LANCOM™ Techpaper
Smart WLAN Controlling

Der weit verbreitete Einsatz von Wireless Access Points und Wireless Routern hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt.

Im Laufe der letzten Jahre waren die drahtlosen Netzwerke dabei einem grundlegenden strukturellen Wandel unterworfen: Die autonomen Access Points der ersten Generation wurden im Zuge der rasant steigenden WLAN-Verbreitung durch zentral verwaltete Lösungen ersetzt. Um die signifikanten Nachteile der zentralisierten WLANs zu überwinden, setzen moderne WLAN-Architekturen auf eine intelligente Arbeitsteilung zwischen Access Points und WLAN-Controllern – das Smart WLAN Controlling.

WLAN-Architekturen der ersten Generation

Bei allen Vorzügen der WLANs gegenüber drahtgebundenen Netzwerken bleiben einige offene Aspekte:

- Die Installation, Konfiguration und Wartung der Access Points ist aufwendig und erfordert qualifiziertes Personal.
- Wichtige Funktionen wie das Einrichten von Gastzugängen oder die Erkennung von unerwünschten Access Points und WLAN-Clients (Rogue-Detection) müssen auf jedem Access Point separat vorgenommen werden.
- Frequenzüberlagerungen können nur durch manuelle Anpassung der verwendeten Funkkanäle vermieden werden.
- Änderungen der Konfiguration oder Struktur wirken sich nicht gleichzeitig auf alle Access Points aus, sondern erst mit zeitlichem Verzug.
- Access Points an öffentlich zugänglichen Orten stellen ein potenzielles Sicherheitsrisiko dar, weil mit den Geräten auch die darin gespeicherten, sicherheitsrelevanten Daten wie Kennwörter etc. gestohlen werden können.

Als Ergebnis steigen die Kosten für den Betrieb von WLANs drastisch mit der Anzahl der eingesetzen Access Points.

Die 2. Generation: WLAN-Switching

Der erste Ansatz zur Überwindung dieser Nachteile in großen WLAN-Installationen bestand in der vollständigen Verlagerung der „Intelligenz“ in eine zentrale Komponente, dem WLAN-Switch. Beim WLAN-Switching agieren die Access Points nur als verlängerte Antennen dieser zentralen Instanz. Die auch als „Thin Access Point“ bezeichneten Geräte benötigen keine Konfiguration und übertragen alle empfangenen Daten aus dem WLAN direkt über das LAN an den WLAN-Switch.

Das Konzept des WLAN-Switching reduziert den Aufwand und die Kosten für den Betrieb der drahtlosen Netzwerke zwar deutlich, dafür entsteht in dem WLAN-Switch ein Flaschenhals für die übertragenen Daten und ein „Single Point of Failure“. Der Ausfall des Switches würde somit zu einem Totalausfall des gesamten WLANs führen.

Smart WLAN Controlling

Das **Smart WLAN Controlling** kombiniert die Vorteile der beiden ersten Ansätze und realisiert ein WLAN-System nach den folgenden Anforderungen:

- Flexible Datenauskopplung je nach Anwendung und Benutzer:
  - Auskopplung am Access Point für Daten mit hohem Bandbreitebedarf (z. B. IEEE 802.11n) oder für Access Points an entfertner Standorten.
  - Auskoppeln am WLAN-Controller zur Realisierung des Layer-3-Roaming für Anwendungen wie VoWLAN oder Gastzugänge.
- Alle Access Points und Wireless Router werden zentral im WLAN-Controller authentifiziert und konfiguriert.
- Reduzierung der anfänglichen Installationskosten durch schnellere Ausbreitung der Access Points.
- Firmware-Updates können von zentraler Stelle aus und idealerweise automatisch durchgeführt werden.
- Ausweitung der sicherheitsrelevanten Zonen auch auf angeschlossene Access Points in Home-Offices oder Filialen.
- Automatische Funkfeldoptimierung für den störungsfreien Betrieb von WLANs innerhalb der Reichweite anderer Access Points.
- Layer-3-Roaming zur Überwachung von kritischen IP-Verbindungen im zentralen WLAN-Controller.
- Sicheres Fall-Back- und Redundanz-Konzept bei Ausfall des WLAN-Controllers ohne Speichern sicherheitsrelevanter Daten in den Access Points.
- Automatische Zuordnung der WLAN-Clients zu bestimmten Netzwerken.
- Zentrale Rogue-AP- und Client-Detection.

Die folgenden Abschnitte zeigen, wie diese Ziele des Smart WLAN Controllings auf Basis des CAPWAP-Standards erreicht werden.

Der CAPWAP-Standard

Mit dem CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) stellt die IETF (Internet Engineering Task Force) einen Draft-Standard für das zentrale Management großer WLAN-Strukturen vor.

CAPWAP verwendet unterschiedliche Kanäle für die Datenübertragung:

- Kontrollkanal, verschlüsselt mit DTLS. Über diesen Kanal werden die Verwaltungsinformationen zwischen dem WLAN-Controller und dem Access Point ausgetauscht.
- Datenkanal, optional ebenfalls verschlüsselt mit DTLS. Über diesen Kanal werden die Nutzdaten aus dem WLAN vom Access Point über den WLAN-Controller ins LAN übertragen – gekapselt in das CAPWAP-Protokoll.

LANCOM Systems

LANCOM™ Techpaper
Smart WLAN Controlling

Das Smart WLAN Controlling nutzt gezielt die Möglichkeiten der unterschiedlichen CAPWAP-Kanäle: Nur die Daten, die für den WLAN-Controller wichtig sind, werden durch den CAPWAP-Tunnel zum Controller geleitet. Das deutliche größere Datenvolumen der Nutzdaten kann direkt am Access Point ausgekoppelt und ins LAN übertragen werden.

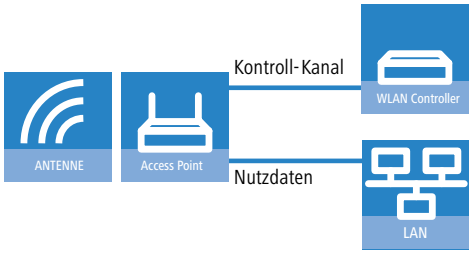
Die Smart-Controller-Struktur

In einer dezentralen WLAN-Struktur mit autonomen Access Points (Stand-Alone-Betrieb als so genannte „Rich Access Points") sind alle Funktionen für die Datenübertragung, die Kontroll-Funktionen sowie die Management-Funktionen in den Access Points enthalten. Mit dem zentralen WLAN-Management werden diese Aufgaben auf zwei verschiedene Geräte aufgeteilt:

- Der zentrale WLAN-Controller übernimmt die Verwaltungsaufgaben.
- Die verteilten Access Points übernehmen die Datenübertragung.

CAPWAP beschreibt drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLAN-Controller.

- Remote-MAC: Hier werden **alle** WLAN-Funktionen vom Access Point an den WLAN-Controller übertragen. Die Access Points dienen hier nur als „verlängerte Antennen" ohne eigene Intelligenz.
- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLAN-Controller übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem Access Point abgearbeitet, die nicht zeitkritischen Anwendungen (Non-Realtime-Applikationen) werden über den zentralen WLAN-Controller abgewickelt.
- Local-Mac: Die dritte Möglichkeit sieht eine vollständige Verwaltung und Überwachung des WLAN-Datenverkehrs direkt in den Access Points vor. Zwischen dem Access Point und dem WLAN-Controller werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration der Access Points und zum Management des Netzwerks ausgetauscht.



Das Smart WLAN Controlling setzt das Local-MAC-Verfahren ein. Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der WLAN-Controller in einer solchen Struktur nicht zum zentralen Flaschenhals, der große Teile des gesamten Datenverkehrs verarbeiten muss. In Remote-MAC- und Split-MAC-Architekturen müssen immer **alle** Nutzdaten zentral über den WLAN-Controller laufen. In Local-MAC-Architekturen können die Nutzdaten jedoch alternativ auch direkt von den Access Points in das LAN ausgekoppelt werden, sodass eine hochperformante Datenübertragung ermöglicht wird.

Der Smart Controlling-Ansatz eignet sich daher auch für WLANs nach dem Standard IEEE 802.11n mit deutlich höheren Datenraten als in den bisher bekannten WLANs. Bei der Auskopplung in das LAN können die Daten auch direkt in spezielle VLANs geleitet werden, die Einrichtung von geschlossenen Netzwerken z. B. für Gast-Zugänge sind so leicht möglich.

Authentifizierung und Konfiguration

Die Kernaufgabe des WLAN-Controllers besteht darin, den angeschlossenen Access Points jederzeit eine aktuelle Konfiguration zuweisen zu können. Damit der WLAN-Controller entscheiden kann, ob er einem anfragenden Access Point ein solche Konfiguration überhaupt zuweisen darf, muss sich der Access Point zu Beginn der Kommunikation authentifizieren. Die Authentifizierung wird dabei auf Basis von digitalen Zertifikaten durchgeführt.

Bei einem Rollout von Access Points in größeren Installationen, die sich teilweise auch über mehrere Standorte hinweg erstrecken können, sind die benötigten Zertifikate jedoch noch nicht in den Access Points vorhanden. LANCOM WLAN Controller bieten daher eine Funktion, mit der das Zertifikat zu Beginn der Verhandlung an den Access Point übertragen werden kann. Dabei werden nur solche Access Points berücksichtigt, die bereits über einen entsprechenden Eintrag im WLAN-Controller bekannt sind. Alternativ können mit der „Auto-Accept"-Funktion

LANCOM Systems

LANCOM™ Techpaper
Smart WLAN Controlling

für einen kurzen Zeitraum alle im LAN angeschlossenen Access Points – auch ohne Eintrag im WLAN-Controller – akzeptiert und mit einem gültigen Zertifikat ausgestattet werden.

Mit Hilfe des Zertifikats kann sich der Access Point in der Folgezeit gegenüber dem WLAN-Controller authentifizieren und erhält von diesem eine gültige Konfiguration. Die Konfiguration für einen Access Point wird anhand der MAC-Adresse gezielt im WLAN-Controller hinterlegt. Auch bei der Zuweisung der Konfiguration können Access Points ohne Eintrag im WLAN-Controller berücksichtigt werden: eine Default-Konfiguration kann für diese Geräte den Betrieb im WLAN ermöglichen.

Die eigentlichen Konfigurationsdaten für die Access Points werden in so genannten „Profilen" im WLAN-Controller hinterlegt und von dort an die Access Points übertragen.

Rollout mit Zero-Touch-Management

Mit der Auto-Accept-Funktion und der Default-Konfiguration bieten LANCOM WLAN Controller die Möglichkeit, den anfragenden Access Points Zertifikate und Konfigurationen automatisch zuweisen zu lassen und realisieren so ein echtes „Zero-Touch-Management". Neue Access Points müssen nur noch mit dem LAN verbunden werden, es sind keine weiteren Konfigurationsschritte erforderlich. Diese Reduzierung auf die reine Installation der Geräte entlastet die IT-Abteilungen gerade bei verteilten Strukturen, da an den entfernten Standorten kein spezielles IT- oder WLAN-Know-How zur Inbetriebnahme erforderlich ist.

Vererbung von Parametern

Mit einem LANCOM WLAN Controller können sehr viele unterschiedliche Access Points an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten Access Points gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können bestimmte WLAN-Parameter ausgewählte Eigenschaften von anderen Einträgen „erben".

Bei der Vererbung sind auch Ketten über mehrere Stufen (Kaskadierung) möglich. So können z. B. länder- und gerätespezifische Parameter komfortabel zusammengestellt werden. Auch Rekursionen sind möglich – Profil A erbt von Profil B, gleichzeitig erbt B aber auch von A.

Split-Management für entfernte Access Points

LANCOM Access Point können ihren WLAN-Controller in entfernten Netzen suchen – eine einfache IP-Verbindung z. B. über eine VPN-Strecke reicht aus. Da die WLAN-Controller nur den WLAN-Teil der Konfiguration im Access Point beeinflussen, können alle anderen Funktionen separat verwaltet werden. Durch diese Aufteilung der Konfigurationsaufgaben können LANCOM WLAN Controller ideal für den Aufbau einer firmenweiten WLAN-Infrastruktur in der Zentrale inklusive aller angeschlossenen Niederlassungen und Home-Offices eingesetzt werden. Fehlkonfigurationen der WLAN-Einstellungen in den entfernten Access Points, durch die unerlaubte Clients Zugang zum Firmennetzwerk erhalten, werden so verhindert.

Layer-3-Tunneling und Layer-3-Roaming

Generell setzt das Smart WLAN Controlling auf die Trennung der Nutzdaten von den Kontrolldaten: Nur die für den WLAN-Controller relevanten Kontrolldaten werden durch den Layer-3-Tunnel übertragen, das restliche und deutlich größere Datenvolumen wird von den Access Point direkt in das LAN ausgekoppelt. Auf diese Weise wird der Datendurchsatz im WLAN-Controller deutlich reduziert, so dass der WLAN-Controller nicht zum zentralen Flaschenhals wird.

In manchen Anwendungen ist es jedoch erwünscht, dass auch die Nutzdaten durch den Layer-3-Tunnel an den WLAN-Controller übertragen werden. Bei Applikationen wie Voice over WLAN (VoWLAN) können WLAN-Clients in eine andere Funkzelle wechseln, die zugrunde liegende IP-Verbindung bleibt jedoch ohne Unterbrechung, da sie fortlaufend vom zentralen WLAN-Controller verwaltet wird (Layer-3-Roaming). Mobile SIP-Telefone können auf diese Weise auch während eines Gesprächs komfortabel „roamen".

Zentrales Firmware- und Skript-Management

Mit dem zentralen Firmware- und Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt. Der WLAN-Controller prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion den Bestand und vergleicht die verfügbaren Dateien mit den Versionen in den Geräten – alternativ kann dieser Vorgang auch über einen Cron-Job z. B. nachts erledigt werden. Wenn ein Update durchgeführt werden kann, oder nicht die gewünschte Version auf dem

LANCOM™ Techpaper
Smart WLAN Controlling

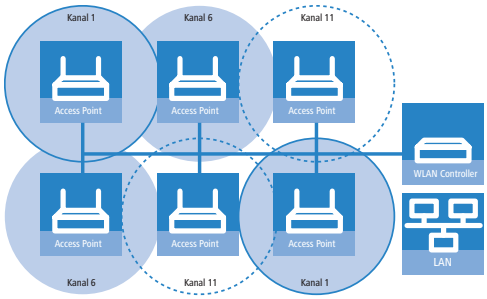
Access Point läuft, lädt der WLAN-Controller diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und Access Points ein.

Mit der Einstellung des Firmware- und Skript-Managements kann die Distribution der Dateien gezielt gesteuert werden. So kann die Nutzung von bestimmten Firmware-Versionen z. B. auf bestimmte Gerätetypen oder MAC-Adressen beschränkt werden.

Automatische Funkfeldoptimierung

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein Access Point für seine logischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem Access Point verbinden wollen, müssen den gleichen Kanal im gleichen Frequenzband verwenden. Im 2,4 GHz-Band stehen je nach Land die Kanäle 1 bis 13, im 5 GHz-Band die Kanäle 36 bis 64 zur Verfügung. Auf einem Kanal kann dabei jeweils nur ein Access Point Daten übertragen. Um in der Funkreichweite eines anderen Access Points ein WLAN störungsfrei betreiben zu können, muss jeder Access Point einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.

Mit der automatischen Funkfeldoptimierung bieten die LANCOM WLAN Controller ein Verfahren, um die optimalen Kanäle der Access Points für das 2,4 GHz-Band automatisch einzustellen. Dabei werden im ersten Schritt die Kanal-Listen der Access Points gelöscht und durch den WLAN-Controller neu definiert. Anschließend werden die WLAN-Module ausgeschaltet und sukzessive wieder eingeschaltet. Beim Einschalten suchen die Module dann automatisch einen freien Kanal und optimieren so die Verteilung der Kanäle im Funkfeld.



Die automatische Funkfeldoptimierung kann gemeinsam für alle von einem WLAN-Controller verwalteten Access Points oder gezielt nur für einzelne Geräte gestartet werden.

Autarker Weiterbetrieb

In Installationen mit einem einzigen WLAN-Controller wird dieses Gerät zum „Single Point of Failure": bei einer Störung sind sofort alle angeschlossenen WLANs ebenfalls gestört.

LANCOM WLAN Controller bieten die Möglichkeit des autarken Weiterbetriebs der Wireless Router und Access Points auch bei einer vorübergehenden Störung der zentralen Verwaltung. Da die komplette Verwaltung der Nutzdaten beim Smart WLAN Controlling weiterhin auf den Access Points verbleibt, muss der WLAN-Controller nur für die Aktualisierung der Konfiguration sorgen.

Die Konfiguration wird dem Access Point vom WLAN-Controller zugewiesen und normalerweise nur im RAM gespeichert. Zur Erhöhung der Betriebssicherheit können die Konfigurationsdaten jedoch auch optional im Flash gespeichert werden (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLAN-Controller unterbrochen wird, arbeitet der Access Point für eine zuvor definierte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der Access Point mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist und die Verbindung zum WLAN-Controller noch nicht wiederhergestellt wurde, wird die Konfiguration im Flash gelöscht – der Access Point stellt seinen Betrieb ein. Sobald der WLAN-Controller wieder erreichbar ist, wird die Konfiguration erneut vom WLAN-Controller zum Access Point übertragen. Durch diese Option kann der Access Point auch dann weiter arbeiten, wenn die Verbindung zum WLAN-Controller kurzfristig unterbrochen wird.

Eigene IP-Netzwerke für Access Points

Mit der Konfiguration von eigenen IP-Parametern können die Access Points weiter unabhängig vom zentralen WLAN-Controller gemacht werden. Dabei werden wichtige IP-Parameter wie Domäne, Netzmaske, Gateway oder DNS-Server-Adressen für jeden Access Point separat definiert – mit dieser IP-Konfiguration arbeitet das Gerät im laufenden Betrieb auch dann, der WLAN-Controller ausfällt. Somit ist DHCP nur noch für das erstmalige Finden eines WLAN-Controllers nötig und wird nach einmaliger Konfiguration des Access Points durch den WLAN-Controller nicht mehr benutzt.

Backup-Lösungen

LANCOM WLAN Controller verwalten eine große Zahl von Access Points, bei denen wiederum zahlreiche WLAN-Cli-

LANCOM Systems

LANCOM™ Techpaper
Smart WLAN Controlling

ents eingebucht sein können. Die WLAN-Controller haben daher eine zentrale Bedeutung für die Funktionsfähigkeit der gesamten WLAN-Struktur – die Einrichtung einer Backup-Lösung für den vorübergehenden Ausfall eines WLAN-Controllers ist daher in vielen Fällen unverzichtbar.

In einem Backup-Fall soll sich ein gemanagter Access Point mit einem anderen WLAN-Controller verbinden. Da diese Verbindung nur gelingen kann, wenn das Zertifikat des Access Points von dem Backup-Controller authentifiziert wird, verwenden alle WLAN-Controller in einer Backup-Lösung identische Root-Zertifikate.

Für die Backup-Struktur selbst stehen zwei Ansätze zur Auswahl:

- Beim Backup mit redundanten WLAN-Controllern wird jedes Gerät 1:1 durch ein zweites Gerät abgesichert. Im Backup-Controller sind dabei neben den identischen Zertifikaten auch alle Profile und Konfigurationen des WLAN-Controllers redundant vorhanden.
- Beim Einsatz mehrerer WLAN-Controller können sich die Geräte untereinander absichern und im Backupfall die Access Points eines anderen WLAN-Controllers mit verwalten. Dazu werden mehr WLAN-Controller im Verbund eingesetzt, als eigentlich für die Verwaltung der vorhandenen Access Points notwendig wären. Die Access Points werden dann in die AP-Tabelle von allen WLAN-Controllern eingetragen, damit bei Ausfall eines WLAN-Controllers ein anderes Gerät die entsprechenden Profile zuweisen kann.

  Ein LANCOM WLAN Controller kann in seiner AP-Tabelle die fünffache Anzahl der von ihm selbst maximal verwalteten Access Points aufnehmen. Für jeweils fünf WLAN-Controller (mit gleicher Ausstattung) reicht also ein zusätzlicher WLAN-Controller aus, um eine vollständige Absicherung bei Ausfall eines Gerätes zu realisieren.

Authentifizierung und Accounting für WLAN-Clients

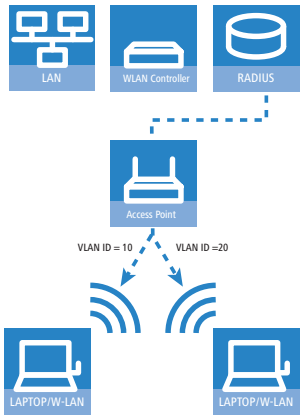
Zur Realisierung einer Zugangsprüfung bzw. zur Abrechnung evtl. fälliger Gebühren wird in der Regel ein RADIUS-Server eingesetzt. Für den Zugriff auf einen RADIUS-Server durch die Access Points stehen zwei Varianten zur Auswahl:

- Wenn keine besondere Konfiguration vorgenommen wird, reichen die Access Points alle RADIUS-Anfrage der WLAN-Clients an den zentralen WLAN-Controller weiter. der WLAN-Controller verwendet dann entweder seine eigene Benutzertabelle oder gibt seinerseits die RADIUS-Anfrage an den bei ihm definierten Server weiter.
- Um auch die RADIUS-Anfragen unabhängig vom zentralen WLAN-Controller zu machen, kann in den Profilen für die Access Point ein eigener RADIUS-Server konfiguriert werden. In diesem Falle leitet der Access Point die RADIUS-Anfragen nicht über den WLAN-Controller, sondern koppelt diese direkt in das LAN an den gewünschten RADIUS-Server aus.

Dynamische VLAN-Zuweisung

In einer größeren WLAN-Struktur ist es oft sinnvoll, den einzelnen WLAN-Clients ein bestimmtes Netzwerk zuzuweisen. Solange sich die WLAN-Clients immer in der Reichweite des gleichen Access Points befinden, kann diese Zuweisung über die SSID in Verbindung mit einem bestimmten IP-Netzwerk realisiert werden. Wechseln die WLAN-Clients hingegen häufig die Position und buchen sich dann bei unterschiedlichen Access Points ein, befinden sie sich je nach Konfiguration in einem anderen IP-Netzwerk.

Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID wird die VLAN-ID dabei dem WLAN-Client von einem RADIUS-Server direkt zugewiesen.



Beispiel: Zwei WLAN-Clients buchen sich über den gleichen Access Point in das WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den Access Point gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLAN-Controller weitergereicht. Dieser

LANCOM Systems

LANCOM™ Techpaper
Smart WLAN Controlling

leitet die Anfragen seinerseits an den konfigurierten RADIUS-Server weiter. Der RADIUS-Server kann die Zugangsberechtigung der WLAN-Clients prüfen. Darüber hinaus kann er allerdings auch z. B. anhand der MAC-Adresse eine bestimmte VLAN-ID zuweisen. Dabei erhält z. B. der WLAN-Client **A** die VLAN-ID '10' und der WLAN-Client **B** die '20'.

Fazit

Das Smart WLAN Controlling von LANCOM Systems bietet eine ganze Reihe an Funktionen für den komfortablen Betrieb von großen WLAN-Installationen.

Automatische Authentifizierung und Konfiguration erleichtern den Rollout auch an Standorten ohne geschultes IT-Personal. Mit automatischen Firmware-Updates können die Access Points jederzeit aktuell gehalten werden und die Nutzung der freien Funkkanäle kann ebenfalls automatisch optimiert werden.

Durch die gezielte Trennung der Nutzdaten von den Kontrolldaten erreichen die LANCOM WLAN Controller einen idealen Lastausgleich im Netzwerk und vermeiden den Datenstau im Controller. Für einzelne Anwendungen können die Nutzdaten gezielt über den WLAN-Controller geführt werden, um unterbrechungsfreie IP-Beziehungen auch bei Wechsel der Funkzelle zu ermöglichen (Layer-3-Roaming).

Die WLAN-Konfiguration an entfernten Standorten mit Split-Management bezieht auch Home-Offices oder Filialen in das WLAN-Sicherheitskonzept mit ein, und die dynamische VLAN-Zuweisung eignet sich hervorragend zur Abschirmung der kritischen Netzwerksegmente bei Gast-Zugängen.

Eine kurzfristige Störung des WLAN-Controllers können die Access Points vorübergehend autark überbrücken, für eine höhere Ausfallsicherheit stehen verschiedene Backup-Strategien zur Verfügung.

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de I Internet www.lancom.de

LANCOM Systems