VoIP-Kabelrouter mit WLAN-Funktion
CVE-30360

Benutzerhand-buch

Version 1.0 - 07/2014

hitron

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Über dieses Benutzerhandbuch

Was in diesem Benutzerhandbuch beschrieben wird

In diesem Benutzerhandbuch wird beschrieben, wie die Funktionen des CVE-30360 über seine grafische Benutzeroberfläche konfiguriert werden.

Verwendung dieses Benutzerhandbuchs

Dieses Handbuch beschreibt jede Eingabemaske des CVE-30360 sowie die Verwendung der unterschiedlichen Funktionen.

- In der Einführung (Seite 15) finden Sie eine Übersicht über die in diesem Handbuch beschriebenen Themen.
- Im Inhaltsverzeichnis (Seite 7), Abbildungsverzeichnis (Seite 11) und Tabellenverzeichnis (Seite 13) können Sie schnell die Informationen zu einer bestimmten Eingabemaske oder einem Thema finden.
- Im Index (Seite 110) erhalten Sie Informationen zu bestimmten Schlüsselwörtern.
- Im Rest des Benutzerhandbuchs erhalten Sie eine ausführliche Beschreibung der Funktionen des CVE-30360.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Weitere Dokumente

- **Installations-Kurzanleitung**: In dieser Anleitung wird kurz beschrieben, wie der CVE-30360 installiert wird. Sie enthält Informationen zu den Systemvoraussetzungen, zum Packungsinhalt, zur Installation und Hinweise zur Fehlerbehebung.
- **Online-Hilfe**: Jede Maske der Benutzeroberfläche des CVE-30360 verfügt über eine **Hilfe**-Taste. Wenn Sie auf diese Taste klicken, erhalten Sie zusätzliche Informationen zum Konfigurieren der Einstellungen.

Zum Gebrauch dieses Dokuments

In diesem Benutzerhandbuch werden bestimmte Inhaltstypen mit bestimmten typographischen Merkmalen und Stilmerkmalen gekennzeichnet:

- Aufzählungen dienen dazu, verschiedene Einträge aufzulisten und auf Optionen hinzuweisen.

1. Nummerierte Absätze beschreiben die einzelnen Verfahrensschritte.

HINWEIS: Hinweise enthalten weiterführende Informationen zu einem Thema.

Warnungen enthalten Informationen zu Handlungsweisen, bei denen das Gerät beschädigt werden kann.

Produktbezeichnungen, Feldbezeichnungen, Auswahlfelder usw. sind **fett** geschrieben. Beispiel:

> Wählen Sie **UDP**, um das "User Datagram Protocol" zu verwenden.

Ein Mausklick in einer Eingabemaske ist durch eine spitze Klammer (>) gekennzeichnet. Beispiel:

> "Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen**."

bedeutet, dass Sie in der Maske zunächst auf **Einstellungen** und dann auf **Erweiterte Einstellungen** klicken.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tasten werden mit Großbuchstaben in eckigen Klammern dargestellt. Beispiel:

> Drücken Sie zum Fortfahren auf [ENTER].

Kundenbetreuung

Wenn Sie technische Hilfe benötigen oder andere Probleme auftreten, wenden Sie sich an Ihren Hitron-Vertreter.

Standard-Anmeldedaten

Die IP-Adresse und die sonstigen Standard-Anmeldedaten des CVE-30360 können der folgenden Tabelle entnommen werden. Weitere Informationen dazu finden Sie unter Anmelden beim CVE-30360 auf Seite 24.

Tabelle 1: Standard-Anmeldedaten

IP-Adresse	192.168.0.1
Benutzername	admin
Passwort	password

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Copyright © 2011 Hitron Technologies. Alle Rechte vorbehalten. Alle Marken und eingetragenen Marken sind das Eigentum der jeweiligen Eigentümer.

HAFTUNGSAUSSCHLUSS: Die in diesem Benutzerhandbuch enthaltenen Informationen sind zum Zeitpunkt der Druckstellung richtig. Dieses Benutzerhandbuch liegt in der vorliegenden Form vor und enthält keine ausdrücklichen oder impliziten Garantien/Gewährleistungen. Hitron Technologies und seine Vertreter übernehmen weder die Haftung für Ungenauigkeiten in diesem Benutzerhandbuch noch für Verluste, die durch die Beachtung oder Nicht-Beachtung der Anweisungen in diesem Benutzerhandbuch entstehen.

Inhaltsverzeichnis

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildungsverzeichnis

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabellenverzeichnis

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

1

Einführung

In diesem Kapitel erhalten Sie eine Übersicht über den CVE-30360 und eine Einführung in seine Benutzeroberfläche.

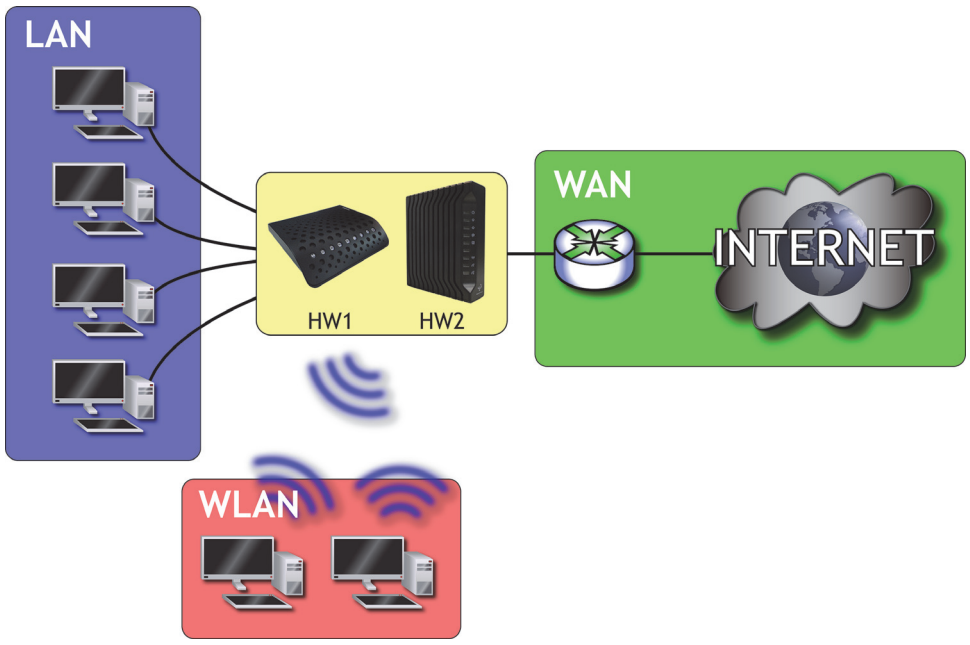
1.1 Übersicht über den CVE-30360

Der CVE-30360 ist gleichzeitig ein VECM-Kabelmodem und ein drahtloser Zugangspunkt (AP). An das Gerät können Sie Ihre Computer, analogen Telefone, Drahtlosgeräte und anderen Netzwerkgeräte anschließen, um sie miteinander und über die Kabelverbindung mit dem Internet zu verbinden.

Computer, die über ein Kabel mit dem CVE-30360 verbunden sind, befinden sich im lokalen Netzwerk, dem LAN. Computer, die drahtlos mit dem CVE-30360 verbunden sind, befinden sich im drahtlosen lokalen Netzwerk, dem WLAN. Der CVE-30360 stellt wiederum die Verbindung zum Internetdienstanbieter über das Weitbereichsnetzwerk, dem WAN, her.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 1: Übersicht über die Funktionen



1.1.1 Die wichtigsten Funktionen

Der CVE-30360 bietet:

- IPv4- oder DS-Lite-Betrieb.
- Internetverbindung zum Kabelmodemdienst über den **CATV**-Port (HF-Anschluss Typ F)
- Voice-over-IP-Verbindung (VoIP) zum Telefoniedienstanbieter.
- LAN-Verbindung über vier Ethernet-Ports mit einer Verbindungsgeschwindigkeit von 10/100/1000 Mbps (Megabits pro Sekunde)
- DHCP-Protokoll (Dynamic Host Configuration Protocol) für Geräte im LAN
- LAN-Fehlerbehebungstools (Ping und Traceroute)
- IEEE 802.11b/g/n drahtloses MIMO-Networking (Multiple-In, Multiple-Out) mit Geschwindigkeiten von bis zu 300 Mbps

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

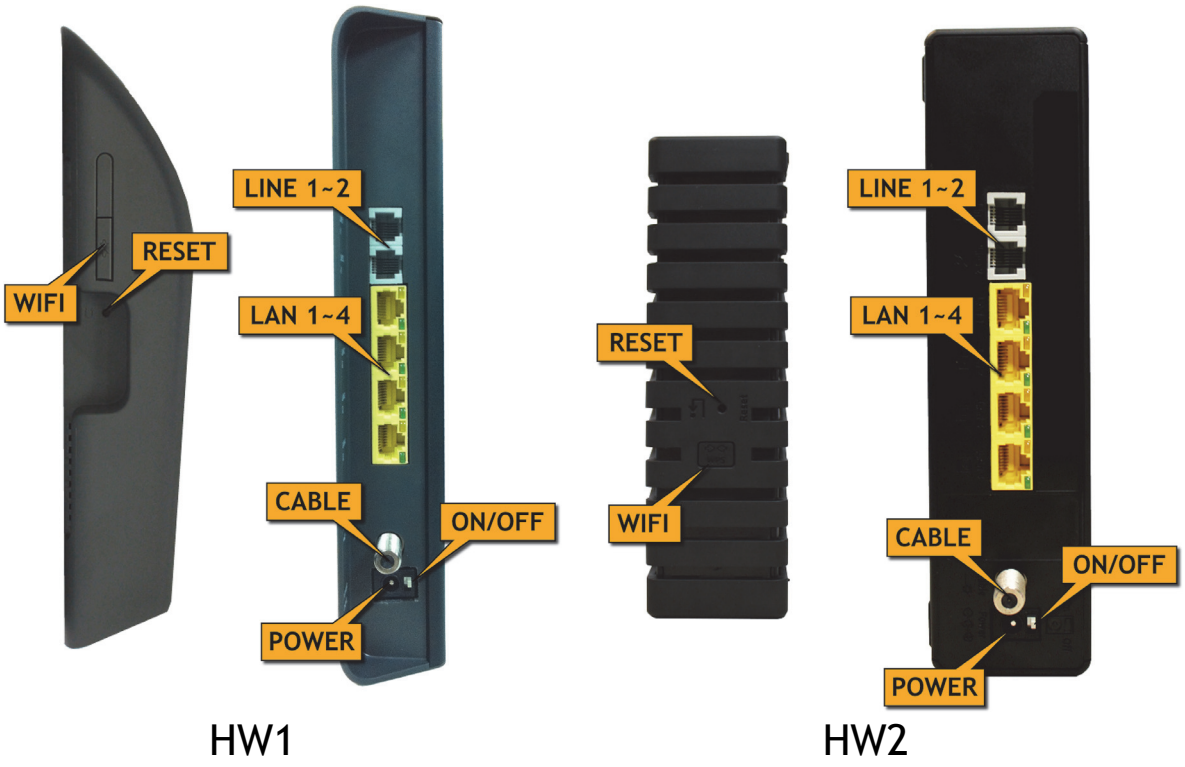
- Sicherheit bei der Drahtlosverbindung: WEP-, WPA-PSK- und WPA2-PSK-Verschlüsselung, Wifi Protected Setup (WPS), Push-Button- und PIN-Konfiguration und MAC-Filter
- Sicherheit bei der Kabelverbindung: Stateful-Inspection-Firewall mit Intrusion-Detection-System, IP- und MAC-Filter, Portweiterleitung und Port-Triggering sowie DMZ (De-Militarized Zone)
- Kindersicherung: Programmierte Websiteblockierung und Zugriffsprotokolle
- Einstellungen sichern und wiederherstellen
- Sichere Konfigurationsschnittstelle, zugänglich über Webbrowser

1.2 Hardwareverbindungen

In diesem Abschnitt werden die Ports und Tasten des CVE-30360 beschrieben.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 2: Hardwareverbindungen



HW1 HW2

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 2: Hardwareverbindungen

WIFI	Mit dieser Taste können Sie das Drahtlosnetzwerk ein- oder ausschalten und die WPS PBC-Prozedur starten (weitere Informationen finden Sie unter WPS auf Seite 61). • Drücken Sie 1 bis 5 Sekunden lang auf diese Taste, um das Drahtlosnetzwerk ein- oder auszuschalten. • Um die WPS PBC-Verbindungsprozedur zu starten, müssen Sie diese Taste drücken und 5 bis 10 Sekunden lang gedrückt halten. Drücken Sie innerhalb der folgenden 2 Minuten auf die PBC-Tasten der Drahtlosgeräte, die sich innerhalb der Sendereichweite befinden, um sie zum Drahtlosnetzwerk hinzuzufügen.
Reset	Mit dieser Taste können Sie den CVE-30360 neu starten oder zurücksetzen. • Drücken Sie auf diese Taste, und halten Sie sie kurz gedrückt, um den CVE-30360 neu zu starten. Der CVE-30360 wird mit den bestehenden Einstellungen neu gestartet. • Drücken Sie auf diese Taste, und halten Sie sie länger als 10 Sekunden lang gedrückt, um alle benutzerdefinierten Einstellungen zurückzusetzen und den CVE-30360 mit den Standardeinstellungen neu zu starten.
LAN1	An diese Ports werden Ihr Computer und andere Netzwerkgeräte angeschlossen. Verwenden Sie dazu Ethernet-Kabel der Kategorie 5 oder 6 mit RJ45-Stecker.
LAN2	
LAN3	
LAN4	
LINE 1	An diese Ports werden Ihre Analogtelefone für VoIP-Dienste angeschlossen. Verwenden Sie dazu Kabel mit RJ11-Stecker.
LINE 2	
CABLE	Hier schließen Sie ein HF-Kabel Typ F für die Verbindung mit dem Internet an.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 2: Hardwareverbindungen

POWER	Hier schließen Sie den 12 V/2 A-Netzadapter an, der im Lieferumfang des CVE-30360 enthalten ist. **Verwenden Sie NIEMALS einen anderen Netzadapter für die Stromversorgung des CVE-30360. Anderenfalls kann der CVE-30360 beschädigt werden.**
ON/OFF	Mit diesem Schalter können Sie den CVE-30360 ein- oder ausschalten. • Um den CVE-30360 einzuschalten, schieben Sie den Schalter in die Position ON. • Um den CVE-30360 auszuschalten, schieben Sie den Schalter in die Position OFF.

1.3 LEDs

In diesem Abschnitt werden die LED-Lampen des CVE-30360 beschrieben.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 3: LEDs

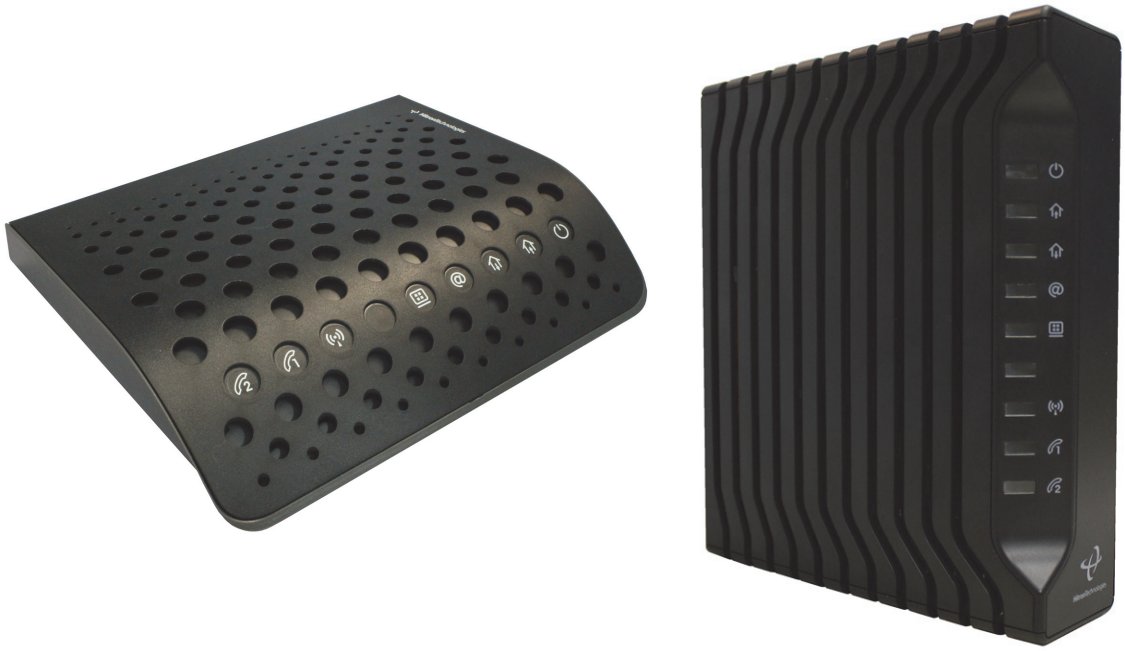


Tabelle 3: LEDs

LED	STATUS	**BESCHREIBUNG**
LINE 1 LINE 2 	Leuchtet nicht	Ihr Dienstvertrag umfasst keine Voice-Dienste. HINWEIS: Wieviele **LINE**-LEDs leuchten, hängt von den von Ihnen gebuchten Voice-Diensten ab.
	Blinkt	Am entsprechenden **LINE**-Port ist ein Telefon angeschlossen. Der Telefonhörer ist gerade abgehoben.
	Leuchtet	Ihr Dienstvertrag umfasst Voice-Dienste. HINWEIS: Wieviele **LINE**-LEDs leuchten, hängt von den von Ihnen gebuchten Voice-Diensten ab.
WIRELESS 	Leuchtet nicht	Über das Drahtlosnetzwerk werden Daten weder gesendet noch empfangen.
	Blinkt	Über das Drahtlosnetzwerk werden Daten gesendet oder empfangen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 3: LEDs

ETH 	Leuchtet nicht	Es ist kein Gerät an den **LAN**-Ports angeschlossen.
	Blinkt	Es ist ein Gerät über die schnelle Ethernet-Verbindung an einen **LAN**-Port angeschlossen. Dieses Gerät sendet oder empfängt gerade daten.
	Leuchtet	Es ist ein Gerät über die schnelle Ethernet-Verbindung an einen **LAN**-Port angeschlossen. Es sendet oder empfängt gerade keine Daten.
Status 	Blinkt	Das Kabelmodem des CVE-30360 registriert sich gerade beim Dienstanbieter.
	Leuchtet	Das Kabelmodem des CVE-30360 hat sich erfolgreich beim Dienstanbieter registriert.
US 	Blinkt	Der CVE-30360 sucht gerade nach einer Upstream-Frequenz in der **CATV**-Verbindung.
	Leuchtet	Der CVE-30360 hat erfolgreich eine Upstream-Frequenz in der **CATV**-Verbindung gefunden und sich festgelegt.
DS 	Blinkt	Der CVE-30360 sucht gerade nach einer Downstream-Frequenz in der **CATV**-Verbindung.
	Leuchtet	Der CVE-30360 hat erfolgreich eine Downstream-Frequenz in der **CATV**-Verbindung gefunden und sich festgelegt.
Power 	Leuchtet	Der CVE-30360 wird mit Strom versorgt.
	Leuchtet nicht	Der CVE-30360 wird nicht mit Strom versorgt.

Wenn Sie den CVE-30360 einschalten, beginnen die LEDs in der folgenden Reihenfolge zu leuchten:

- **Power**
- **US**
- **DS**
- **Status**
- Die LEDs **ETH 1-4** leuchten, sobald an den entsprechenden Ports Aktivität ermittelt wird, die LEDs **LINE 1-2** leuchten, wenn Ihr Dienstvertrag auch Telefonie umfasst (die Anzahl der leuchtenden LEDs ist abhängig von Ihrem Tarif). Die **WIRELESS**-LED leuchtet, sobald das Drahtlosnetzwerk bereit ist.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

1.4 Einrichten der IP-Adresse

Wenn Sie die Benutzeroberfläche des CVE-30360 aufrufen möchten, müssen sich die IP-Adresse des Computers und die des CVE-30360 im LAN im selben Subnetz befinden. Dadurch ist die Kommunikation des Computers mit dem CVE-30360 möglich.

HINWEIS: Hintergrundinformationen finden Sie unter IP-Adressen und Subnetze auf Seite 30.

Der CVE-30360 verfügt über einen integrierten DHCP-Server. Sobald er aktiviert ist, kann er Computern im LAN IP-Adressen zuweisen. Wenn der DHCP-Server aktiv ist, können Sie automatisch eine IP-Adresse beziehen. Der DHCP-Server ist standardmäßig aktiviert.

Wenn Ihr Computer so konfiguriert ist, dass er eine IP-Adresse automatisch beziehen kann, oder wenn Sie das nicht genau wissen, versuchen Sie zunächst, sich beim CVE-30360 anzumelden (siehe Anmelden beim CVE-30360 auf Seite 24).

- Wenn die Anmeldemaske erscheint, ist der Computer bereits richtig konfiguriert.
- Wenn die Anmeldemaske nicht erscheint, ist entweder der DHCP-Server des CVE-30360 nicht aktiviert, oder der Computer ist nicht richtig konfiguriert. Folgen Sie der Anweisung gemäß Manuelles Einrichten der IP-Adresse auf Seite 23, und richten Sie den Computer so ein, dass er eine IP-Adresse automatisch bezieht. Versuchen Sie erneut, sich anzumelden. Wenn Sie sich nicht anmelden können, richten Sie wie unten beschrieben noch einmal manuell eine IP-Adresse ein. Versuchen Sie erneut, sich anzumelden.

HINWEIS: Wenn die Anmeldemaske weiterhin nicht angezeigt wird, wurden möglicherweise die Einstellungen des CVE-30360 geändert. Wenn Sie die neue Adresse des CVE-30360 nicht kennen, sollten Sie die Standardeinstellungen wiederherstellen. Siehe Zurücksetzen des CVE-30360 auf Seite 28. Beachten Sie, dass dabei ALLE benutzerdefinierten Einstellungen verloren gehen.

1.4.1 Manuelles Einrichten der IP-Adresse

Standardmäßig ist die lokale IP-Adresse des CVE-30360 **192.168.0.1**. Wenn der CVE-30360 die IP-Standardadresse verwendet, muss die IP-Adresse des Computers zwischen **192.168.0.2** und **192.168.0.254** liegen.

HINWEIS: Wenn der DHCP-Server des CVE-30360 aktiviert ist, richten Sie den Computer so ein, dass er bei Schritt 5 automatisch eine IP-Adresse bezieht. Der CVE-30360 weist dann dem Computer eine IP-Adresse zu. Der DHCP-Server ist standardmäßig aktiviert.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Führen Sie die folgenden Schritte aus, um die IP-Adresse Ihres Computers für die Verbindung mit dem CVE-30360 manuell einzurichten:

HINWEIS: In diesem Beispiel wurde als Betriebssystem Windows XP verwendet. Bei anderen Betriebssystemen kann das Verfahren abweichen.

1. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
2. Klicken Sie in dem nun angezeigten Fenster doppelt auf **Netzwerkverbindungen**.
3. Klicken Sie mit der rechten Maustaste auf Ihre Netzwerkverbindungsart (normalerweise **LAN-Verbindung**), und klicken Sie dann auf **Eigenschaften**.
4. Scrollen Sie in der Liste **Diese Verbindung verwendet folgende Elemente** in der Registerkarte **Allgemein** nach unten, und wählen Sie **Internetprotokoll (TCP/IP)**. Klicken Sie auf **Eigenschaften**.
5. Sie können eine IP-Adresse automatisch beziehen oder manuell festlegen:
   - Wenn der DHCP-Server des CVE-30360 aktiviert ist, wählen Sie die Option **IP-Adresse automatisch beziehen**.
   - Wenn der DHCP-Server des CVE-30360 nicht aktiviert ist, wählen Sie die Option **Folgende IP-Adresse verwenden**. Geben Sie in das Feld **IP-Adresse** eine Adresse zwischen **192.168.0.2** und **192.168.0.254** (Standard) ein. Geben Sie in das Feld **Subnetzmaske 255.255.255.0** (Standard) ein.

HINWEIS: Wenn der CVE-30360 nicht die IP-Standardadresse verwendet, wählen Sie die IP-Adresse und Subnetzmaske so, dass der Computer im selben Subnetz liegt wie der CVE-30360.

6. Klicken Sie auf **OK**. Das Fenster **Internetprotokoll (TCP/IP)** schließt sich. Klicken Sie im Fenster **LAN-Verbindungseigenschaften** auf **OK**.

Der Computer erhält jetzt eine IP-Adresse vom CVE-30360 oder verwendet die von Ihnen festgelegte IP-Adresse. Er kann dann mit dem CVE-30360 kommunizieren.

1.5 Anmelden beim CVE-30360

Führen Sie die folgenden Schritte aus, um sich beim CVE-30360 anzumelden und die Benutzeroberfläche aufzurufen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

HINWEIS: Sie können sich zwar über die Drahtlosschnittstelle beim CVE-30360 anmelden, es wird aber empfohlen, den CVE-30360 über eine Kabelverbindung mit dem LAN zu konfigurieren.

1 Öffnen Sie ein Browserfenster.

2 Geben Sie in die Adresszeile des Browsers die IP-Adresse des CVE-30360 ein (Standard **192.168.0.1**). Die Eingabemaske **Anmelden** erscheint.

Abbildung 4: Anmelden

3 Geben Sie den **Benutzernamen** und das **Passwort** ein. Der Anmeldebenutzername ist standardmäßig **admin**, das Anmeldepasswort ist **password**.

HINWEIS: Beachten Sie bei der Eingabe des Benutzernamens und Passworts die Groß- und Kleinschreibung - “admin” ist nicht dasselbe wie “Admin”.

4 Klicken Sie auf **Anmelden**. Die Maske **Systeminfo** wird angezeigt (siehe Die Eingabemaske Systeminfo auf Seite 36).

1.6 Übersicht über die Benutzeroberfläche

In diesem Abschnitt wird die Benutzeroberfläche des CVE-30360 beschrieben.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 5: Übersicht über die Benutzeroberfläche

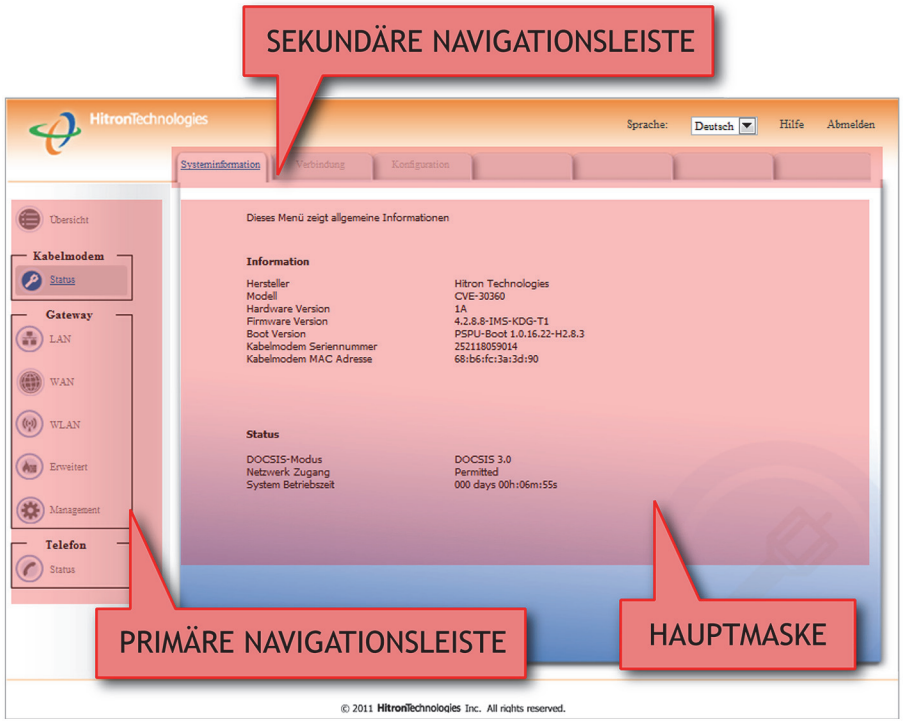


Tabelle 4: Übersicht über die Benutzeroberfläche

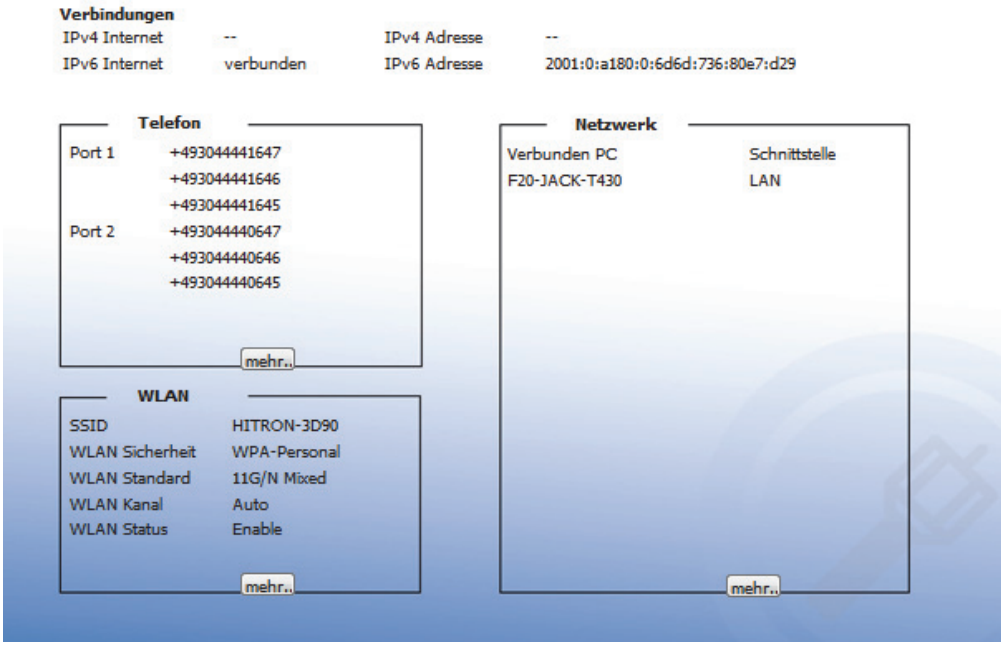
Primäre Navigationsleiste	In diesem Bereich können Sie von einem Bereich der Benutzeroberfläche zu einem anderen Bereich wechseln.
Sekundäre Navigationsleiste	In diesem Bereich können Sie von einer zugehörigen Eingabemaske zu einer anderen wechseln.
Hauptmaske	In diesem Bereich finden Sie Informationen zur Konfiguration des CVE-30360, und hier können Sie die Konfigurationen ändern.

1.7 Die Eingabemaske Übersicht

Die Eingabemaske Übersicht erscheint, wenn Sie sich beim CVE-30360 anmelden. Sie enthält die wichtigsten Informationen zum Systemstatus.

HINWEIS: Diese Eingabemaske unterscheidet sich je nachdem, ob der im IPv4- oder im DS-Lite-Modus arbeitet.

Abbildung 6: Die Eingabemaske Übersicht



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 5: Die Eingabemaske Kabel > Systeminfo

Verbindungen	
IPv4 Internet	Diese Option wird als **Verbunden** angezeigt, wenn der CVE-30360 im IPv4-Modus arbeitet und mit dem Internet verbunden ist.
IPv6 Internet	Diese Option wird als **Verbunden** angezeigt, wenn der CVE-30360 im DS-Lite-Modus arbeitet und mit dem Internet verbunden ist.
IPv4 Adresse	Hier wird eine IPv4-Adresse angezeigt, wenn der CVE-30360 im IPv4-Modus arbeitet und an der WAN-Schnittstelle eine IP-Adresse empfangen hat.
IPv6 Adresse	Hier wird eine IPv6-Adresse (XXX.XXX.XXX.XXX) angezeigt, wenn der CVE-30360 im DS-Lite-Modus arbeitet und an der WAN-Schnittstelle eine IP-Adresse empfangen hat.
Telefonie	
Port 1	In diesem Abschnitt werden Informationen über Telefonieaktivitäten an Port 1 angezeigt.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 5: Die Eingabemaske Kabel > Systeminfo (Fortsetzung)

Port 2	In diesem Abschnitt werden Informationen über Telefonieaktivitäten an Port 1 angezeigt.
mehr...	Wenn Sie hier klicken, erhalten Sie weitere Informationen über die Telefonieaktivitäten des CVE-30360. Siehe Die Maske Telephony Status auf Seite 104.
Netzwerk	
PC	Hier werden die Namen aller Computer angezeigt, die an das LAN- oder WLAN-Netzwerk des CVE-30360 angeschlossen sind.
Schnittstelle	Für jeden einzelnen an den CVE-30360 angeschlossenen Computer wird angezeigt, ob dieser über das lokale Netzwerk (**LAN**) oder über das drahtlose Netzwerk (**WLAN**) angeschlossen ist.
mehr...	Wenn Sie hier klicken, erhalten Sie weitere Informationen über den Netzwerkstatus des CVE-30360. Siehe Die Eingabemaske Lokale Netzwerk Benutzer auf Seite 46.
WLAN	
SSID	Hier wird der Name des WLAN-Netzwerks des CVE-30360 angezeigt.
WLAN Sicherheit	Hier wird der aktuell verwendete Sicherheitstyp angezeigt, mit dem das WLAN-Netzwerk des CVE-30360 geschützt ist.
WLAN Standard	Hier wird angezeigt, welchen WLAN-Netzwerktyp der CVE-30360 gerade nutzt.
WLAN Kanal	Hier wird die Bezeichnung des Frequenzbands angezeigt, in dem das WLAN-Netzwerk des CVE-30360 aktuell arbeitet.
WLAN Status	Hier wird angezeigt, ob die WLAN-Schnittstelle des CVE-30360 aktiv ist.
mehr...	Wenn Sie hier klicken, erhalten Sie weitere Informationen über die Netzwerkaktivität des CVE-30360. Siehe Die Eingabemaske Wireless-Grundeinstellungen auf Seite 62.

1.8 Zurücksetzen des CVE-30360

Wenn Sie die Standardeinstellungen des CVE-30360 wiederherstellen, gehen alle benutzerdefinierten Einstellungen verloren, und der CVE-30360 wird auf seinen ursprünglichen Konfigurationsstatus zurückgesetzt.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Der CVE-30360 kann auf zwei Arten zurückgesetzt werden:

- Drücken Sie auf die **RESET**-Taste des CVE-30360, und halten Sie diese mindestens 10 Sekunden lang gedrückt.
- Klicken Sie auf **Kabelmodem** > **Konfiguration**. Klicken Sie in der folgenden Maske auf die Schaltfläche **Zurücksetzen**.
- Klicken Sie auf **Management** (Verwaltung). Klicken Sie in der folgenden Maske auf die Schaltfläche **Zurücksetzen**.

Der CVE-30360 schaltet sich aus und mit den Standardeinstellungen wieder ein.

HINWEIS: Entsprechend der vorherigen Konfiguration des CVE-30360 müssen eventuell die IP-Einstellungen des Computers neu konfiguriert werden (siehe Einrichten der IP-Adresse auf Seite 23).

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

2

Kabelmodem

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **Kabelmodem** klicken. Es umfasst die folgenden Abschnitte:

2.1 Übersicht über den Menüpunkt Kabelmodem

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **Kabelmodem** beschrieben.

2.1.1 DOCSIS

Die DOCSIS-Spezifikation (Data Over Cable Service Interface) ist ein Telekommunikationsstandard, der die Bereitstellung von Datendiensten (Internetzugriff) über ein herkömmliches Kabelfernsehnetzwerk (CATV) definiert.

Der CVE-30360 unterstützt die DOCSIS-Version 3.0.

2.1.2 IP-Adressen und Subnetze

Jeder Computer des Internets muss eine eindeutige IP-Adresse haben. Die IP-Adresse legt den Ort fest, zu dem Informationen gesendet werden. Sie entspricht etwa der Straße und Hausnummer in einer Adresse. In einem Netzwerk können zwei Computer nicht dieselbe IP-Adresse haben.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

2.1.2.1 IP-Adressformat

IP-Adressen (Version 4) bestehen aus 4 Oktetts (entspricht 32 Bits) und werden in der Form **192.168.1.1** dargestellt. Jedes Oktett (Byte) hat einen Mindestwert von 0 und einen Höchstwert von 255.

Eine IP-Adresse enthält zwei wichtige Informationen: die “Netzwerknummer” (die gesamte Netzwerkadresse), die etwa der Straße in einer Adresse entspricht, und die “Host-ID”, die etwa der Hausnummer entspricht. Die “Host-ID” bestimmt den Computer (oder ein anderes Netzwerkgerät) eindeutig.

2.1.2.2 IP-Adressvergabe

Die IP-Adressen können von drei Stellen vergeben werden:

- von der IANA (Internet Assigned Numbers Agency)
- von Ihrem Internetdienstanbieter
- von Ihrem privaten Netz (oder von Ihren Netzwerkgeräten)

Die IANA ist für die Vergabe der IP-Adressen auf globaler Ebene zuständig, und die Internetdienstanbieter weisen ihren Kunden IP-Adressen zu. Sie selbst können in einem privaten Netzwerk eigene IP-Adressen vergeben, in öffentlichen Netzwerken ist das jedoch nicht möglich.

Die IP-Adresse des CVE-30360:

- Das öffentliche Netzwerk (Wide Area Netzwerk oder WAN) ist die Verbindung zwischen dem Kabelanschluss (CATV) und Ihrem Internetdienstanbieter. Die IP-Adresse des CVE-30360 in diesem Netzwerk wird Ihnen von Ihrem Dienstanbieter zugewiesen.
- Das private Netzwerk (im Routing-Modus - siehe Routing-Modus auf Seite 34) ist Ihr LAN-Netzwerk (Local Area Network) und ggf. Ihr WLAN-Netzwerk (Wireless Local Area Network). Sie können den Computern im LAN und WLAN manuell die IP-Adressen zuweisen oder sie vom CVE-30360 automatisch mit dem DHCP (Dynamic Host Configuration Protocol) zuweisen lassen. IANA hat für private Netzwerke nur die folgenden IP-Adressblöcke reserviert:

Tabelle 6: Private IPv4-Adressbereiche

VON...	...BIS
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Wenn Sie Adressen manuell vergeben, müssen diese sich im LAN-Subnetz des CVE-30360 befinden.

2.1.2.3 Subnetze

Ein Subnetz oder Subnetzwerk ist beim Internetprotokoll ein Teilnetz eines Netzwerks. Ein Subnetz kann z. B. alle Computer eines Büros umfassen, während das gesamte Netz alle Geräte aller Büros in einer Firma umfasst.

Um den Umfang eines Subnetzes festzulegen, und um es vom Gesamtnetzwerk zu unterscheiden, wird eine Subnetzmaske verwendet. Diese “Masken” sind der Teil der IP-Adresse, der sich auf das Gesamtnetzwerk bezieht. Der andere Teil der IP-Adresse bezieht sich auf das Subnetzwerk.

Jede IPv4-Subnetzmaske besteht wie jede IPv4-Adresse aus 32 Bits (Binärziffern):

- Der Binärwert **1** in der Subnetzmaske bedeutet, dass das entsprechende Bit in der IP-Adresse Teil des Gesamtnetzwerks ist.
- Der Binärwert **0** in der Subnetzmaske bedeutet, dass das entsprechende Bit in der IP-Adresse Teil des Subnetzwerks ist.

Die folgende Tabelle zeigt die IPv4-Adresse eines Computers (**192.168.1.1**) in dezimaler und in binärer Form (jedes Feld in der Tabelle enthält ein Oktett):

Tabelle 7: IP-Adresse: Dezimale und binäre Form

192	168	0	1
11000000	10101000	00000000	00000001

Die folgende Tabelle zeigt eine Subnetzmaske, die die ersten 24 Bits der IP-Adresse “maskiert”, in dezimaler und in binärer Form.

Tabelle 8: Subnetzmaske: Dezimale und binäre Form

255	255	255	0
11111111	11111111	11111111	00000000

Bei diesem Subnetz legen die ersten drei Oktette (in der IP-Beispieladresse **192.168.1**) das Gesamtnetzwerk und das letzte Oktett (in der IP-Beispieladresse **1**) die Adresse des Computers im Subnetz fest.

Die dezimale und die binäre Schreibweise sind die gebräuchlichsten Formen zur Darstellung einer Subnetzmaske:

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- Dezimal: Die Subnetzmaske wird in derselben Form wie die IP-Adresse geschrieben, z. B.: **255.255.255.0**.
- Binär: Die Subnetzmaske wird mit einem Schrägstrich an die IP-Adresse angehängt. Sie gibt die Anzahl der Binärziffern an, die sie maskiert. Die Subnetzmaske **255.255.255.0** maskiert die ersten 24 Bits der IP-Adresse. Sie würde also folgendermaßen geschrieben werden: 192.168.1.1**/24**.

2.1.3 DHCP

Das DHCP-Protokoll (Dynamic Host Configuration Protocol) legt das Verfahren fest, mit ein Gerät des Netzwerks Computern und anderen Netzwerkgeräten automatisch IPv4-Adressen zuweist. Dieses Gerät ist der so genannte DHCP-Server. Er vergibt allen DHCP-Clients eine IP-Adresse.

Um eine IP-Adresse per DHCP zu erhalten, muss der Computer diese zunächst beim DHCP-Server anfordern (es ist eine Broadcast-Anfrage nach Adressangeboten im gesamten Netzwerk). Der DHCP-Server empfängt die Anfrage und weist daraufhin dem anfragenden Computer eine IP-Adresse zu.

Wenn ein Computer nicht so eingestellt ist, dass er die IP-Adresse automatisch beim DHCP-Server anfordert, muss die IP-Adresse manuell konfiguriert werden, damit dieser Computer auf andere Computer und Gerät im Netzwerk zugreifen kann. Weitere Informationen dazu finden Sie unter Einrichten der IP-Adresse auf Seite 23.

Standardmäßig ist der CVE-30360 als DHCP-Client im WAN (die CATV-Verbindung) eingestellt. Er sendet eine IP-Adresse über das Kabelnetzwerk und empfängt eine vom Internetdienstanbieter. Standardmäßig ist der CVE-30360 ein DHCP-Server im LAN. Er weist den Computern im LAN bei Anfrage eine IP-Adressen zu.

2.1.4 DHCP-Lease

“DHCP-Lease” bezeichnet die Dauer, die ein DHCP-Server einen DHCP-Client eine IP-Adresse nutzen lässt. Normalerweise fragt der DHCP-Client nach einer Erneuerung des DHCP-Lease, bevor sie abgelaufen ist. Dann kann er diese IP-Adresse für eine weitere Lease-Periode nutzen. Wenn der Client jedoch keine Erneuerung anfragt, untersagt der DHCP-Server dem Client die weitere Nutzung der IP-Adresse.

Da die Anzahl von IP-Adressen begrenzt ist, wird auf diese Weise verhindert, dass IP-Adressen von Computern verwendet werden, die diese nicht mehr benötigen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

2.1.5 MAC-Adressen

Jedes Netzwerkgerät hat eine so genannte MAC-Adresse (Media Access Control). Diese ist ein eindeutiger alphanumerischer Code, der dem Gerät werkseitig vergeben wird und der in den meisten Fällen auch nicht geändert werden kann (es gibt Geräte, die sich durch “MAC-Spoofing” die MAC-Adresse eines anderen Geräts erschleichen können).

Da sich die IP-Adressen mit der Zeit ändern können (manuell oder über den DHCP-Server), kann man Netzwerkgeräte am zuverlässigsten anhand ihrer MAC-Adressen identifizieren.

Jede MAC-Adresse besteht aus 6 durch Doppelpunkte (manchmal auch Bindestriche) getrennte Gruppen von jeweils zwei Hexadezimalziffern, z. B. **00:AA:FF:1A:B5:74**.

HINWEIS: Die einzelnen Gruppen, die aus zwei Hexadezimalziffern bestehen, sind so genannte “Oktette”, da sie jeweils für 8 Bits stehen.

Eine MAC-Adresse stellt einen Computer im Netzwerk nicht genau dar. Sie stellt lediglich ein Netzwerkgerät dar, das Teil eines Computers (oder eines anderen Geräts) sein kann. Wenn z. B. ein Einzelcomputer sowohl eine Ethernet-Karte (um den CVE-30360 über einen **LAN**-Port anzuschließen) als auch eine WLAN-Karte (um den CVE-30360 über eine Drahtlosverbindung anzuschließen) hat, sind die MAC-Adressen der zwei Karten unterschiedlich. So hat auch beim CVE-30360 jedes interne Modul (Kabelmodem-Modul, Ethernet-Modul, WLAN-Modul usw.) eine eigene MAC-Adresse.

2.1.6 Routing-Modus

Wenn sich der CVE-30360 im Routing-Modus befindet, ist er für die Computer im LAN das Gateway für den Internetzugriff. Der Internetdienstanbieter weist dem CVE-30360 im WAN eine IP-Adresse zu. Der gesamte Datenverkehr für die LAN-Computer wird dann an diese IP-Adresse gesendet. Wenn DHCP aktiv ist, weist der CVE-30360 den LAN-Computern private IP-Adressen zu und sendet den entsprechenden Datenverkehr an die jeweiligen privaten IP-Adressen.

HINWEIS: Wenn DHCP nicht aktiv ist und sich der CVE-30360 im Routing-Modus befindet, muss jedem Computer im LAN eine IP-Adresse im Subnetz des CVE-30360 manuell zugewiesen werden.

Wenn sich der CVE-30360 nicht im Routing-Modus befindet, weist der Internetdienstanbieter jedem Computer, der am CVE-30360 angeschlossen ist, direkt eine IP-Adresse zu. Der CVE-30360 führt dann keine Routing-Operationen aus, d. h. der Datenverkehr fließt zwischen den Computern und dem Internetdienstanbieter.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Der Routing-Modus ist nicht vom Benutzer konfigurierbar. Er wird vom Internetdienstanbieter in der Konfigurationsdatei des CVE-30360 festgelegt.

2.1.7 Konfigurationsdateien

Die Konfigurationsdatei des CVE-30360 ist ein Dokument, das der CVE-30360 über das Internet automatisch vom Server des Internetdienstanbieters bezieht. Sie legt die Einstellungen fest, die der CVE-30360 verwenden soll. Sie enthält verschiedene Einstellungen, die in der benutzerdefinierbaren Bedienoberfläche nicht vorhanden sind und die nur vom Internetdienstanbieter festgelegt werden können.

2.1.8 Downstream- und Upstream-Datenübertragung

Die Begriffe “Downstream” und “Upstream” bezeichnen die Richtung des Datenverkehrsflusses. Bei “Downstream” fließt der Datenverkehr vom Internetdienstanbieter zum CVE-30360, bei “Upstream” fließt der Datenverkehr vom CVE-30360 zum Internetdienstanbieter.

2.1.9 Kabelfrequenzen

Wie bei Funkübertragung auch, erfolgt die Datenübertragung im Kabelnetzwerk auf unterschiedlichen Frequenzen, um Signalinterferenzen zu vermeiden.

Für den Datenverkehr wird ein anderes Frequenzband verwendet als für die TV-Übertragung. Außerdem sind auch alle Datenkanäle getrennt.

2.1.10 Modulation

Datenübertragungen über das Kabelnetzwerk basieren auf einer starken, hochfrequenten periodischen Wellenform, einer so genannten “Trägerwelle”, die das Datensignal “trägt”. Das Datensignal selbst zeichnet sich durch die Variationen der Trägerwelle aus. Der Vorgang, bei dem die Trägerwelle für den Transport von Datensignalinformationen verändert wird, bezeichnet man als “Modulation”. Das Datensignal ist entsprechend das “Modulationssignal”.

Für die Kabelübertragung werden verschiedene Verfahren zur Modulation (und zur “Decodierung” bzw. “Demodulation” des empfangenen Signals) verwendet. Folgende Modulationsmethoden sind im DOCSIS 3 definiert:

- **QPSK**: Quadrature Phase-Shift Keying

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- **QAM**: Quadrature Amplitude Modulation
- **QAM TCM**: Trellis Modulated Quadrature Amplitude Modulation

In vielen Fällen wird dem Modulationstyp eine Zahl vorangesetzt (z. B. **16 QAM**). Diese Zahl bezeichnet die Komplexität der Modulation. Je höher die Zahl ist, um so mehr Daten können in jedem Symbol verschlüsselt werden.

HINWEIS: Bei modulierten Signalen ist jedes individuelle modulierte Zeichen (z. B. jeder von einem Modem bei der Übertragung über die Telefonleitung erzeugter Ton) ein so genanntes Symbol.

Da mehr Informationen von einem einzelnen Zeichen dargestellt werden können, bedeutet eine höhere Zahl auch eine höhere Datenübertragungsrate.

2.1.11 TDMA, FDMA und SCDMA

TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) und SCDMA (Synchronous Code Division Multiple Access) sind Kanalzugriffsverfahren, die es ermöglichen, dass mehrere Benutzer denselben Frequenzkanal verwenden.

- Bei TDMA können mehrere Benutzer durch die zeitliche Trennung der Datenübertragungen denselben Frequenzkanal verwenden. Jedem Benutzer wird eine bestimmte Anzahl von Zeitfenstern zugewiesen, in denen die Datenübertragung erfolgen kann.
- Bei FDMA können mehrere Benutzer durch die Zuweisung eines Frequenzbandes innerhalb des Kanals denselben Frequenzkanal verwenden.
- Bei SCDMA können mehrere Benutzer durch die Zuweisung eines eindeutigen orthogonalen Codes denselben Frequenzkanal verwenden.

2.2 Die Eingabemaske Systeminfo

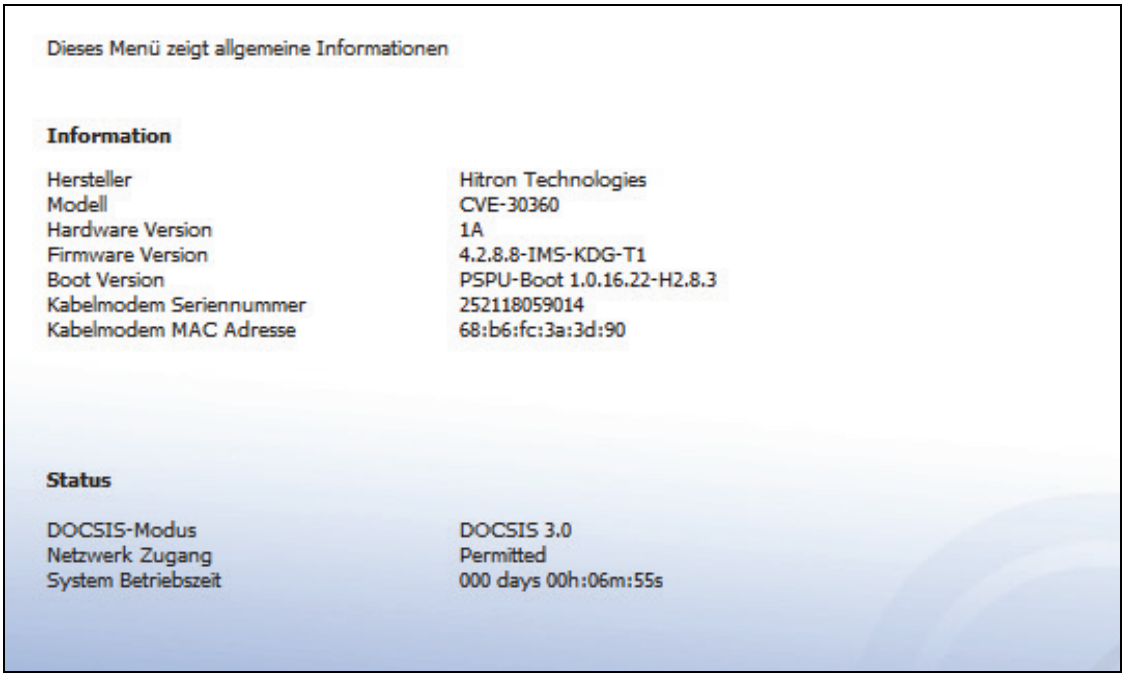
In dieser Eingabemaske werden allgemeine Informationen zur Hardware und Software des CVE-30360 sowie zur Internetverbindung angezeigt.

HINWEIS: Die meisten hier angezeigten Informationen benötigen Sie nur im Falle einer Fehlerbehebung. Hier finden Sie u. a. auch Informationen zur MAC-Adresse, die Sie zum Einrichten des Netzwerks benötigen.

Klicken Sie auf **Kabelmodem** > **Systeminfo**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 7: Die Eingabemaske Kabelmodem > Systeminfo



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 9: Die Eingabemaske Kabelmodem > Systeminfo

Information	
Hersteller	Hier wird der Name des Herstellers des CVE-30360 angezeigt.
Modell	Hier wird der Gerätemodellname angezeigt (CVE-30360).
Hardware Version	Hier wird die Versionsnummer der Hardware des CVE-30360 angezeigt.
Firmware Version	Hier wird die Versionsnummer der Software des CVE-30360 angezeigt.
Boot Version	Hier wird die Versionsnummer des Programms angezeigt, die den Bootvorgang (während die Hauptsoftware geladen wird) des CVE-30360 steuert.
Kabelmodem Seriennummer	Hier wird die Identifikationsnummer des Kabelmodems angezeigt. Der Hersteller weist jedem Gerät eine eigene Nummer zu.
Kabelmodem MAC Adresse	Hier wird die MAC-Adresse des Kabelmodems angezeigt, durch die das Gerät im Netzwerk erkennbar ist.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 9: Die Eingabemaske Kabelmodem > Systeminfo (Fortsetzung)

Status	
DOCSIS-Modus	Hier wird die Version des DOCSIS-Standards angezeigt, dem der CVE-30360 entspricht.
Netzwerk Zugang	Hier wird angezeigt, wenn Sie mit Ihrem Internetdienstanbieter verbunden sind, und Sie können hier erkennen, ob der Internetdienstanbieter Ihnen den Zugriff auf das Internet über die **CATV**-Verbindung erlaubt. • Wenn Sie auf das Internet zugreifen können, erscheint **Permitted** (Zugelassen). • Wenn Sie nicht auf das Internet zugreifen können, erscheint **Denied** (Verweigert).
System Betriebszeit	Hier wird die Dauer in Tagen, Stunden, Minuten und Sekunden seit dem letzten Einschalten oder Neustart des CVE-30360 angezeigt.

2.3 Die Eingabemaske Verbindung

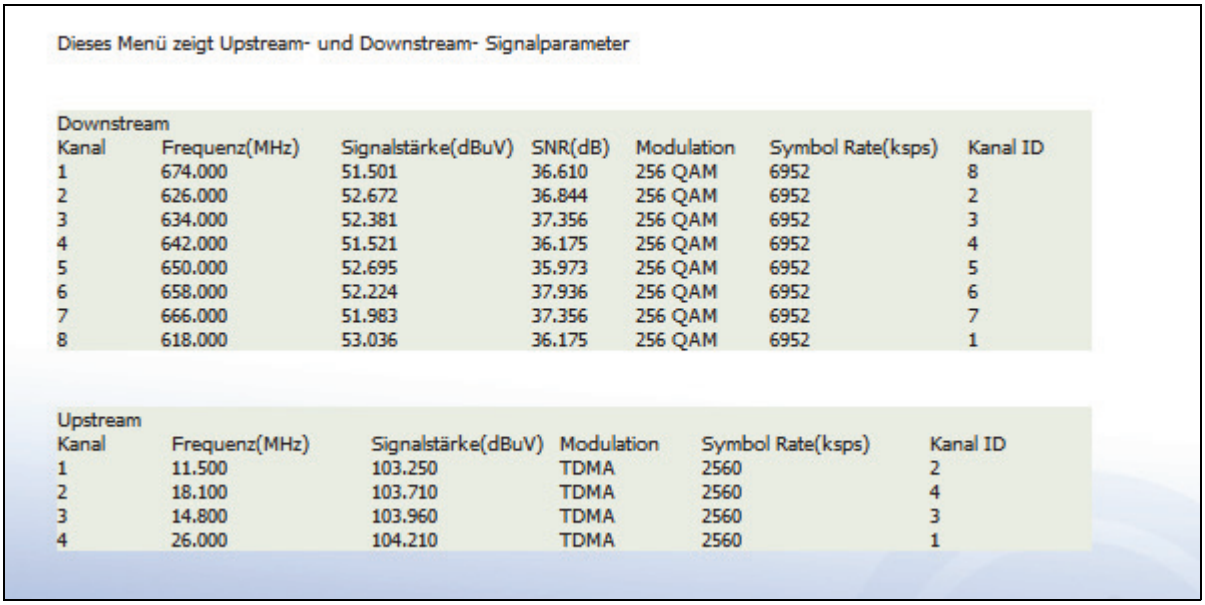
Auf dieser Eingabemaske erhalten Sie die folgenden Informationen:

- Die Art der Upstream- und Downstreamverbindung zwischen dem CVE-30360 und dem Gerät, mit dem er über die **CATV**-Schnittstelle verbunden ist.
- IP-Informationen der WAN-Verbindung des CVE-30360.

Klicken Sie auf **Kabelmodem** > **Verbindung**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 8: Die Eingabemaske Kabelmodem > Verbindung



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 10: Die Eingabemaske Kabelmodem > Verbindung

Downstream HINWEIS: Das Downstream-Signal ist das zum CVE-30360 gesendete Signal.	
Kanal	Hier werden die Indexnummern der Downstream-Kanäle des CVE-30360 angezeigt.
Frequenz	Hier wird die gerade verwendete Frequenz aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Signalstärke	Hier wird die Signalstärke (in dBmV) aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
SNR (dB)	Hier wird das Signal-Rausch-Verhältnis (in dB) aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Modulation	Hier wird der Modulationstyp angezeigt, die jeder Downstream-Kanal verwendet.
Symbol Rate (ksps)	Hier wird die Anzahl der bei der Downstream-Übertragung erfolgreich übertragenen Symbole angezeigt (Tausend Symbole pro Sekunde - KSPS).

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 10: Die Eingabemaske Kabelmodem > Verbindung (Fortsetzung)

Kanal ID	Hier wird die Identifikationsnummer aller Downstream-Datenkanäle angezeigt, mit denen der CVE-30360 kommuniziert.
Upstream HINWEIS: Das Upstream-Signal ist das vom CVE-30360 gesendete Signal.	
Kanal	Hier werden die Indexnummern der Upstream-Kanäle des CVE-30360 angezeigt.
Frequenz	Hier wird die gerade verwendete Frequenz aller Upstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Signalstärke	Hier wird die Signalstärke in dBmV (Dezibel über/unter 1 Millivolt) aller Upstream-Datenkanäle angezeigt, mit denen der CVE-30360 verbunden ist.
Modulation	Hier wird der Modulationstyp angezeigt, die jeder Upstream-Kanal verwendet.
Symbol Rate (ksps)	Hier wird die Anzahl der bei der Upstream-Übertragung erfolgreich übertragenen Symbole angezeigt (Tausend Symbole pro Sekunde - KSPS).
Kanal ID	Hier wird die Identifikationsnummer aller Upstream-Datenkanäle angezeigt, mit denen der CVE-30360 kommuniziert.

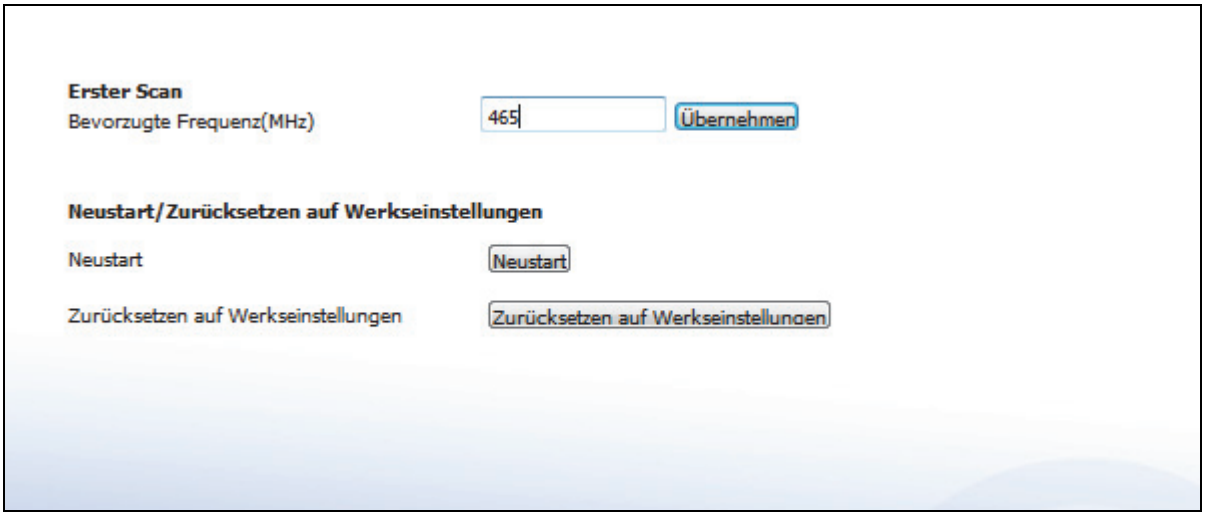
2.4 Die Eingabemaske Konfiguration

Auf dieser Eingabemaske können Sie die Downstream-Mittenfrequenz konfigurieren oder den CVE-30360 neu starten oder auf die Standardeinstellungen zurücksetzen.

Klicken Sie auf **Kabelmodem** > **Konfiguration**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 9: Die Eingabemaske Kabelmodem > Konfiguration



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 11: Die Eingabemaske Kabelmodem > Verbindung

Erster Scan	
Bevorzugte Frequenz	Hier wird die aktuelle Mittenfrequenz in Hertz (Hz) angezeigt, über die die Daten über die **CATV**-Schnittstelle zum CVE-30360 gesendet werden. Auf diese Frequenz ist der CVE-30360 so lange festgelegt, bis diese Frequenz nicht mehr verfügbar ist. Wenn Sie möchten, dass sich der CVE-30360 mit einer anderen Frequenz verbindet, geben Sie diese in dieses Feld ein, und klicken Sie auf **Übernehmen**. HINWEIS: Die Frequenz sollte aber nur geändert werden, wenn es unbedingt nötig ist.
Neustart/Zurücksetzen auf Werkseinstellungen	
Neustart	Klicken Sie hier, um den CVE-30360 zurückzusetzen.
Zurücksetzen auf Werkseinstellungen	Klicken Sie hier, um den CVE-30360 auf die Standardeinstellungen zurückzusetzen. HINWEIS: In diesem Fall gehen alle benutzerdefinierten Einstellungen verloren und können nicht wiederhergestellt werden.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

3

LAN

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **LAN** klicken. Es umfasst die folgenden Abschnitte:

3.1 Übersicht über den Menüpunkt LAN

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **LAN** beschrieben.

3.1.1 LAN-Netzwerke

Ein LAN-Netzwerk (Local Area Network) ist ein Netzwerk von Computern und anderen Geräten, das normalerweise einen kleinen begrenzten Bereich (z. B. ein Gebäude) abdeckt. Das LAN des CVE-30360 besteht aus allen Computern und Netzwerkgeräten, die an die Ports **LAN 1**-**4** angeschlossen sind. Es ist Ihr privates Netzwerk (im Routing-Modus - siehe Routing-Modus auf Seite 34).

Das LAN ist ein vom WAN (Wide Area Network) abgetrenntes Netzwerk. Für den CVE-30360 umfasst das WAN alle Computer und sonstigen Geräte, die in der Kabelverbindung (**CATV**) verfügbar sind.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Standardmäßig können Computer des WAN nicht einzelne Computer eines LAN identifizieren. Sie erkennen nur den CVE-30360. Der CVE-30360 wickelt das Routing von und zu den einzelnen Computern im LAN ab.

3.1.2 LAN IP-Adressen und Subnetze

IP-Adressen im LAN werden entweder vom DHCP-Server des CVE-30360 gesteuert (siehe DHCP auf Seite 33) oder von Ihnen selbst festgelegt, wenn Sie Ihren Computern manuell IP-Adressen zuweisen.

Weitere allgemeine Informationen zu IP-Adressen und Subnetzen finden Sie unter IP-Adressen und Subnetze auf Seite 30.

3.1.3 Domain-Suffix

Eine Domain ist eine Position in einem Netzwerk, z. B. **example.com**. Im Internet werden die IP-Adressen in der Form eines Domainnamens entsprechend des Domainnamensystems umgesetzt. Dadurch gelangen Sie bei Eingabe von “www.example.com” in den Browser auch dann zur entsprechenden Position im Internet, wenn sich die IP-Adresse des Website-Servers geändert hat.

Ähnlich haben Sie auch beim CVE-30360 die Möglichkeit, einen **Domain-Suffix** für das LAN festzulegen. Wenn Sie den Domain-Suffix in den Browser eingeben, erreichen Sie den CVE-30360 unabhängig von seiner IP-Adresse im LAN.

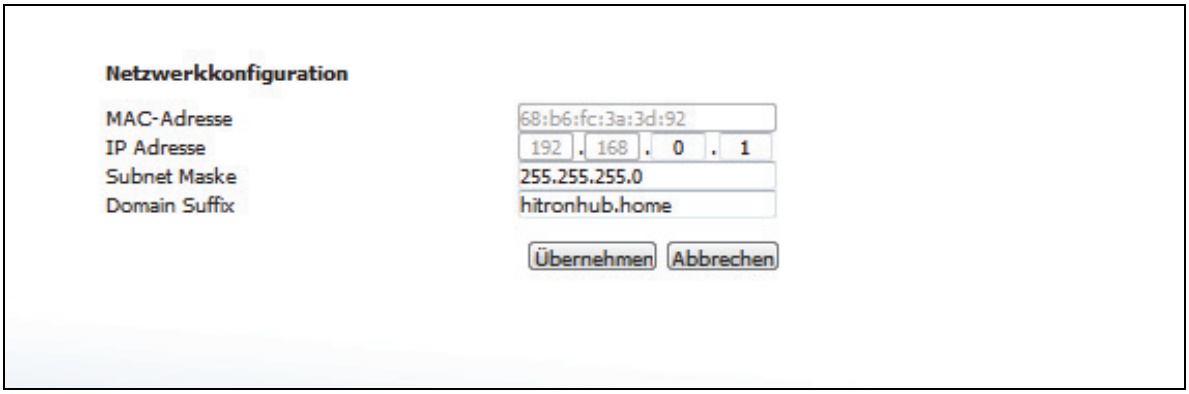
3.2 Die Eingabemaske LAN IP

Die LAN IP-Adresse, die Subnetzmaske und den Domain-Suffix des CVE-30360 konfigurieren.

Klicken Sie auf **LAN** > **LAN Setup**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 10: Die Eingabemaske LAN > LAN Setup



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 12: Die Eingabemaske LAN > LAN Setup

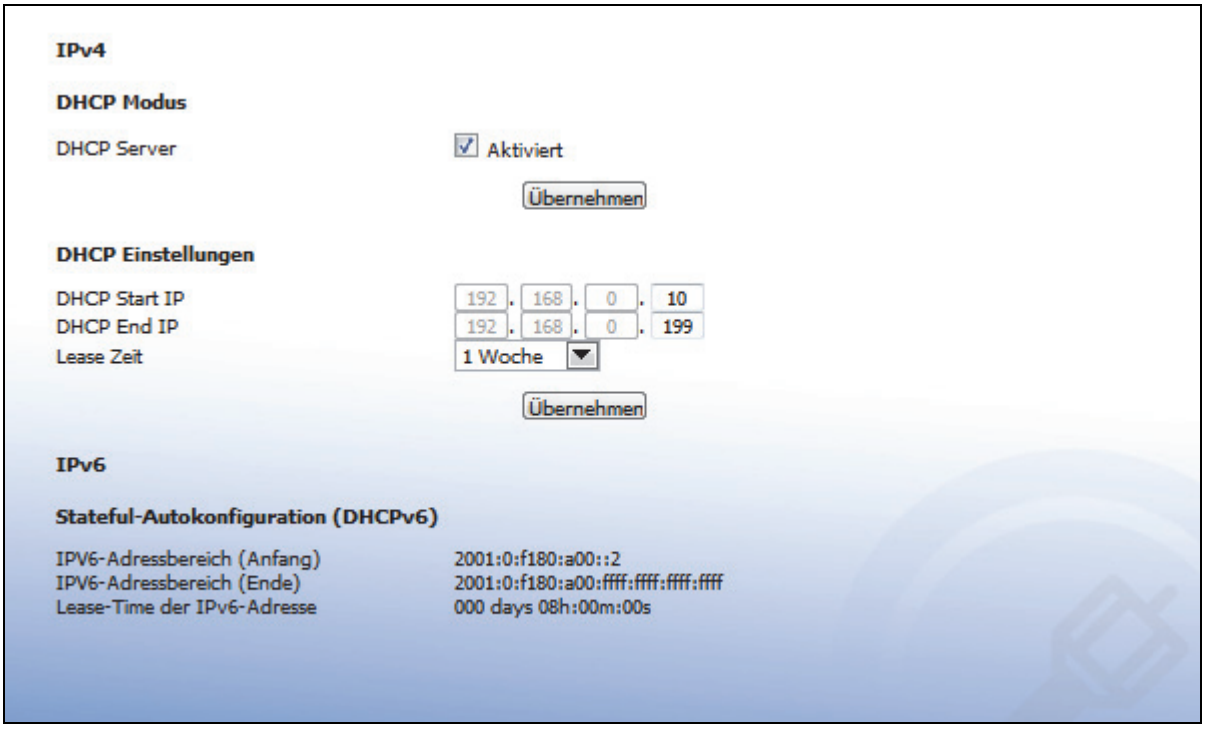
Netzwerkkonfiguration	
MAC-Adresse	Hier wird die MAC-Adresse des CVE-30360 im LAN angezeigt.
IP Adresse	In diesem Feld können Sie die IP-Adressen des CVE-30360 im LAN festlegen.
Subnet Maske	In diesem Feld können Sie das LAN-Subnetz festlegen. Verwenden Sie die Dezimalschreibweise mit Trennpunkten (z. B. **255.255.255.0**).
Domain Suffix	In diesem Feld können Sie die Domain festlegen, die anstelle einer IP-Adresse in einen Webbrowser eingegeben werden kann, um im LAN auf den CVE-30360 zuzugreifen. HINWEIS: Der **Domain-Suffix** ist standardmäßig **hitronhub.home**.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.

3.3 Die Eingabemaske DHCP

Auf dieser Eingabemaske können Sie den internen DHCP-Server des CVE-30360 konfigurieren.

HINWEIS: Diese Eingabemaske unterscheidet sich je nachdem, ob der CVE-30360 im IPv4- oder im DS-Lite-Modus arbeitet.

Abbildung 11: Die Eingabemaske LAN > DHCP



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 13: Die Eingabemaske LAN > DHCP

IPv4 HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4.	
DHCP Server (DHCP-Server)	Wählen Sie die Option **Aktiviert**, wenn der CVE-30360 den Netzwerkgeräten im IPv4-Modus im LAN automatisch IP-Adressen zuweisen soll. Entfernen Sie die Markierung bei dieser Option, wenn bereits ein DHCP-Server im LAN vorhanden ist oder wenn Sie den Computern und anderen Netzwerkgeräten manuell IP-Adressen zuweisen möchten. Klicken Sie auf **Übernehmen**, um die Änderungen in dieser Eingabemaske zu übernehmen.
DHCP Start IP	In diesem Feld können Sie die erste IP-Adresse festlegen, die der CVE-30360 einem Gerät im LAN zuweist (wenn im IPv4-Modus DHCP aktiviert ist).

Tabelle 13: Die Eingabemaske LAN > DHCP (Fortsetzung)

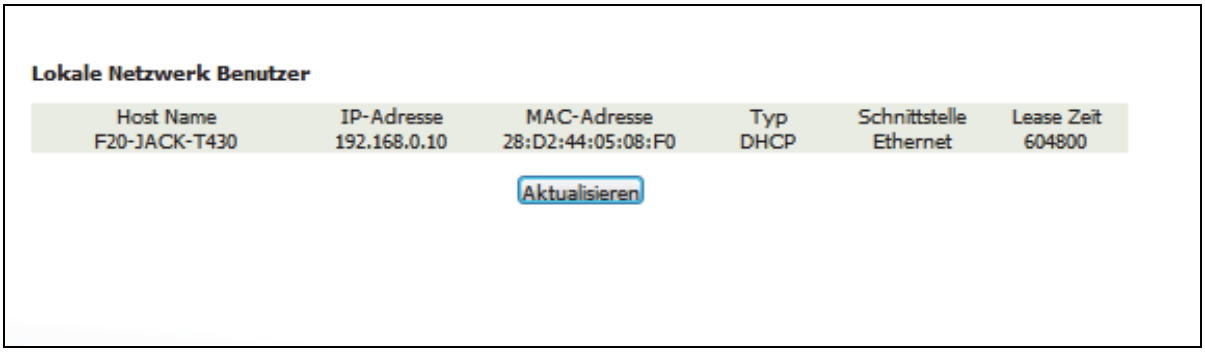
DHCP End IP	In diesem Feld können Sie die letzte IP-Adresse festlegen, die der CVE-30360 einem Gerät im LAN zuweist (wenn im IPv4-Modus DHCP aktiviert ist). HINWEIS: Geräten, die eine IP-Adresse anfordern, erhalten keine IP-Adresse mehr, wenn alle IP-Adressen aus dem DHCP-Pool verbraucht sind.
Lease Zeit	In diesem Feld können Sie festlegen, nach welcher Zeit der CVE-30360 die IP-Adressen aller im LAN an den CVE-30360 angeschlossenen Netzwerkgeräte erneuern soll (wenn DHCP aktiviert ist).
Übernehmen	Klicken Sie hier, um die Änderungen im Abschnitt **DHCP Einstellung** zu übernehmen.
IPv6 HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf den DS-Lite-Betrieb.	
IPv6-Adressbereich (Anfang)	In diesem Feld können Sie die erste IPv6-Adresse festlegen, die der CVE-30360 einem Gerät im DS-Lite-Modus im LAN zuweist.
IPv6-Adressbereich (Ende)	In diesem Feld können Sie die letzte IPv6-Adresse festlegen, die der CVE-30360 einem Gerät im DS-Lite-Modus im LAN zuweist. HINWEIS: Geräten, die eine IP-Adresse anfordern, erhalten keine IP-Adresse mehr, wenn alle IP-Adressen aus dem DHCP-Pool verbraucht sind.
Lease-Time der IPv6-Adresse	In diesem Feld können Sie festlegen, nach welcher Zeit der CVE-30360 im DS-Lite-Modus die IPv6-Adressen aller im LAN an den CVE-30360 angeschlossenen Netzwerkgeräte erneuern soll.

3.4 Die Eingabemaske Lokale Netzwerk Benutzer

Auf dieser Eingabemaske können Sie Informationen über die im LAN an den CVE-30360 angeschlossenen Geräte abrufen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 12: Die Eingabemaske LAN > Lokale Netzwerk Benutzer



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 14: Die Eingabemaske LAN > LAN Users (LAN-Nutzer)

Host Name	Hier werden die Namen aller mit dem LAN verbundenen Netzwerkgeräte angezeigt.
IP-Adresse	Hier werden die IP-Adressen aller mit dem LAN verbundenen Netzwerkgeräte angezeigt.
MAC-Adresse	Hier werden die MAC-Adressen aller mit dem LAN verbundenen Netzwerkgeräte angezeigt.
Typ	Hier wird angezeigt, ob die IP-Adresse des Geräts vom DHCP-Server (**DHCP-IP**) oder manuell selbst vergeben wurde.
Schnittstelle	Hier wird angezeigt, ob das Gerät über das LAN (**Ethernet**) oder das WLAN (**Wireless(x)** verbunden ist. Das **x** steht für den Drahtlosmodus **b**, **g** oder **n**).
Lease Zeit	Hier wird angezeigt, wie viele Sekunden vergangen sind, seit dem im LAN angeschlossenen Netzwerkgerät die IP-Adresse zugewiesen wurde.
Aktualisieren	Klicken Sie hier, um die Daten auf dieser Eingabemaske zu aktualisieren.

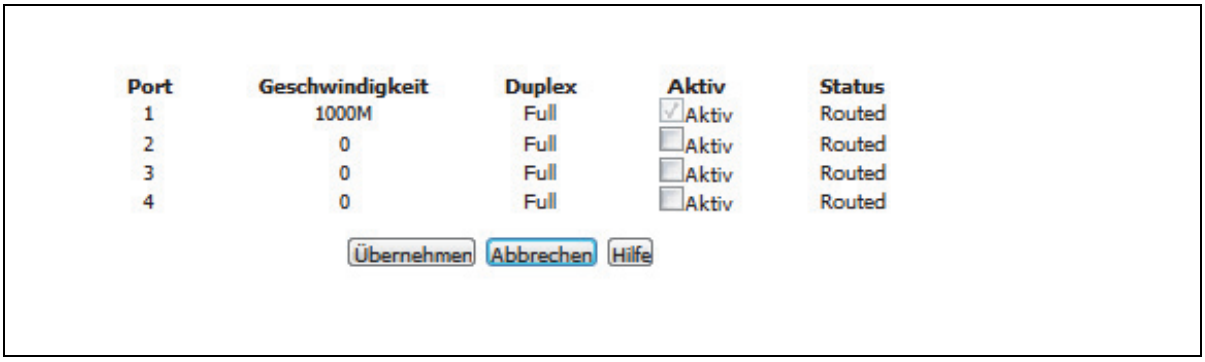
3.5 Die Eingabemaske Switch-Setup

Diese Maske enthält Informationen über die Datenrate und den Datenfluss aller **LAN**-Ports des CVE-30360, und hier können Sie die einzelnen Ports aktivieren oder deaktivieren.

Klicken Sie auf **LAN** > **Switch-Setup**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 13: Die Eingabemaske LAN > Switch-Setup



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 15: Die Eingabemaske LAN > Switch-Setup

Port	Hier wird die LAN-Portnummer angezeigt.
Geschwindigkeit	Hier wird die maximal erreichbare Datengeschwindigkeit in Megabits pro Sekunde (MBPS) angezeigt.
Duplex	▸ Hier erscheint **Full** (Voll), wenn die Daten zwischen dem CVE-30360 und dem angeschlossenen Gerät in beide Richtungen gleichzeitig fließen können. ▸ Hier erscheint **Half** (Halb), wenn die Daten zwischen dem CVE-30360 und dem angeschlossenen Gerät in jeweils nur einer Richtung fließen können.
Aktiv	▸ Markieren Sie das Kontrollkästchen eines **Ports**, um die Kommunikation zwischen dem CVE-30360 und den an den Port angeschlossenen Geräten zu aktivieren. ▸ Entfernen Sie die Markierung aus dem Kontrollkästchen eines **Ports**, wenn keine Daten zwischen dem CVE-30360 und den an den Port angeschlossenen Geräten ausgetauscht werden sollen.
Status	Hier wird der aktuelle Routing-Status des Ports angezeigt.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

4

WAN

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **WAN** klicken. Es umfasst die folgenden Abschnitte:

4.1 Übersicht über den Menüpunkt WAN

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **WAN** beschrieben.

4.1.1 Fehlersuche (Ping und Traceroute)

Der CVE-30360 verfügt über einige Tools, mit denen Sie eine Netzwerkdiagnose im WAN durchführen können:

- Ping: Bei diesem Tool können Sie eine IP-Adresse eingeben und prüfen, ob ein Computer (oder ein anderes Netzwerkgerät) mit dieser Adresse im Netzwerk reagiert. Die Bezeichnung ist abgeleitet vom Impuls, den ein Unterwasserschallgerät aussendet, wenn es nach Objekten unter Wasser sucht. Beim Ping wird ähnlich vorgegangen. Mit diesem Tool können Sie feststellen, ob eine IP-Adresse genutzt wird oder ob ein Gerät oder Dienst (dessen IP-Adresse Sie kennen) richtig funktioniert.
- Traceroute: Mit diesem Tool können Sie nachverfolgen, welchen Weg bestimmte Datenpakete genommen haben, um vom CVE-30360 zum festgelegten Ziel zu gelangen. Mit diesem Tool können Sie Routing-Probleme lösen oder Firewalls erkennen, die den Zugriff auf einen Computer oder Dienst blockieren.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

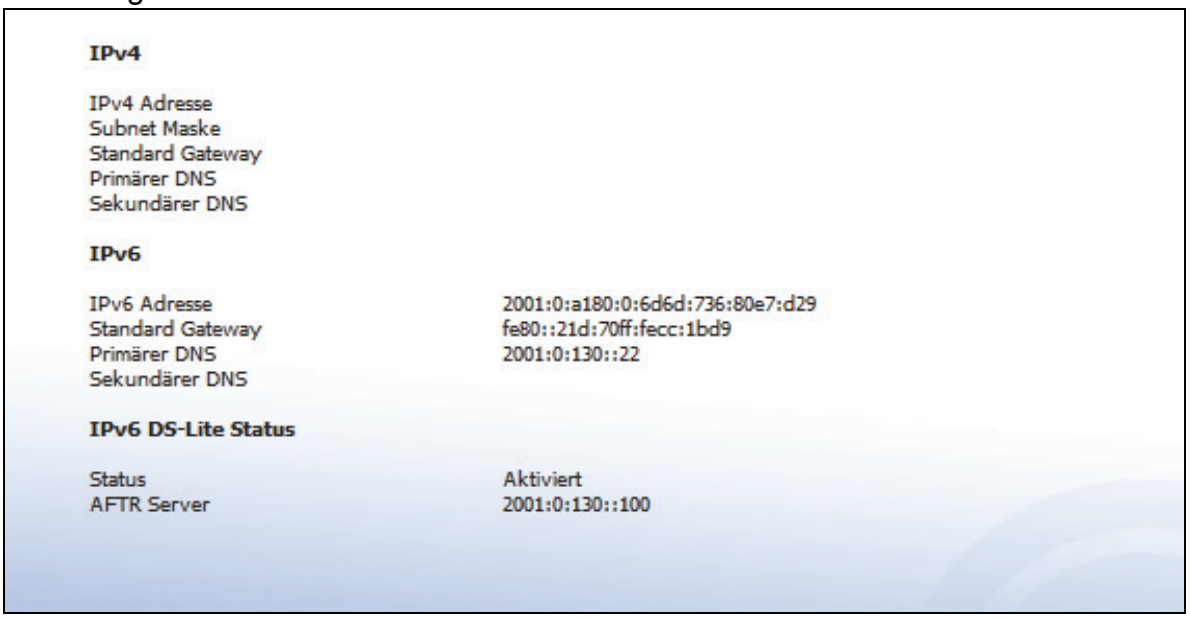
4.2 Die Maske WAN Status

In dieser Eingabemaske werden Informationen zur Internetverbindung des CVE-30360 und zum DS-Lite-Verbindungsstatus angezeigt.

Klicken Sie auf **WAN** > **WAN Status**. Die folgende Eingabemaske erscheint.

HINWEIS: Diese Eingabemaske unterscheidet sich je nachdem, ob der CVE-30360 im IPv4- oder im DS-Lite-Modus arbeitet.

Abbildung 14: Die Maske WAN > WAN Status



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 16: Die Maske WAN > WAN Status

IPv4 HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4.	
IPv4 Adresse	Im IPv4-Modus werden hier die IPv4-Adresse und Subnetzmaske des CVE-30360 angezeigt, die das Gerät vom Internetdienstanbieter bezieht.
Subnetzmaske	
Standard Gateway	Im IPv4-Modus wird hier die IP-Adresse des Gateways des CVE-30360 im WAN angezeigt.
Primärer DNS	Im IPv4-Modus wird hier die IP-Adresse des primären DNS-Servers des CVE-30360 angezeigt.

Tabelle 16: Die Maske WAN > WAN Status (Fortsetzung)

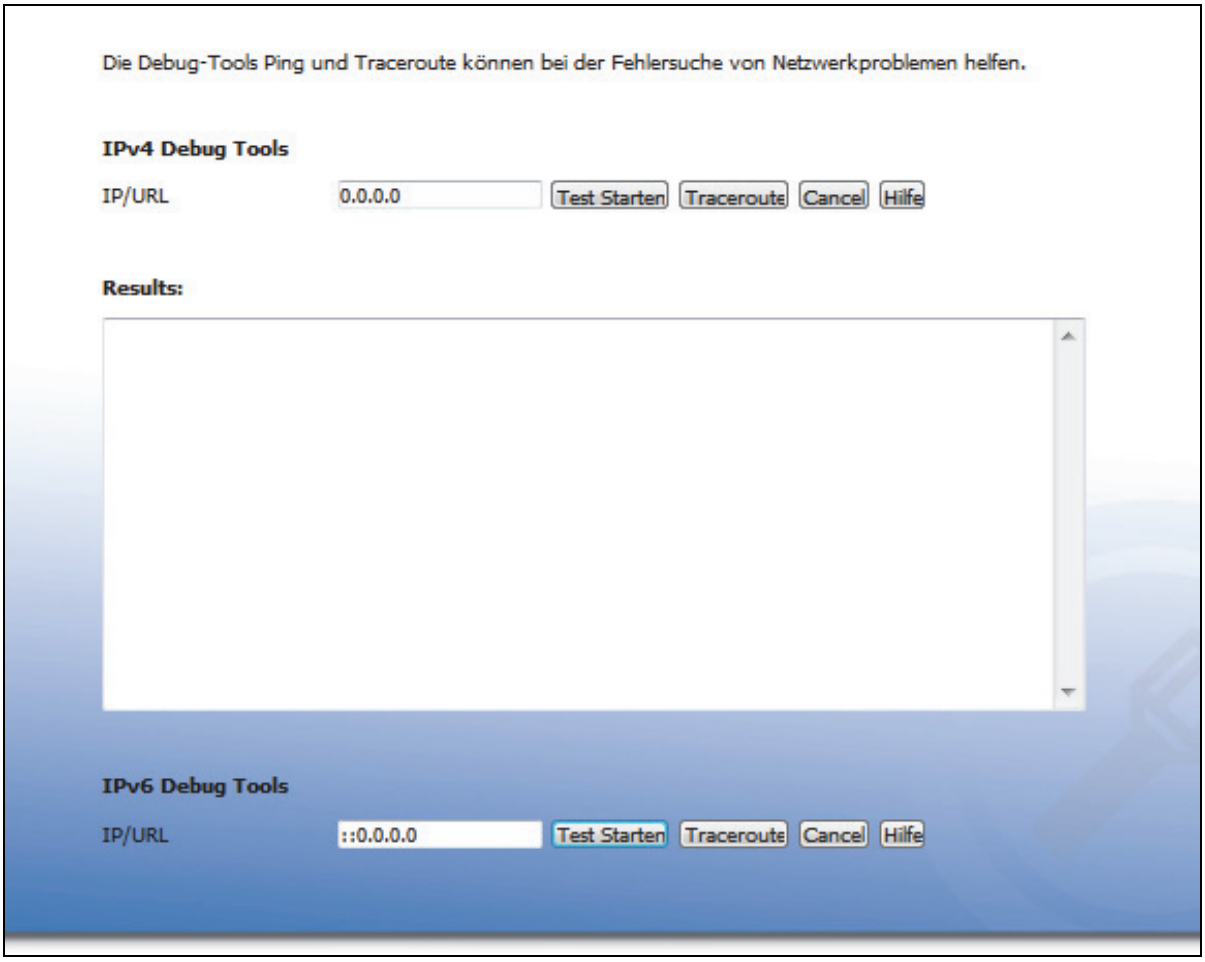
Sekundärer DNS	Im IPv4-Modus wird hier die IP-Adresse des sekundären DNS-Servers des CVE-30360 angezeigt.
IPv6 HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf den DS-Lite-Betrieb.	
IPv6 Adresse)	Im IPv6-Modus werden hier die IPv6-Adresse und Subnetzmaske des CVE-30360 angezeigt, die das Gerät vom Internetdienstanbieter bezieht.
Standard Gateway	Im IPv6-Modus wird hier die IP-Adresse des Gateways des CVE-30360 im WAN angezeigt.
Primärer DNS	Im IPv6-Modus wird hier die IP-Adresse des primären DNS-Servers des CVE-30360 angezeigt.
Sekundärer DNS	Im IPv6-Modus wird hier die IP-Adresse des sekundären DNS-Servers des CVE-30360 angezeigt.
IPv6 DS-Lite Status HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf den DS-Lite-Betrieb.	
Status	Diese Option ist **Aktiviert**, wenn der CVE-30360 im DS-Lite-Modus läuft. Sie ist **Deaktiviert**, wenn der CVE-30360 im IPv4-Modus arbeitet.
AFTR Server	Hier wird die IPv6-Adresse des AFTR-Servers (Address Family Transition Router) angezeigt, der den DS-Liste-Verkehr im Netzwerk verwaltet.

4.3 Die Eingabemaske WAN Debug

Auf dieser Maske können Sie Pings und Traceroute-Tests für IP-Adressen oder URLs ausführen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 15: Die Maske WAN > Debug



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 17: Die Maske WAN > Debug

IPv4 Debug Tools HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4.	
IP/URL	Geben Sie die IPv4-Adresse oder die URL ein, die Sie prüfen möchten.
Ping	Wählen Sie den Testtyp aus, den Sie auf die von Ihnen eingegebene **IP/URL** anwenden möchten.
Traceroute	
IPv6 Debug Tools HINWEIS: Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf den DS-Lite-Betrieb.	

Tabelle 17: Die Maske WAN > Debug (Fortsetzung)

IP/URL	Geben Sie die IPv6-Adresse oder die URL ein, die Sie prüfen möchten.
Ping	Wählen Sie den Testtyp aus, den Sie auf die von Ihnen eingegebene **IP/URL** anwenden möchten.
Traceroute	
Results	In diesem Feld werden die Daten des letzten Testlaufs angezeigt.
Cancel	Klicken Sie hier, um einen Testlauf zu stoppen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

5

Wireless

Dieses Kapitel ist eine Einführung in die Arbeit mit WLAN-Netzwerken. Es werden einige allgemeine Schritte zum Einrichten von WLAN-Netzwerken beschrieben und die Eingabemasken erläutert, die angezeigt werden, wenn Sie in der Symbolleiste auf **WLAN** klicken. Es umfasst die folgenden Abschnitte:

- WLAN - Grundlagen auf Seite 54: In diesem Abschnitt wird beschrieben, wie WLAN-Netzwerke arbeiten und gesichert werden.
- Anleitung zur Nutzung der Drahtlosfunktion auf Seite 56: In diesem Abschnitt wird beschrieben, wie Sie mit dem CVE-30360 allgemeine Einstellungen für das WLAN-Netzwerk konfigurieren können.
- Erweiterte Netzwerkfunktionen auf Seite 60: Dieser Abschnitt enthält ausführlichere Informationen zu diesem Thema.
  Wenn Sie Ihr WLAN-Netzwerk in einer Standard-Konfiguration errichten möchten, können Sie diesen Abschnitt überspringen.
- Die Eingabemasken für die Drahtloskonfiguration auf Seite 62: In diesem Abschnitt erhalten Sie ausführliche Informationen zu allen WLAN-Eingabemasken des CVE-30360.
  Dieser Abschnitt ist nützlich, wenn Sie Informationen zu einer bestimmten Eingabemaske oder zu einem Eingabefeld benötigen.

5.1 WLAN - Grundlagen

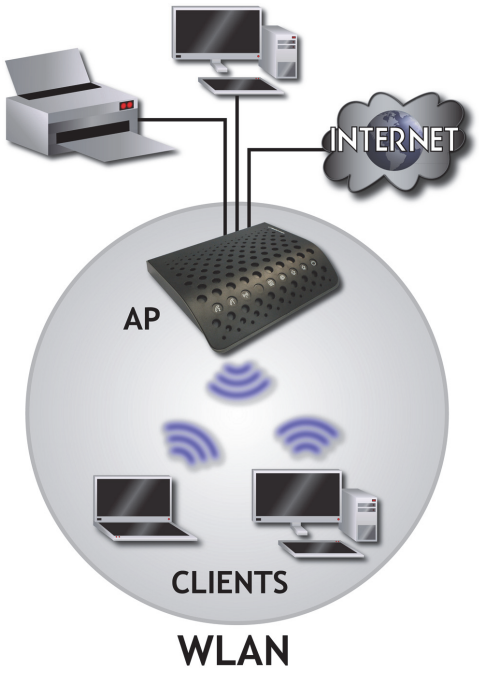
In diesem Abschnitt wird beschrieben, wie WLAN-Netzwerke arbeiten und gesichert werden.

Das WLAN-Netzwerk des CVE-30360 ist Teil des LAN-Netzwerks (Local Area Network). WLAN steht für Wireless LAN (drahtloses LAN). Das WLAN ist ein Netzwerk von Funkverbindungen zwischen dem CVE-30360 und den anderen angeschlossenen Computern und Geräten.

In der folgenden Abbildung ist das Drahtlosnetzwerk durch den Kreis gekennzeichnet. Das Notebook und der PC sind die Wireless Clients, die an den CVE-30360, dem Zugriffspunkt oder auch Access Point (AP) angeschlossen sind. Die Wireless Clients nutzen den AP, um auf andere Geräte (z. B. den Drucker) oder auf das Internet zuzugreifen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 16: Beispiel für ein Drahtlosnetzwerk



5.1.1 WLAN-Standards

Wie Drahtlosgeräte miteinander kommunizieren, wird vom Institute of Electrical and Electronics Engineers (IEEE) standardisiert. Die IEEE-Standards für Wireless LANs sind an ihrer Bezeichnung 802.11 zu erkennen. Es gibt verschiedene WLAN-Standards, von denen der CVE-30360 nur die Folgenden unterstützt (sortiert nach Einführung - von alt nach neu - und Datenübertragungsgeschwindigkeit - von niedrig nach hoch):

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

5.1.2 SERVICE SETS UND SSIDS

Alle Geräte eines Drahtlosnetzwerks bilden zusammen das so genannte Service Set.

Jedes Service Set ist durch einen Service Set IDentifier (SSID) gekennzeichnet. Dieses ist der Name des Netzwerks. Den Wireless Clients muss die SSID bekannt sein, damit sie die Verbindung zum AP herstellen können.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Sie können den CVE-30360 so konfigurieren, dass er die SSID sendet (in diesem Fall kann jeder Client, der die Funkwellen abtastet, die SSID erkennen), oder die SSID verbirgt (in diesem Fall wird sie nicht ausgesendet, sodass nur die Benutzer, welche die SSID kennen, eine Verbindung herstellen können). Weitere Informationen dazu finden Sie unter Verbergen des Netzwerks auf Seite 59.

5.1.3 Grundlagen für die WLAN-Sicherheit

Die Funkübertragung ist an sich ein unsicheres Medium, da sie innerhalb der Reichweite von jedem empfangen werden kann, der über ein Empfangsgerät verfügt. Aus diesem Grund gibt es unterschiedliche Verfahren, diese Art der Übertragung sicherer zu machen.

Diese Verfahren steuern die Authentifizierung (es wird festgelegt, wer Zugriff zum Netzwerk haben soll) und die Verschlüsselung (verschlüsselte Signale können nur von authentifizierten Benutzern entschlüsselt werden). Die Ausgereiftheit sowie die Effektivität jeder dieser Sicherheitsverfahren sind sehr unterschiedlich.

Der CVE-30360 unterstützt die folgenden drahtlosen Sicherheitsprotokolle (angeordnet nach Effektivität):

Weitere Informationen zu diesen Sicherheitsprotokollen finden Sie unter Erweiterte Sicherheitseinstellungen im Drahtlosnetzwerk auf Seite 60.

5.2 Anleitung zur Nutzung der Drahtlosfunktion

In diesem Abschnitt werden grundlegende Netzwerkverwaltungsaufgaben beschrieben.

HINWEIS: Eine Beschreibung der Grundlagen zum Einrichten des Drahtlosnetzwerks finden Sie in der Kurzanleitung, die Sie zusammen mit dem CVE-30360 erhalten haben.

Dazu gehören:

- Auswählen eines Sicherheitsverfahrens auf Seite 57

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- Wechseln des Passworts für den Zugriff auf das Drahtlosnetzwerk auf Seite 58
- Ändern des Netzwerknamens (SSID) auf Seite 59
- Verbergen des Netzwerks auf Seite 59
- Verbessern der Leistung des Drahtlosnetzwerks auf Seite 59

5.2.1 Auswählen eines Sicherheitsverfahrens

Welches Sicherheitsverfahren Sie für Ihr Drahtlosnetzwerk auswählen, ist abhängig von den Sicherheitsverfahren, die Ihre Geräte im Netzwerk (der CVE-30360, Ihr PC, Ihr Notebook usw.) unterstützen.

Nicht alle Geräte unterstützen alle Verfahren. Sie müssen also zuerst herausfinden, welche Verfahren die Geräte unterstützen und dann ein Verfahren auswählen, welches von allen Geräten unterstützt wird.

Ziel ist es immer, das bestmögliche Sicherheitsverfahren auszuwählen. Eine Liste der Verfahren, die der CVE-30360 unterstützt, finden Sie unter Grundlagen für die WLAN-Sicherheit auf Seite 56.

So können Sie herausfinden, welche Sicherheitsverfahren die anderen Drahtlosgeräte unterstützen:

- Möglicherweise befindet sich am Gerät ein Etikett, auf dem die unterstützten Verfahren aufgeführt sind.
- Informationen zu den unterstützten Sicherheitsverfahren können in der Dokumentation oder auf der Verpackung des jeweiligen Geräts enthalten sein.
- Im Konfigurationsprogramm des Geräts finden Sie eine Liste der unterstützten Verfahren. Es handelt sich meist um eine Dropdown-Liste, aus der Sie eine Option auswählen können.
- Auf der Website des Geräteherstellers gibt es möglicherweise eine Seite, auf der die Spezifikationen des Geräts aufgeführt sind.

Wenn Sie WPS (siehe WPS auf Seite 61) verwenden möchten, müssen alle Wireless Clients WPS unterstützen. Neben den oben beschriebenen Möglichkeiten gibt es zwei weitere Möglichkeiten herauszufinden, ob das der Fall ist:

- Suchen Sie auf dem Drahtlosgerät nach einer Taste, die mit “WPS” oder ähnlich bezeichnet ist oder ein Wellensymbol (z. B. ) oder das “Wi-Fi Protected Setup”-Logo trägt. Ist das der Fall, unterstützt das Gerät wahrscheinlich das WPS-PBC-Verfahren (“Push-Button Configuration”).

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- Rufen Sie das Konfigurationsprogramm des Drahtlosgeräts auf, und suchen Sie nach einem Menüpunkt mit der Bezeichnung “WPS” oder “Wi-Fi Protected Setup”. Hier sollte zu erkennen sein, ob das Gerät das WPS-PBC-Verfahren, das WPS-PIN-Verfahren oder sogar beide Verfahren unterstützt (einige Geräte verfügen zusätzlich zu oder anstelle einer physischen Taste am Gerät auch über eine PBC-Taste in ihrem Konfigurationsprogramm).

Wenn Sie sich für ein Sicherheitsverfahren entschieden haben, können Sie dieses am CVE-30360 im Menüpunkt **Wireless** > **Sicherheit** bei **Sicherheits Modus** (siehe Die Eingabemaske Sicherheit auf Seite 65) einstellen.

5.2.2 Wechseln des Passworts für den Zugriff auf das Drahtlosnetzwerk

Nur Wireless Clients mit dem richtigen Passwort können auf das Netzwerk zugreifen. Es wird empfohlen, das Passwort des Drahtlosnetzwerks häufiger zu wechseln, vor allem dann, wenn Sie wissen, dass Unbefugte ihr Passwort kennen oder verdächtige Aktivitäten im Netzwerk auftreten.

Das Passwort muss zunächst am CVE-30360 und dann an allen Wireless Clients geändert werden.

Das Verfahren zum Ändern des Passworts am CVE-30360 ist abhängig vom verwendeten Sicherheitsverfahren.

- Wenn Sie das Sicherheitsverfahren WPS-PBC verwenden, bei dem Sie eine Taste am CVE-30360 und dann an den Drahtlosgeräten drücken müssen, damit sich die Geräte automatisch verbinden, müssen Sie lediglich das WPS-PBC-Verfahren nocheinmal durchführen. Weitere Informationen dazu finden Sie in der Kurzanleitung, die Sie zusammen mit dem CVE-30360 erhalten haben.
- Wenn Sie das WPS-PIN-Verfahren verwenden, bei dem Sie bei jedem Gerät im Netzwerk ein WPS-Passwort eingeben müssen, rufen Sie den Menüpunkt **Wireless** > **Grundeinstellungen** auf, und klicken Sie auf die Schaltfläche **PIN**. Geben Sie im nun erscheinenden Fenster die WPS-PIN, die Sie für den CVE-30360 verwenden möchten, oder die WPS-PIN des Client-Geräts, das die zum Netzwerk hinzufügen möchten, ein.
- Wenn Sie WEP verwenden, rufen Sie den Menüpunkt **Wireless** > **Sicherheit** auf. Im Abschnitt **WEP-Einstellungen** können Sie die Schlüssel festlegen, die Sie verwenden möchten. Klicken Sie abschließend auf **Übernehmen**.
- Wenn Sie WPA-PSK oder WPA2-PSK verwenden, rufen Sie den Menüpunkt **Wireless** > **Sicherheit** auf. Geben Sie bei **WPA_Personal** im Feld PSK das neue Passwort ein. Klicken Sie abschließend auf **Übernehmen**.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Unabhängig von der Wahl des Sicherheitsverfahrens: Wenn Sie das Passwort am CVE-30360 ändern, können die anderen Geräte nur dann eine Verbindung zum Netzwerk herstellen, wenn auch bei ihnen das Passwort geändert wurde.

Wie Sie das Passwort an den Client-Geräten ändern, ist abhängig vom Hersteller und vom Modell. Normalerweise müssen Sie sich im Konfigurationsprogramm des Geräts anmelden, und dann ähnlich wie beim CVE-30360 vorgehen. Nur beim WPS-PBC-Verfahren müssen Sie lediglich auf die WPS-Taste des CVE-30360 drücken und dann innerhalb von zwei Minuten danach auf die WPS-Tasten der anderen Geräte.

HINWEIS: Wenn Sie das WPS-PBC-Verfahren verwenden müssen Sie sich darüber im Klaren sein, dass alle Geräte, die WPS unterstützen, innerhalb dieserVerbindungszeit die Verbindung zum CVE-30360 herstellen können. Es ist also kein geeignetes Verfahren für öffentliche Bereiche, oder wenn Sie den Verdacht haben, dass Unbefugte versuchen, auf das Netzwerk zuzugreifen.

5.2.3 Ändern des Netzwerknamens (SSID)

Wenn Sie die SSID (der Name, der angezeigt wird, wenn Sie mit Ihrem Wireless Client nach Drahtlosnetzwerken suchen) Ihres Drahtlosnetzwerks ändern möchten, rufen Sie das Fenster **Wireless** > **Grundeinstellungen** auf. Geben Sie den Netzwerknamen in das Feld **SSID-Name** ein, und klicken Sie auf **Übernehmen**.

HINWEIS: Da die SSID für die Verbindung zu einem Netzwerk erforderlich ist, müssen Sie mit den Client-Geräte eine neue Verbindung mit der neuen SSID herstellen.

5.2.4 Verbergen des Netzwerks

Es gibt zahlreiche Gründe dafür, ein Netzwerk für Personen unsichtbar zu machen, die nach verfügbaren drahtlosen Netzwerken suchen. Rufen Sie dazu den Menüpunkt **Wireless** > **Grundeinstellungen** auf. Markieren Sie das Kontrollkästchen verborgen, und klicken Sie auf **Übernehmen**.

5.2.5 Verbessern der Leistung des Drahtlosnetzwerks

Zwei Hauptfaktoren können sich auf die Kommunikation Ihrer Drahtlosgeräte auswirken:

1. Störungen durch physische Objekte
2. Hochfrequenz-Störungen (HF)

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

So können Sie Störungen durch physische Objekte minimieren:

- Vergrößern Sie den Abstand vom CVE-30360 zu Wänden, schweren Möbeln oder massiven oder metallischen Gegenständen wie Kühlschränken usw.
- Installieren Sie den CVE-30360 in einer höher gelegenen Position.

So können Sie Hochfrequenz-Störungen minimieren:

- Vergrößern Sie den Abstand des CVE-30360 zu Hochfrequenzenergiequellen wie der Basisstation von Schnurlostelefonen, Mikrowellengeräten usw.
- Prüfen Sie vor Ort, ob andere Netzwerke mit Ihrem Netzwerk Störungen verursachen. Ist das der Fall, können Sie für die Drahtlosverbindung einen weniger belegten Kanal verwenden.

  Um diese Vor-Ort-Prüfung am CVE-30360durchzuführen, rufen Sie den Menüpunkt **Wireless** > **WiFi Site Survey** auf. Klicken Sie auf **Scan**. Die jetzt erscheinende Maske zeigt die Drahtlosnetzwerke der Umgebung an. Im Feld **ch** ist zu sehen, welcher Kanal verwendet wird, und im Feld **signal (%)** wird angezeigt, wie stark der CVE-30360 das Signal empfängt (beachten Sie, dass die Stärke eines Netzwerks am CVE-30360 nicht unbedingt der Stärke desselben Netzwerks an der Position des Wireless Clients entspricht, dort kann das Signal viel stärker sein).

  Verwenden sehr viele Netzwerke oder ein sehr starkes Netzwerk einen Kanal oder eine Gruppe von Kanälen, können Sie den CVE-30360 auf einen weiter entfernten Kanal verlegen. Wenn Sie den CVE-30360 auf einen anderen Kanal legen möchten, rufen Sie den Menüpunkt **Wireless** > **Grundeinstellungen** auf, und wählen Sie eine Option aus der **Channel**-Liste aus. Wählen Sie einen Kanal aus, der so weit weg wie möglich vom belegten Bereich liegt.

  Ideal ist ein Abstand von fünf Kanälen. Je nach Konfiguration muss unter Umständen auch der Kanal an den Client-Geräten neu eingestellt werden.

5.3 Erweiterte Netzwerkfunktionen

In diesem Abschnitt erhalten Sie ausführlichere technische Informationen über Drahtlosnetzwerke.

HINWEIS: Dieser Abschnitt kann übersprungen werden, wenn Sie das Drahtlosnetzwerk nur in einer Standardkonfiguration einrichten möchten (beschrieben unter Anleitung zur Nutzung der Drahtlosfunktion auf Seite 56).

5.3.1 Erweiterte Sicherheitseinstellungen im Drahtlosnetzwerk

In diesem Abschnitt werden die vom CVE-30360 unterstützten Sicherheitsprotokolle ausführlicher beschrieben.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- **WEP** (Wired Equivalency Protocol): Dieses Protokoll verwendet eine Reihe von “Schlüsseln” oder Zeichenketten, um den Wireless Client am Zugriffspunkt zu authentifizieren und um Daten zu verschlüsseln, die über die Drahtlosverbindung gesendet werden. WEP ist ein veraltetes Protokoll, das nur verwendet werden sollte, wenn es der einzige Sicherheitsstandard ist, der von allen Wireless Clients unterstützt wird. WEP bietet nur eine geringe Sicherheit, da es vielfältige Programme gibt, die diesen Sicherheitsschlüssel in wenigen Minuten “knacken” können.
- **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA wurde entwickelt, um die Unzulänglichkeiten des WEP-Protokolls zu lösen. Es gibt zwei WPA-Typen: Für die “Unternehmens”-Version (auch bekannt als WPA) wird ein zentraler Authentifizierungs-Datenbankserver benötigt. Bei der “privaten” Version (vom CVE-30360 unterstützt) kann sich der Benutzer mit einem “PSK”-Schlüssel oder einem Passwort authentifizieren. Auch wenn WPA relativ sicher ist, kann es Angriffe durch “brute-force” Passwort-Raten (bei dem ein Angreifer den AP mit unzähligen verschiedenen Passwörtern “bombardiert”) nicht standhalten. Deshalb wird für eine optimale Sicherheit empfohlen, ein zufälliges Passwort zu wählen, das ausmindestens dreizehn Zeichen besteht und keine tatsächlich existierenden Wörter enthält.
- **WPA2-PSK**: WPA2 ist eine Weiterentwicklung von WPA. Der grundlegende Unterschied liegt darin, dass WPA den mit Schwachstellen behaftetenTKIP-Verschlüsselungsstandard (Temporal Key Integrity Protocol) verwendet, während WPA2 den stärkeren AES-Standard (Advanced Encryption Standard) im CCMP-Protokoll nutzt. Dieser trägt das höchste Prüfsiegel der US-Regierung für Kommunikationssicherheit. Da WPA2-PSK denselben PSK-Mechanismus wie WPA-PSK verwendet, treffen auch hier bei der Verwendung unsicherer oder einfacher Passwörter dieselben Vorbehalte zu.

5.3.2 Sonstige Informationen über Drahtlosnetzwerke

In diesem Abschnitt erhalten Sie weitergehende Informationen über Drahtlosnetzwerke.

5.3.2.1 WPS

WPS (WiFi-Protected Setup) ist ein standardisiertes Verfahren, mit dem sich Drahtlosgeräte bei sehr großer Sicherheit schnell und einfach mit Drahtlosnetzwerken verbinden können. Der CVE-30360 bietet zwei WPS-Authentifizierungsverfahren:

- **PBC (Push-Button Configuration)**: Wenn der Benutzer die **PBC**-Taste am AP (entweder eine physische Taste oder eine virtuelle Taste in der Benutzeroberfläche) drückt, kann jeder Benutzer eines Wireless Clients, der WPS unterstützt, innerhalb der zwei darauffolgenden Minuten ebenfalls auf die jeweilige **PBC**-Taste am Client drücken, um das Gerät mit dem Netzwerk zu verbinden.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- **PIN-Konfiguration (Personal Identification Number)**: Alle WPS-fähigen Geräte haben eine PIN (diese befindet sich normalerweise auf einem Etikett am Gehäuse des Geräts). Wenn Sie ein anderes Gerät so konfigurieren, dass es dieselbe PIN verwendet, können sich die zwei Geräte gegenseitig authentifizieren.

Nach der Authentifizierung verwenden Geräte, die sich mit WPS mit einem Netzwerk verbunden haben, den Sicherheitsstandard WPA2.

5.3.2.2 WMM

WMM (WiFi MultiMedia) ist eine QoS-Verbesserung (Quality of Service), durch die bestimmte Datentypen bei der Übertragung im Drahtlosnetzwerk priorisiert werden. WMM bietet vier Datentypenklassifizierungen (geordnet nach Priorität: von der höchsten zurniedrigsten):

- Sprache
- Video
- Best effort (Beste Bemühung)
- Hintergrund

Wenn Sie die Leistung von Ton und Bild verbessern möchten (auf Kosten anderer, weniger zeitkritischer Anwendungen wie Internetbrowsing und FTP-Übertragungen), können Sie WMM aktivieren. Sie können auch die WMM QoS-Parameter bearbeiten. Das sollten Sie aber nur tun, wenn es unbedingt nötig ist.

5.4 Die Eingabemasken für die Drahtloskonfiguration

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **Wireless** beschrieben.

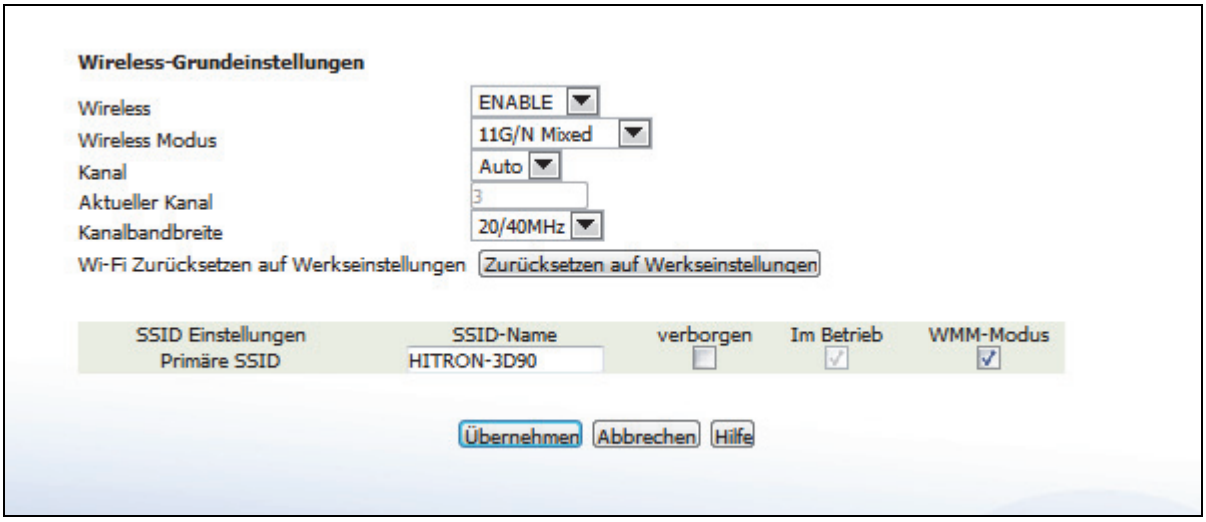
5.4.1 Die Eingabemaske Wireless-Grundeinstellungen

In dieser Eingabemaske konfigurieren Sie die Grundeinstellungen für die Drahtlosverbindung des CVE-30360. Sie können das Drahtlosmodul ein- oder ausschalten, den Drahtlosmodus und Kanal auswählen, WPS ausführen und die SSID des Drahtlosnetzwerks konfigurieren.

Klicken Sie auf **Wireless** > **Basic**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 17: Die Eingabemaske Wireless > Basic



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 18: Die Eingabemaske Wireless > Basic

Wireless-Grundeinstellungen	
Wireless	In diesem Feld können Sie das Drahtlosnetzwerk ein- oder ausschalten. ▸ Wählen Sie **ENABLE** (Aktivieren), um das Drahtlosnetzwerk einzuschalten. ▸ Wählen Sie **DISABLE** (Deaktivieren), um das Drahtlosnetzwerk auszuschalten.
Wireless Modus	Wählen Sie den Drahtlosnetzwerktyp, den Sie verwenden möchten: ▸ **11B/G Mixed**: IEEE 802.11b und 802.11n ▸ **11B Only**: IEEE 802.11b ▸ **11G Only**: IEEE 802.11g ▸ **11N Only**: IEEE 802.11n ▸ **11G/N Mixed**: IEEE 802.11g und 802.11N ▸ **11B/G/N Mixed**: IEEE 802.11b, 802.11g und 802.11N HINWEIS: Nur Wireless Clients, die das gewählte Netzwerkprotokoll unterstützen, können die Verbindung zum Drahtlosnetzwerk herstellen. Ist Ihnen das Protokoll nicht bekannt, sollten Sie **11B/G/N** (Standardeinstellung) verwenden.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 18: Die Eingabemaske Wireless > Basic (Fortsetzung)

Kanal	Wählen Sie den drahtlosen Kanal aus, der verwendet werden soll, oder wählen Sie **Auto**, damit der CVE-30360 automatisch den optimalen Kanal auswählt. HINWEIS: Es wird empfohlen, die Option **Auto** zu verwenden.
Aktueller Kanal	Hier wird die Identifikationsnummer des Wireless-Kanals angezeigt, mit dem der CVE-30360 aktuell verbunden ist.
Kanalbandbreite	In diesem Feld können Sie die Bandbreite des Funkkanals festlegen, auf dem der CVE-30360 mit den Wireless Clients kommuniziert (nur IEEE 802.11n). Bei Nutzung der vollen Bandbreite von 40 MHz verdoppelt sich die Datengeschwindigkeit. • Wählen Sie **20 MHz**, um nur ein 20-MHz-Band zu nutzen. • Wählen Sie **20/40 MHz**, um ein 40-MHz-Band zu nutzen, wenn es möglich ist. Ist das nicht möglich, wird ein 20-MHz-Band genutzt. • Wählen Sie **40 MHz**, um nur ein 40-MHz-Band zu nutzen.
Wi-Fi zurücksetzen auf Werkseinstellungen	Klicken Sie hier, um die WLAN-Einstellungen des CVE-30360 auf die werkseitigen Einstellungen zurückzusetzen.
SSID Einstellungen	Hier wir die **Primäre SSID** angezeigt. HINWEIS: Je nach Vertragsumfang mit Ihrem Netzbetreiber können Sie auch weitere BSSIDs haben.
SSID-Name	Geben Sie den Namen ein, den Sie für das Drahtlosnetzwerk verwenden möchten. Dieser Name bezeichnet das Netzwerk, mit dem die Wireless Clients verbunden werden. HINWEIS: Aus Sicherheitsgründen wird empfohlen, die SSID zu ändern.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 18: Die Eingabemaske Wireless > Basic (Fortsetzung)

verborgen	Mit der Auswahl dieser Option können Sie das Netzwerk für andere Drahtlosgeräte sichtbar oder unsichtbar machen. • Markieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass der CVE-30360 den Netzwerknamen (SSID) an alle Drahtlosgeräte sendet, die sich innerhalb der Reichweite befinden. Nur die Benutzer, die die SSID kennen, können die Verbindung zum Netzwerk herstellen. • Entfernen Sie die Markierung, wenn Sie möchten, dass der Netzwerkname (SSID) öffentlich sichtbar ist. Alle Drahtlosgeräte, die sich innerhalb der Reichweite befinden, können die SSID erkennen und versuchen, die Verbindung zum Netzwerk herzustellen.
Im Betrieb	In diesem Feld wird bestimmt, ob die SSID verwendet wird oder nicht. HINWEIS: Zum Zeitpunkt der Druckstellung ist dieses Feld nicht vom Benutzer konfigurierbar.
WMM-Modus	Markieren Sie dieses Kontrollkästchen, wenn Sie die WMM QoS-Einstellungen (Wifi MultiMedia Quality of Service) auf diese SSID anwenden möchten.

5.4.2 Die Eingabemaske Sicherheit

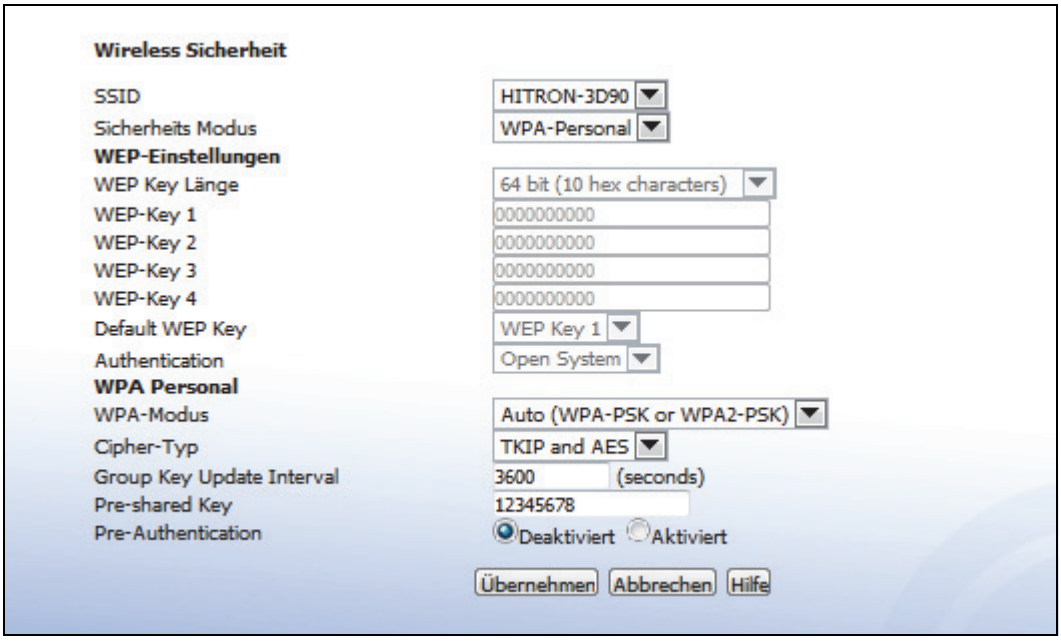
Auf dieser Eingabemaske werden die Authentifizierung und Verschlüsselung desDrahtlosnetzwerks konfiguriert.

HINWEIS: Es wird dringend empfohlen, das Netzwerk zu sichern, da anderenfalls jeder auf das Netzwerk zugreifen kann, der sich innerhalb der Funkreichweite befindet.

Klicken Sie auf **Wireless** > **Sicherheit**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 18: Die Eingabemaske Wireless > Sicherheit



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 19: Die Eingabemaske Wireless > Sicherheit

Wireless Sicherheit	
SSID	Hier wählen Sie die SSID aus, für die Sie die Sicherheitseinstellungen vornehmen möchten. HINWEIS: Zum Zeitpunkt der Druckstellung ist nur eine SSID verfügbar.
Sicherheits Modus	Wählen Sie den Sicherheitstyp, den Sie verwenden möchten: • Wählen Sie **None**, wenn Sie keine Sicherheit konfigurieren möchten. Jeder, der sich innerhalb der Reichweite befindet, kann auf das Netzwerk zugreifen. • Wählen Sie **WEP**, um das Sicherheitsprotokoll Wired Equivalent Privacy (WEP) zu verwenden. • Wählen Sie **WPA-Personal**, um das Sicherheitsprotokoll WiFi Protected Access (Personal) (WPA-Personal) zu verwenden. HINWEIS: **WEP** sollten Sie aufgrund seiner Unzulänglichkeiten nur verwenden, wenn dieses das einzige Sicherheitsprotokoll ist, dass alle Wireless Clients unterstützen. Sofern es möglich ist, sollten Sie unbedingt **WPA-Personal** verwenden.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 19: Die Eingabemaske Wireless > Sicherheit (Fortsetzung)

WEP-Einstellungen HINWEIS: Diese Felder sind nur konfigurierbar, wenn Sie bei **Sicherheits Modus** die Option **WEP** ausgewählt haben.	
WEP Key Länge	In diesem Feld legen Sie die Länge des Sicherheitsschlüssels fest, mit dem die Drahtlosgeräte Zugriff auf das Netzwerk erhalten. Je länger der Schlüssel ist, um so sicherer ist er. • Wählen Sie **64-bit**, um einen zehnstelligen Sicherheitsschlüssel zu verwenden. • Wählen Sie **128-bit**, sechsundzwanzigstelligen Sicherheitsschlüssel zu verwenden.
WEP-Key 1-4	In diesen Feldern legen Sie die Sicherheitsschlüssel fest, die alle Drahtlosgeräte des Netzwerks verwenden müssen, um auf das Netzwerk zugreifen zu können. Der CVE-30360 unterstützt bis zu vier WEP-Schlüssel, von denen Sie einen als Standardschlüssel festlegen können. In den Wireless Clients des Netzwerks müssen dieselben vier Schlüssel in derselben Reihenfolge eingegeben werden. Der CVE-30360 und die Wireless Clients können unterschiedliche Standardschlüssel verwenden, solange alle vier Schlüssel in der richtigen Reihenfolge vorhanden sind. Wenn Ihr Wireless Client nur einen einzigen WEP-Schlüssel unterstützt, müssen Sie den Standardschlüssel des CVE-30360 verwenden. Geben Sie die Schlüssel im Hexadezimalformat (mit den Ziffern **0**-**9** und den Buchstaben **A**-**F**) ein.
Default WEP Key	Wählen Sie die Nummer des Sicherheitsschlüssels, den der CVE-30360 als Standardschlüssel zum Authentifizieren der Übertragungen verwenden soll.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 19: Die Eingabemaske Wireless > Sicherheit (Fortsetzung)

Authentication	Wählen Sie einen Authentifizierungsmodus aus: • Wählen Sie **Open System**, müssen sich die Wireless Clients zunächst vor dem CVE-30360 authentifizieren (legitimieren), bevor sie die Sicherheitsdaten (WEP-Schlüssel) vorweisen. • Wählen Sie **Shared Key**, wird für die Authentifizierung der WEP-Schlüssel verwendet. Wenn ein Client die Verbindung zum Netzwerk herstellen möchten, sendet der CVE-30360 eine unverschlüsselte Abfragenachricht. Der Client muss die Abfragenachricht mit dem WEP-Schlüssel verschlüsseln und zum CVE-30360 zurücksenden. Dieser entschlüsselt diese Nachricht und vergleicht das Ergebnis mit der Ursprungsnachricht. Die **Open System**-Authentifizierung ist der sicherere dieser zwei Authentifizierungstypen. Obwohl das Shared Key-System auf den ersten Blick sehr widerstandsfähig wirkt, können die Daten der Abfragenachrichten abgefangen werden. • Wenn Sie **Auto** wählen, wählt der CVE-30360 das Authentifizierungsverfahren automatisch.
WPA_Personal HINWEIS: Diese Felder sind nur konfigurierbar, wenn sie bei **Sicherheits Modus** die Option **WPA-Personal** ausgewählt haben.	
WPA-Modus	Wählen Sie einen WPA-Sicherheitstyp: • Wählen Sie **WPA-PSK**, um den WPA-PSK-Modus (Wifi Protected Access (Pre-Shared Key)) zu verwenden. • Wählen Sie **WPA2-PSK**, um den WPA2-PSK-Modus (Wifi Protected Access 2 (Pre-Shared Key)) zu verwenden. • Wählen Sie **Auto (WPA-PSK oder WPA2-PSK)**, damit alle Clients unabhängig vom Modus die Verbindung zum CVE-30360 herstellen können.
Cipher Typ	Wählen Sie einen Verschlüsselungstyp: • Wählen Sie **TKIP**, um das TKIP-Protokoll (Temporal Key Integrity Protocol) zu verwenden. • Wählen Sie AES, um den AES-Standard (AdvancedEncryption Standard) zu verwenden. • Wenn Sie TKIP und AES wählen, können die Clients eine der beiden Verschlüsselungstypen verwenden, wenn Sie die Verbindung zum CVE-30360 herstellen möchten.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 19: Die Eingabemaske Wireless > Sicherheit (Fortsetzung)

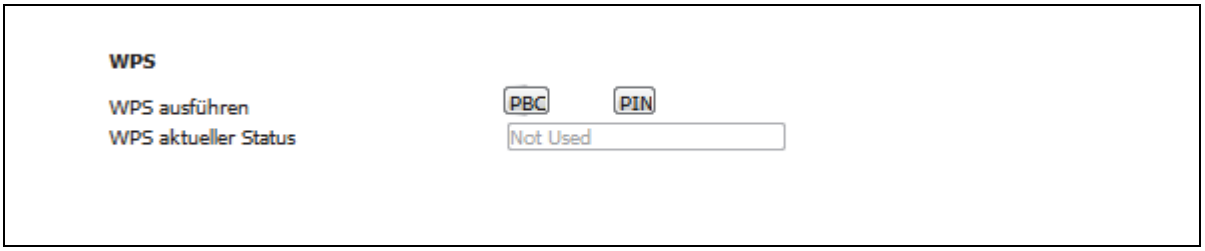
Group Key Update Interval	Geben Sie die Frequenz (in Sekunden) ein, mit der der CVE-30360 neue PSK-Schlüssel erzeugen und an die Wireless Clients ausgeben soll.
PSK	Geben Sie den PSK ein, den Sie für das Drahtlosnetzwerk verwenden möchten. Sie müssen diesen Schlüssel bei Ihren Wireless Clients eingeben, damit diese eine Verbindung zum Netzwerk herstellen können.
Pre-Authentication	In diesem Feld können Sie bei WPA2 eine Vor-Authentifizierung zulassen (**Aktiviert**) oder Vor-Authentifizierungsanfragen abweisen (**Deaktiviert**). Bei der Vor-Authentifizierung kann ein Wireless Client mit WPA2 eine Authentifizierung mit anderen drahtlosen Zugriffspunkten durchführen, die sich innerhalb der Reichweite befinden, auch wenn er immer noch mit dem aktuellen drahtlosen Zugriffspunkt verbunden ist. Auf diese Weise können mobile Wireless Clients für ein effizienteres Roaming schneller auf Zugriffspunkte zugreifen.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

5.4.3 Die Eingabemaske WPS

In dieser Eingabemaske werden die WPS-Funktionen des CVE-30360 konfiguriert.

Klicken Sie auf **WLAN** > **WPS**. Die folgende Eingabemaske erscheint.

Abbildung 19: Die Eingabemaske WPS



Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 20: Die Eingabemaske WPS

WPS-Einstellungen	
WPS-Verfahren	Mit diesen Tasten wird das WPS-Verfahren (WiFi Protected Setup) ausgeführt: • Klicken Sie auf die **PBC**-Taste und dann auf **Push Button**, um die Push-Button-Konfiguration zu starten. Drücken Sie dann innerhalb der nächsten zwei Minuten auf die PBC-Tasten der Wireless Clients, um diese beim Drahtlosnetzwerk anzumelden. • Klicken Sie auf die **PIN**-Taste, um die PIN-Konfiguration zu starten. Geben Sie im nun erscheinenden Fenster die WPS-PIN, die Sie für den CVE-30360 verwenden möchten, oder die WPS-PIN des Client-Geräts, das die zum Netzwerk hinzufügen möchten, ein.
WPS aktueller Status	Hier wird angezeigt, ob der CVE-30360 WPS nutzt.

5.4.4 Die Eingabemaske Zugangskontrolle

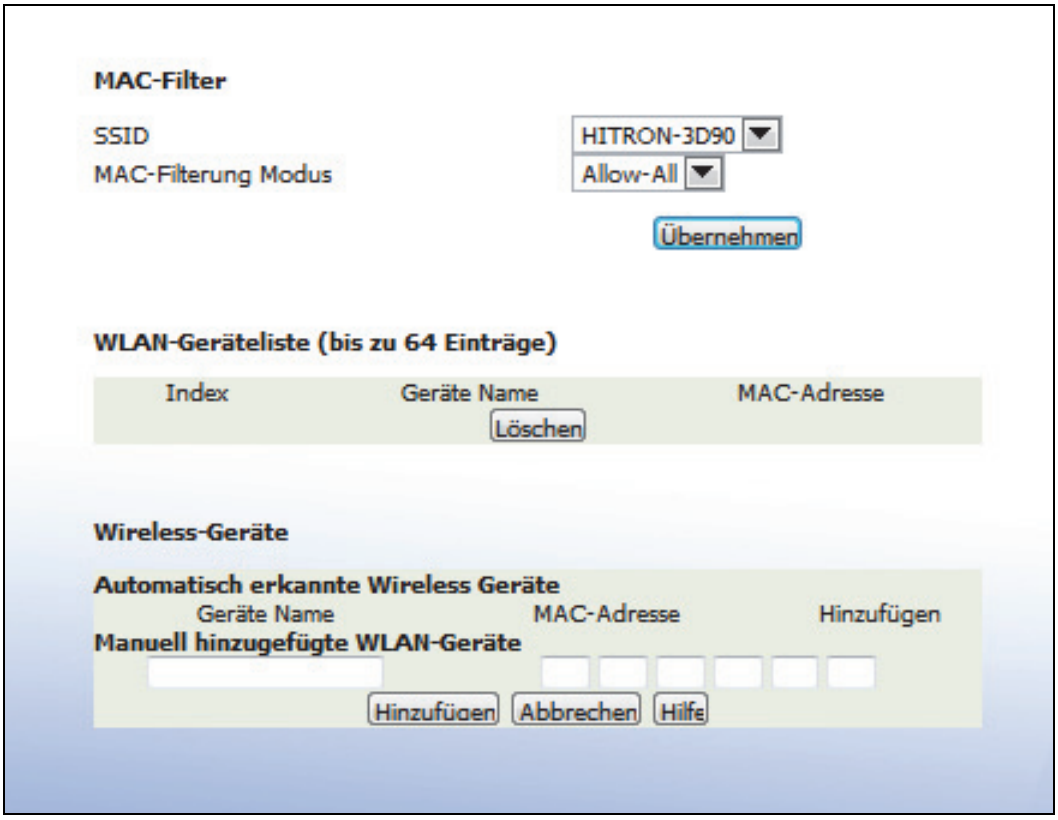
Auf dieser Eingabemaske konfigurieren Sie die MAC-Adressfilterfunktion im Drahtlosnetzwerk.

Sie können den CVE-30360 so einstellen, dass er nur bestimmten Geräten den drahtlosen Zugriff zum CVE-30360 und zum Netzwerk gewährt, ihn aber anderen Geräten verweigert.

Klicken Sie auf **Wireless** > **Zugangskontrolle**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 20: Klicken Sie auf Wireless > Zugangskontrolle.



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 21: Die Eingabemaske Wireless > Zugangskontrolle

MAC-Filter	
SSID	Wählen Sie die SSID, für die Sie die drahtlose Zugriffskontrolle konfigurieren möchten. HINWEIS: Zum Zeitpunkt der Drucklegung unterstützt der CVE-30360 nur eine einzige SSID.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 21: Die Eingabemaske Wireless > Zugangskontrolle (Fortsetzung)

MAC-Filterung Modus	Hier können Sie festlegen, ob der CVE-30360 im WLAN einen MAC-Filter anwenden soll. • Wählen **Sie Allow-all** (Alle zulassen), um den MAC-Filter auszuschalten. Alle Geräte können drahtlos auf den CVE-30360 und auf das Netzwerk zugreifen. • Wählen **Sie Allow** (Zulassen), damit nur Geräte, deren MAC-Adresse sich in der WLAN-Geräteliste befinden, auf den CVE-30360 und das Netzwerk drahtlos zugreifen können. Allen anderen Geräten wird der Zugriff verwehrt. • Wenn **Sie Deny** (Verweigern) wählen, erhalten alle Geräte mit den in der **Wireless Control List** eingerichteten MAC-Adressen den drahtlosen Zugriff auf den CVE-30360 und auf das Netzwerk. Den angegebenen Geräten wird der Zugriff verweigert.
Übernehmen	Klicken Sie hier, um die Änderungen im Abschnitt MAC-Filter zu speichern.
WLAN-Geräteliste (bis zu 16 Einträge)	
Index	Hier wird die Indexnummer des Drahtlosgeräts angezeigt, dem der Zugriff gewährt oder verweigert wurde.
Geräte Name	Hier wird der Name des Geräts angezeigt, dem der Zugriff gewährt oder verweigert wurde.
MAC-Adresse	Hier wird die MAC-Adresse des Geräts angezeigt, dem der Zugriff gewährt oder verweigert wurde.
Löschen	Wählen Sie die Optionsschaltfläche ( ) eines zugelassenen oder verweigerten Geräts aus der Liste. Das Gerät hat dann keinen Zugriff mehr auf den CVE-30360 und auf das Netzwerk.
Automatisch erkannte Wireless Geräte	
Geräte Name	Hier wird der Name aller Netzwerkgeräte angezeigt, die im Drahtlosnetzwerk mit dem CVE-30360verbunden sind.
MAC-Adresse	Hier wird die MAC-Adresse aller Netzwerkgeräte angezeigt, die im Drahtlosnetzwerk mit dem CVE-30360 verbunden sind.
Manuell hinzugefügte WLAN-Geräte	

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 21: Die Eingabemaske Wireless > Zugangskontrolle (Fortsetzung)

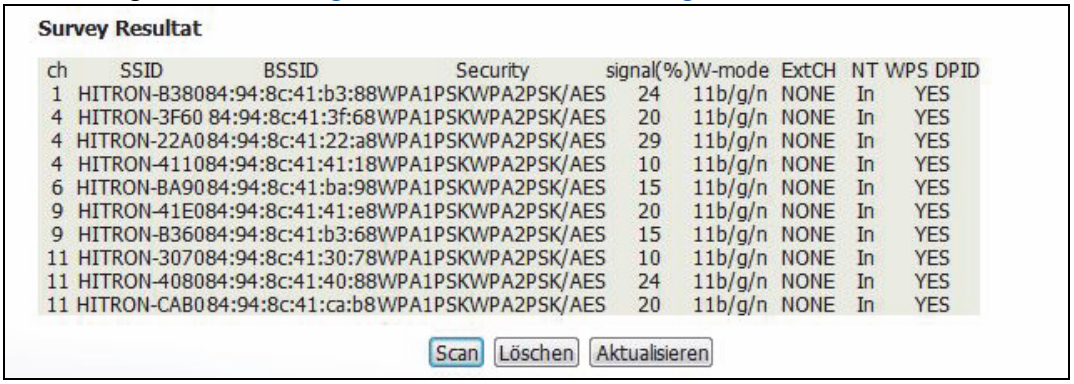
Geräte Name	Geben Sie den Namen des Geräts ein, dem der drahtlose Zugriff zum CVE-30360 und zum Netzwerk gewährt oder verweigert werden soll. HINWEIS: Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
MAC-Adresse	Geben Sie die MAC-Adresse des Netzwerkgeräts ein, für das Sie den drahtlosen Zugriff auf den CVE-30360 und das Netzwerk zulassen oder verweigern möchten.
Hinzufügen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

5.4.5 Die Eingabemaske Neighbor APs

Auf dieser Eingabemaske erhalten Sie Informationen über die WLAN-Netzwerke, die in der Reichweite des CVE-30360 liegen.

Klicken Sie auf **WLAN** > **Neighbor APs**. Die folgende Eingabemaske erscheint.

Abbildung 21: Die Eingabemaske WLAN > Neighbor APs



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 22: Die Eingabemaske WLAN > Neighbor APs

Survey Resultat	
ch	Hier wird die Nummer des Funkkanals angezeigt, den das Drahtlosnetzwerk verwendet.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 22: Die Eingabemaske WLAN > Neighbor APs (Fortsetzung)

SSID	In diesem Feld wird die SSID des Drahtlosnetzwerks angezeigt.
BSSID	In diesem Feld wird die BSSID des Drahtlosnetzwerks angezeigt. Das ist normalerweise die MAC-Adresse des Drahtlosnetzwerks.
Sicherheit	Hier wird der Sicherheitstyp angezeigt, den das Drahtlosnetzwerk verwendet.
Signal (%)	In diesem Feld wird die vom CVE-30360 empfangene Signalstärke angezeigt. Die Signalstärke wird in Prozent als Wert zwischen 0 (kein Empfang) und 100 (hervorragender Empfang) dargestellt.
W-mode	In diesem Feld wird der Netzwerkstandard (z. B. 11n) angezeigt, den das Drahtlosnetzwerk verwendet. Hier wird die Nummer des Funkkanals angezeigt, den das Drahtlosnetzwerk verwendet.
ExtCH	Bei IEEE 802.11n-Netzwerken, die drahtlose Übertragungen mit 40 MHz unterstützen, wird in diesem Feld angezeigt, ob das Netzwerk Kanäle bündelt. Gleichzeitig wird angegeben, ob der erweiterte Kanal über oder unter dem primären Steuerkanal liegt. HINWEIS: Mit der Kanalbündelung kann der Zugriffspunkt den Datendurchsatz durch die gleichzeitige Verwendung zweier Drahtloskanäle anstelle nur eines Kanals erhöhen. Wenn Sie die Kanalbündelung wählen, gibt es einen primären Steuerungskanal und einen Erweiterungskanal. Der Erweiterungskanal kann entweder direktüber dem Steuerungskanal liegen oder direkt darunter. • Bei IEEE 802.11n-Netzwerken, die die Kanalbündelung verwenden, befindet sich der Erweiterungskanal über dem Hauptkanal, es erscheint **ABOVE**. • Bei IEEE 802.11n-Netzwerken, die die Kanalbündelung verwenden, befindet sich der Erweiterungskanal unter dem Hauptkanal, es erscheint **BELOW**. • Bei Netzwerken, die keine Kanalbündelung verwenden, erscheint **NONE**.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 22: Die Eingabemaske WLAN > Neighbor APs (Fortsetzung)

Nt	In diesem Feld wird angezeigt, ob das Netzwerk den Infrastruktur- oder den Ad-Hoc-Modus verwendet. HINWEIS: Im Infrastrukturmodus verbinden sich die Drahtlosgeräte mit einem zentralen Zugriffspunkt (AP), der dann über eine Kabelverbindung die Verbindung zum Internet oder einem anderen Netzwerk herstellt. Im Ad-Hoc-Modus verbinden sich die Drahtlosgeräte als Peers miteinander.
WPS DPID	In diesem Feld wird angezeigt, ob das Zielnetzwerk WPS (WiFi Protected Setup) verwendet. Ist das der Fall, steht in diesem Feld, ob es den PIN-Modus oder den PBC-Modus verwendet. • Verwendet das Zielnetzwerk nicht WPS, erscheint **NO**. • Verwendet das Zielnetzwerk WPS, und lässt es zu, dass Drahtlosgeräte die Verbindung mit dem **PIN**-Modus herstellen, erscheint PIN. • Verwendet das Zielnetzwerk WPS, und lässt es zu, dass Drahtlosgeräte die Verbindung mit dem PBC-Modus herstellen, erscheint **PBC**. HINWEIS: Weitere Informationen zu WPS und zum Unterschied zwischen dem PIN- und PBC-Modus finden Sie unter WPS auf Seite 61.

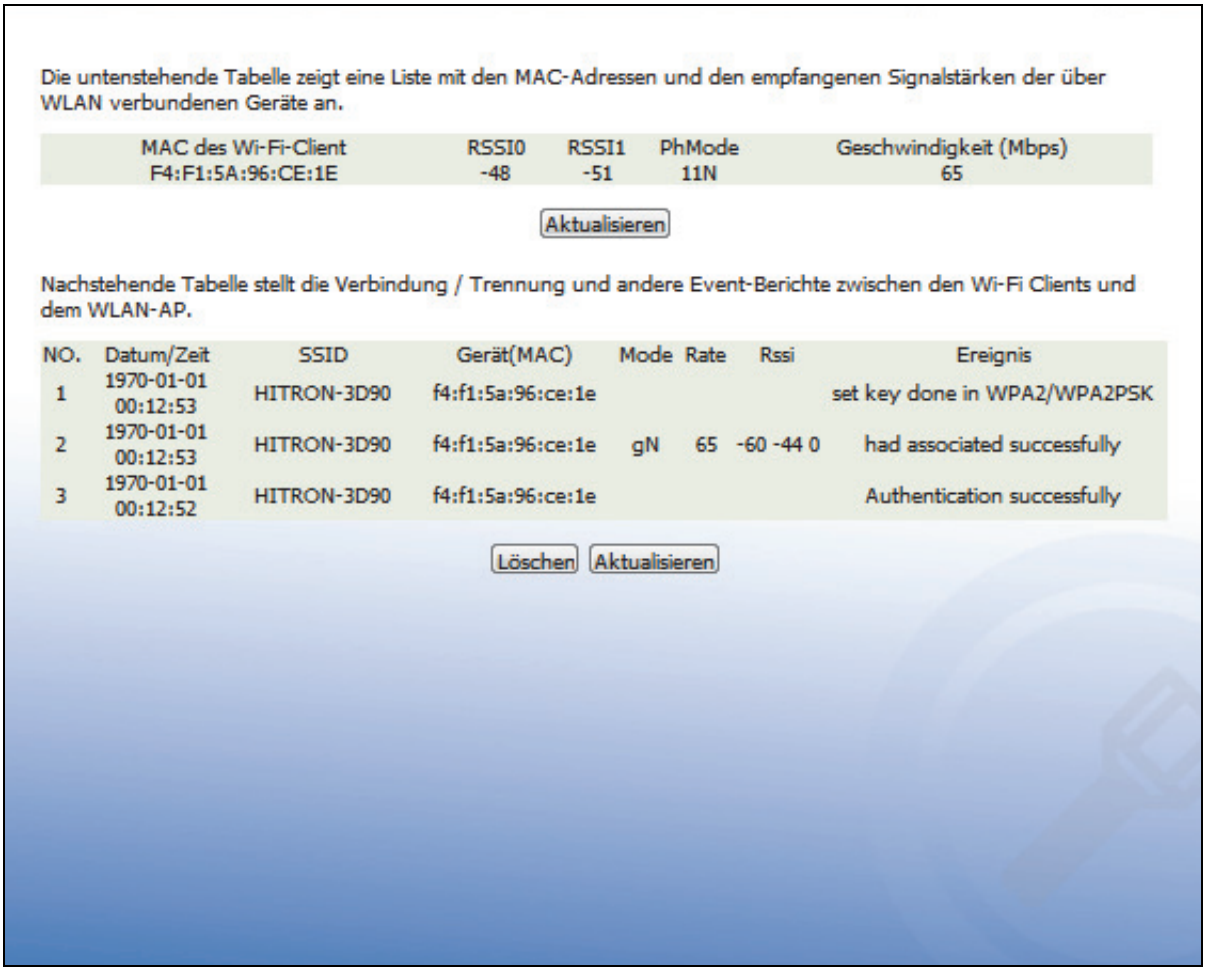
5.4.6 Die Eingabemaske WLAN Clients

Auf dieser Eingabemaske erhalten Sie Informationen über die Wireless-Clients, die mit dem WLAN des CVE-30360 verbunden sind. Hier erscheint auch ein Protokoll aller unerwarteten und ungewöhnlichen Ereignisse im Drahtlosnetzwerk.

Klicken Sie auf **WLAN** > **WLAN Clients**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 22: Die Eingabemaske WLAN Clients



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 23: Die Eingabemaske WLAN Clients

Liste der WLAN-Clients	
MAC des Wi-Fi-Client	Hier werden die MAC-Adressen aller an das Drahtlosnetzwerk des CVE-30360 angeschlossenen Wireless-Clients angezeigt.
RSSI0	In diesen Feldern wird für alle Antennen des CVE-30360 die RSSIO (Received Signal Strength Indication) aller an das Drahtlosnetzwerk des CVE-30360 angeschlossenen Wireless-Clients angezeigt.
RSSI1	
Geschwindigkeit	Hier wird die Übertragungsgeschwindigkeit aller an das WLAN des CVE-30360 angeschlossenen Geräte angezeigt.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 23: Die Eingabemaske WLAN Clients (Fortsetzung)

PhMode	Hier wird der physikalische Modus (die IEEE 802.11-Version) aller an das WLAN des CVE-30360 angeschlossenen Geräte angezeigt.
Ereignis	
No.	Dieses ist die Indexnummer jedes Protokolleintrags.
Datum/Zeit	Hier werden das Datum und die Uhrzeit angezeigt, zu der das Ereignis stattgefunden hat.
SSID	Hier wird angezeigt, mit welchem WLAN des CVE-30360 der Wireless-Client des betreffenden Ereignisprotokolls verbunden war.
Gerät (MAC)	Hier wird die MAC-Adresse des Wireless-Clients mit dem betreffenden Ereignisprotokoll angezeigt.
Mode	Hier wird der physikalische Modus (die IEEE 802.11-Version) des Wireless-Clients mit dem betreffenden Ereignisprotokoll angezeigt.
Rate	Hier wird die Übertragungsgeschwindigkeit des Wireless-Clients mit dem betreffenden Ereignisprotokoll angezeigt.
RSSI	Hier wird die kombinierte Signalstärke zwischen dem CVE-30360 und dem Wireless-Client, die zu dem Zeitpunkt vorhanden war, als das Ereignisprotokoll erstellt wurde.
Ereignis	Hier wird die Art des Ereignisses erläutert.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

6

Advanced

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **Advanced** klicken. Es umfasst die folgenden Abschnitte:

6.1 Übersicht über den Menüpunkt Advanced

In diesem Abschnitt werden alle Eingabemasken des Menüpunkts **Advanced** beschrieben.

6.1.1 Firewall

“Firewall” (Brandmauer) ist ursprünglich ein bautechnologischer Begriff. Er bezeichnet eine Mauer, die verhindern soll, dass sich ein Feuer auf andere Räume oder Gebäude ausbreitet. Ebenso verhindert die Firewall Ihres CVE-30360 Eindringversuche und andere unerwünschte Aktivitäten aus dem WAN, um die Computer Ihres LAN zu schützen. Sie können mit bestimmten Filtern festlegen, welche Computer und anderen Geräte auf das LAN zugreifen dürfen und welcher Datenverkehr vom LAN zum WAN verhindert werden soll.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

6.1.2 Intrusion-Detection-System

Ein Intrusion-Detection-System überwacht die Netzwerkaktivität und sucht Regelverstöße und bösartige oder verdächtige Aktivitäten.

6.1.3 MAC-Filter

Jedes Netzwerkgerät hat eine eindeutige MAC-Adresse, welche das Gerät im Netzwerk identifiziert. Wenn Sie den MAC-Adressfilter in der Firewall des CVE-30360 aktivieren, können Sie eine Liste von MAC-Adressen zusammenstellen und dann entscheiden, ob

- den Geräten auf der Liste soll der Zugriff zum CVE-30360 und zum Netzwerk verwehrt werden soll (alle anderen Geräte können auf das Netzwerk zugreifen)

oder

- den Geräten auf der Liste der Zugriff auf das Netzwerk erlaubt werden soll (alle anderen Geräte können dann nicht auf das Netzwerk zugreifen).

6.1.4 IP-Filter

Mit dem IP-Filter können Sie verhindern, dass Computer des LAN bestimmte Datentypen in das WAN senden. Mit diesem Filter können Sie eine unerwünschte Kommunikation nach außen vermeiden. Legen Sie die IP-Adresse des Computers im LAN fest, von dem aus keine Kommunikation stattfinden soll. Legen Sie dann den Port-Bereich für die Kommunikation fest, die vermieden werden soll. Der CVE-30360 verwirft dann ausgehende Datenpakete, die den festgelegten Kriterien entsprechen.

6.1.5 Portweiterleitung

Die Portweiterleitung ermöglicht es einem Computer im LAN, bestimmte Daten aus dem WAN zu empfangen. Das wird normalerweise verwendet, um bestimmte Anwendungen (z. B. Spiele) für einen bestimmten Computer im LAN durch die Firewall zuzulassen. Die Portweiterleitung wird auch häufig verwendet, um einen öffentlichen HTTP-Server von einem privaten Netzwerk aus laufen zu lassen.

Sie können für jede Anwendung, für die Sie Ports in der Firewall öffnen möchten, eine Portweiterleitungsregel festlegen. Wenn der CVE-30360 Daten aus dem WAN empfängt, deren Ziel ein Port ist, der einer Portweiterleitungsregel entspricht, werden die Daten zu der LAN IP-Adresse und Portnummer weitergeleitet, die in der Portweiterleitungsregel festgelegt wurden.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

HINWEIS: Informationen dazu, welche Ports für eine bestimmte Anwendung geöffnet werden müssen, finden Sie in der Anleitung zur jeweiligen Anwendung.

HINWEIS: Diese Funktion ist nicht verfügbar, wenn DS-lite aktiviert ist.

6.1.6 Port-Triggering

Port-Triggering ist ein Mittel der automatischen Portweiterleitung. Der CVE-30360 prüft den ausgehenden Datenverkehr (vom LAN zum WAN), um festzustellen, ob Sie für die angegebenen Zielports Port-Triggering-Regeln festgelegt haben. Wenn es Übereinstimmungen gibt, öffnet der CVE-30360 in Erwartung von eingehendem Verkehr automatisch die in der Regel festgelegten Eingangsports.

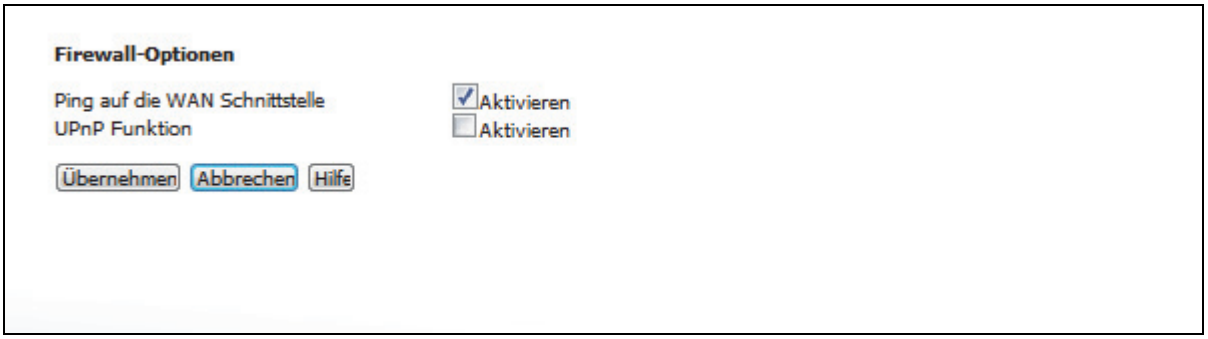
HINWEIS: Diese Funktion ist nicht verfügbar, wenn DS-lite aktiviert ist.

6.2 Die Eingabemaske Advanced Options

Auf dieser Eingabemaske können Sie die Firewall-Funktionen ein- oder ausschalten. Sie können die UPnP-Unterstützung des CVE-30360 aktivieren oder deaktivieren und Reaktionen auf ICMP-Anfragen aus dem WAN zulassen oder verhindern.

Klicken Sie auf **Advanced** > **Firewall-Optionen**. Die folgende Eingabemaske erscheint.

Abbildung 23: Die Eingabemaske Advanced > Firewall-Optionen



Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 24: Die Eingabemaske Advanced > Firewall-Optionen

Ping bei WAN Schnittstelle	• Mit dieser Option können Sie Reaktionen auf ICMP-Anfragen aus dem WAN verhindern. • Mit dieser Option können Sie Reaktionen auf ICMP-Anfragen aus dem WAN zulassen.
UPnP Funktion	Markieren Sie dieses Kontrollkästchen, um die UPnP-Funktion des CVE-30360 zu aktivieren, bzw. entfernen Sie die Markierung, um sie zu deaktivieren.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.3 Die Eingabemaske MAC-Filter

Auf dieser Eingabemaske konfigurieren Sie die MAC-Adressfilterfunktion im LAN.

HINWEIS: Eine Beschreibung, wie der MAC-Adressfilter im WLAN konfiguriert wird, finden Sie unter Die Eingabemaske Zugangskontrolle auf Seite 70.

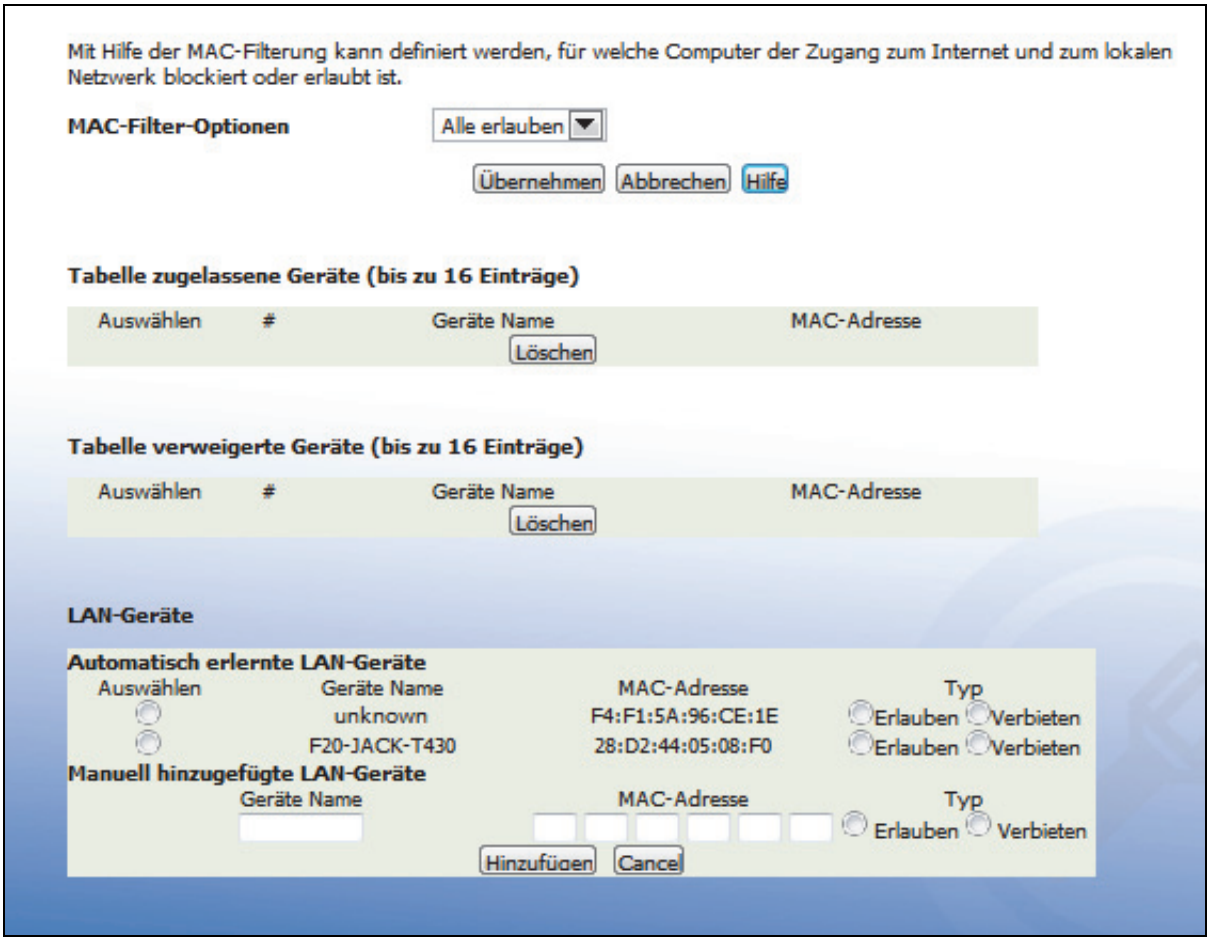
Sie können den CVE-30360 so einstellen, dass er nur bestimmten Geräten den Zugriff zum CVE-30360 und zum Netzwerk gewährt, ihn aber anderen Geräten verweigert.

HINWEIS: Eine Liste aller Computer, die im LAN mit dem CVE-30360 verbunden sind, können Sie aufrufen, indem Sie bei **Advanced** > **IP-Filter**, **Portweiterleitung** > **Port-Triggering** oder **Host Port** auf die Schaltfläche **Angeschlossene Computer** klicken.

Klicken Sie auf **Advanced** > **MAC-Filter**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 24: Die Eingabemaske Advanced > MAC-Filter



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 25: Die Eingabemaske Advanced > MAC-Filter

MAC-Filter-Optionen	
MAC-Filter-Optionen	Hier können Sie festlegen, ob der CVE-30360 einen MAC-Filter anwenden soll. ▸ Wählen Sie **Alle erlauben**, um den MAC-Filter auszuschalten. Alle Geräte können auf den CVE-30360 und auf das Netzwerk zugreifen. ▸ Wählen Sie **Erlauben**, damit nur Geräte, deren MAC-Adresse sich in der **Tabelle "Erlauben"** befinden, auf den CVE-30360 und das Netzwerk zugreifen können. Allen anderen Geräten wird der Zugriff verwehrt. ▸ Wählen Sie **Verweigern** wählen, erhalten alle Geräte den Zugriff auf den CVE-30360 und auf das Netzwerk. Ausgenommen sind die Geräte, deren MAC-Adresse in der **Tabelle "Verweigern"** stehen. Den angegebenen Geräten wird der Zugriff verweigert.

 Copyright © 2014 Hitron Technologies

Tabelle 25: Die Eingabemaske Advanced > MAC-Filter (Fortsetzung)

Tabelle zugelassene Geräte (bis zu 16 Einträge)	
#	Hier wird die Indexnummer der zugelassenen Gerät angezeigt.
Geräte Name	Hier wird der Name des zugelassenen Geräts angezeigt.
MAC-Adresse	Hier wird die MAC-Adresse des zugelassenen Geräts angezeigt.
Löschen	Klicken Sie auf die Optionsschaltfläche eines zugelassenen Geräts ( ), um das Gerät aus der Liste zu entfernen. Das Gerät hat dann keinen Zugriff mehr auf den CVE-30360 und auf das Netzwerk. HINWEIS: Löschen Sie auf keinen Fall Ihren Verwaltungscomputer aus der Liste. Sollte das doch einmal passieren, müssen Sie sich von einem anderen Computer aus wieder anmelden oder den CVE-30360 zurücksetzen.
Tabelle verweigerte Geräte (bis zu 16 Einträge)	
Geräte Name	Hier wird der Name des nicht zugelassenen Geräts angezeigt.
MAC-Adresse	Hier wird die MAC-Adresse des nicht zugelassenen Geräts angezeigt.
Löschen	Klicken Sie auf die Optionsschaltfläche eines abgelehnten Geräts ( ), um das Gerät aus der Liste zu entfernen. Das Gerät hat dann wieder Zugriff mehr auf den CVE-30360 und auf das Netzwerk.
Autom. gelernte LAN-Geräte	
Geräte Name	Hier wird der Name aller Netzwerkgeräte angezeigt, die im LAN mit dem CVE-30360 verbunden sind.
MAC-Adresse	Hier wird die MAC-Adresse aller Netzwerkgeräte angezeigt, die im LAN mit dem CVE-30360 verbunden sind.
Typ	In diesem Feld können Sie die Liste auswählen, zu der Sie das Gerät hinzufügen möchten. ▸ Wählen Sie **Erlauben**, um das Gerät zur **Tabelle "Erlauben"** hinzuzufügen. ▸ Wählen Sie **Verweigern**, um das Gerät zur **Tabelle "Verweigern"** hinzuzufügen.
Manuell hinzugefügte LAN-Geräte	
Geräte Name	Geben Sie den Namen des Netzwerkgeräts ein, dem der Zugriff zum CVE-30360 und zum Netzwerk gewährt oder verweigert werden soll. HINWEIS: Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 25: Die Eingabemaske Advanced > MAC-Filter (Fortsetzung)

MAC-Adresse	Geben Sie die MAC-Adresse des Netzwerkgeräts ein, für das Sie den Zugriff auf den CVE-30360 und das Netzwerk zulassen oder verweigern möchten.
Typ	In diesem Feld können Sie die Liste auswählen, zu der Sie das Gerät hinzufügen möchten. ▸ Wählen Sie **Erlauben**, um das Gerät zur **Tabelle "Erlauben"** hinzuzufügen. ▸ Wählen Sie **Verweigern**, um das Gerät zur **Tabelle "Verweigern"** hinzuzufügen.
Hinzufügen	Klicken Sie hier, um das Gerät zu der von Ihnen festgelegten Liste hinzuzufügen.
Abbrechen	Klicken Sie hier, um die Felder **Manuell hinzugefügte LAN-Geräte** zu löschen.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.4 Die Eingabemaske Portweiterleitung

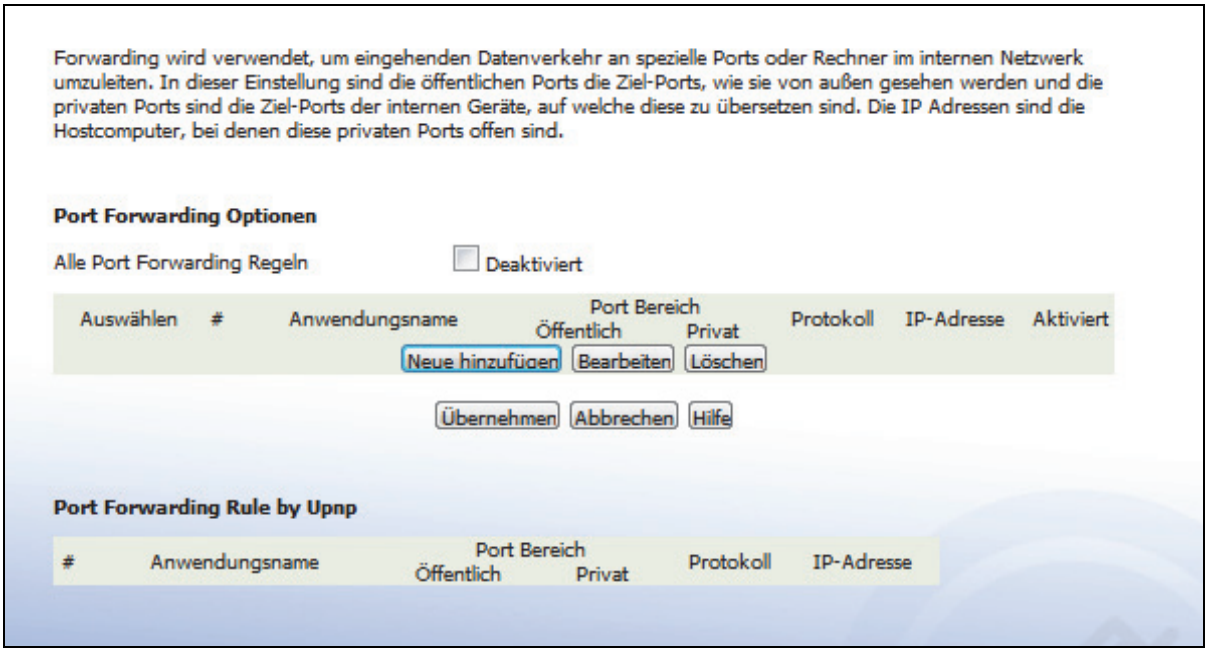
Auf dieser Eingabemaske konfigurieren Sie die Portweiterleitung zwischen den Computern im WAN und den Computern im LAN. Sie können die Portweiterleitung aktivieren oder deaktivieren, vorhandene Portweiterleitungsregeln ändern und neue konfigurieren.

HINWEIS: Diese Eingabemaske ist nur verfügbar, wenn sich der CVE-30360 im IPv4-Modus befindet.

Klicken Sie auf **Advanced** > **Port Forwarding**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 25: Die Eingabemaske Advanced > Port Forwarding



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 26: Die Eingabemaske Advanced > Port Forwarding

Alle Port Forwarding Regeln	In diesem Feld können Sie die Portweiterleitung ein- oder ausschalten. • Markieren Sie das Kontrollkästchen, um die Portweiterleitung zu aktivieren. • Entfernen Sie die Markierung aus dem Kontrollkästchen, um die Portweiterleitung zu deaktivieren.
Auswählen	Wählen Sie die Optionsschaltfläche einer Portweiterleitungsregel (◉), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der Portweiterleitungsregel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.
Port Bereich	In diesen Feldern werden die Ports angezeigt, für die die Regel gilt: • Im Feld **Öffentlich** wird der eingehende Portbereich angezeigt. Das sind die Ports, auf denen der CVE-30360 Daten vom Host im WAN erhalten hat. • Im Feld **Privat** wird der Portbereich angezeigt, zu dem der CVE-30360 Daten, die an das Gerät im LAN adressiert sind, weiterleitet.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 26: Die Eingabemaske Advanced > Port Forwarding (Fortsetzung)

Protokoll	In diesem Feld wird das/werden die Protokoll(e) angezeigt, für die diese Regel gilt: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Transmission Control Protocol und User Datagram Protocol (**TCP/UDP**) • Generic Routing Encapsulation (**GRE**) • Encapsulating Security Protocol (**ESP**)
IP Adresse	Hier wird die IP-Adresse Computers im LAN angezeigt, zu dem der Datenverkehr weitergeleitet wird, der den Bedingungen **Öffentlich** und **Protokoll** entspricht.
Aktivieren	Hier können Sie jede Portweiterleitungsregel ein- oder ausschalten. • Markieren Sie dieses Kontrollkästchen, um die Portweiterleitungsregel zu aktivieren. • Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die Portweiterleitungsregel zu deaktivieren.
Hinzufügen	Klicken Sie hier, um eine neue Portweiterleitungsregel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Portweiterleitungsregel auf Seite 86.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der Portweiterleitungsregel ( ), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Portweiterleitungsregel auf Seite 86.
Löschen	Klicken Sie die auf die Optionsschaltfläche der Portweiterleitungsregel ( ), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.4.1 Hinzufügen oder Bearbeiten einer Portweiterleitungsregel

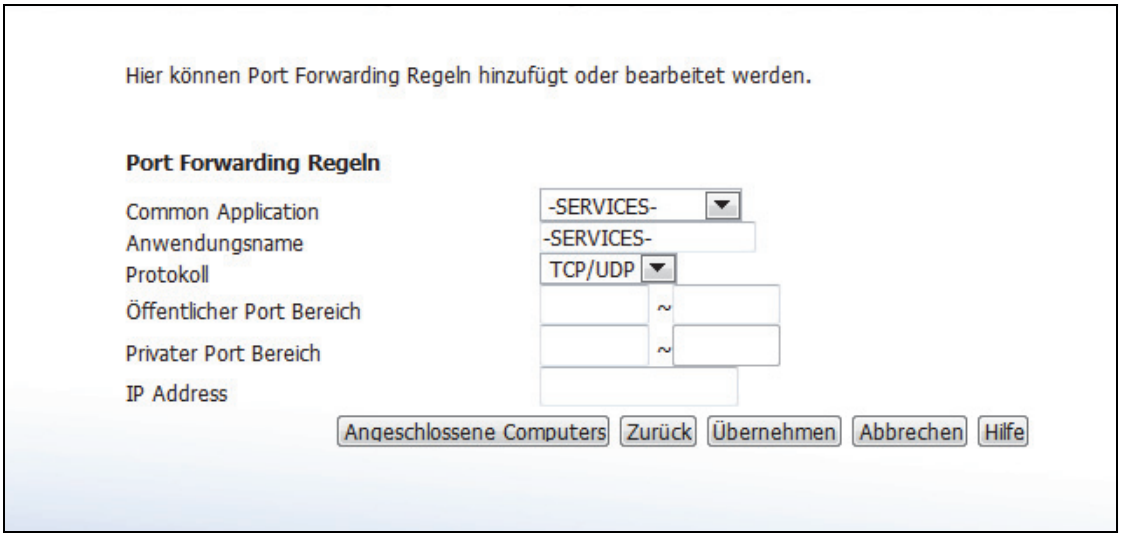
- Um eine neue Portweiterleitungsregel hinzuzufügen, klicken Sie in der Eingabemaske **Advanced** > **Forwarding** auf **Hinzufügen**.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- Um eine vorhandene Portweiterleitungsregel zu bearbeiten, wählen Sie die Optionsschaltfläche ( ) auf der Eingabemaske **Advanced** > **Forwarding** und klicken Sie auf die Schaltfläche **Bearbeiten**.

Die folgende Eingabemaske erscheint.

Abbildung 26: Die Eingabemaske Advanced > Forwarding > Hinzufügen/Bearbeiten



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 27: Die Eingabemaske Advanced > Forwarding > Hinzufügen/Bearbeiten

Anwendungsname	Geben Sie einen Namen für die Anwendung ein, für die Sie eine neue Regel festlegen möchten. HINWEIS: Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Öffentlicher Port Bereich	In diesen Feldern können Sie den eingehenden Portbereich festlegen. Das sind die Ports, auf denen der CVE-30360 Daten vom Host im WAN erhalten hat. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.
Privater Port Bereich	In diesen Feldern können Sie die Ports festlegen, an die der empfangene Datenverkehr weitergeleitet werden soll. Geben Sie die erste Portnummer in das erste Feld ein. Die Anzahl der Ports muss mit der unter **Öffentlicher Port Bereich** festgelegten Anzahl übereinstimmen. Der CVE-30360 ergänzt dann automatisch das zweite Feld.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 27: Die Eingabemaske Advanced > Forwarding > Hinzufügen/Bearbeiten

Protokoll	Hier können Sie festlegen, ob der CVE-30360 eine der folgenden Kommunikationstypen weiterleiten soll: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Transmission Control Protocol und User Datagram Protocol (**TCP/UDP**) • Generic Routing Encapsulation (**GRE**) • Encapsulating Security Protocol (**ESP**) HINWEIS: Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**TCP/UDP**) beibehalten.
IP Address	In dieses Feld können Sie die IP-Adresse des Computers im LAN eingeben, zu dem der Datenverkehr weitergeleitet werden soll.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
Zurück	Klicken Sie hier, um zur Eingabemaske **Advanced** > **Forwarding** zurückzukehren, ohne die Änderungen in der Portweiterleitungsregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.5 Die Eingabemaske IP-Filterung

Auf dieser Eingabemaske konfigurieren Sie den IP-Filter. Sie können den IP-Filter aktivieren oder deaktivieren und bestehende IP-Filterregeln ändern und neue konfigurieren.

Klicken Sie auf **Advanced** > **IP-Filterung**. Die folgende Eingabemaske erscheint.

HINWEIS: Diese Eingabemaske unterscheidet sich je nachdem, ob der CVE-30360 im IPv4- oder im DS-Lite-Modus arbeitet. Der IPv4- und der IPv6-Filter können separat konfiguriert werden. Wählen Sie die Tabelle entsprechend dem Betriebsmodus des CVE-30360 (IPv4 oder IPv6 für DS-Lite).

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 27: Die Eingabemaske Advanced > IP-Filterung

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 28: Die Eingabemaske Advanced > IP-Filterung

Alle IP-Filter-Regeln	Mit dieser Option können Sie den IP-Filter für den ausgewählten Modus (IPv4 oder IPv6) ein- bzw. ausschalten. • Entfernen Sie die Markierung aus dem Kontrollkästchen, um den IP-Filter zu aktivieren. • Markieren Sie das Kontrollkästchen, um den IP-Filter zu deaktivieren (Standardeinstellung). HINWEIS: Sie können IP-Filterregeln nur dann hinzufügen, bearbeiten oder löschen, wenn dieses Kontrollkästchen nicht markiert ist.
Auswählen	Wählen Sie die Optionsschaltfläche einer IP-Filterregel ( ), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der IP-Filterregel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.
Port Bereich	Hier werden der Start- und Endport des Bereichs angezeigt, dem die Kommunikation mit den festgelegten IP-Adressen untersagt ist.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 28: Die Eingabemaske Advanced > IP-Filterung (Fortsetzung)

Protokoll	Hier werden die nicht zugelassenen Kommunikationstypen angezeigt: • **TCP** - die Kommunikation mit dem Transmission Control Protocol ist nicht zugelassen. • **UDP** - die Kommunikation mit dem User Datagram Protocol ist nicht zugelassen. • **TCP/UDP** - die Kommunikation mit dem Transmission Control Protocol und dem User Datagram Protocol ist nicht zugelassen.
IP Adress Bereich	Hier wird die erste und letzte IP-Adresse des Bereichs angezeigt, dem die Kommunikation mit den festgelegten Ports untersagt wird.
Aktiv	Hier können Sie jede IP-Filterregel ein- oder ausschalten. • Markieren Sie dieses Kontrollkästchen, um die IP-Filterregel zu aktivieren. • Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die IP-Filterregel zu deaktivieren.
Hinzufügen	Klicken Sie hier, um eine neue IP-Filterregel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer IP-Filterregel auf Seite 90.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der IP-Filterregel ( ), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer IP-Filterregel auf Seite 90.
Löschen	Klicken Sie die auf die Optionsschaltfläche der IP-Filterregel ( ), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.5.1 Hinzufügen oder Bearbeiten einer IP-Filterregel

- Um eine neue IP-Filterregel hinzuzufügen, klicken Sie in der Eingabemaske **Advanced** > **IP-Filterung** auf **Hinzufügen**.

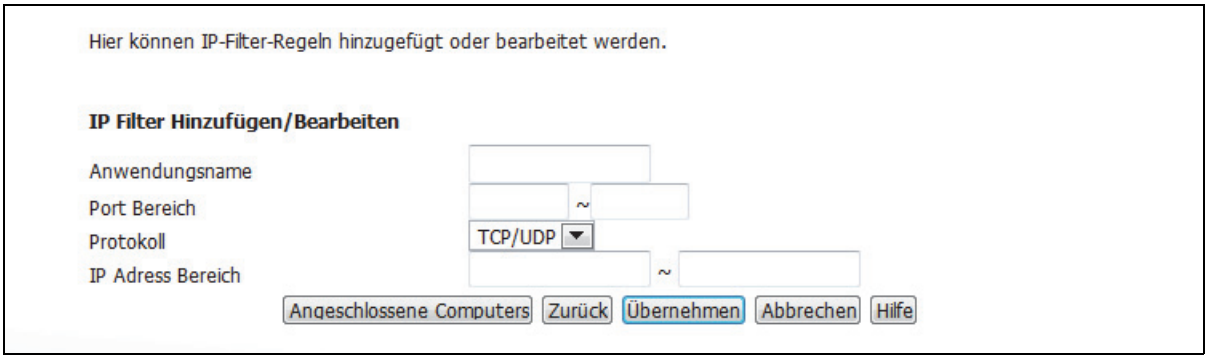
Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

HINWEIS: Der IPv4- und der IPv6-Filter können separat konfiguriert werden. Wählen Sie die Tabelle entsprechend dem Betriebsmodus des CVE-30360 (IPv4 oder IPv6 für DS-Lite).

- Um eine vorhandene IP-Filterregel zu bearbeiten, wählen Sie die Optionsschaltfläche ( ) auf der Eingabemaske **Advanced** > **IP-Filterung** und klicken Sie auf die Schaltfläche **Bearbeiten**.

Die folgende Eingabemaske erscheint.

Abbildung 28: Die Eingabemaske Advanced > IP-Filterung > Hinzufügen/Bearbeiten



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 29: Die Eingabemaske Advanced > IP-Filterung > Hinzufügen/Bearbeiten

Anwendungsname	Geben Sie den Namen für die Anwendung ein, die Sie sperren möchten. HINWEIS: Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Port Bereich	Hier können Sie den Zielportbereich festlegen für den die Kommunikation gesperrt ist. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 29: Die Eingabemaske Advanced > IP-Filterung > Hinzufügen/Bearbeiten

Protokoll	Hier können Sie festlegen, ob der CVE-30360 eine der folgenden Kommunikationstypen sperren soll: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • **Beide** - TCP und UDP HINWEIS: Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**Beide**) beibehalten.
IP Adress Bereich	In diesen Feldern können Sie den IP-Adressbereich der lokalen Computer festlegen deren Kommunikation gesperrt werden soll. Geben Sie die erste IP-Adresse in das erste Feld und die letzte IP-Adresse in das zweite Feld ein. Wenn Sie nur eine einzelne IP-Adresse festlegen möchten, geben Sie in beide Felder dieselbe Adresse ein.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
Zurück	Klicken Sie hier, um zur Eingabemaske **Advanced** > **IP-Filterung** zurückzukehren, ohne die Änderungen in der IP-Filterregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.6 Die Eingabemaske Port Triggering

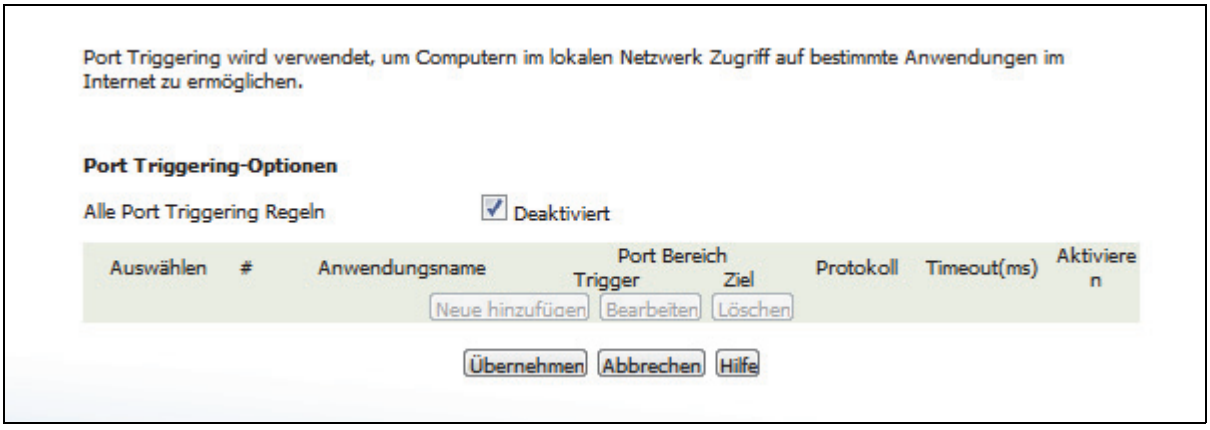
Auf dieser Eingabemaske konfigurieren Sie das Port-Triggering. Sie können das Port-Triggering aktivieren oder deaktivieren, vorhandene Port-Triggering-Regeln ändern und neue konfigurieren.

HINWEIS: Diese Eingabemaske ist nur verfügbar, wenn sich der CVE-30360 im IPv4-Modus befindet.

Klicken Sie auf **Advanced** > **Port Triggering**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 29: Die Eingabemaske Advanced > Port Triggering



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 30: Die Eingabemaske Advanced > Port Triggering

Alle Port Triggering Regeln	In diesem Feld können Sie das Port-Triggering ein- oder ausschalten. ▸ Markieren Sie das Kontrollkästchen, um das Port-Triggering zu aktivieren. ▸ Entfernen Sie die Markierung aus dem Kontrollkästchen, um das Port-Triggering zu deaktivieren.
Auswählen	Wählen Sie die Optionsschaltfläche einer Port-Triggering-Regel ( ), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der Port-Triggering-Regel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.
Port Bereich	In diesen Feldern werden die Ports angezeigt, für die die Regel gilt: ▸ Im Feld **Trigger** wird der Bereich der ausgehenden Ports angezeigt. Wenn der CVE-30360 an diesen Ports von den Computern des LAN ausgehenden Datenverkehr erkennt, öffnet er automatisch die **Ziel**-Ports. ▸ Im Feld **Ziel** wird der Bereich der getriggerten Ports angezeigt. Diese Ports werden automatisch geöffnet, wenn der CVE-30360 Aktivitäten von den Computern des LAN an den **Trigger**-Ports erkennt.
Protokoll	Hier wird das Protokoll der Port-Triggering-Regel angezeigt.

Tabelle 30: Die Eingabemaske Advanced > Port Triggering (Fortsetzung)

Timeout (ms)	Nachdem der CVE-30360 die **Ziel**-Ports geöffnet hat, wird hier die Zeit (in Millisekunden) angezeigt, nach der die Ports wieder geschlossen werden müssen.
Aktivieren	Hier können Sie jede Port-Triggering-Regel ein- oder ausschalten. ▸ Markieren Sie dieses Kontrollkästchen, um die Port-Triggering-Regel zu aktivieren. ▸ Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die Port-Triggering-Regel zu deaktivieren.
Neue hinzufügen	Klicken Sie hier, um eine neue Port-Triggering-Regel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Port-Triggering-Regel auf Seite 94.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der Port-Triggering-Regel ( ), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer Port-Triggering-Regel auf Seite 94.
Löschen	Klicken Sie die auf die Optionsschaltfläche der Port-Triggering-Regel ( ), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

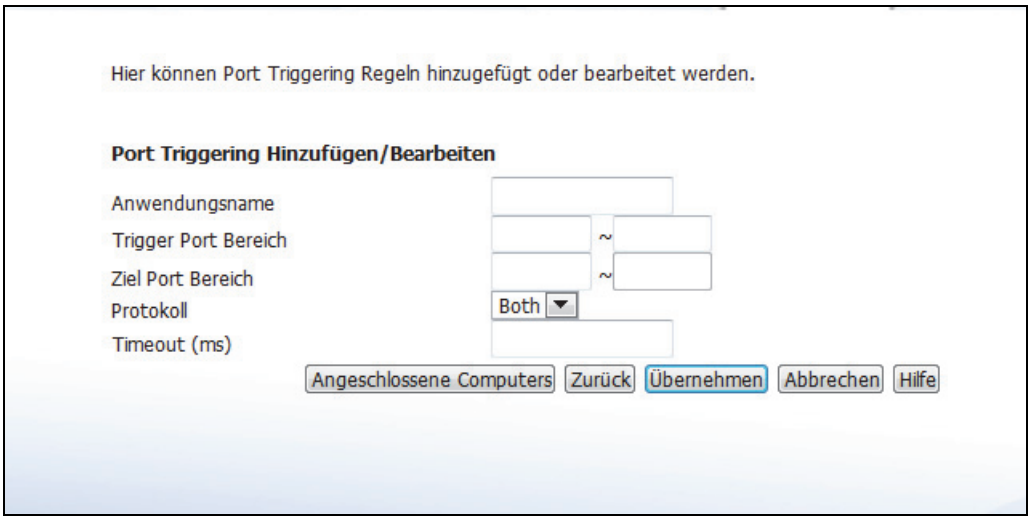
6.6.1 Hinzufügen oder Bearbeiten einer Port-Triggering-Regel

- Um eine neue Port-Triggering-Regel hinzuzufügen, klicken Sie in der Eingabemaske **Advanced** > **Port Triggering** auf **Neue hinzufügen**.
- Um eine vorhandene Port-Triggering-Regel zu bearbeiten, wählen Sie die Optionsschaltfläche ( ) auf der Eingabemaske **Advanced** > **Port Triggering**, und klicken Sie auf die Schaltfläche **Bearbeiten**.

Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 30: Die Eingabemaske Advanced > Port Triggering > Hinzufügen/ Bearbeiten



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 31: Die Eingabemaske Advanced > Port Triggering > Hinzufügen/Bearbeiten

Anwendungsname	Geben Sie einen Namen für die Anwendung ein, für die Sie eine neue Regel festlegen möchten. HINWEIS: Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Trigger Port Bereich	In diesen Feldern können Sie die Trigger-Ports festlegen. Wenn der CVE-30360 an einem dieser Ports Aktivitäten von einem Computer des LAN erkennt, öffnet er in Erwartung von eingehendem Datenverkehr automatisch die **Ziel**-Ports. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.
Ziel Port Bereich	In diesen Feldern können Sie die Ziel-Ports festlegen. Der CVE-30360 öffnet diese Ports in Erwartung von eingehendem Datenverkehr, sobald er Aktivitäten an einem der **Trigger**-Ports ermittelt. Der eingehende Datenverkehr wird an diese Ports des mit dem LAN verbundenen Computers weitergeleitet. Geben Sie die erste Portnummer des Bereichs in das erste Feld und die letzte Portnummer in das zweite Feld ein. Wenn Sie nur einen einzelnen Port festlegen möchten, geben Sie in beide Felder dieselbe Nummer ein.

Tabelle 31: Die Eingabemaske Advanced > Port Triggering > Hinzufügen/Bearbeiten

Protokoll	In diesem Feld können Sie festlegen, ob der CVE-30360 diesen Trigger aktivieren soll, wenn er Aktivitäten mit den folgenden Protokollen erkennt: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Transmission Control Protocol und User Datagram Protocol (**Beide**) HINWEIS: Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**Beide**) beibehalten.
Timeout (ms)	Geben Sie hier die Zeit (in Millisekunden) nachdem der CVE-30360 die **Ziel**-Ports geöffnet hat, nach der die Ports wieder geschlossen werden sollen.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
Zurück	Klicken Sie hier, um zur Eingabemaske **Advanced** > **Forwarding** zurückzukehren, ohne die Änderungen in der Portweiterleitungsregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.7 Die Eingabemaske Host-Port

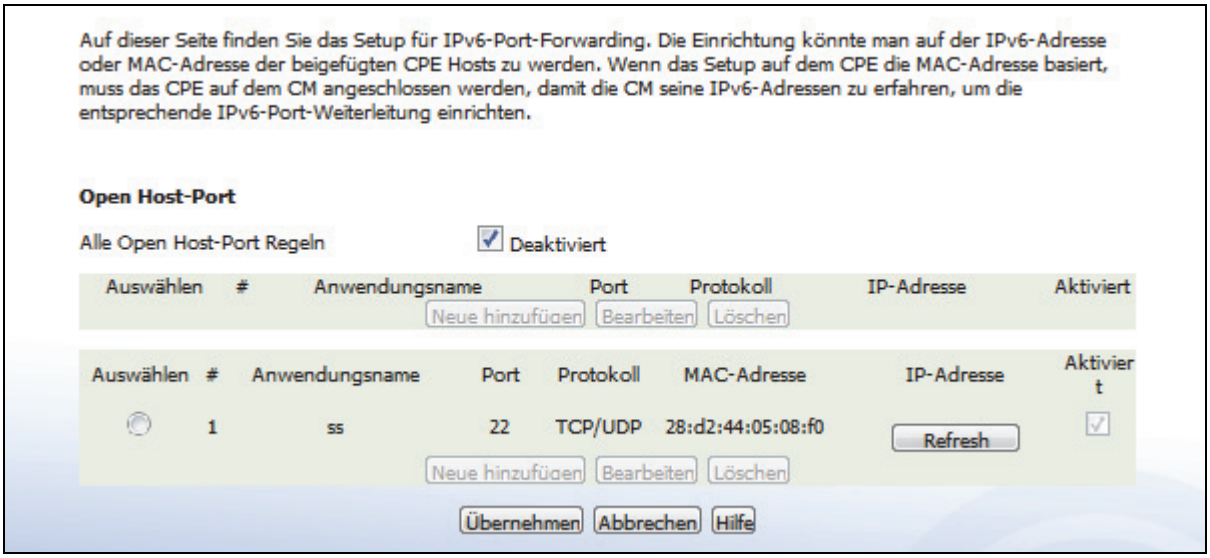
Auf dieser Eingabemaske können Sie die Portweiterleitung konfigurieren, wenn sich der CVE-30360 im DS-Lite-Modus (IPv6) befindet. Sie können den Host-Port aktivieren oder deaktivieren und bestehende Host-Port-Regeln ändern und neue konfigurieren.

HINWEIS: Diese Eingabemaske ist nur verfügbar, wenn sich der CVE-30360 im IPv6-Modus befindet.

Klicken Sie auf **Advanced** > **Host-Port**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 31: Die Eingabemaske Advanced > Host-Port



Auf dieser Eingabemaske befinden sich zwei Listen mit Host-Port-Regeln Die erste Liste enthält Regeln, die abhängig von einer bestimmten IP-Adresse gelten, die zweite Liste enthält Regeln, die abhängig von einer bestimmten MAC-Adresse gelten.

Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 32: Die Eingabemaske Advanced > Host-Port

All Open Host-Port Regeln	In diesem Feld können Sie die IPv6-Portweiterleitung ein- oder ausschalten. • Markieren Sie das Kontrollkästchen, um die Portweiterleitung zu aktivieren. • Entfernen Sie die Markierung aus dem Kontrollkästchen, um die Portweiterleitung zu deaktivieren.
Auswählen	Wählen Sie die Optionsschaltfläche einer IPv6-Portweiterleitungsregel ( ), und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
#	Hier wird die frei wählbare Identifikationsnummer angezeigt, die der IPv6-Portweiterleitungsregel zugewiesen wurde.
Anwendungsname	Hier wird der frei wählbare Name angezeigt, den Sie beim Konfigurieren der Regel festgelegt haben.
Port	In diesem Feld wird der Port angezeigt, für den die Regel gilt.
Protokoll	Hier wird das Protokoll der IPv6-Portweiterleitungsregel angezeigt.
MAC-Adresse	Hier wird die MAC-Adresse des Ziel-Hosts angezeigt, auf den diese IPv6-Portweiterleitungsregel zutrifft.
IP-Adresse	Hier wird die IP-Adresse des Hosts angezeigt, auf den diese IPv6-Portweiterleitungsregel zutrifft (soweit bekannt).

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Tabelle 32: Die Eingabemaske Advanced > Host-Port (Fortsetzung)

Aktiviert	Hier können Sie alle IPv6-Portweiterleitungsregeln ein- oder ausschalten. • Markieren Sie dieses Kontrollkästchen, um die Port-Triggering-Regel zu aktivieren. • Entfernen Sie die Markierung aus diesem Kontrollkästchen, um die Port-Triggering-Regel zu deaktivieren.
Neue hinzufügen	Klicken Sie hier, um eine neue IPv6-Portweiterleitungsregel festzulegen. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer IPv6-Portweiterleitungsregel auf Seite 98. HINWEIS: Verwenden Sie die Schaltfläche der ersten Liste, wenn Sie eine auf der IP-Adresse basierende Regel erstellen möchten. Verwenden Sie die Schaltfläche der zweiten Liste, wenn Sie eine auf der MAC-Adresse basierende Regel erstellen möchten.
Bearbeiten	Klicken Sie die auf die Optionsschaltfläche der IPv6-Portweiterleitungsregel ( ), um die Regel zu bearbeiten. Was auf dieser Eingabemaske angezeigt wird, finden Sie unter Hinzufügen oder Bearbeiten einer IPv6-Portweiterleitungsregel auf Seite 98.
Löschen	Klicken Sie die auf die Optionsschaltfläche der IPv6-Portweiterleitungsregel ( ), um die Regel zu löschen. Die Daten der gelöschten Regel können nicht wiederhergestellt werden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

6.7.1 Hinzufügen oder Bearbeiten einer IPv6-Portweiterleitungsregel

- Um eine neue IPv6-Portweiterleitungsregel hinzuzufügen, klicken Sie in der Eingabemaske **Advanced** > **Host-Port** auf **Neue hinzufügen**.

HINWEIS: Die Eingabemaske Advanced > Host-Port enthält zwei Listen mit Regeln. Verwenden Sie die Schaltfläche der ersten Liste, wenn Sie eine auf der IP-Adresse basierende Regel erstellen möchten. Verwenden Sie die Schaltfläche der zweiten Liste, wenn Sie eine auf der MAC-Adresse basierende Regel erstellen möchten.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

- Um eine vorhandene IPv6-Portweiterleitungsregel zu bearbeiten, wählen Sie die Optionsschaltfläche ( ) auf der Eingabemaske **Advanced** > **Host-Port**, und klicken Sie auf die Schaltfläche **Bearbeiten**.

Je nachdem, ob eine auf einer IP-Adresse oder eine auf einer MAC-Adresse basierenden Regel erstellt wird, erscheint eine der folgenden Eingabemasken.

Abbildung 32: Die Eingabemaske Advanced > Host-Port > IP-Adresse - Neue hinzufügen/Bearbeiten

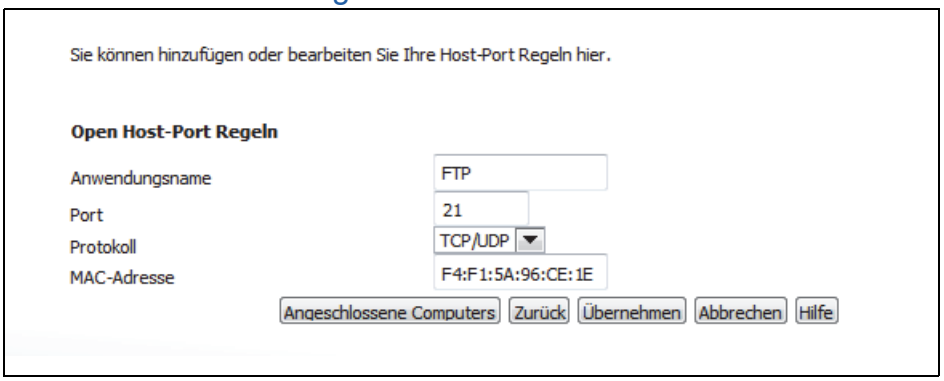
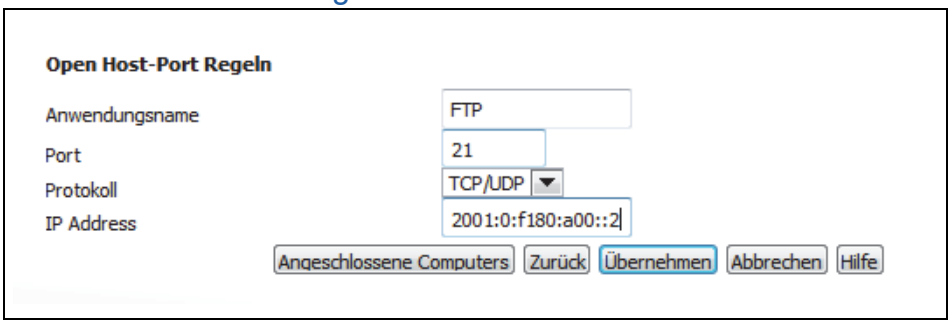


Abbildung 33: Die Eingabemaske Advanced > Host-Port > MAC-Adresse - Neue hinzufügen/Bearbeiten



Die folgende Tabelle erläutert die Bezeichnungen in dieser Eingabemaske.

Tabelle 33: Die Eingabemaske Advanced > Host-Port > Neue hinzufügen/ Bearbeiten

Anwendungsname	Geben Sie einen Namen für die Anwendung ein, für die Sie eine neue Regel festlegen möchten. HINWEIS: Dieser Name ist frei wählbar. Er wirkt sich in keiner Weise auf die Funktionsfähigkeit aus.
Port	Hier wird der Port festgelegt, für den die Regel angewendet werden soll.

Tabelle 33: Die Eingabemaske Advanced > Host-Port > Neue hinzufügen/ Bearbeiten (Fortsetzung)

Protokoll	Hier können Sie festlegen, ob der CVE-30360 eine der folgenden Kommunikationstypen weiterleiten soll: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Transmission Control Protocol und User Datagram Protocol (**TCP/UDP**) • Generic Routing Encapsulation (**GRE**) • Encapsulating Security Protocol (**ESP**) HINWEIS: Wenn Sie sich hier nicht sicher sind, sollten Sie die Standardeinstellung (**TCP/UDP**) beibehalten.
MAC-Adresse	In dieses Feld wird die MAC-Adresse des Ziel-Hosts angegeben.
IP Address	In dieses Feld wird die IP-Adresse des Ziel-Hosts angegeben.
Angeschlossene Computer	Klicken Sie hier, um die Liste der Computer aufzurufen, die aktuell mit dem CVE-30360 im LAN verbunden sind.
Zurück	Klicken Sie hier, um zur Eingabemaske **Advanced** > **Host-Port** zurückzukehren, ohne die Änderungen in der Portweiterleitungsregel zu speichern.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Änderungen zu verwerfen und die alten Einstellungen wieder zu aktivieren.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

HINWEIS: Wenn Sie die Konfiguration der Regel abgeschlossen haben und zur Eingabemaske **Advanced** > **Host-Port** zurückkehren, stellen Sie sicher, dass das Kontrollkästchen **Aktiv** markiert ist.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

7

Management

In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **Management** klicken. Es umfasst die folgenden Abschnitte:

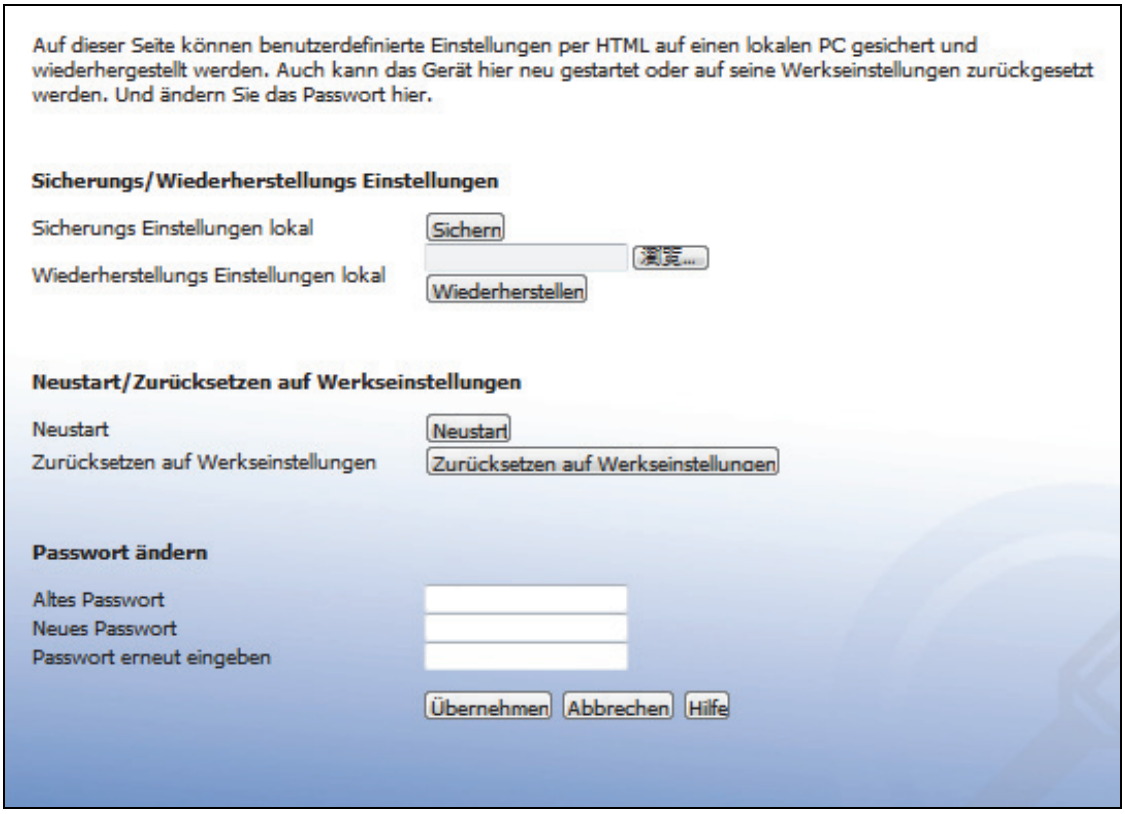
7.1 Die Maske Management

Auf dieser Eingabemaske können Sie Ihre Einstellungen des CVE-30360 auf Ihrem Computer sichern, die Sicherung früherer Einstellungen laden, den CVE-30360 neu starten, ihn auf seine Standardeinstellungen zurücksetzen oder das Passwort ändern, mit dem Sie sich beim CVE-30360 anmelden.

Klicken Sie auf **Management**. Die folgende Eingabemaske erscheint.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Abbildung 34: Die Maske Management



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 34: Die Maske Management

Sicherungs/Wiederherstellungs Einstellungen	
Wiederherstellungs Einstellungen lokal	Klicken Sie hier, um alle Einstellungen des CVE-30360 auf dem Computer zu sichern.
Wiederherstellungs Einstellungen lokal	Hier können Sie die Einstellungen des CVE-30360 entsprechend einer früheren Sicherung wiederherstellen. Klicken Sie auf **Durchsuchen**, um eine Sicherungsdatei auszuwählen, und dann auf **Wiederherstellen**, um die Einstellungen des CVE-30360 entsprechend denen der Sicherungsdatei zu konfigurieren.
Neustart/Zurücksetzen auf Werkseinstellungen	
Neustart	Klicken Sie hier, um den CVE-30360 zurückzusetzen.

Tabelle 34: Die Maske Management (Fortsetzung)

Zurücksetzen auf Werkseinstellungen	Klicken Sie hier, um den CVE-30360 auf die Standardeinstellungen zurückzusetzen. HINWEIS: In diesem Fall gehen alle benutzerdefinierten Einstellungen verloren und können nicht wiederhergestellt werden.
Passwort ändern	
Altes Passwort	Geben Sie das Passwort ein, mit dem Sie sich aktuell beim CVE-30360 anmelden müssen.
Neues Passwort	Geben Sie das neue Passwort für die Anmeldung beim CVE-30360 ein.
Passwort erneut eingeben	
Passwort-Leerlaufzeit (bis erneute Passworteingabe)	Geben Sie hier die Anzahl der Leerlauf-Minuten ein, nach der sich der CVE-30360 automatisch abmeldet. Sobald diese Zeit abgelaufen ist, müssen Sie sich erneut anmelden.
Übernehmen	Klicken Sie hier, um die Änderungen in dieser Eingabemaske zu übernehmen.
Abbrechen	Klicken Sie hier, um die Einstellungen auf dieser Eingabemaske auf die zuvor gespeicherten Einstellungen zurückzusetzen.
Hilfe	Hier erhalten Sie Informationen zu den Feldern dieser Eingabemaske.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

8

Telephony

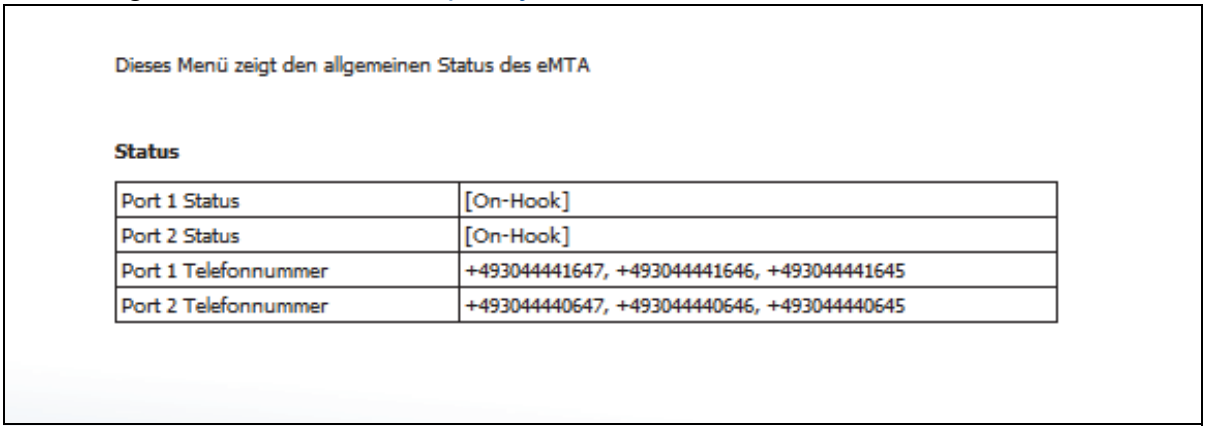
In diesem Kapitel werden die Eingabemasken beschrieben, die erscheinen, wenn Sie in der Symbolleiste auf **Telephony** klicken. Diese Masken enthalten Informationen über die Telefonie-Ports des CVE-30360. Es umfasst die folgenden Abschnitte:

8.1 Die Maske Telephony Status

Diese Maske enthält allgemeine Informationen über die Telefonie-Ports des CVE-30360.

Klicken Sie auf **Telephony** > **Status**. Die folgende Eingabemaske erscheint.

Abbildung 35: Die Maske Telephony > Status



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 35: Die Maske Telephony > Status

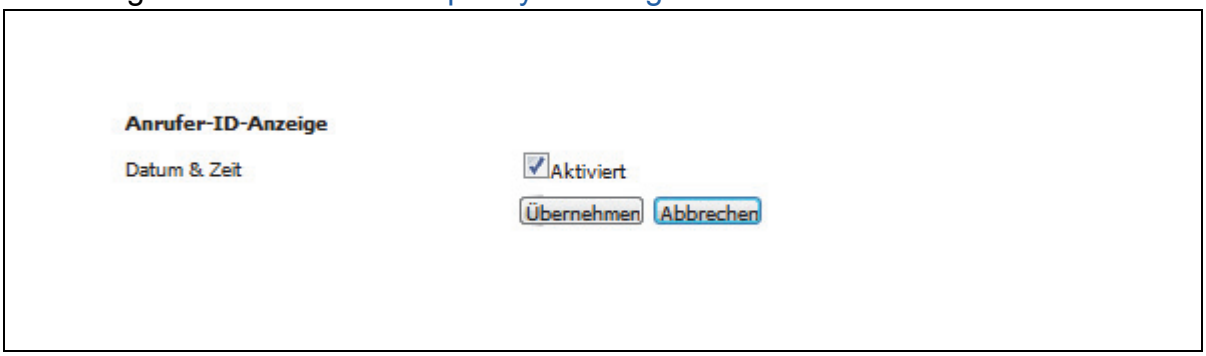
Port 1 Status	In diesen Feldern wird der aktuelle Status der an den jeweiligen Telefonanschlüssen des CVE-30360 angeschlossenen Telefone angezeigt.
Port 2 Status	
Port 1 Telefonnummer	In diesen Feldern werden die Telefonnummern angezeigt, die den Telefonanschlüssen des CVE-30360 zugewiesen sind (falls zutreffend).
Port 2 Telefonnummer	

8.2 Die Eingabemaske Konfiguration

Auf dieser Eingabemaske können Sie die Anzeige der Anruferkennung, des Datums und der Uhrzeit ein- bzw. ausschalten.

Klicken Sie auf **Telephony** > **Configuration**. Die folgende Eingabemaske erscheint.

Abbildung 36: Die Maske Telephony > Configuration



Die folgende Tabelle erläutert die Konfigurationsmöglichkeiten in dieser Eingabemaske.

Tabelle 36: Die Maske Telephony > Configuration

Anrufer-ID-Anzeige	
Datum & Zeit	Markieren Sie dieses Kontrollkästchen, damit die Datums- und Uhrzeitinformationen für die an die Telefonanschlüsse des CVE-30360 angeschlossenen Telefone angezeigt werden.
Übernehmen	Klicken Sie hier, um alle auf dieser Eingabemaske vorgenommenen Änderungen zu speichern.
Abbrechen	Klicken Sie hier, um die Einstellungen auf dieser Eingabemaske auf die zuvor gespeicherten Einstellungen zurückzusetzen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

9

Fehlerbehebung

Mit Hilfe dieses Abschnitts können Sie allgemeine Probleme mit dem CVE-30360 und Ihrem Netzwerk lösen.

Problem: Keine der LEDs leuchtet

Der CVE-30360 wird nicht mit Strom versorgt, oder das Gerät hat einen Fehler.

1. Stellen Sie sicher, dass Sie den richtigen Netzadapter verwenden.

Wenn Sie einen anderen Netzadapter verwenden als den, der im Lieferumfang des CVE-30360 enthalten war, kann der CVE-30360 beschädigt werden.

2. Stellen Sie sicher, dass der Netzadapter richtig an den CVE-30360 und an das Stromnetz angeschlossen ist.
3. Stellen Sie sicher, dass die Stromquelle einwandfrei funktioniert. Wechseln Sie kaputte Sicherungen aus, und setzen Sie alle ausgelösten Schutzschalter zurück.
4. Trennen Sie den Netzadapter vom Stromnetz und vom CVE-30360, und stellen Sie dann beide Verbindungen wieder her.
5. Wenn das Problem mit keinem der oben genannten Schritte behoben werden kann, wenden Sie sich an Ihren Händler.

Problem: Eine der LEDs leuchtet nicht wie erwartet

1. Lesen Sie noch einmal nach, wie die LED normalerweise leuchten müsste (siehe LEDs auf Seite 20).
2. Stellen Sie sicher, dass die Hardware des CVE-30360 richtig angeschlossen wurde. Siehe dazu auch die Installations-Kurzanleitung.
3. Trennen Sie den Netzadapter vom CVE-30360, und schließen Sie ihn wieder an.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

4 Wenn das Problem mit keinem der oben genannten Schritte behoben werden kann, wenden Sie sich an Ihren Händler.

Problem: Sie haben die IP-Adresse des CVE-30360 vergessen

1 Die LAN IP-Standardadresse des CVE-30360 ist **192.168.0.1**.

2 Sie können die Benutzeroberfläche desCVE-30360 aufrufen, indem Sie in einem an das LANangeschlossenen Computer den LAN-Domain-Suffix in die Adresszeile Ihres Browsers eingeben. Der Standardsuffix der LAN-Domain ist **hitronhub.home**. Weitere Informationen dazu finden Sie unter Die Eingabemaske LAN IP auf Seite 43.

3 Abhängig von Ihrem Betriebssystem und Netzwerk können Sie auch die IP-Adresse des CVE-30360 mit Hilfe des Standard-Gateways des Computers herausfinden. Bei den meisten Windows-Computern müssen Sie dazu auf **Start** > **Ausführen** klicken. Geben Sie dann “cmd” und “ipconfig” ein. Beziehen Sie die IP-Adresse des **Standard-Gateways**, und geben Sie diese in die Adresszeile Ihres Browsers ein.

4 Wenn Sie weiterhin keinen Zugriff auf den CVE-30360 haben, müssen Sie den CVE-30360 zurücksetzen. Siehe Zurücksetzen des CVE-30360 auf Seite 28. Wenn der CVE-30360 auf seine Standardeinstellungen zurückgesetzt wird, gehen alle benutzerdefinierten Daten verloren. Wenn Sie zuvor eine neuere Version Ihrer Einstellungen des CVE-30360 gesichert haben, können Sie diese jetzt auf den CVE-30360 hochladen (siehe Die Maske Management auf Seite 101).

Problem: Sie haben den Administrator-Benutzernamen oder das Passwort für den Zugriff auf den CVE-30360 vergessen

1 Der Standard-Benutzername ist **admin** und das Standard-Passwort ist **password**.

2 Wenn dieser Benutzername und das Passwort nicht funktionieren, müssen Sie den CVE-30360 auf seine Standardeinstellungen zurücksetzen. Siehe Zurücksetzen des CVE-30360 auf Seite 28. Wenn der CVE-30360 auf seine Standardeinstellungen zurückgesetzt wird, gehen alle benutzerdefinierten Daten verloren. Wenn Sie zuvor eine neuere Version Ihrer Einstellungen des CVE-30360 gesichert haben, können Sie diese jetzt auf den CVE-30360 hochladen (siehe Die Maske Management auf Seite 101).

Problem: Sie haben keinen Zugriff auf den CVE-30360 oder das Internet

1 Stellen Sie sicher, dass Sie für den CVE-30360 die richtige IP-Adresse verwenden.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

2 Prüfen Sie die Hardwareverbindungen in Ihrem Netzwerk, und stellen Sie sicher, dass die LEDs des CVE-30360 richtig leuchten (siehe LEDs auf Seite 20).

3 Stellen Sie sicher, dass sich der Computer im selben Subnetz befindet wie der CVE-30360 (siehe Einrichten der IP-Adresse auf Seite 23).

4 Wenn Sie versuchen, eine WLAN-Verbindung herzustellen, könnte das Problem bei der Drahtlosverbindung liegen. Schließen Sie das Gerät an den **LAN**-Port an.

5 Wenn das Problem mit den oben beschriebenen Schritten nicht behoben werden kann, muss der CVE-30360 zurückgesetzt werden. Siehe Zurücksetzen des CVE-30360 auf Seite 28. Wenn der CVE-30360 auf seine Standardeinstellungen zurückgesetzt wird, gehen alle benutzerdefinierten Daten verloren. Wenn Sie zuvor eine neuere Version Ihrer Einstellungen des CVE-30360 gesichert haben, können Sie diese jetzt auf den CVE-30360 hochladen (siehe Die Maske Management auf Seite 101).

6 Wenn das Problem dadurch nicht behoben werden kann, wenden Sie sich an Ihren Händler.

Problem: Sie können nicht auf das Internet zugreifen, und die LED-Lampen DS und US blinken

Möglicherweise hat Ihr Internetdienstanbieter Ihren Internetzugriff deaktiviert. Prüfen Sie in der Maske **Kabel** > **Systeminfo** das Feld Netzwerkzugriff (siehe Die Eingabemaske Systeminfo auf Seite 36).

Problem: Sie können mit Ihrem Drahtlosgerät keine Verbindung herstellen

1 Stellen Sie sicher, dass das Drahtlosgerät richtig funktioniert und richtig konfiguriert ist. Lesen Sie dazu u. U. in der Dokumentation des Drahtlosgeräts nach.

2 Stellen Sie sicher, dass sich das Drahtlosgerät innerhalb der Sendereichweite des CVE-30360 befindet. Hindernisse (Wände, Fußböden, Bäume usw.) und elektrische Störungen (andere Funktransmitter, Mikrowellenöfen usw.) verringern die Signalqualität und die Sendereichweite des CVE-30360.

3 Stellen Sie sicher, dass der CVE-30360 und das Drahtlosgerät auf denselben Drahtlosmodus, dieselbe SSID (siehe Die Eingabemaske Wireless-Grundeinstellungen auf Seite 62) und dieselben Sicherheitseinstellungen (siehe Die Eingabemaske Sicherheit auf Seite 65) eingestellt ist.

4 Geben Sie alle Sicherheitsdaten (WEP-Schlüssel, WPA(2)-PSK-Passwort oder WPS PIN) noch einmal ein.

5 Wenn Sie die PBC-Funktion des WPS verwenden, stellen Sie sicher, dass Sie innerhalb von zwei Minuten, nachdem Sie auf die PBC-Taste des CVE-30360 gedrückt haben, die PBC-Taste des Drahtlosgeräts betätigen.

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

Index

Zahlen

A

B

C

D

E

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

F

G

H

I

K

L

M

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

N

O

P

Q

R

S

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies

T

U

V

W

Z

Version 1.0, 07/2014. Copyright © 2014 Hitron Technologies