktualisierung der Software erforderlich.

Gleichzeitige Erkennung

Mit der von der CleanAir-Technologie verwendeten Klassifizierung können mehrere gleichzeitig betriebene Geräte erkannt werden, die Interferenzen verursachen. Dabei kann es sich um Geräte des gleichen Typs oder unterschiedlichen Typs handeln. Tatsächlich ist die CleanAir-Technologie in der Lage, 10 gleichzeitig betriebene Störgeräte per Funk zu melden. Dies ist wichtig, da in der Realität die Anzahl der gleichzeitig auftretenden Funkaktivitäten ziemlich groß sein kann. Alle Lösungen von Mitbewerbern, die nicht in der Lage sind, mehrere gleichzeitig betriebene Geräte zu unterscheiden, werden in der Leistung sehr schnell abfallen, und ihre Ergebnisse sind lediglich ausreichend für Demonstrationen und Labortests.

Erkennungszeit

Die Auswirkung von Störgeräten kann vorübergehend sein, entweder, weil sie kurz hintereinander an- und ausgeschaltet werden, oder weil sich der Benutzer in einem Gebäude bewegt. Aus diesem Grund muss die Klassifizierung schnell erfolgen, bevor das Gerät nicht mehr festgestellt werden kann. Die CleanAir-Technologie ermöglicht Access Points die Klassifizierung von Geräten innerhalb von 30 Sekunden, häufig reichen für eine Klassifizierung sogar nur 5 Sekunden aus. (Beachten Sie, dass die Berichterstellung leicht verzögert erfolgen kann, wenn die Konsolidierung der Daten über mehrere Access Points erfolgt.)

Wahrscheinlichkeit falscher Erkennungen

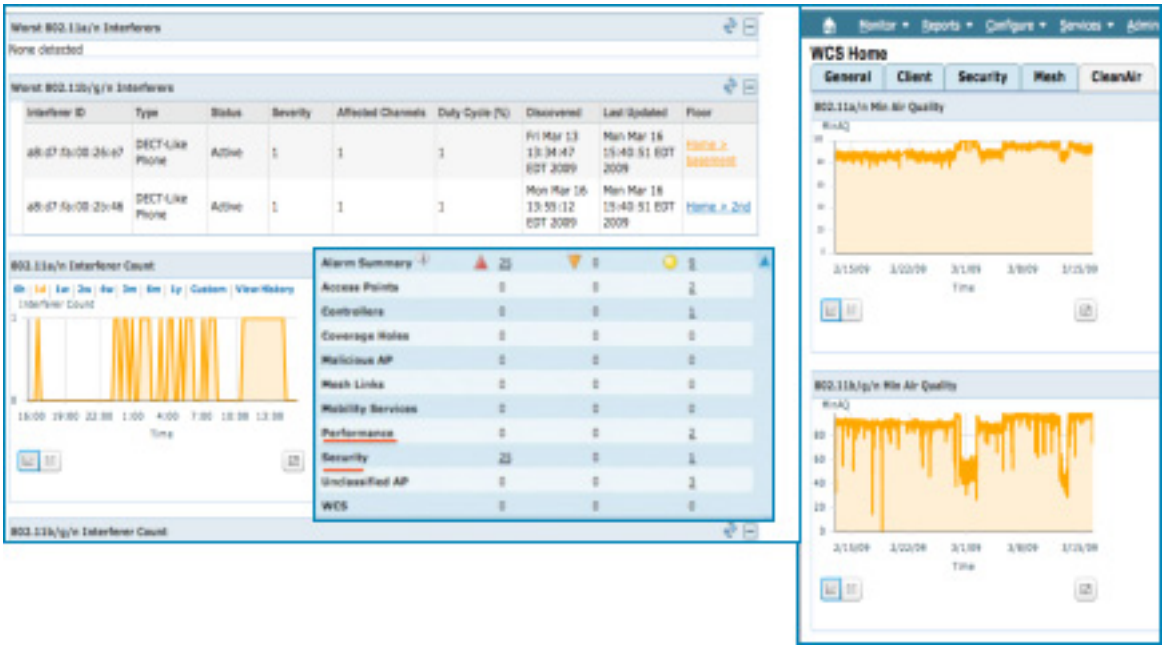
Es ist wichtig, keine Störungsquelle zu übersehen, und es ist genauso wichtig, keine „Phantominterferenzen“ zu melden, wenn keine vorhanden sind oder Interferenzen falsch zu kennzeichnen, sodass IT-Mitarbeiter nach dem falschen Gerät suchen. Die CleanAir-Technologie wurde für möglichst geringe Falscherkennungsraten entwickelt, selbst in stark ausgelasteten Funkumgebungen, in denen hunderte von Wi-Fi- und Nicht-Wi-Fi-Geräten gleichzeitig betrieben werden. Durch die Verringerung von Falscherkennungen hilft die CleanAir-Technologie den IT-Mitarbeitern Zeit zu sparen.

CleanAir-Technologie: Die Wichtigkeit von integrierter Spektrumintelligenz und von Spektrum-Management

Auch wenn das Produkt „Spectrum Expert“ und Tool-basierte Lösungen vor der Bereitstellung eines Netzwerks eine wichtige Rolle spielen, bietet die Integration von SI-Technologie in die Wi-Fi-Infrastruktur wesentlich größere Vorteile. In der integrierten CleanAir-Lösung ist die SI-Engine direkt in die Access Points integriert, und die SI-Informationen werden anschließend vollständig in die Netzwerkarchitektur und die Management-Systeme integriert, um ein intelligentes Spektrum-Management zu ermöglichen.

Ein Vorteil der CleanAir-Technologie ist der, dass sie täglich 24 Stunden aktiv ist und Interferenzen und Probleme mit der Funkqualität überwacht (siehe Abbildung 2). Dies ermöglicht IT-Mitarbeitern ein proaktiveres Konzept bei der Spektrumverwaltung. Anstatt darauf zu warten, dass ein Benutzer eine Interferenz meldet (in Form eines Problemtickets) und dann ein Tool zur Problemanalyse bereitzustellen, können IT-Mitarbeiter Interferenzen feststellen, sobald sie auftreten und unverzüglich Maßnahmen ergreifen. Die Verfügbarkeit eines Verlaufsprotokolls für 24 Stunden und 7 Tage in der Woche ermöglicht zudem eine Überprüfung zurückliegender Ereignisse. Mithilfe von Verlaufsdaten lassen sich auf einfache Weise Trends über eine länger Zeit analysieren.

Abbildung 2. Überwachung von Störgeräten, Trends der Funkqualität und Warnungen im Cisco Wireless Control System



Möglichkeit zur Zuordnung von erkannten Geräten über mehrere Access Points

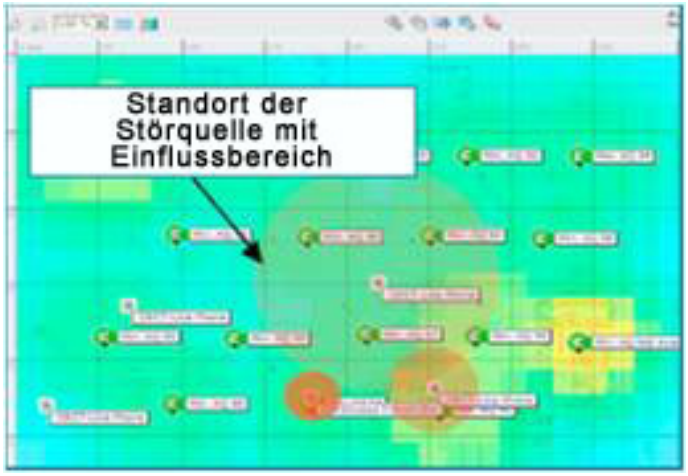
In einem WLAN mit integriertem Spektrum-Management ist es ziemlich wahrscheinlich, dass das gleiche Störgerät von mehreren Access Points erkannt wird. Wenn dieses Gerät von jedem Access Point separat gemeldet würde, würde der Administrator zu viele Warnungen erhalten. Mit der CleanAir-Technologie wird jedem von einem Access Point erkannten Gerät auf der Grundlage seiner Geräteattribute eine PMAC-Adresse (Pseudo-MAC) zugewiesen. Die PMACs werden anschließend auf den unterschiedlichen Access Points verglichen. Wenn die PMACs von zwei Geräten übereinstimmen (und sich die Access Points ausreichend nah beieinander befinden), werden die Berichte der beiden Access Points als Cluster zusammengefasst. Daraufhin kann dem Administrator dieser Cluster als einzelnes Gerät gemeldet werden.

Die Zusammenfassung in Clustern spielt auch eine entscheidende Rolle bei der Lokalisierung von Geräten. Ein Cluster von übereinstimmenden PMACs stellt dem System mehrere Leistungsmessungen des gleichen Geräts zur Verfügung, sodass der Standort des Geräts per Kreuzpeilung bestimmt werden kann. Eine wichtige Eigenschaft der Zusammenfassung von Geräten in Clustern ist die zuverlässige Zusammenfassung von Geräten, ohne dass zu viele Cluster erstellt werden (indem Geräte zusammengefasst werden, die nicht zusammengefasst werden sollten), oder dass zu wenig Cluster erstellt werden (Meldung mehrerer Geräte, obwohl nur eines vorhanden ist).

Ein weiterer Vorteil der CleanAir-Technologie ist die Möglichkeit einer Bedienung per Fernzugriff. In zahlreichen Wi-Fi-Bereitstellungen müssen IT-Mitarbeiter von einem Standort aus Geräte in mehreren Gebäuden eines Campus oder an mehreren geografisch verteilten Standorten verwalten, sodass es schwierig sein kann, ein Tool zu diesen entfernt verwalteten Standorten zu versenden. Dies gilt vor allem in Bereitstellungen mit zahlreichen Zweigstellenbüros, oder wenn die Interferenz nur zeitweilig auftritt. Durch die Integration von Spektrum-Management in die Infrastruktur können IT-Mitarbeiter Interferenzen überall im Netzwerk per Fernzugriff feststellen.

Die Cisco CleanAir-Technologie kann Störgeräte auch physisch lokalisieren (Abbildung 3). In den meisten Fällen wird das gleiche Störgerät von mehreren Access Points erkannt. Cisco hat eine leistungsfähige Technologie entwickelt, mit der sich die von mehreren Access Points gemeldeten Geräte vergleichen lassen und festgestellt werden kann, welche Berichte tatsächlich von dem gleichen Gerät hervorgerufen werden. Nachdem eine Wechselbeziehung zwischen den Geräten hergestellt wurde, lässt sich der genaue Standort des Geräts mithilfe von Kreuzpeilung genau bestimmen, ähnlich dem Verfahren, mit dem Infrastrukturgeräte zurzeit in der Lage sind, Wi-Fi-Clients und Tags zu lokalisieren.

Abbildung 3. Lokalisierung von Störgeräten und ihres Einflussbereichs



Der vermutlich größte Vorteil der Integration der CleanAir-Technologie in das WLAN besteht darin, dass SI-Daten für das RRM-System der Access Points verfügbar sind, sodass sie rund um die Uhr an sieben Tagen in der Woche für die automatisierte Vermeidung von Interferenzen verwendet werden können. Dies ist in der Tat die nächste Generation von RRM, die wesentlich zuverlässiger arbeitet als frühere Versionen, die Interferenzen gegenüber blind waren. Mit der CleanAir-Technologie kann das Netzwerk so eingestellt werden, dass zahlreiche Arten von Interferenzen automatisch umgangen werden.

Funktionen von Cisco Unified Wireless Network mit der CleanAir-Technologie

Funkqualität und Leistungswarnungen

Die Cisco CleanAir-Technologie liefert zahlreiche detaillierte Informationen zu Interferenzen. Um den Überblick über die das Netzwerk beeinträchtigenden Interferenzen zu erleichtern, werden die detaillierten Informationen in einer vereinfachten, leicht verständlichen Maßeinheit mit dem Namen Funkqualität (Air Quality, AQ) zusammengefasst. Die Funkqualität wird auf Kanal-, Etagen- und Systemebenen erfasst, und sie unterstützt Warnmeldungen, sodass Sie sich automatisch benachrichtigen lassen können, wenn die Funkqualität einen festgelegten Schwellenwert unterschreitet.

Kartenbasierte Visualisierungen

In einem WLAN mit aktivierter CleanAir-Technologie werden analysierte und erkannte Geräte auch in die visuellen Zuordnungsanzeigen der Management-Systeme Cisco Wireless Control System (WCS) und Mobility Services Engine (MSE) integriert. Sie sehen auf der Karte nicht nur die Access Points und Clients, sondern können auch feststellen, wo auf der Karte sich Störgeräte befinden.

Leistungsaspekt - Die Darstellung der Störgeräte (sowie ihrer Einflussbereiche) auf der Karte ermöglicht es, festzustellen, welche Access Points, Clients und Bereiche auf Ihrer Etage beeinträchtigt sind.

Sicherheitsaspekt - Die Kennzeichnung von Geräten auf einer Karte ermöglicht die unverzügliche Entsendung von Sicherheitspersonal zum entsprechenden Standort.

Sicherheitswarnungen

Es können nicht nur alle die Sicherheit beeinträchtigenden Geräte angezeigt werden, es können auch Warnmeldungen standortspezifisch angepasst werden, z. B. für eine bestimmte Etage im Gebäude. Diese leistungsstarke Funktion ist insbesondere dann wichtig, wenn bestimmte Geräte in einigen Bereichen eines Gebäudes (beispielsweise in der Handelsabteilung) als eine Bedrohung angesehen werden, in anderen Bereichen (z. B. im Empfangsbereich) aber nicht.

Funktionen zur Problembehebung

Die CleanAir-Technologie bietet nicht nur eine flexible Bereitstellung, sondern auch fortschrittliche automatisierte Reaktionen auf Interferenzen. Diese automatisierten Reaktionen beinhalten die Vermeidung persistenter Geräte sowie ereignisgesteuertes RRM.

Die Vermeidung persistenter Geräte erkennt, dass bestimmte Geräte einen statischen Standort und eine statische Frequenz besitzen, z. B. Mikrowellenherde und drahtlose Videokameras. Aus diesem Grund wird davon ausgegangen, dass diese Geräte an einem bestimmten Standort wieder aktiv werden, an dem sie zuvor schon einmal erkannt wurden, selbst wenn sie zurzeit nicht auf einem bestimmten Kanal an einem bestimmten Standort erkannt werden. Das System verfolgt diese Arten von Geräten und versucht bei der Kanalauswahl Kanäle an Standorten zu vermeiden, an denen persistente Geräte festgestellt wurden.

Das ereignisgesteuerte RRM erkennt, dass einige Interferenzen sehr schwerwiegend und sogar fatal sein können. Beispielsweise kann ein schnurloses Telefon mit einem kontinuierlichen Funksignal einen Ausfall von mehreren Minuten verursachen (so lange das Telefon aktiv ist). Aus diesem Grund veranlasst ein signifikanter Abfall der Funkqualität das System zu einer unverzüglichen Prüfung eines Kanalwechsels des betroffenen Access Point. Beachten Sie, dass ein Kanalwechsel nur für den betroffenen Access Point erfolgt, während nachfolgende Beeinträchtigungen des Kanalplans benachbarter Access Points vermieden werden.

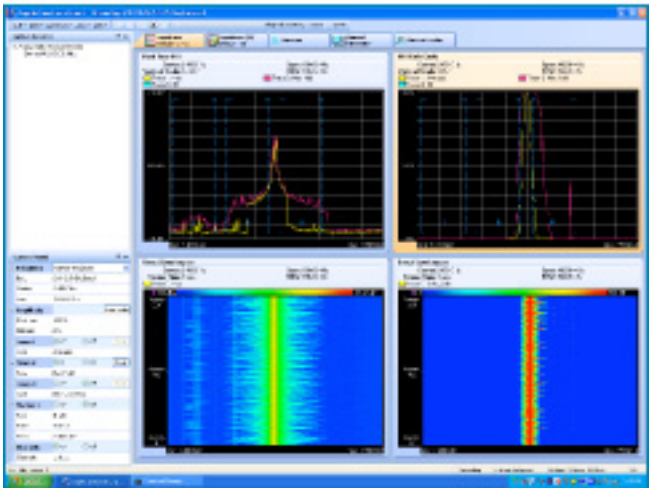
Auch wenn in zahlreichen Fällen die beste Reaktion auf eine Interferenz darin besteht, dass der Administrator das Störgerät manuell umplatziert, entfernt, ersetzt oder abschirmt, ist die automatische Problembehebung eine ausgesprochen hilfreiche Funktion, um die Leistung kurzfristig aufrechtzuerhalten, bevor andere Maßnahmen ergriffen werden können. Und in einigen Fällen kann es auch unmöglich sein, die Störquelle überhaupt zu entfernen, wenn sie sich beispielsweise außerhalb des Gebäudes befindet.

Access Points als Analysatoren

Schließlich bietet die CleanAir-Technologie weiterhin eine Expertenansicht mit detaillierten Spektrum-Plots, vergleichbar denjenigen des Analysetools „Spectrum Expert“. Jeder CleanAir Access Point kann als an das Netzwerk angeschlossener Sensor konfiguriert werden, um die Spektrum-Plots direkt anzuzeigen, wie sie von den Funkeinrichtungen des Access Point empfangen werden.

Obwohl das System umfassende und übersichtliche analysierte Daten bereitstellt, einschließlich klassifizierte Geräte und Funkqualität, wird es immer Situationen geben, in denen eine Anzeige der Spektrumrohdaten in Echtzeit bevorzugt wird. Selbst in Unternehmen, die über keinen Experten für Funktechnologie verfügen, kann die in Abbildung 4 dargestellte Funktion „Spectrum Expert Connect“ von einem Experten verwendet werden, der zu einem bestimmten Diagnoseproblem um Hilfe gebeten wird.

Abbildung 4. Verwenden der Funktion „Spectrum Expert Connect“ zur Diagnose eines Problems an einem Access Point



Schlussfolgerungen

Da Wi-Fi in einem gemeinsam genutzten unlizenzierten Band betrieben wird, sind integrierte Spektrumintelligenz und Spektrum-Management absolute Voraussetzung für die Gewährleistung von hoher Leistung, Sicherheit und Zuverlässigkeit in Ihrem Wi-Fi-Netzwerk. Spektrum-Management ist entscheidend für die Bereitstellung einer umfassenden und zuverlässigen Mobilitätsumgebung für Endbenutzer mit unternehmenswichtigen drahtlosen Anwendungen.

Da die eingeschränkten Funkerkennungsfähigkeiten von kommerziellen Wi-Fi-Chipsets nicht ausreichend sind, hat Cisco speziell für die Analyse von Interferenzen entwickelte patentierte Spektrum-Verarbeitungshardware und -software integriert und so ein Wi-Fi-Chipset in Unternehmensqualität entwickelt. Mit dieser zugrundeliegenden Chipset-Funktion kann die Cisco CleanAir-Technologie einzelne Störungsquellen klassifizieren und lokalisieren und Sie informieren, wie sich diese auf die Leistung oder Sicherheit Ihres Netzwerks auswirken.

Spektrumintelligenz (SI) ist zwar auch in der Form von Tools wie „Spectrum Expert“ verfügbar, die in der Vorbereitungsphase der Bereitstellung hilfreich sind, die beste Möglichkeit ist jedoch, SI direkt in die Infrastruktur zu integrieren. Die Cisco CleanAir-Technologie bietet leistungsstarke Spektrum-Management-Funktionen wie proaktive Überwachung von Interferenzen rund um die Uhr an 7 Tagen in der Woche, Warnmeldungen zu Spektrumsicherheit und Leistung sowie die Lokalisierung von Störgeräten. Der wichtigste Aspekt ist jedoch, dass integrierte SI eine neue Stufe von automatisiertem Spektrum-Management ermöglicht, das die Auswirkungen von Interferenzen erkennt und auf intelligente Weise eliminiert.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Gedruckt in den USA C11-599260-00 04/10

