LANline

Februar 2008

konradin MEDIENGRUPPE

Das Magazin für Netze, Daten- und Telekommunikation www.lanline.de

Nachhaltiger IT-Betrieb

Green IT auf dem Prüfstand

Energieeffiziente Rechenzentren

Strom sparende Speichertechnik

mit Marktübersicht RZ-Planungswerkzeuge

Sonderdruck Wireless Switching

Testreihe WLAN-Controller, Teil 2: D-Link DWS-3024

WLAN-Installation mit „gutem Gefühl“

Mit dem DWS-3024 bietet D-Link einen WLAN-Controller, der auf kleine und mittlere Unternehmen ausgerichtet ist. Der Layer-2+-Switch kontrolliert bis zu 48 Access Points und stellt an jedem seiner 24 Gigabit-Ethernet-Ports Power over Ethernet zur Verfügung. LANline hat das System im Rahmen ihrer Reihe „WLAN-Controller“ getestet.

Ein WLAN im Unternehmen sehen viele Administratoren mit gemischten Gefühlen. Neben den unbestrittenen Vorteilen bleibt die berechtigte Furcht vor Hacker-Angriffen über das Medium Funk. WLAN-Controller können Abhilfe schaffen, indem sie die Verwaltung und Konfiguration zentralisieren und vereinfachen. Da immer mehr Unternehmen – auch kleine und mittelständische Firmen – die Vorteile von WLAN ausnutzen wollen, sind mittlerweile auch WLAN-Controller für diese Zielgruppe auf dem Markt. In die entsprechende Kategorie fällt das System von D-Link, das LANline als zweites im Rahmen der Testreihe WLAN-Controller vorstellt (Teil 1: Cisco 2106, LANline 11/2007).

Mit den Modellen DWS-3024 und DWS-3026 bietet D-Link sogar zwei WLAN-Controller für das untere Enterprise-Segment. Maximal 48 Access Points (APs) vom Typ DWL-3500AP oder DWL-8500AP kontrolliert ein Switch. Wer mehr benötigt, kann vier Switches zusammenschalten – dann sind 192 Access Points möglich. Der DWS-3026 gleicht seinem kleineren Bruder bis aufs Detail, abgesehen von zwei Erweiterungsschächten auf der Rückseite. Dort lässt sich der 3026 mit einem 10-Gigabit-Ethernet-Modul und einem zweiten Netzteil ausrüsten. Zum Test stand ein DWS-3024 zur Verfügung; die Ergebnisse sollten sich auch auf den DWS-3026 übertragen lassen.

Vollversorgung

D-Link stattet ihre WLAN-Controller üppig aus. An der Front ist Platz für 24 Gigabit-Ethernet-Ports, die alle parallel Power-over-Ethernet-(PoE-)Verbraucher speisen können. Praktisch, denn mit 24 Access Points kommen kleine Unternehmen schon recht weit, und dank PoE genügt schon das Netzwerkkabel am gewünschten Standort zur Installation. Die APs besitzen aber eine zusätzliche Buchse für das mitgelieferte Netzteil und lassen sich so auch an einem anderen Switch, der kein PoE bietet, anschließen. Zusätzlich sind vier SFP-Modulschächte in dem WLAN-Controller eingebaut, die einen Uplink via Glasfaserkabel ermöglichen. Die Leuchtdioden an den Ports geben entweder über den Link-Status oder – per Knopfdruck – über die PoE-Belastung Auskunft. Bis zu 370 Watt (15,4 Watt pro Port) kann der Switch maximal an die Verbraucher verteilen – eine Menge Leistung für das nur eine Höheneinheit dicke Gerät. D-Link wollte deshalb wohl kein Risiko eingehen und kühlt den Switch mit vier Lüftern. Die resultierende Geräuschkulisse verbietet den Einsatz in jedem Raum, in dem sich Menschen länger als ein paar Minuten aufhalten. Daher lässt sich auch die Option, den Switch nicht im 19-Zoll-Rack sondern als Desktop-Gerät zu betreiben, nicht ganz ernst nehmen.

Gigabit Ethernet und PoE: Der DWS-3024 versorgt Access Points mit Strom und Daten.

Die (interne) Basis der beiden WLAN-Controller von D-Link ist ein Layer-„2+“-Switch. Zum „echten“ Layer-3-Switch fehlen ein paar Funktionen, allerdings bietet der Switch deutlich mehr als gewöhnliche Layer-2-Modelle: daher die Kompromissbezeichnung „2+“. So lassen sich mit dem WLAN-Controller auch sichere Tunnel durch verschiedene Subnetze etablieren und grundlegende Routing-Aufgaben wahrnehmen.

Das Testgerät erreichte uns mit einer vorkonfigurierten IP-Adresse – im normalen Lieferzustand muss der Administrator entweder per serieller Konsole eine Adresse vergeben oder über die „Default“-IP-Adresse 10.90.90.90 mit dem Switch Kontakt aufnehmen. Wie beim bereits getesteten Cisco-2106-Controller beschrieben, kann es inzwischen schwierig sein, einen PC mit serieller Schnittstelle im Büro zu finden. Es wird Zeit, dass die Hersteller auf USB als Management-Port umstellen.

Die Konfiguration und Verwaltung läuft wie heute üblich per Webbrowser, wenn auch leider nicht mit HTTPS wie beim Gerät von Cisco, sondern nur unverschlüsselt. Für einen sicheren Administrationszugang bleibt der Weg über SSH: D-Link hat SSH1/2-Unterstützung in den Switch eingebaut. Auch Telnet-Sessions sind möglich, die aber natürlich ebenso ungeschützt sind wie eine HTTP-Verbindung. Die Kommunikation mit den Access Points läuft allerdings über eine gesicherte SSL-Verbindung, selbst wenn der Anwender nicht von weitergehenden Funktionen wie Layer-3-Tunneling Gebrauch macht.

Wer sich zum ersten Mal in den DWS-3024 als „Admin“ einloggt (kein Passwort) dürfte von der Fülle der Funktionen überrascht sein. Im linken Navigationsfenster steht eine lange Liste mit Auswahlmöglichkeiten, die allerdings weitgehend nichts mit der WLAN-Controller-Funktion zu tun haben. D-Link hat LAN- und WLAN-Funktionen auf zwei Registerkarten aufgeteilt: Standardmäßig zeigt die Benutzeroberfläche als erstes den LAN-Bereich an. Abgesehen von ein paar grundlegenden Einstellungen wie der IP-Adresse und den SNMP-Basisinformationen, kann die LAN-Seite allerdings zunächst außen vor bleiben. Sicher, wenn es um die Authentifizierung der Managementbenutzer oder um PoE-Einstellungen geht, muss sich der Administrator wieder mit diesen Optionen beschäftigen – für die reine WLAN-Controller-Aufgabe sind sie nicht notwendig.

Erst sichern, dann klicken

Im Lieferzustand ist die komplette WLAN-Funktionalität beim ersten Start des Geräts abgeschaltet. Dies ist auch gut so, denn das vorkonfigurierte „Default“-Profil enthält keinerlei Sicherheitsmaßnahmen. Wäre Letzteres sofort nach dem Einschalten aktiv, hätte jeder drahtlose Client Zugriff auf das Netz. Im Normalfall sollte der Administrator zunächst ein oder mehrere Profile definieren. In diesen lassen sich die Eckdaten des Funknetzes festlegen: also SSID, Verschlüsselungsfunktionen, QoS und – falls gewünscht – 802.1X-Authentifizierung über einen externen Radius-Server. Mehrere Profile sind möglich und können frei an die Access Points verteilt werden. Pro AP und sogar pro Funkeinheit – also 802.11a oder 802.11g – sind bis zu acht SSIDs realisierbar.

Die Konfiguration ist übersichtlich aufgeteilt und letztlich einfach zu handhaben – mit ausreichenden Erklärungen in der Hilfefunktion. Wer sich nicht von der scheinbaren Komplexität des ersten Eindrucks abschrecken lässt, wird feststellen, dass der DWS-3024 in der Tat eine erhebliche Erleichterung beim Management des drahtlosen Netzwerks darstellt. Allerdings hat es D-Link versäumt, selbst im überschaubaren WLAN-Menüangebot stringente Vorgaben für die Benutzerführung einzuführen: Einige Funktionen sind schlicht an völlig unerwarteter Stelle untergebracht. Dies ist zwar kein gravierendes Manko – nach ein wenig Beschäftigung mit dem Gerät ist dem Anwender klar, wo was zu finden ist. Aber es bleibt hier noch Raum für Verbesserungen.

Statusinformationen: alle gemanagten Access Points und ihre Daten auf einen Blick

Wünschenswert wäre beispielsweise auch ein Wizard, der den Administrator bei wiederkehrenden Aufgaben wie der Einrichtung eines neuen AP-Profils durch alle notwendigen Schritte führt. Im Handbuch ist eine entsprechende Leitlinie zwar abgedruckt. Aber auch dort fehlt beispielsweise ein deutlicher Hinweis, dass nur ein abschließender „Push“ das Profil an die gewünschten APs verschiebt. Diesen vergisst der Administrator am Anfang nur zu leicht, und obwohl die Änderungen mit einem Klick auf den „Submit“-Button vom Controller übernommen werden, wissen die APs noch nichts davon. Dies ist zum Beispiel bei der Änderung von Sicherheitseinstellungen wie einem neuen Pre-Shared Key bei WPA/WPA2 recht irritierend. Obwohl der Administrator glaubt, die Änderung im Profil per „Submit“ durchgeführt zu haben, arbeiten die Access Points immer noch mit dem alten Passwort. Erst ein weiteres „Apply“ in einem anderen Menü führt zur Neuprogrammierung der APs, alternativ hat auch ein Reset der APs den gleichen Effekt.

Ebenfalls leicht zu übersehen ist am Anfang das „Tools“-Menü. Die Entwickler haben dieses zwischen Navigationsleiste (links) und Aktionsfeld (rechts) eingefügt – als Ausklappmenü am oberen Bildschirmrand. Hier verstecken sich unter anderem die Befehle, um die aktuelle Konfiguration in den Flash-Speicher zu schreiben. Wer sich allerdings per Kommandozeile mit dem Controller auseinandersetzt, ist nicht mit solchen Schwierigkeiten konfrontiert: Dort warnt das System, wenn Änderungen noch nicht in den Flash geschrieben wurden. Allerdings ist die Lernkurve beim Command-Line-Interface (CLI) am Anfang recht steil: Die Befehle sind nicht gerade eingängig. Wer diese beherrscht, kommt mit der Kommandozeile schneller zum Ziel, der Lernaufwand lohnt sich aber nur für Administratoren, die viel mit D-Link-Produkten zu tun haben. Lobenswert: D-Link hat ein eigenes Handbuch für die CLI-Konfiguration beigelegt.

Flexible Access Points

Die beiden AP-Modelle, die D-Link für die Zusammenarbeit mit dem WLAN-Controller an bietet, unterscheiden sich in den Funkstandards: Der DWL-3500AP kommt nur mit 802.11b/g-Radioeinheit, während der DWL-8500AP 802.11a/b/g unterstützt – ein AP für 802.11n ist in Planung, soll aber erst Ende 2008 verfügbar sein. Im Gegensatz etwa zu Cisco stellt dies insgesamt eine relativ beschränkte Auswahl dar, wobei sich die beiden Access-Point-Modelle immerhin recht universell sowohl im Büro als auch in einfachen Industrieumgebungen einsetzen lassen. Beide APs besitzen zwar eine eigene Recheneinheit, auf die prinzipiell per Telnet zugegriffen werden kann. Im Normalfall hat der Administrator aber mit diesen Geräten nichts direkt zu tun – jedenfalls spätestens dann, wenn der Controller die APs kennt: Denn die MAC-Adresse der Geräte muss in der entsprechenden Datenbank des Controllers eingetragen sein. Dies lässt sich auf mehrere Arten realisieren: Der Administrator kann die MAC-Adressen von Hand eintragen, er

kann in den APs aber auch die IP-Adresse des Controllers konfigurieren oder den im Netz verwendeten DHCP-Server (im DWS-3024 ist ebenfalls einer integriert) per Option 43 mit der IP-Adresse des Controllers bestücken. Wenn die APs eine DHCP-Anfrage an den Server stellen, erhalten sie im letzteren Fall die korrekte IP-Adresse über das Optionsfeld.

Einmal mit dem WLAN-Controller verbunden, arbeiten die APs anstandslos. Die Kontrolle über die Geräte ist vollständig – selbst ein Firmware-Update lässt sich zentral und für alle oder ausgewählte APs anstoßen. Dies dauert allerdings wie auch wahrheitsgemäß im entsprechenden Menü vermerkt etwa zwölf bis 15 Minuten. Also Vorsicht mit dem Update, wenn die Benutzer das WLAN zur Arbeit benötigen. Bei den Sende- und Empfangeigenschaften konnten die APs mit außergewöhnlich guten Reichweiten überzeugen. Die Access Points kamen im Test mit einer ganzen Reihe unterschiedlicher Clients zurecht – sowohl in aktuellen Notebooks eingebaute Adapter als auch ältere PCMCIA-Modelle oder USB-Stifte. Verbindungsabbrüche kamen im Test überhaupt nicht vor, auch das Roaming zwischen mehreren APs funktionierte tadellos.

Im der Testumgebung benutzen wir lediglich ein „flaches“ Netz mit einem VLAN für alle APs. Der WLAN-Controller unterstützt aber auch mehrer VLANs nach dem 802.1Q-Standard. Eine sehr elegante Layer-3- beziehungsweise Layer-„2+“-Funktion in diesem Zusammenhang ist das Tunneln von Wireless-Paketen durch unterschiedliche Subnetze. So können die APs im dafür vorgesehenen Subnetz verbleiben und die Pakete verschlüsselt durch den Layer-3-Tunnel zum Controller schicken. Die dabei durchquerten Transportnetze sehen die Originalpakete nicht und bleiben auch von Attacken unberührt, die möglicherweise über die Access Points durchgeführt werden.

Die letztere Funktion stellt ein gutes Beispiel dar für den etwas zwiespältigen Eindruck, den der DWS-3024 hinterlässt. So glänzt der LAN-Teil mit umfangreichen Layer-2-/Layer-3-Funktionen, während der WLAN-Part seine Grundaufgaben zwar erfüllt, aber stellenweise echte Defizite zeigt. So existiert Nachholbedarf bei allem, was über die reine Bereitstellung des WLAN-Zugangs hinausgeht. Letzteren erledigt der Controller in der Tat sehr ordentlich und unterstützt auch alle wichtigen Sicherheitsfunktionen wie WPA/WPA, PSK, Radius, PEAP, TKIP und AES. Darin steht er dem bereits getesteten Cisco 2106 in nichts nach und kommt sogar mit weniger Konfigurationsaufwand aus. Doch schon ein Webportal, das Gäste zur Zwangsauthentifizierung abfängt, wie es der WLAN-Controller von Cisco bietet, ist nicht eingebaut. D-Link kündigt allerdings Abhilfe beim nächsten Release an.

Rogue Access Points sehen

Schlichtweg zu kurz kommt bei D-Link auf jeden Fall das Handling so genannter Rogue Access Points. Diese zeigt das System zwar ordentlich nach MAC-Adresse, SSID, Kanal und Funkmodus an. Dank der sehr guten Empfangseigenschaften der D-Link-APs fanden sich im Test auch bis zu 40 APs in der Liste. Aber die Information, ob und wie ein Rogue-AP verschlüsselt, fehlt in der Auflistung. Dabei wäre ein ungeschützter AP für den Administrator von großem Interesse: Schließlich könnte sich ein legitimer Client versehentlich über diesen mit dem Netz verbinden. Dass D-Link auf Maßnahmen wie Disassozierung von Clients oder andere aktive Abwehraktionen verzichtet, fällt weniger ins Gewicht: Solche „Rambo“-Methoden sind den meisten Administratoren schon aus rechtlichen Gründen suspekt und allenfalls beim Einsatz auf weiträumigen, eigenen Geländen realistisch einsetzbar.

Deutlich stört zudem, dass die Access Points – legitime und unbekannte zugleich – in der eigentlich sehr schönen Kartenansicht nicht automatisch platziert werden. Seine eigenen APs kann der Administrator zumindest noch von Hand in der Karte hin und her schieben, er weiß schließlich wo sie installiert sind. Doch die Rogue Access Points sollte der Controller durchaus selbst im Verhältnis dazu eintragen, sonst ergibt die Liste mit den MAC-Adressen der gefundenen fremdem APs im Grundriss keinen Sinn. Schade, denn die Administration kann APs sogar in einen „Scan-only“-Modus versetzten, sodass sich diese ausschließlich um die Überwachung des Luftraums kümmern. Hier sollte D-Link nachbessern – Spezialisten im WLAN-Controller-Bereich wie Aruba (siehe LANline 4/2006) bieten hier deutlich mehr Funktionalität und auch der Cisco 2106 beherrscht bessere Tricks.

Fazit

Für ein kleines bis mittelständisches Unternehmen, das ein sicheres WLAN auf einfache Weise konfigurieren will, ist der D-Link DWS-3024 in Kombination mit den 3500/8500-Access-Points eine sehr empfehlenswerte Lösung. Der WLAN-Controller verzichtet auf die Komplexität eines Cisco 2106 und bietet dafür robuste Grundfunktionen, mit denen die Verwaltung eines drahtlosen Netzwerks wirklich einfach und schnell vonstatten geht. Die zusätzlich möglichen Layer-3-Funktionen des Switches stellen einen interessanten Bonus in entsprechend umfangreichen Infrastrukturen dar.

Leider sind die Funktionen beim Monitoring und der Benachrichtigung im WLAN zu eingeschränkt: Events werden nur per SNMP-Trap oder Syslog verteilt, E-Mail-Benachrichtigungen existieren nicht, und für Rogue Access Points sind schlicht zu wenige Informationen verfügbar. WLAN-Controller von spezialisierten Anbietern wie Aruba haben hier einen deutlichen Vorsprung – allerdings in der Regel auch zum Preis größerer Komplexität und höherer Kosten.

Für den D-Link DWS-3024 sind 8400 Euro zu veranschlagen und für die zugehörigen Access-Point-Modelle 310 Euro (DWL-3500AP) beziehungsweise 453 Euro (DWL-8500AP).

Elmar Török/pf

D-Link (Deutschland) GmbH
Schwalbacher Str. 74
65760 Eschborn
Telefon: 0 61 96 / 77 99-0
Fax: 0 61 96 / 77 99-300
Internet: http://www.dlink.de
http://wireless-switching.dlink.de