APs unter Kontrolle

Aufbau und Management sicherer WLAN-Infrastrukturen

Kai-Oliver Detken

WLANs (Wireless Local Area Network) haben sich in Unternehmen längst etabliert, trotz der weiteren Entwicklung der Festnetze. Dies hängt zum einen damit zusammen, dass auch die WLAN-Techniken nicht stehengeblieben sind und immer neuere Innovationssprünge vollziehen. Zum anderen lassen manche Anwendungen und mobile Endgeräte keine andere Technik zu. So ist ein verstärktes Aufkommen von Smartphones und Tablet-PCs in den Unternehmen zu verzeichnen, die sich natürlich in sinnvoller Weise nur über WLANs anbinden lassen. Der Verwaltung dieser sicherheitssensiblen IT-Infrastruktur kommt daher eine bedeutende Rolle zu.

Nachdem der 802.11-Standard mit einer niedrigen Bruttodatenrate von 1 – 2 Mbit/s vor ca. 15 Jahren startete, hat sich viel in der Entwicklung getan. Damals wurden WLANs kaum eingesetzt; ihre Nettodatenrate war einfach zu gering, um Laptops sinnvoll anschließen zu können. Erst der Standard 802.11b brachte 1999 den Durchbruch, durch die Erweiterung der physischen Schicht auf eine Bruttoübertragungsrate von immerhin 11 Mbit/s. Dies entsprach einer Nettodatenrate von 4 Mbit/s, wenn man sich quasi allein im Sende- und Empfangsbereichs eines Access Points (AP) befand. Diese Übertragungsrate war für Laptops bereits akzeptabel, wenn sich die Teilnehmerdichte in Grenzen hielt, und für kleinere mobile Geräte wie Handys, PDAs, Lagerscanner allemal ausreichend. Aus diesem Grund sind diese WLAN-APs auch heute noch in großer Anzahl anzutreffen.

Trotzdem begnügte man sich nicht mit dieser Entwicklung, da man auch eine Alternative zum Festnetz schaffen wollte. Dementsprechend wurde die physische Schicht durch die Standards 802.11g, 802.11a, 802.11h und 802.11n immer weiter verbessert. Die ersten drei Spezifikationen hoben die Bruttodatenrate auf 54 Mbit/s, wobei sich die 802.11g-Variante am besten durchsetzen konnte. Sie baut auf dem gleichen Modulationsverfahren wie seine Vorgänger auf und sendet im gleichen Frequenzband (2,4 GHz – 2,4835 GHz) lizenzkostenfrei. Dies ist bei den anderen beiden Verfahren nicht der Fall. Sie hoben das Frequenzband auf 5 GHz an, um weniger Störungen von bereits verlegten WLAN-Infrastrukturen und anderen Drahtlostechniken wie z.B. Bluetooth zu bekommen und größere Entfernungen drahtlos überbrücken zu können. Dabei hatte man aber nicht bedacht, dass in diesem Frequenzbereich auch militärische Radar- und Satellitensysteme zum Einsatz kommen, was zumindest in Deutschland dazu führte, diesen Frequenzbereich erst einmal nicht zuzulassen. Aus diesem Grund haben beide Standards hierzulande heute eigentlich keine Bedeutung mehr, obwohl ein 5-GHz-Betrieb seit 2007 möglich wäre.

Standard	Bruttodatenrate	Frequenzbereich	Modulation
802.11	1-2 Mbit/s	2,400 - 2,485 GHz	FHSS, DSSS
802.11b	11 Mbit/s	2,400 - 2,485 GHz	DSSS
802.11a	54 Mbit/s	ca. 5,2 - 5,8 GHz	OFDM
802.11h	54 Mbit/s	ca. 5,2 - 5,8 GHz	OFDM, DFS, TPC
802.11g	54 Mbit/s	2,400 - 2,485 GHz	DSSS
802.11n	600 Mbit/s	2,4 und 5 GHz	OFDM, MIMO

Tabelle 1: Vergleich der unterschiedlichen WLAN-Standards

Seitdem im Jahr 2003 der 802.11g-Standard heraus kam, arbeitete man weiter an einer Erhöhung der Datenrate. Beispielsweise sollte mit dem Standard 802.11n die Datenrate signifikant auf 600 Mbit/s erhöht werden. Der Fortschritt bei der Spezifikation dieses neuen Standards verzögerte sich allerdings zunehmend, so dass immer mehr Hersteller mit proprietären Lösungen auf den Markt kamen. Erst im Jahr 2009 wurde der Draft von 2006 endgültig von der IEEE ratifiziert. So konnten nicht vor 2010 standardkonforme Lösungen entwickelt werden. Selbst heute sind daher noch proprietäre Systeme am Markt vorhanden, die nicht exakt nach der aktuellen Spezifikation arbeiten.

Der Standard 802.11n hatte allerdings auch einige technische Hürden zu nehmen. So nutzt diese Technik das MIMO-Verfahren (Multiple Input Multiple Output), um entweder die gleiche Datenrate über größere Distanzen oder höhere Datenrate über geringere Distanzen zu ermöglichen. Die Ver-

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

breiterung der Übertragungskanäle von 20 MHz auf 40 MHz und der Einsatz von gleichzeitig vier Antennen ermöglichte dann diese hohe Datenrate. Das heißt, eine Antenne muss eine Bruttodatenrate von 150 Mbit/s erreichen, damit bei voller Ausnutzung der 600 Mbit/s die Antennenleistungen gebündelt werden können. Manche Hersteller (z.B. D-Link) schaffen die volle Datenrate aber auch bereits mit drei Antennen, indem zwei Datenströme mit je 300 Mbit/s unterstützt werden. Der neue Standard ist mit den älteren kompatibel, so dass auch ein Technikmix möglich ist. Allerdings kann es bei Parallelnutzung zu Leistungsabfällen kommen, weshalb auch eine Deaktivierung des sog. Greenfield-Modus oftmals anzuraten ist.

Zentrales Management

Nachdem WLAN-Access-Points immer mehr Einzug in Unternehmensgebäude und Lagerhallen gehalten haben, wurde das Management der Einzelkomponenten immer aufwendiger. Da gerade im Wireless-Umfeld die IT-Sicherheit im Vordergrund steht, musste ohne zentrales Management jeder einzelne AP kontinuierlich auf dem neuesten Stand gehalten werden, was ab einer bestimmten Unternehmensgröße nicht mehr effizient möglich war. Es lassen sich daher folgende offene Aspekte durch ein fehlendes Management ableiten:

- Alle WLAN-APs benötigen dieselbe Konfiguration und ein entsprechendes Monitoring zum Erkennen von unerwünschten WLAN-Clients.
- Die Administration erfordert bei größeren WLAN-Infrastrukturen aufgrund der einzustellenden Sicherheitsmechanismen eine höhere Qualifikation und Erfahrung.
- Die manuelle Anpassung der Konfiguration hat zur Folge, dass es unterschiedliche Firmware-Versionen und Einstellungen auf den WLAN-APs gibt, da diese Form der Administration erhebliche Zeitressourcen bindet.
- Durch die gemeinsame Nutzung des Übertragungsmediums Luft ist eine effektive Koordinierung der WLAN-APs notwendig, um Frequenzüberlagerungen zu vermeiden und die Netz-Performance zu optimieren.
- WLAN-APs an öffentlich zugänglichen Orten könnten entwendet und die sicherheitsrelevanten Daten ausgelesen werden.
- Es können unbemerkt fremde WLAN-APs mit dem LAN verbunden werden und so die geltenden Sicherheitsregeln umgangen werden.

Durch ein zentrales WLAN-Management lassen sich solche Probleme in den Griff bekommen. Die Konfiguration der WLAN-APs wird dann durch eine zentrale Instanz – den WLAN-Controller – vorgenommen. Er authentifiziert die einzelnen WLAN-APs und überträgt den Geräten die vorher festgelegte Konfiguration. Dadurch kann die Verwaltung aller Einzelkomponenten zentral von einer Stelle aus erfolgen. Konfigurationsänderungen werden nur einmal vorgenommen und zeitgleich auf alle Knoten überspielt. Optional könnte die Konfiguration auch im RAM und nicht im Flash der WLAN-APs hinterlegt werden, damit auch bei einem Diebstahl keine sicherheitsrelevanten Daten abgefragt werden können.

Die IETF hat mit dem Protokoll „Control and Provisioning of Wireless Access Points“ (Capwap) nach RFC-5415 einen Standard für das zentrale Management geschaffen. Capwap verwendet einen verschlüsselten Kontrollkanal für die Verwaltungsinformationen zwischen dem WLAN-Controller und den WLAN-APs sowie einen verschlüsselten Datenkanal für die Nutzdaten. In einer dezentralen WLAN-Umgebung besitzt jeder WLAN-AP alle Funktionen, wie Datenübertragung auf der physischen Schicht (PHY), Kontrollfunktionen auf dem MAC-Layer und Managementfunktionen. Mit Hilfe der zentralen Struktur werden diese Aufgaben aufgeteilt:

- Der zentrale WLAN-Controller übernimmt die Verwaltungsaufgaben.
- Die verteilten WLAN-APs übernehmen die Datenübertragung auf dem PHY-Layer und die MAC-Funktionen.
- Optional kann eine dritte Komponente zur Authentifizierung der WLAN-Clients eingesetzt werden (z.B. ein Radius-Server).

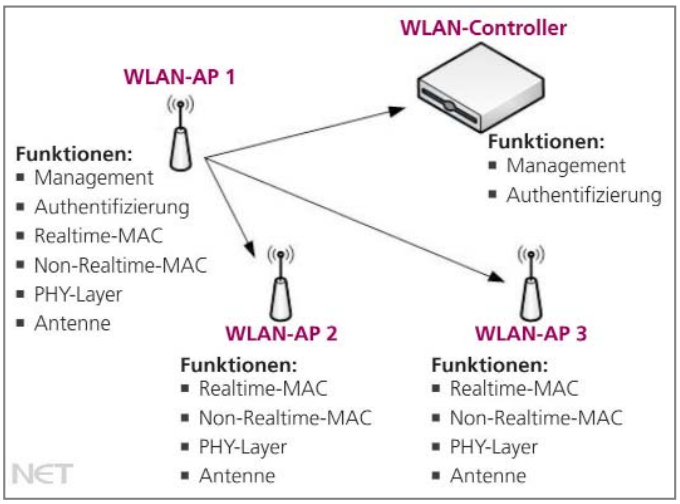

Bild 1: Capwap-Variante Local-MAC

Capwap beschreibt nun drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLAN-Controller:

- Remote-MAC: Hier werden alle WLAN-Funktionen vom WLAN-AP an den WLAN-Controller übertragen. Die WLAN-APs dienen nur als verlängerte Antenne, ohne eigene Intelligenz.
- Split-MAC: Hier wird nur ein Teil der WLAN-Funktionen an den WLAN-Controller übertragen. Alle zeitkritischen Anwendungen werden normalerweise weiterhin über den WLAN-AP abgearbeitet, während die nicht zeitkritischen Anwendungen über den WLAN-Controller abgewickelt werden.
- Local-MAC: Sieht eine vollständige Verwaltung und Überwachung des Datenverkehrs direkt in den WLAN-APs vor. Zwischen dem WLAN-Controller und den WLAN-APs werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration und zum Management des Netzes ausgetauscht.

Die letzte Variante bietet letztendlich die optimalste Skalierbarkeit, da die

zentralisierten Aufgaben reduziert über das Netz geschickt werden. Auch wird dadurch der zentrale WLAN-Controller nicht zum Engpass, da er nicht große Teile des Datenverkehrs verarbeiten muss. Das heißt, die WLAN-APs können die Daten alternativ auch direkt in das lokale Netz schicken. Das hat auch Vorteile, z.B. bei einem etwaigen Ausfall des WLAN-Controllers. Der stellt nämlich in den anderen beiden Varianten einen Single Point of Failure (SPoF) dar, wodurch auch dieser wieder doppelt ausgelegt werden müsste. Durch die direkte Auskopplung in das Netz lässt sich der hochleistungsfähige neue Standard 802.11n auch effektiver nutzen und belastet nicht zusätzlich den WLAN-Controller.

Hat man erst einmal eine solche zentralisierte Managementinfrastruktur geschaffen, kann das Netz wesentlich besser als vorher verwaltet werden. Alle bekannten WLAN-APs sind im WLAN-Controller gelistet. Dieser kann dann automatisiert die Sende- und Empfangsleistungsstärke der einzelnen Knotenpunkte optimiert regulieren. Auch die Kanäle lassen sich so automatisch einstellen, so dass bei einer Neuinstallation der Aufwand ebenfalls verringert wird oder je nach Änderung der Räumlichkeiten eine kontinuierliche Anpassung stattfindet. WLAN-APs, die nicht bekannt sind, werden nicht in die vorhandene WLAN-Infrastruktur aufgenommen und stehen dadurch auch im Unternehmensnetz nicht zur Verfügung.

Als weiteres Leistungsmerkmal lässt sich die Möglichkeit des Layer-3-Tunneling oder Roaming nennen. Durch das Tunneling können ausgewählte Applikationen wie Voice over IP (VoIP) über den zentralen WLAN-Controller transportiert werden. Bei einem Wechsel des WLAN-AP wird die IP-Verbindung dann ohne Unterbrechung weitergeleitet (Roaming), da diese kontinuierlich von dem WLAN-Controller überwacht wird. Zudem entfällt in solchen Umgebungen die Konfiguration von VLANs auf den Switch-Ports, da alle Capwap-Tunnel zentral verwaltet werden.

Standard	Beschreibung	Verabschiedung
802.11e	Dienstegüte und Streaming: Unterstützung von Quality of Service (QoS)	2004
802.11f	Handover: Interoperabilität zwischen Basisstationen	2003
802.11k	bessere Möglichkeiten für Funkparameter (z.B. Signalstärke)	2007
802.11m	Maintenance: Ergänzungen und Fehlerauslese	2006
802.11p	Kommunikation von Fahrzeug zu Fahrzeug	2010
802.11r	schneller Handover: Erweiterung vom f-Standard für VoIP	2008
802.11s	vermaschte Netze: für MAC-Ebene	in Arbeit
802.11t	Messverfahren: Leitungsparameter	in Arbeit
802.11u	Internetworking: Bindung zu Nicht-802-Netzen	2011
802.11v	Netzmanagement	in Arbeit
802.11w	Sicherheitserweiterung für Management Frames	in Arbeit
802.11ac	Wireless Computer Networking	in Arbeit

Tabelle 2: Auswahl von IEEE-WLAN-Standards

Ausblick

Bei der Einführung von WLANs war man anfangs nur von einer reinen Datennutzung ausgegangen. Das änderte sich spätestens mit der immer größeren Anzahl von VoIP-Systemen, die auch die Anbindung mobiler SIP-Clients notwendig werden ließ. Damit die Echtzeitdaten gegenüber dem reinen Datenverkehr geschützt werden können, wurde der Standard 802.11e eingeführt. Dieser ermöglichte es, dass VoIP-Sender die Sprachpakete im WLAN mit einer Priorität versehen können, damit diese bevorzugt behandelt werden. Das funktioniert ähnlich dem Quality-of-Service-Verfahren Differentiated Services (DiffServ) nach RFC-2474. Der Standard ermöglicht, eine gewisse Bandbreite im Netz für VoIP zu reservieren und die Latenz gering zu halten. Das Verfahren ist aber nicht mit einer Qualitätsgarantie gleichzusetzen. Weitere wichtige Standards für VoIP sind Handover-Unterstützung nach 802.11f und 802.11r. Letzterer ist speziell für VoIP verbessert worden.

Ein weiterer interessanter Standard, der sich aber noch in Arbeit befindet, ist 802.11s. Dieser implementiert als Hauptfunktionen den Verbindungsaufbau und das Routing für drahtlose vermaschte Netze, die nicht kabelgebunden untereinander verbunden sind. Dadurch kann eine flächendeckende Abdeckung ermöglicht werden, ohne physische Infrastruktur. Im Gegensatz zu heutigen Ansätzen, arbeitet man hier auf der MAC-Ebene und ermöglicht daher eine höhere Effizienz, die sich im geringeren Energieverbrauch und in geringeren Hardwareanforderungen niederschlägt. Der Standard 802.11p soll hingegen die WLAN-Technik in Personenkraftwagen etablieren, um eine zuverlässige Schnittstelle für Anwendungen intelligenter Verkehrssysteme zu schaffen.

Aber auch bei der Datenübertragung wird nicht Halt gemacht. Die Bestrebungen bei der Entwicklung des Standards 802.11ac haben eine Bruttoübertragungsrate von mindestens 1 Gbit/s zum Ziel. Das bedeutet, dass man die MIMO-Streams noch weiter bündeln muss – entsprechend sind bis zu acht separate MIMO-Streams vorgesehen. Zusätzlich ist eine weitere Verbreiterung der Übertragungskanäle auf 80 MHz definiert worden, optional sogar auf 160 MHz. Der Standard wird ausschließlich im 5-GHz-Band arbeiten, um vorhandene WLANs nicht zu stören. Durch das sog. Beamforming arbeiten die verschiedenen Antennen noch effizienter zusammen, um ein stärkeres Signal zum Empfänger zielgerichtet senden zu können (siehe auch den Beitrag auf S. 29).

Eine Verabschiedung ist für das nächste Jahr geplant, weshalb man mit Vorsicht auf bereits erschienene Produkte reagieren sollte, da zukünftig eventuell mit Kompatibilitäts- und Performance-Problemen zu rechnen ist. Erste Endgeräte sollen aber ebenfalls bereits ab 2013 erhältlich sein. Die Hersteller erhoffen sich so eine schnellere Verbreitung dieser neuen Technik. Cisco Systems, Netgear, Buffalo und Belkin u.a. stehen bereits in den Startlöchern, denn der WLAN-Markt boomt. *(bk)*