



Madge WLAN Enterprise Access Server 300

Datenblatt

Part Numbers 95-90
95-91

zentralisiertes Management und höchste Sicherheit für drahtlose Netzwerke



- vereinfacht die Implementierung von WLANs
- verbindet Sicherheit und Management von drahtlosen Netzwerken
- integriert drahtlose und herkömmliche LANs
- Unterstützung für das Management von Access Points vieler verschiedener Hersteller
- offenes und standard-basierendes System

Ein sicheres WLAN-Management-System

Mit dem Madge WLAN Enterprise Access Server 300 (Access Server) steht eine Palette sicherer, skalierbarer und standard-konformer Services bereit, durch die sich die Sicherheits- und Integrationsprobleme in Verbindung mit der Implementierung einer Wireless-Infrastruktur drastisch reduzieren lassen.

Der Access Server ermöglicht eine zentralisierte Administration des Wireless-Netzwerks und übernimmt die Verwaltung der Sicherheit und der drahtlosen Geräte und Schnittstellen zwischen dem Wireless- und dem Wired-Netzwerk.

Sie können Ihr gesamtes Wireless-Netzwerk von einem einzigen, zentralen Punkt aus kontrollieren, da der Access Server Ihnen die Einrichtung einer Sicherheitsstrategie ermöglicht, die sich automatisch auf nahezu alle per SNMP verwaltbaren Multivendor-Enterprise-Access Points anwenden lässt.

Darüber hinaus stellt der Access Server eine ganze Reihe integrierter Funktionen bereit, für die normalerweise eine separate Installation und Verwaltung erforderlich sind, z. B. RADIUS-Server, Firewalls, Wired- und Wireless-Integration, Certificate Authority und Management.

Der Rückgriff auf den Access Server ermöglicht einem Unternehmen die einfache und skalierbare Implementierung von Wireless-Netzwerk-Management-Protokollen - für eine Arbeitsgruppe oder Zweigstelle bis hin zur Abdeckung zahlreicher Unternehmensstandorte.

Die Multivendor-WLAN-Technologie 'Loadable Module'

Eine zentrale Aufgabe des Access Server ist die Einrichtung einer Sicherheitsstrategie, die sich automatisch auf die Access Points in Ihrem Netzwerk anwenden lässt. Die Madge Loadable Module-Technologie unterstützt neben den Madge Access Points noch zahlreiche andere per SNMP verwaltbare Access Points, u. a. Geräte von Cisco, Proxim, Symbol, D-Link, 3Com, Intel und Avaya.

Die Loadable Module-Technologie von Madge ermöglicht die Integration zukünftiger Wireless-Technologien und garantiert dabei den Schutz Ihrer Investitionen in die bereits vorhandenen WLAN-Produkte.

Einfaches Setup und Zero-Konfiguration

Kunden, die mit Madge WLAN Access Points arbeiten, profitieren von der automatischen Setup-Funktion beim Verbindungsaufbau mit dem Access Server, der darüber hinaus direkt die von Ihnen vorgegebene Sicherheitsstrategie anwendet. Damit steht ein optimiertes Zero-Konfigurationskonzept bereit, das Ihr Netzwerk vor Angriffen über nicht bzw. nur unzureichend konfigurierte Access Points schützt.

Wenn zusätzlicher Schutz vor Rogue-Access Points oder anderen Wireless-basierten Attacken benötigt wird, ziehen Sie die Implementierung von **Madge WLAN Probe 2** (97-03) und **Madge WLAN Probe Monitor** (95-71) in Betracht.

Eine skalierbare WLAN-Lösung

Der Access Server führt problemlos Skalierungen durch, um Unterstützung für umfangreiche Wireless-Installationen mit dutzenden, wenn nicht sogar tausenden von Benutzern bereitzustellen. Dank des Multitechnologie-Aspekts der Access Server-Unterstützung können dabei sowohl 802.11a-, 802.11b- und 802.11g- als auch Bluetooth-Geräte berücksichtigt werden.

Enterprise-Class-Sicherheitsmanagement

Der Access Server implementiert industriestandard-konforme Sicherheitsmechanismen, die die Unternehmensdaten vor Wireless-Eindringlingen schützen - so wird z. B. uneingeschränkte Unterstützung für 802.1x mit dem EAP-TLS-Mechanismus geboten, der aufgrund der damit verbundenen gegenseitigen Zertifikatsauthentifizierung als leistungsstärkste Authentifizierungslösung gilt. Das bedeutet im Klartext: Wenn die 802.1x-Strategie auf einen vom Access Server kontrollierten Access Point angewendet wird, verhindert dieser Access Point jeden Verbindungsaufbau mit Ihrem Wired-Netzwerk durch nicht-authentifizierte Wireless-Clients.

Einfaches Setup

Durch die Integration der RADIUS- und der Certificate Authority-Funktionalität in den Access Server erhält der Benutzer die Möglichkeit, mit ein paar einfachen Mausklicks Zertifikate für Clients zu erstellen und eine allgemein gültige Strategie zu wählen. Der RADIUS-Server, der zur Authentifizierung der Clients verwendet wird, agiert vollständig trans-

parent und erfordert keinerlei Konfiguration durch den Benutzer. Gleichzeitig ermöglicht Ihnen die Certificate Authority die Generierung von Zertifikaten für Clients bereits ein paar Sekunden nach dem Erststart des Servers - ein nicht zu verachtender Vorteil im Vergleich zu anderen Systemen.

Im Rahmen Ihrer Sicherheitsstrategie können Sie darüber hinaus noch folgende Elemente definieren:

- Eine Access Control List (ACL) für MAC-Adressen, durch die für spezifische Clients festgelegt werden kann, ob ein Verbindungsaufbau mit Ihrem Access Point genehmigt oder verweigert wird. Radius-MAC wird unterstützt.
- Der Typ der für alle Clients zu verwendenden WEP-Verschlüsselung. Beachten Sie, dass mit 802.1x eine automatische WEP-Schlüsselverwaltung bereitgestellt wird, sodass keine unendlich langen Schlüsselfolgen mehr in alle Geräte eingegeben werden müssen.
- Firewall-Dienste zur Genehmigung oder Verweigerung des Zugriffs auf spezifische IP-Ports und -Dienste (im Gateway-Modus - siehe Rahmen).
- Ein VPN (Virtual Private Network), um IPSec-Clients die Kommunikation über hochgradig gesicherte Tunnels per Wireless-Verbindung zu ermöglichen.

Einfache Integration in vorhandene Netzwerke

Der Access Server lässt sich unter Rückgriff auf die SNMP-Schnittstelle in bereits vorhandene Netzwerk-Management-Systeme integrieren. Mithilfe der umfassenden Funktionspalette für Statistikerstellung und Ereignisprotokollierung, Gruppenverwaltung und Software-Upgrading lässt sich das Wireless-Netzwerk detailliert überwachen und problemlos verwalten.

802.11-Access-Point-Management

Es können jederzeit neue Loadable-Module für die Kontrolle und Überwachung zusätzlicher 802.11a/b/g-Multivendor-Access Points hinzugefügt werden, ohne dass dazu die gesamte Softwareanwendung neu geladen werden muss. Derzeit wird die Verwaltung von Access Points der Hersteller Cisco, Proxim, Symbol, D-Link, 3Com, Intel, Avaya und Madge unterstützt.

Management-Tools

Strategiebasiertes Management (Policy)

Die Verwaltung von Wireless-Netzwerken mit zahlreichen Benutzern, Wireless-Geräten und Access Points wird durch die Einrichtung einer strategiebasierten Managementmethode erleichtert. Dadurch können Schlüssel-Features und Plattformparameter für Benutzer, Wireless-Geräte und Access Points gruppenweise eingerichtet werden und müssen nicht für jedes Element einzeln konfiguriert werden.

Der Access Server stellt zwei Betriebsmodi zur Auswahl:

- **Gateway-Modus:** Der Access Server benötigt hierzu zwei Netzwerkschnittstellen, eine für die Anbindung an das Wired-Netzwerk, die andere für die Verbindung mit dem Wireless-Netzwerk (d. h. mit dem Access Points). Hierbei handelt es sich um die sicherste Installationsmethode, da das Wired-Netzwerk unter Rückgriff auf die integrierte Firewall-Funktionalität vom Wireless-Netzwerk getrennt wird.
- **Controller-Modus:** Der Access Server benötigt in diesem Fall lediglich eine Netzwerkschnittstelle für die Verbindung mit dem LAN. Dieser Modus stellt eine größere Skalierbarkeit als der Gateway-Modus bereit und wird für die meisten Installationen empfohlen.

Sicheres webbasiertes Management

Die Verwaltung eines Wireless-Netzwerks kann mithilfe eines Webbrowsers über dessen Web-Administrationsoberfläche erfolgen. Für den Zugriff auf diese Oberfläche kann eine gesicherte HTTPS-Verbindung verwendet werden, um nicht-autorisierte Benutzer davon abzuhalten, Änderungen an der Konfiguration des Wireless-Netzwerks vorzunehmen.

Statistikerstellung und Ereignisprotokollierung

Ereignisse und Warnungen werden automatisch protokolliert und können über die Browser-Benutzeroberfläche angezeigt werden. Auf diese Weise lassen sich die Leistung des Wireless-Netzwerks und die Logging-Aktivität überwachen, z. B. der Aufbau und die Trennung von Benutzerverbindungen.

Sicherheits-Features

Certificate Management

Digitale Standardzertifikate werden eingesetzt, um das höchstmögliche Sicherheitsniveau bei der Verwendung von 802.1x bereitzustellen. Der Access Server umfasst eine Certificate Authority (CA) für die Ausstellung von Zertifikaten (sowohl für Clients als auch für Server) und ermöglicht zudem den Import von Zertifikaten externer Certificate Authorities.

Security Wizard

Bereitgestellt wird ebenfalls ein Security Wizard, um die schnelle Implementierung verschiedener Sicherheitsstrategien zu ermöglichen. Zur Auswahl stehen drei vorkonfigurierte Standardinstellungen (ultra-secure, normal

und low), wobei der Benutzer natürlich auch bedarfsgerecht eine Anpassung der Einstellungen vornehmen kann. Der Security Wizard leitet den Netzwerkadministrator durch alle Arbeitsschritte, die zur Implementierung der verschiedenen Sicherheitsebenen ausgeführt werden müssen. Auch eine benutzerdefinierte Sicherheitsstrategie kann eingerichtet werden. Da der Access Server ein zentralisiertes Management für das gesamte Wireless-Netzwerk ermöglicht, ist keine separate Verwaltung der einzelnen Access Points erforderlich (d. h. sofern dies nicht ausdrücklich erwünscht ist, beispielsweise bei der Einrichtung eines Funkkanal-Zuweisungsplans zur Vermeidung von Interferenzen zwischen Access Points).

Admin-Sicherheit

Da die gesamte Verwaltung des Access Server über einen Standard-Webbrowser erfolgt, muss der Netzwerkadministrator einen Benutzernamen mit zugehörigem Kennwort eingeben, um Zugriff zu erhalten. Durch die Verwendung von HTTPS wird eine sichere Verwaltung des Servers gewährleistet.

Gerät

Der Verbindungsaufbau mit dem Wireless-Netzwerk durch einen Wireless-Client kann verweigert werden, solange dieser nicht über die entsprechende Autorisierung verfügt. Alle Wireless-Geräte werden anhand einer eindeutigen Nummer (d. h. der MAC-Adresse eines 802.11-Geräts) identifiziert. Der Access Server verwaltet diese Adressen und konfiguriert die Access Points entsprechend, sodass direkt beim Aufbau einer Verbindung mit dem Wireless-Netzwerk ein Schutzmechanismus zum Einsatz kommt.

Benutzer

Durch die gegenseitige Authentifizierung wird sichergestellt, dass ausschließlich zertifizierte Clients Zugriff auf zertifizierte Server erhalten. Die Authentifizierung der Clients erfolgt durch den Rückgriff auf digitale Zertifikate im Rahmen des 802.1x-Protokolls - unter Verwendung des EAP-TLS-Mechanismus, der als leistungsstärkste Mechanismus von 802.1x gilt. Sobald ein digitales Zertifikat das Ende seiner Gültigkeitsdauer erreicht, wird eine entsprechende Warnung ausgegeben.

Verbindung

Das Auslesen kritischer Informationen, die über eine Wireless-Verbindung übertragen werden, wird durch eine Verschlüsselung auf Sitzungsbasis verhindert. Bei jeder Authentifizierung des Benutzers wird ein einmaliger Schlüssel (d. h. 128-Bit-WEP) generiert, der dann zur Verschlüsselung des Datenaustauschs über die Wireless-Verbindung herangezogen wird. Der Schlüssel wird in benutzerdefinierten Intervallen neu generiert, wodurch eine transparente Neu-Authentifizierung des Clients forciert wird. Der Access Server ist ebenfalls in

der Lage, statische WEP-Schlüssel zu verwalten, wenn spezifische Wireless-Geräte keine Unterstützung für dynamische Schlüssel bieten.

VPN

Ein IPSec-VPN-Server steht bereit, der den Wireless-Benutzern ausgehend von ihrem Wireless-Client den Aufbau einer gesicherten Verbindung (über IPSec-Tunnels) mit dem im Access Server integrierten VPN-Server ermöglicht. Somit wird kein zusätzlicher und kosten-trächtiger VPN-Server benötigt. Für den Schutz der Daten vor Lauschangriffen wird das hochgradig sichere und industrieweit standardisierte Verschlüsselungsverfahren 3DES verwendet. Die Authentifizierung der Benutzer sowie die Verhinderung eines Datenzugriffs durch nicht-autorisierte Benutzer kann mit Hilfe von digitalen Zertifikaten (IKE) und Kennwörtern (MD5) erfolgen.

Wireless Firewall

Die Wireless-Firewall dient der Verhinderung eines unberechtigten Zugriffs auf das drahtgebundene Netzwerk durch die Filterung der Datenpakete. Die Firewall kann aktiviert und deaktiviert und zudem für die Aktivierung bzw. Deaktivierung gemeinsamer Anwendungen oder Protokolle konfiguriert werden. Es können auch spezifische Ports aktiviert werden, um Anwendungen zuzulassen, für deren Ausführung ein spezieller Port erforderlich ist.

Schnittstellen

SNMP- und HTTP-Schnittstelle
Alle internen Access Server-Ereignisse und -Warnungen können so konfiguriert werden, dass SNMP-Traps oder HTTP-Posts generiert werden, um das Netzwerk-Management-System bzw. andere Anwendungen davon in Kenntnis zu setzen.

RADIUS-Server und -Client

Der Access Server umfasst einen RADIUS-Server, der die Authentifizierung sämtlicher Wireless-Benutzer ermöglicht, die per 802.1x eine Verbindung zum Netzwerk herstellen.

DHCP-Relais

Dieses Relais ermöglicht Wireless-Clients das Auslesen ihrer IP-Adresse aus einem im Wired-Netzwerk angesiedelten DHCP-Server, wenn der Access Server im Gateway-Modus läuft.

XML-API

Dieses Interface ermöglicht die Integration weiterer Anwendungen für eine Nutzung in Verbindung mit den Mobilitäts-Features eines Wireless-Netzwerks. Anhand der über das API bereitgestellten Informationen können andere Anwendungen die verbundenen Geräte, deren Verbindungsdauer, den für die Verbindung verwendeten Access Point sowie den Umfang der jeweils gesendeten und empfangenen Daten identifizieren.

Spezifikationen

SCHNITTSTELLEN:

- 10/100 Ethernet (2 off)
- 4/16/100 Token Ring (optional)
- Serial port (DB9)

ANFORDERUNGEN AN DIE KONSOLE:

- Standard-Webbrowser

STROMVERSORGUNG:

100 - 240V AC, 50-60Hz
Wärmestreuung: 180W
AC-Nennstrombereich: 2A@115V,
1A @240V

MONTAGE / ABMESSUNGEN:

19 Zoll 1U Rack-Montage oder freistehend
Abmessungen (B x H x T): 17,7 x 1,75 x 12,8 in (450 x 45 x 325 mm)
Gewicht: Etwa 11 lbs (5 kg)

UMGEBUNG:

Temperaturbereich bei Betrieb: 10 - 35° C
Temperaturbereich bei Stillstand: -25° C bis +60° C
Luftfeuchtigkeit bei Betrieb: 10 - 90 % (nicht kondensierend)
Sicherheit:
EN60950-1:2001
IEC 60950-1:2001
UL60950-1:2003
ETL-Zertifizierung (Kanada, USA)
CE-Kennzeichnung
EMC:
FCC CFR 47, Teil 15, Unterkapitel B, Klasse A
EN55022
EN55024
Including
EN61000-3-2
EN61000-3-3

Geschäftsstellen

Worldwide Headquarters

Madge Limited
Madge House
Priors Way
Maidenhead
UK
SL6 2HP
Tel +44 (0) 1628 408000
Fax +44 (0) 1628 408010

Deutschland

Madge Limited
Humboldtstr. 12
85609 Dornach
Tel: +40 (0) 89-944 90 260
Fax: +49 (0) 89-944 90 460

United States of America

Madge Limited
28465 Cleveland Street
Livonia
MI 48150
USA
Tel (734) 266 1915
Fax (734) 266 1916

Bestellinformationen

Part No	WLAN Enterprise Access Server
95-90*	WLAN Enterprise Access Server 300 Appliance including 25 device licenses
95-91*	WLAN Enterprise Access Server 300 Appliance including 25 device licenses and Token Ring Interface
95-60	Additional 5 device license pack
95-61	Additional 10 device license pack
95-66	Additional 15 device license pack
95-62	Additional 50 device license pack
95-63	Additional 100 device license pack

* Order power cord separately

Wireless and Token Ring Networking

Madge Limited is a global supplier of advanced networking product solutions to enterprises, and is the market leader in Token Ring networking. Madge is pioneering next generation networking solutions, which enable the painless and secure deployment of Wireless networks in enterprises while protecting customers' investments in existing LAN and Token Ring. Madge's principal business centres are located in Maidenhead, United Kingdom; Munich, Germany; and the USA. Information about Madge's complete range of products and services can be accessed at www.madge.com.

Madge reserves the right to change specifications without notice. Madge, the Madge logo, and product names are trademarks and in some jurisdictions may be registered trademarks of Madge. Other trademarks appearing in this document are the property of their respective owners.