



# Ubee EVW32C

## Advanced Wireless Voice Gateway

Firmware Version: 2.2.xxxx

## Benutzerhandbuch

März 2017

[www.ubeeinteractive.com](http://www.ubeeinteractive.com)  
Polarisavenue 77  
2132 JH Hoofddorp  
Niederlande  
+31(0)203038371  
Verkauf: [eusales@ubeeinteractive.com](mailto:eusales@ubeeinteractive.com)  
Kundenbetreuung: [eusupport@ubeeinteractive.com](mailto:eusupport@ubeeinteractive.com)

# Hinweise und Urheberrecht

Copyright 2017 Ubee Interactive. Alle Rechte vorbehalten. Dieses Dokument enthält urheberrechtlich geschützte Informationen der Firma Ubee und darf nur im Einklang mit anwendbaren Verträgen offengelegt werden. Dieses Material ist durch die Urheberrechte der USA und anderen Ländern geschützt. Es darf nur im Einklang mit anwendbaren Vereinbarungen, Verträgen oder Lizenzen oder nur unter ausdrücklicher schriftlicher Genehmigung von Ubee und dem Besitzer des Materials durch jegliche - im Verhältnis zu Ubee intern oder extern wirkende - juristische Personen vervielfältigt, verteilt oder geändert werden.

Die Firma Ubee Interactive verbessert ihre Produkte kontinuierlich und behält sich das Recht vor, das vorliegend beschriebene Produkt unangekündigt zu ändern. Sie haftet nicht für den Gebrauch des hier beschriebenen Produkts.

Sämtliche in dieser Schrift erwähnten Handelsmarken sind dem Eigentumsrecht ihrer entsprechenden Besitzer zuzuordnen.

Dieses Gerät ist WiFi-Alliance-zertifiziert:



# Inhalt

<b>1 Einleitung</b> .....	<b>1</b>
<b>1.1 Informationen über Sicherheit und gesetzliche Vorgaben</b> .....	<b>1</b>
1.1.1 Sicherheitsrelevante Informationen .....	1
1.1.2 Umwelterklärungen .....	2
1.1.3 Regulatorische Anforderungen.....	2
<b>1.2 Anschlüsse und Einsatzbereiche</b> . .....	<b>3</b>
<b>1.3 Überprüfen der gelieferten Geräteteile</b> . .....	<b>3</b>
1.3.1 Front- und Rückplatte .....	5
1.3.2 Geräteverbindungen .....	5
1.3.3 LED-Verhalten . .....	6
<b>1.4 Spezifikationen, Standards und Firmware</b> . .....	<b>8</b>
<b>1.5 Vorgabewerte und Anmeldevorgänge</b> .....	<b>10</b>
<b>1.6 Geräteetikett</b> . .....	<b>11</b>
<b>2 Installation des EVW32C</b> .....	<b>13</b>
<b>2.1 Das EVW32C aufstellen und anschließen</b> .....	<b>13</b>
2.1.1 Wandmontage. ....	14
<b>2.2 Geräte an das Netzwerk anschließen</b> .....	<b>15</b>
2.2.1 Ein Ethernet-Gerät anschließen .....	15
2.2.2 Ein drahtloses Gerät (WiFi) anschließen .....	16
2.2.3 Eine Telefonverbindung anschließen .....	17
<b>2.3 Fehlerbehebung bei der Installation</b> .....	<b>17</b>
<b>3 Web-basierte Nutzeroberfläche</b> .....	<b>19</b>
<b>3.1 Lokaler Zugriff auf die web-basierte Nutzeroberfläche</b> .....	<b>19</b>
<b>3.2 Von der web-basierten Nutzeroberfläche abmelden</b> .....	<b>21</b>

<b>4 Kabelmodem-Menü .....</b>	<b>23</b>
<b>4.1 Status-Option .....</b>	<b>23</b>
4.1.1 Option: Systeminformation .....	24
4.1.2 Verbindungs-Option .....	25
4.1.3 Konfigurations-Option .....	26
<b>4.2 Bereitstellungs-Option.....</b>	<b>27</b>
<b>4.3 Management-Option. ....</b>	<b>29</b>
<b>4.4 Diagnose-Option. ....</b>	<b>30</b>
<b>5 Telefonie-Menü.....</b>	<b>32</b>
<b>5.1 Status-Option . ....</b>	<b>32</b>
<b>6 Gateway-Menü.....</b>	<b>34</b>
<b>6.1 LAN-Option.....</b>	<b>35</b>
6.1.1 Setup-Option .....	35
6.1.2 DHCP-Option .....	36
6.1.3 Static Lease Option.....	37
<b>6.2 WAN-Option. ....</b>	<b>38</b>
<b>6.3 WLAN-Option. ....</b>	<b>39</b>
6.3.1 Basic-Option. ....	39
6.3.2 Sicherheits-Option.....	42
6.3.3 WPS-Option. ....	43
6.3.4 Zugangskontroll-Option. ....	44
6.3.5 Drahtloses Netzwerk: Inbetriebnahme und Fehlerbehebung .....	46
<b>6.4 Erweiterte Optionen. ....</b>	<b>51</b>
6.4.1 Option: Angeschlossene Geräte .....	52
6.4.2 Options-Option. ....	53
6.4.3 Port-Weiterleitungs-Option.....	54

6.4.4 IP-Filter-Option .....	59
6.4.5 MAC-Filter-Option.....	59
6.4.6 Port-Filter-Option.....	60
6.4.7 Option: Port Auslösen .....	61
6.4.8 Firewall-Option.....	64
6.4.9 DMZ-Option.....	65
6.4.10 DDNS-Option.....	66
<b>6.5 Management-Option .....</b>	<b>67</b>
6.5.1 Datensicherungs-Option .....	67
<b>6.6 VPN-Option.....</b>	<b>70</b>
6.6.1 Basic-Option.....	71
6.6.2 IPsec-Option. ....	72
<b>6.7 Elternkontrolle .....</b>	<b>75</b>
6.7.1 Benutzereinrichtung .....	76
6.7.2 Grundeinstellungen.....	77
6.7.3 Zeitfilter.....	78

# 1 Einleitung

Willkommen! Sie sind nun Besitzer eines Datennetzwerkprodukts der Firma Ubee Interactive. Diese Anleitung bezieht sich konkret auf das Gerät mit der Bezeichnung **EVW32C Advanced Wireless Voice Gateway** und dient Kunden des Kabelanbieters in folgendem Rahmen:

- Anweisungen zur Installation, Verbindung und Betrieb des EVW32C.
- Anweisungen zum Zugriff der web-basierten Nutzeroberfläche für die Konfiguration und die Geräteverwaltung
- Definition sämtlicher relevanten Gerätestandards und technischer Daten.

## Themen:



Schlagen Sie hier nach:

- [Informationen über Sicherheit und gesetzliche Vorgaben - Seite 1](#)
- [Anschlüsse und Einsatzbereiche - Seite 3](#)
- [Überprüfen der gelieferten Geräteteile - Seite 3](#)
- [Spezifikationen, Standards und Firmware - Seite 8](#)
- [Vorgaben und Anmeldevorgänge - Seite 10](#)
- [Geräteetikett - Seite 11](#)

## 1.1 Informationen über Sicherheit und gesetzliche Vorgaben

Im Folgenden werden Sicherheits- und Gesetzesvorgaben zur Installation, Wartung und der Nutzung des EVW32C dargelegt.

### 1.1.1 Sicherheitsrelevante Informationen

**ACHTUNG:** Es folgen sicherheitsrelevante Informationen für JEDEN, der das EVW32C installiert und wartet. Lesen Sie sämtliche hier aufgeführten Sicherheitsanweisungen, bevor Sie das Gerät auspacken, installieren, betreiben oder an das Stromnetz anschließen. Folgen Sie sämtlichen Anweisungen auf den Geräteetiketten. Folgen Sie unbedingt den unten stehenden Sicherheitsrichtlinien zum ordnungsgemäßen Gerätebetrieb.



Folgen Sie den grundlegenden Sicherheitsvorkehrungen zum Brandschutz sowie zur Abwendung von Elektro- und Verletzungsgefahren. Zum Brandschutz und der Abwehr von Stromschlägen ist das Gerät weder Regen, Feuchtigkeit noch wassernahen Standorten auszusetzen. Niemals Flüssigkeiten über oder in das Gerät verschütten. Niemals flüssige Reinigungsmittel oder Reinigungssprays auf dem Gerät oder in dessen Nähe verwenden. Nur mit trockenen, weichen Tüchern reinigen.



Keine scharfen Gegenstände in die Öffnungen oder freien Schlitze der Gerätemodule einsetzen. Ansonsten fügen Sie dem Gerät ggf. Schäden zu bzw. lösen Stromschläge aus.

Elektrostatische Entladungen können Halbleiterelemente und -geräte dauerhaft zerstören. Folgen Sie den Richtlinien zur Vermeidung elektrostatischer Entladungen im Rahmen des Geräteumgangs und der -lagerung.

Nur Stromadapter aus dem Lieferumfang verwenden. Stromkabel nicht auf Gebäudeoberflächen oder Fußböden anbringen.

- Stromadapter frei beweglich und zugänglich positionieren. Keine schweren Gegenstände auf das Stromkabel stellen. Stromkabel weder missbrauchen noch betreten.
- Keine schweren Gegenstände auf das Gerät stellen. Gerät nur auf standfesten Möbelstücken bzw. Ständern montieren. Andernfalls kann es herunterfallen und Schaden nehmen.
- Schlitze und Öffnungen in den Modulgehäusen der Überhitzungsschutzventilatoren nicht blockieren. Das Gerät darf nicht direktem Sonnenlicht ausgesetzt werden. Dieses Gerät ist nicht in die Nähe anderer heißer Geräte zu verbringen, weil es ggf. sonst mit einer abgeschwächten Leistung arbeitet oder beschädigt werden kann.
- Gerät auf kühle Oberflächen stellen. Andernfalls besteht Überhitzungsgefahr und somit sind das Gerät sowie der jeweilige Untergrund (etwa: Möbel) schadensgefährdet.

### 1.1.2 Umwelterklärungen

Die folgenden Umwelterklärungen finden für das EVW32C Anwendung:

#### **Vorgaben zur Verpackungsentsorgung und Geräteverwertung:**

Das Gerät ist kein Hausmüll. Bitte bei Behörden Informationen über die Entsorgung elektrischer Geräte einholen. Weitere Informationen über die Verpackungsentsorgung und -verwertung innerhalb konkreter Rechtsprechungen stellt Ubee Interactive auf [www.ubeeinteractive.com](http://www.ubeeinteractive.com) zur Verfügung.

### 1.1.3 Regulatorische Anforderungen

Die Ubee Interactive Corporation garantiert, dass das EVW32C Advanced Wireless Voice Gateway den in den folgenden Verordnungen enthaltenen Vorgaben entspricht:

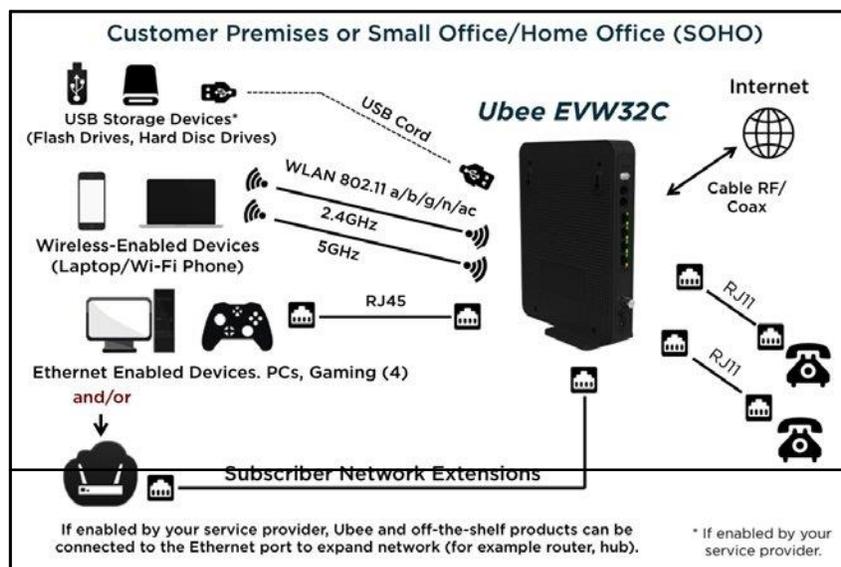
- Richtlinie 2002/95/EG (RoHS-Richtlinie) zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten.
- Richtlinie 2002/96/EG (WEEE-Richtlinie) über Elektro- und Elektronik-Altgeräte. (Zur Vermeidung/Reduzierung von Elektroschrott).
- Richtlinie 2006/95/EG (Niederspannungsrichtlinie) zur Regulierung von Gesundheits- und Sicherheitsrisiken durch elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen.
- Richtlinie 2004/108/EG (EMV-Richtlinie): Ein Gerät, das im Rahmen dieser Richtlinie betrieben wird, (i) stört mit seinen elektromagnetischen Emissionen nicht den Radiobetrieb, die Telekommunikation oder andere Geräte und (ii) ist störfest
- Richtlinie 1999/5/EG (R&TTE-Richtlinie): Endgeräte der Radiokommunikation und der Telekommunikation sind im Einklang mit dieser Richtlinie betriebssicher und verursachen keine Störungen für Rundfunkdienste und andere Geräte.
- 2009/125/EG (Ökodesign-Richtlinie) zur Schaffung eines Rahmens für die Festlegung von Anforderungen an die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte wie auch jegliche in diesem Rahmen erfolgte Direktiven, nämlich u. a. die Bereitschaftsrichtlinie (EG) Nr. 1275/2008 hinsichtlich der Ökodesign-Anforderungen an den Stromverbrauch elektrischer und elektronischer Haushalts- und Bürogeräte im Bereitschafts- und im Aus-Zustand (Standby-Verordnung) und Verordnung (278/2009) (Netzteil-Verordnung).

Die folgenden Standards finden Anwendung:

- EN300328
- EN301893
- EN301489-1
- EN301489-17
- EN50385
- EN55022
- EN55024
- EN60950-1
- EN301893

## 1.2 Anschlüsse und Einsatzbereiche

Das folgende Diagramm illustriert die allgemeine Verbindungstopologie und die Anwendungen des EVW32C.



## 1.3 Überprüfen der gelieferten Geräteteile

Im Lieferumfang des EVW32C sind enthalten:

Artikel	Beschreibung
	<p>1 - RJ45 Kabel (Ethernet) Länge ~ 2 m RoHS &amp; UL-konform</p> <p><i>Beispielbild. Für das tatsächliche Erscheinungsbild sind Änderungen vorbehalten.</i></p>
	<p>1 - RJ11 Kabel (Telefonie)</p> <p><i>Beispielbild. Für das tatsächliche Erscheinungsbild sind Änderungen vorbehalten.</i></p>
	<p>1 - Netzadapter Eingangsleistung: 100-120VAC ~, 50-60Hz CE und UL-zertifiziert</p> <p><i>Beispielbild. Für das tatsächliche Erscheinungsbild sind Änderungen vorbehalten.</i></p>

### 1.3.1 Front- und Rückplatte

Die folgenden Bilder zeigen die Front- und Rückplatten des Geräts. Verbindungsbeschreibungen gelten gemäß 1.3.2, LED-Beschreibungen gemäß 1.3.3.



**Frontplatte**



**Rückplatte**

### 1.3.2 Geräteverbindungen

Die Verbindungen am Gerät werden in der folgenden Tabelle beschrieben.

Artikel	Beschreibung
<b>RESET</b>	Stellt die Geräteeinstellungen (u. a. WiFi-Einstellungen, benutzerdefinierte Einstellungen des Gateways) zurück. Reset-Knopf mit einem spitzen Gegenstand nach unten drücken. Stromversorgungstest: Knopf für weniger als 5 Sekunden gedrückt halten. Zurückstellen auf Werkseinstellungen: Knopf für mehr als 5 Sekunden gedrückt halten.
<b>TEL1 / TEL2</b>	Verbindung zu Standardtelefonen mithilfe eines RJ11-Kabels. Telefondienst muss durch Dienstleister aktiviert werden.
<b>ETHERNET 1-4</b>	Verbindung mit Ethernet-Geräten, wie Computern, Spielkonsolen bzw. Routern/Hubs mithilfe eines RJ45-Kabels. Jede Ethernet-Schnittstelle auf der Rückplatte hat 2 LEDs, um den Verbindungsstatus anzuzeigen, wenn ein Ethernet-Gerät angeschlossen ist.

Artikel	Beschreibung
<b>CABLE RF</b>	Verbindung zum Kabelausgang (Kabel vom Serviceanbieter bereitgestellt) oder einem Kabelverteiler, der mit dem Kabelausgang verbunden ist.
<b>EIN/ AUS</b>	Schaltet das EVW32C ein und aus.
<b>STROM</b>	Verbindung mit dem Stromadapter. Nur Stromadapter aus dem Lieferumfang des EVW32C verwenden.
<b>USB-SCHNITTSTELLE</b>	USB 2.0-Host-Anschluss zur Unterstützung der Linux-Anwendungen für Ubee und Anwendungen Dritter.
<b>WPS</b>	Dieser Knopf befindet sich auf der Frontplatte und dient zur Einstellung eines geschützten Netzwerks, um ein PIN-geschütztes WiFi-Gerät an das Kabelmodem anzuschließen. Siehe <a href="#">WPS-Option auf Seite 40</a> für weitere Informationen.

### 1.3.3 LED-Verhalten

Die folgenden Tabellen erläutern das Verhalten der LEDs auf der Front- und Rückplatte des EVW32C.

FRONTPLATTE									
Position	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6	LED 7	LED 8	Button (Frontplatte)
Farbe	Grün								
Etikett	STROM	DS	US	ONLINE	TEL 1	TEL 2	2.4GHZ	5.0GHz	WPS
Status:									
EINGESCHALTET	An	An	An	An	An	Aus	Aus	Aus	Aus
Selbsttest	keine Angabe								
Ethernet-Schalter initialisieren	An	Blinken	Blinken	Blinken	Aus	Aus	Aus	Aus	Aus
WLAN initialisieren	An	Blinken	Blinken	Blinken	Aus	An	An	Aus	Aus
Router initialisieren	An	Blinken	Blinken	Blinken	Aus	An	An	Aus	Aus
Nachgeschaltete Suchmaske	An	Blinken	Aus	Aus	Aus	An	An	Aus	Aus
Nachschtaltung gesperrt	An	An	Aus	Aus	Aus	An	An	Aus	Aus
Vorgeschalteter, ursprünglicher Bereich	An	An	Blinken	Aus	Aus	An	An	Aus	Aus

FRONTPLATTE									
Position	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6	LED 7	LED 8	Button (Frontplatte)
Registrierung	An	An	An	Blinken	Aus		An	An	Aus
Registrierung abgeschlossen Netzwerkzugang aktiviert	An	An	An	An	Aus		An	An	Aus
Registrierung abgeschlossen Netzwerkzugang deaktiviert	An	An	An	Aus	Aus		An	An	Aus
Bereitstellung des Routers	An	An	An	Aus	Aus		An	An	Aus
Gerät per WPS anschließen	An	An	An	An	Blinken - VoIP-Registrieren On - VoIP-Registrierung abgeschlossen		An	An	AUS - WPS Stop  Blinken- WPS Start  An - Gerät anfüge
VoIP-Registrierung	An	An	An	An	Blinken		An/ Blinkend bei Link- Aktivität	An/ Blinkend bei Link- Aktivität	Aus
VoIP-Registrierung abgeschlossen	An	An	An	An	An		An/ Blinkend bei Link- Aktivität	An/ Blinkend bei Link- Aktivität	Aus
Abschalten der VoIP	An	An	An	An	Blinken		An/ Blinkend bei Link- Aktivität	An/ Blinkend bei Link- Aktivität	Aus
MTA ist nicht bereitgestellt	An	An	An	An	Aus		An/ Blinkend bei Link- Aktivität	An/ Blinkend bei Link- Aktivität	Aus
TEL1 ist bereitgestellt, aber FXS2 wird nicht genutzt	An	An	An	An	An	Aus	An/ Blinkend bei Link- Aktivität	An/ Blinkend bei Link- Aktivität	Aus

RÜCKPLATTE		
LED	Farbe	Bedeutung
ETHERNET 1-4	Grün/ Orange	<p><b>Grün An</b>– Ein Ethernet-Gerät ist mit dem Gerät bei 1000 Mbps angeschlossen (Gigabit Ethernet).</p> <p><b>Orange An</b>– Ein Ethernet-Gerät ist mit dem Gerät bei 10/100 Mbps angeschlossen.</p> <p><b>Blinkt (in Grün oder Orange)</b> –Datenaustausch zwischen dem Kabelmodem und dem verbundenen Gerät.</p> <p>Die Ethernet-Schnittstellen verbinden z. B. Computer, Spielkonsolen bzw. Router/Hubs mit dem EVW32C unter Einsatz von RJ-45-Kabeln. Jede Ethernet-Schnittstelle ist auf der Rückplatte des Geräts einer LED zugeordnet, um bei einer Verbindung mit dem Ethernet-Gerät den Status anzuzeigen.</p>



## 1.4 Spezifikationen, Standards und Firmware

In der folgenden Liste wird auf die Funktionen und technischen Daten des EVW32C verwiesen.

### Schnittstellen und Standards

- Kabel: Koaxialsteckerbuchse
- LAN: 4 10/100/1000 Mbps RJ45 Schnittstellen, automatische Erfassung MDI-X
- Telefonie: 2 RJ-11 Schnittstellen, PacketCable und EuroPacketCable 1.0/ 1.5/2.0 kompatibel, SIP RFC3261
- 1 USB 2.0 Host-Anschlussstelle
- DOCSIS 3.0 und EuroDOCSIS 3.0 zertifiziert
- CE, EuP, RoHS, WEEE

### Nachgeschaltet\*

- Frequenzbereich: 108MHz ~ 1002MHz, Erfassungsbandbreite: 1GHz
- Modulation: 64 / 256 QAM
- Kanalbandbreite: 8 MHz
- Maximale Datenrate pro Kanal (bis zu 24 Kanäle): EuroDOCSIS = 41,71 Mbps (64 QAM), 55,62 Mbps (256 QAM)
- Gesamtmaximale Bandbreite (24 Kanäle): EuroDOCSIS = 1029 Mbps
- Schrittgeschwindigkeit: 6,952 Msps (EuroDOCSIS)
- RF (Kabel) Eingangsleistung (1 Kanal): -17 bis +17dBmV
- Eingangswiderstand: 75  $\Omega$

### Vorgeschaltet\*

- Frequenzbereich: 5MHz ~ 85MHz (EuroDOCSIS), 5MHz ~ 42MHz (DOCSIS), optional 5 bis 65MHz vorgelagert

- Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CDMA: QPSK, 8, 16, 32, 64, 128QAM
- Datenrate: 0,32 bis 30,72 Mbps pro Kanal (8 Kanäle)
- Schrittgeschwindigkeit: 160, 320, 640, 1280, 2560, 5120 Kbps
- RF (Kabel) Ausgangsleistung (1 Kanal): TDMA: +17dBmV bis +61dBmV, S-CDMA: +17dBmV bis +56dBmV
- RF (Kabel) Ausgangsleistung pro Kanal (2 Kanäle verbunden): TDMA: +17dBmV bis +58dBmV, S-CDMA: +17dBmV bis +53dBmV
- RF (Kabel) Ausgangsleistung pro Kanal (3 oder 4 Kanäle verbunden): TDMA: +17dBmV bis +55dBmV, S-CDMA: +17dBmV bis +53dBmV
- RF (Kabel) Ausgangsleistung pro Kanal (5 oder 8 Kanäle verbunden): TDMA: +17dBmV bis +52dBmV, S-CDMA: +17dBmV bis +53dBmV

\*Die tatsächliche Geschwindigkeit hängt von Faktoren wie z. B. Netzwerkkonfiguration und Service-Ebene ab.

### **Sicherheit und Netzwerk**

- Unterstützt mehrere SSIDs pro Sendevorgang, mit zweifachen und gleichzeitigen Sendevorgängen.
  - 5GHz Band= 802.11a/b/g/n/ac konform mit Bandgeschwindigkeiten von bis zu 1300 Mbps, 3 Tx- und 3 Rx-Antennen
  - 2,4GHz Band= 802.11a/b/g/n konform mit Bandgeschwindigkeiten von bis zu 300 Mbps, 2 Tx- und 2 Rx-Antennen
- 802.11ac Durch die Richtstrahlbildung orientiert sich das Signal auf jeden Client. Die Übertragung wird kontrahiert, so dass eine höhere Datenmenge das jeweilige Gerät erreicht.
- DHCP Client/Server, statische IP-Netzwerk-Zuweisung, RIPv1/ v2, Ethernet 10/100/1000 BaseT, Vollduplex Autoanpassungsfunktionalität, IPv4 - und IPv6 Unterstützung
- NAT Firewall, MAC/IP/Port-Filterung, Elternzugangskontrolle, Zustandsorientierte Paketüberprüfung (SPI), DoS Angriffsschutz, WPS (PIN und PBC) / WPA/ WPA2/ WPA-PSK & 64/128-bit WEP Verschlüsselung, WMM, 802.11e
- UPnP/DLNA
- VPN Pass-Through- und Endpunkt-Unterstützung (IPSec/L2TP/PPTP), TACACS oder RADIUS-Authentifizierung

### **Sprachnachrichten**

- PacketCable und EuroPacketCable 1.5 (NCS) und 2.0 (IMS/SIP)
- Ringspannung: 270 VAC, pk-pk (Tip-Ring), Netzspannungs-Anschluss: -48 V, Schleifenstrom: 20mA / 41mA, Ring-Kapazität: 2K ft., 5REN, Anschluss-Status: Loop-Start-Signalisierung
- Audio-Codec: G.711. G.722, G.723, G.726, iLBC, BV16, G.728
- Anruferkennung: Grundlegende und erweiterte CLASS-Funktionen
- DTMF Tonerkennung, T.38 FAX Relay (G.711), Echounterdrückung (G.168) / Sprechpausenerkennung, Sprachaktivitätserkennung und Generierung von Komfortauschen
- Modem-Unterstützung
- RTCP XR

### **Geräte-Management**

- Web-basierte Benutzeroberfläche
- SNMP v1, v2c, v3

- Serielle Konsole (optional)
- Syslog
- WiFi-Radar
- Konfigurationssicherung und -wiederherstellung
- Spektrumanalysator
- TR-069 - Leistung

#### Physische und ökologische Daten

- Maße bei vertikaler Position: 182mm (Tiefe) x 237mm (Höhe) x 80mm (Breite, inkl. Produktständer)
- Gewicht: 800g
- Leistung: 12V / 2.5A
- Betriebstemperatur: 0 °C ~ 40 °C
- Lagertemperatur: -10 °C ~ 70 °C
- Betriebsfeuchtigkeit: 10~90 % (nicht kondensierend)

## 1.5 Vorgabewerte und Anmeldungsvorgänge

Das EVW32C ist mit den Vorgabewerten des Diensteanbieters vorkonfiguriert. Manche Regionen ändern ggf. die Standardwerte unter Einsatz des Kabelmodems oder der XML-Konfigurationsdatei. Die Kundenbetreuung gibt Auskunft über regionale Standardwerte.

**Verbindungsadresse (lokaler Anschluss): 192.168.100.1.**

**Web-Schnittstelle: http://192.168.100.1**

**Betriebsmodus: NAT-Modus**

**Subnetzmaske: 255.255.255.0**

#### Vorgaben für WiFi:

- Primäre SSID (WiFi Netzwerkname) = Die letzten 6 Zeichen der Kabel-Modem-MAC-Adresse. Es gelten dieselben SSIDs für die folgenden Funkbereiche: 2,4 GHz, 5 GHz. Die SSIDs sind auf dem Geräteetikett aufgedruckt.
  - Beispiel für ein Gerät mit Kabel-Modem-MAC-Adresse 68:14:01:24:A5:98 = **24A598**
  - Wenn der Kunde die SSID ändert, stellt sich das Gerät bei der Zurückstellung nicht auf diese vorgegebene SSID ein, außer wenn eine manuelle Rückstellung auf die Werkseinstellungen über die web-basierte Nutzeroberfläche erfolgt.
  - Die SSID kann ebenfalls über den Basis-Bildschirm des WLAN abgerufen werden. Siehe [Basis-Option auf S. 37](#).
- Verschlüsselungsmethode = Automatisch
- WPA Pre-shared Key = Ein nur einmal pro Gerät vergebener Schlüssel, auch „Netzwerk-Schlüssel“ bezeichnet, „WiFi-Schlüssel“ oder „WiFi-Passwort“. Der Netzwerk-Schlüssel für das EVW32C entspricht den 14 Zeichen der Geräte-Seriennummer.

Beispiel Netzwerk-Schlüssel: EVW32C00000060

Das Passwort wird auf dem WLAN-Sicherheitsbildschirm angezeigt. Siehe Sicherheits-Option auf S. 38. Der Netzwerk-Schlüssel befindet sich ebenfalls auf dem Geräteetikett. Siehe [Geräteetikett auf S. 11](#).

- WPS PIN = Die WPS (WiFi-geschützte Einstellungen) PIN ist eine zufallsgenerierte Zahl. Siehe [WPS-Option auf S. 40](#).
- Gerätebezeichnung: UbeeAP

**Vorgabe für die Anmeldung:**

- Webbasierte Nutzeroberfläche (UI) - Anmeldung  
 Wenn Sie auf die web-basierte Nutzeroberfläche zum ersten Mal zugreifen, werden Sie zum Erstellen eines Benutzernamens und eines Passworts aufgefordert. Siehe [Lokaler Zugriff auf web-basierte Nutzeroberfläche auf S. 19](#) für detaillierte Anweisungen.

## 1.6 Geräteetikett

Es folgt ein Beispiel des Gehäuseetiketts für das EVW32C. Beschreibungen folgen.



Artikel	Beschreibung
<b>Modell-Nr.:</b>	Zeigt die Gerätenummer an.
<b>Ubee Teile-Nr.</b>	Zeigt die Ubee-Teile-Nummer an.
<b>SSID</b>	Zeigt die SSID (Service-Set-Erkennungsmerkmal) an oder den WiFi-Netzwerk-Namen (für beide Funkbänder, nämlich 2,4 GHz/5 GHz) an. Die Standardeinstellung ist die letzten 6 Zeichen der Kabel-Modem-MAC-Adresse. Siehe <a href="#">Vorgaben und Anmeldevorgänge auf S. 10</a> für weitere Informationen.
<b>WPA2-PSD</b>	Zeigt den nur einmal vergebenen Netzwerkschlüssel für das Gerät an. Er wird ebenfalls als WiFi-Schlüssel oder WiFi-Passwort bezeichnet. Die Standardvorgabe für beide Funkbänder (2,4 GHz/5 GHz) entspricht der Geräteseriennummer.
<b>Eingangsleistung</b>	Zeigt die Leistungsaufnahme an.
<b>S/N</b>	Zeigt die Geräteseriennummer an.
<b>CM MAC</b>	Zeigt die Kabel-Modem-MAC-Adresse des Geräts an.

Artikel	Beschreibung
<b>MTA MAC</b>	Zeigt die MTA-MAC-Adresse des Geräts an.
<b>RTR MAC</b>	Zeigt die Router-MAC-Adresse des Geräts an.
<b>H/W Version</b>	Zeigt die interne Versionsnummer an, die das Hardware-Design identifiziert.
<b>Herstellungsland</b>	Zeigt das Montageland des Geräts an.

## 2. Installation des EVW32C

In diesem Kapitel werden die Einrichtung und der Anschluss des EVW32C Advanced Wireless Voice Gateway erläutert, der Anschluss von Zusatzgeräten und die Fehlerbehebung während der Installation.



### Themen:

#### Schlagen Sie hier nach:

- [Das EVW32C aufstellen und anschließen, S. 13](#)
- [Geräte an das Netzwerk anschließen, S. 15](#)
- [Fehlerbehebung bei der Installation, S. 17](#)

### 2.1 Das EVW32C aufstellen und anschließen

Das EVW32C ist wie folgt aufzustellen und anzuschließen: Nach Aufstellen und Anschluss des Geräts gehen Sie weiter zu [Lokaler Zugriff der web-basierten Nutzeroberfläche auf S. 19](#), um das Gerät zu konfigurieren.

**Wichtig:** Kunden müssen ihren Serviceanbieter zur Aktivierung des Internetzugriffs, drahtloser Netzwerke und der Telefonie (Stimme) kontaktieren. Im Besonderen hat der Serviceanbieter im Rahmen des Voice-Services zusätzliche Maßnahmen zu ergreifen, u. a. Stornierung des vorherigen Telefondienstes, Übertragung der Telefonnummer und andere Einzelvorgänge, um Ausfallzeiten während des Übergangs zu minimieren.

Üblicherweise konfiguriert und verbindet der Serviceanbieter das Gerät.

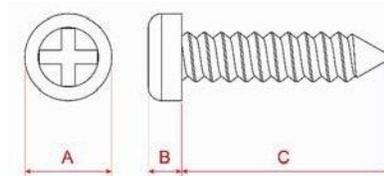
#### Aufstellen des Geräts:

1. Nehmen Sie die Inhalte aus der Verpackung.
  2. Positionieren Sie das EVW32C zentral, so dass Sie auch bequem andere Geräte (PCs, Spielekonsolen) verbinden können. Stellen Sie das Gerät nicht auf dem Boden auf.
- Stellen Sie das EVW32C aufrecht auf, sodass die LED-Etiketten vorne leicht zu lesen sind. Montieren Sie den Ständer (im Lieferumfang enthalten) am Boden des Geräts an, um ein Gleichgewicht herzustellen. Bei horizontaler Lage oder einer Kippstellung wird die WiFi-Leistung drastisch beeinträchtigt, weil die internen Antennen das WiFi-Signal nicht designgerecht übertragen können.
  - Positionieren Sie das EVW32C und andere WiFi-Komponenten auf einer offenen Fläche und nicht in der Nähe von Metallgegenständen, Transformatoren, Schwermotoren, Mikrowellen, Kühlschränken und anderen Betriebsmitteln. Solche Gegenstände können WiFi-Signale beeinträchtigen. Ein WiFi-Signal schwächt sich ggf. ab, wenn es durch Metalle, Beton, Ziegel, Wände oder Fußböden hindurchdringt. Für weitere Informationen zum Thema „Drahtlose Signale“ siehe [Drahtloses Netzwerk: Inbetriebnahme und Fehlerbehebung auf S. 42](#).

- Stellen Sie das Gerät an einem Ort mit einer Umgebungstemperatur zwischen 0°C und 40°C auf. Siehe [Informationen über Sicherheit und gesetzliche Vorgaben auf S. 1](#) für weitere Sicherheitsinformationen.
3. Schalten Sie Ihren PC ein. Der PC muss mit einem Ethernet-Netzwerkadapter oder einer Ethernet-Schnittstelle sowie einem Internet-Browser ausgestattet sein. Die folgenden Browser werden unterstützt:
    - Für Windows 2000, XP, Vista, Windows 8, Windows 7, Google Chrome, Firefox 1.07 und höher, Internet Explorer v7 und darüber hinaus.
    - Für MAC OS X, 10.2 und höher: Firefox 1.07. Safari 1.x und jeweils höher.
  4. Verbinden Sie den Stromadapter (im Lieferumfang enthalten) mit einer Steckdose und das andere Ende mit der Steckbuchse auf der Rückseite des EVW32C.
  5. Verbinden Sie das Ethernetkabel (im Lieferumfang enthalten) mit dem Ethernet-Steckplatz Ihres Computers. Verbinden Sie das andere Ende mit einem der Ethernet-Steckplätze auf der Rückseite des EVW32C.
  6. Verbinden Sie ein Koaxialkabel (nicht im Lieferumfang enthalten) vom Kabelsteckplatz an der Geräterückseite mit der Netzwerksteckdose oder mit einem mit der Wandsteckdose verbundenen Kabelverteiler.
  7. Verbinden Sie ein analoges Telefon (sofern das Gerät für Telefonie benutzt wird) mit einem der Steckplätze TEL 1 oder TEL 2 an der Geräterückseite. Nehmen Sie für eines der Telefone das mitgelieferte RJ-11 Telefonkabel.
  8. Prüfen Sie die Netzwerkverbindung anhand der LEDs des Gerät zur Bestätigung des Betriebs.
    - Die LEDs für die Funkbänder (2,4 GHz, 5 GHz) müssen blinken oder dauerhaft leuchten.
    - Die LEDs für POWER, DS, US, und ONLINE leuchten dauerhaft.
 Siehe [LED-Verhalten auf S. 6](#) für weitere Informationen.

### 2.1.1 Wandmontage

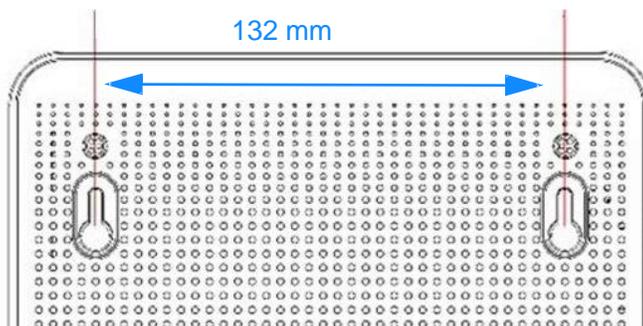
Sie können das EVW32C an einer Wand mit den zwei Befestigungshalterungen an der Geräteseite montieren. Zwei Rund- oder Flachschaublen werden empfohlen. Siehe Abbildung unten.



Etikett	Größe in mm
A	7,2 +/- 0,5
B	2,6 +/- 0,15
C	19,0 +/- 1,2

## Wandmontage des EVW32C:

1. Montieren Sie beide Schrauben horizontal auf einer Wand in einem Abstand von 132 mm. Siehe Abbildung unten.



Lassen Sie die Schrauben von der Wand vorstehen, so dass Sie das Gerät zwischen dem Schraubenkopf und der Wand aufhängen können. Wenn Sie die Schrauben in eine trockene Wand treiben, verwenden Sie Hohlraumdübel, damit sich das Gerät nicht aus der Wand herauszieht wegen der verlängerten Belastung, die vom Kabel und den Stromanschlüssen ausgeht.

2. Montieren Sie das Gerät an der Wand.

## 2.2 Geräte an das Netzwerk anschließen

Befolgen Sie die Anweisungen unten zum Anschluss von Geräten an das Netzwerk und überprüfen Sie danach deren Funktionalität.

### Schlagen Sie hier nach:

- [Ethernet-Gerät anschließen, S. 15](#)
- [Ein drahtloses Gerät \(WiFi\) anschließen, S. 16](#)
- [Telefonverbindung anschließen, S. 17](#)

### 2.2.1 Ein Ethernet-Gerät anschließen

Sie können an das EVW32C bis zu drei weitere Geräte anschließen.

#### Um andere Ethernet-Geräte an das Netzwerk anzuschließen:

1. Schließen Sie ein Ethernet-Kabel vom Ethernet-Gerät (z.B. PC, Spielekonsole) an eine offene Ethernet-Schnittstelle an der Rückseite des EVW32C an.
2. Überprüfen Sie die LEDs zur Betriebsbestätigung des Geräts. Siehe [LED-Verhalten auf S. 6](#) für weitere Informationen.
3. Öffnen Sie einen Browser und überprüfen Sie die Netzwerk-/Internet-Konnektivität mit einer Webseite (z.B. <http://www.wikipedia.org>).
4. Handelt es sich um eine Spielekonsole, führen Sie einen der folgenden Tests aus (z.B. loggen Sie sich bei einem Spieleserver ein, spielen Sie ein Online-Spiel, laden Sie Inhalte herunter).

**HINWEIS:** Siehe [Fehlerbehebung bei der Installation auf S. 17](#) für Informationen zur Fehlerbehebung.

## 2.2.2 Ein drahtloses Gerät (WiFi) anschließen

Folgen Sie folgenden Schritten, um ein drahtloses Gerät an das EVW32C anzuschließen (z.B. Laptop).

Standardeinstellungen sind in den unten aufgeführten Schritten angegeben:

### Ein drahtloses Gerät an das EVW32C anschließen:

1. Rufen Sie die WiFi-Netzwerkfunktion auf Ihrem drahtlosen Gerät auf.

- Windows-Benutzer: Klicken Sie doppelt auf „Drahtlose Netzwerkverbindung“ in der Taskleiste (unten rechts am Windows Desktop). Klicken Sie auf „**Drahtlose Netzwerke abrufen**“.



- Mac-Benutzer: Klicken Sie auf das „WiFi-Symbol“ (Menüleiste oben rechts). Sämtliche verfügbaren drahtlosen Netzwerke werden im Drop-Down-Menü erscheinen.



2. Das EVW32C wird mit einer vorgegebenen SSID versandt. Diese entspricht der Bezeichnung des drahtlosen Netzwerks des Geräts, so dass WiFi-Komponenten mit diesem verbunden werden können.

- Klicken Sie doppelt auf Ihre **SSID** im Fenster, welches die drahtlosen Netzwerke anzeigt.
  - SSID (WiFi-Netzwerkname) = Die letzten 6 Zeichen der Kabel-Modem-MAC-Adresse. Die SSID ist auf dem Geräteetikett aufgedruckt.
    - Beispiel für ein Gerät mit Kabel-Modem-MAC-Adresse 68:14:01:24:A5:98.  
**24A598.**
    - Hinweis: Wenn der Kunde die SSID ändert, stellt sich das Gerät nicht auf diese vorgegebene SSID bei der Zurückstellung ein, außer sofern eine manuelle Rückstellung auf die Werkseinstellungen über die web-basierte Nutzeroberfläche erfolgt.
  - Geben Sie bei der Eingabeaufforderung den Netzwerkschlüssel ein. Jedes Gerät verfügt über einen anderen Netzwerkschlüssel. Der Netzwerkschlüssel für das EVW32C ist für beide Funkbänder (2,4 GHz sowie 5 GHz) derselbe. Das vorgegebene Passwort entspricht den 14 Zeichen der Geräte-Seriennummer. Beispiel: **EVW32C00000060**. Das Passwort wird auf dem WLAN-Sicherheitsbildschirm angezeigt. Siehe [Sicherheits-Option auf S. 38](#). Der Netzwerk-Schlüssel befindet sich ebenfalls auf dem Geräteetikett. Siehe [Geräteetikett auf S. 11](#).
  - Sofern eine WPS zum Einsatz kommt, verwenden Sie die PIN der WPS. Diese ist eine Zufallszahl. Siehe [WPS-Option auf S. 40](#).
  - **AES** wird als Standardverschlüsselungsmethode eingesetzt.
3. Bestätigen Sie die Konnektivität durch die Öffnung eines Web-Browsers und den Aufruf einer Webseite

(z.B. <http://www.wikipedia.org>) oder greifen Sie auf die Web-Benutzeroberfläche des EVW32C zu.

**HINWEIS:** Über die Web-Benutzeroberfläche können Sie die Konfigurationen und Kapazitäten des Geräts einstellen. Eine vollständige Erklärung sämtlicher Funktionen der Web-Oberfläche ist in folgendem Kapitel verfügbar: [Web-basierte Nutzeroberfläche auf S. 19.](#)

Informationen zum Thema „WiFi“ oder „drahtlose Netzwerke“ sind in folgendem Kapitel verfügbar: [Drahtloses Netzwerk: Inbetriebnahme und Fehlerbehebung auf S. 42.](#)

### 2.2.3 Eine Telefonverbindung anschließen

Es können mit dem EVW32C bis zu zwei Telefonverbindungen zur Nutzung der Telefonie (Voice-) Funktionen hergestellt werden.

Der Voice-Service muss vom Serviceanbieter aktiviert werden. Im Besonderen hat der Serviceanbieter im Rahmen des Voice-Services zusätzliche Maßnahmen zu ergreifen, u. a. Stornierung des vorherigen Telefondienstes, Übertragung der Telefonnummer und andere Einzelvorgänge, um Ausfallzeiten während des Übergangs zu minimieren.

#### Anschluss der Telefonverbindung:

1. Schließen Sie ein analoges Telefon an die TEL 1- oder TEL 2-Steckbuchse auf der Rückplatte des EVW32C mit dem mitgelieferten RJ-11-Telefonkabel an.
2. Heben Sie ab und testen Sie den Wählton.
3. Stellen Sie eine Gesprächsverbindung her bzw. lassen Sie sich anrufen, um den Erfolg dieser Telefonverbindung zu testen.

## 2.3 Fehlerbehebung bei der Installation

Hinweise zur Fehlerbehebung bei der Installation.

- **LEDs leuchten bei Einschalten des EVW32C nicht auf.**
  - Überprüfen Sie die Stromzufuhr der Steckdose und die Verbindung zwischen Steckdose und Stromadapter.
  - Überprüfen Sie die Verbindung zwischen Stromadapter und dem EVW32C. Schalten Sie das Gerät aus und nach 5 Sekunden wieder ein. Besteht das Problem weiterhin, liegt ggf. ein Hardware-Problem vor.
- **Die Ethernet-LEDs auf der Rückseite leuchten trotz Ethernet-Verbindung nicht auf.**
  - Starten Sie den Computer neu, sodass dieser erneut eine Verbindung mit dem EVW32C herstellt.
  - Prüfen Sie, ob ein Ressourcenkonflikt vorliegt (nur Windows-Benutzer):
    1. Klicken Sie mit der rechten Maustaste auf **Mein Computer** auf dem Desktop und wählen Sie **Eigenschaften** aus.
    2. Wählen Sie **Gerätemanager** und achten Sie auf ein gelbes Ausrufezeichen oder ein rotes **X** über der Netzwerkkarte (NIC) im Feld „Netzwerkadapter“. Falls Sie eines der beiden sehen, liegt möglicherweise eine Unterbrechungsanforderung (IRQ) vor. Folgen Sie den Anweisungen des Herstellers oder fordern Sie vom Serviceanbieter weitere Hilfestellungen an.
  - Prüfen Sie, ob es sich bei TCP/IP um das Standardprotokoll für Ihre Netzwerkkarte handelt.

- Trennen Sie das EVW32C kurz von der Stromzufuhr (Power cycle), indem Sie den Stecker am elektrischen Ausgang für einen Moment ziehen und wieder einstecken. Dann warten Sie auf die Wiederherstellung der Kommunikation mit Ihrem Kabeldienstanbieter.
- **Allgemeine Verbindungsprobleme prüfen:**
  - Ist Ihr PC mit einem anderen Knotenpunkt oder Gateway verbunden, verbinden Sie den PC direkt mit einer Ethernet-Schnittstelle des EVW32C.
  - Ist ein Kabelverteiler angeschlossen, sollte dieser entfernt werden, sodass der Gateway direkt mit der Kabelsteckdose verbunden wird. Warten Sie, bis die Kommunikation mit dem Kabeldienstanbieter wiederhergestellt wird.
  - Nehmen Sie ein anderes Kabel. Das Ethernet-Kabel ist möglicherweise beschädigt.

## 3 Web-basierte Nutzeroberfläche

Über die web-basierte Nutzeroberfläche des EVW32C können Sie die Einstellungen des Geräts abrufen und konfigurieren. Sie können die Installation durch Zugriff auf die web-basierte Nutzeroberfläche des Geräts überprüfen.



### Themen:

#### Schlagen Sie hier nach:

- [Lokaler Zugriff auf die web-basierte Nutzeroberfläche auf S. 19.](#)
- [Von der web-basierten Nutzeroberfläche abmelden auf S. 21.](#)

### 3.1 Lokaler Zugriff auf die web-basierte Nutzeroberfläche

Greifen Sie auf die web-basierte Nutzeroberfläche des EVW32C über einen Internet-Browser (z.B. Google Chrome für Windows, oder Safari für Mac) zu.

#### Zugriff auf die web-basierte Nutzeroberfläche:

1. Starten Sie einen Internet-Browser, wie Google Chrome, auf Ihrem Computer.
2. Geben Sie die folgende IP-Adresse in das Browser-Fenster ein und bestätigen Sie mit der „Eingabetaste“:

<http://192.168.100.1>

3. Wenn Sie auf die web-basierte Nutzeroberfläche zum ersten Mal zugreifen, werden Sie zum Erstellen eines Benutzernamens und eines Passworts aufgefordert.

The screenshot shows the 'Ubee Wi-Fi Modem' web interface. At the top left, it says 'Ubee Wi-Fi Modem' and at the top right is the Ubee logo with the tagline 'let's make it easy'. The main content area is titled 'Create User Name and Password' and contains the instruction 'Please enter username and password for first time login.' Below this are three input fields: 'Create Username', 'New Password', and 'Retype the Password'. An 'Apply' button is located at the bottom of the form.

4. Geben Sie einen Benutzernamen und ein Passwort ein, und bestätigen Sie das Passwort mit wiederholter Eingabe. Klicken Sie auf **Übernehmen**.



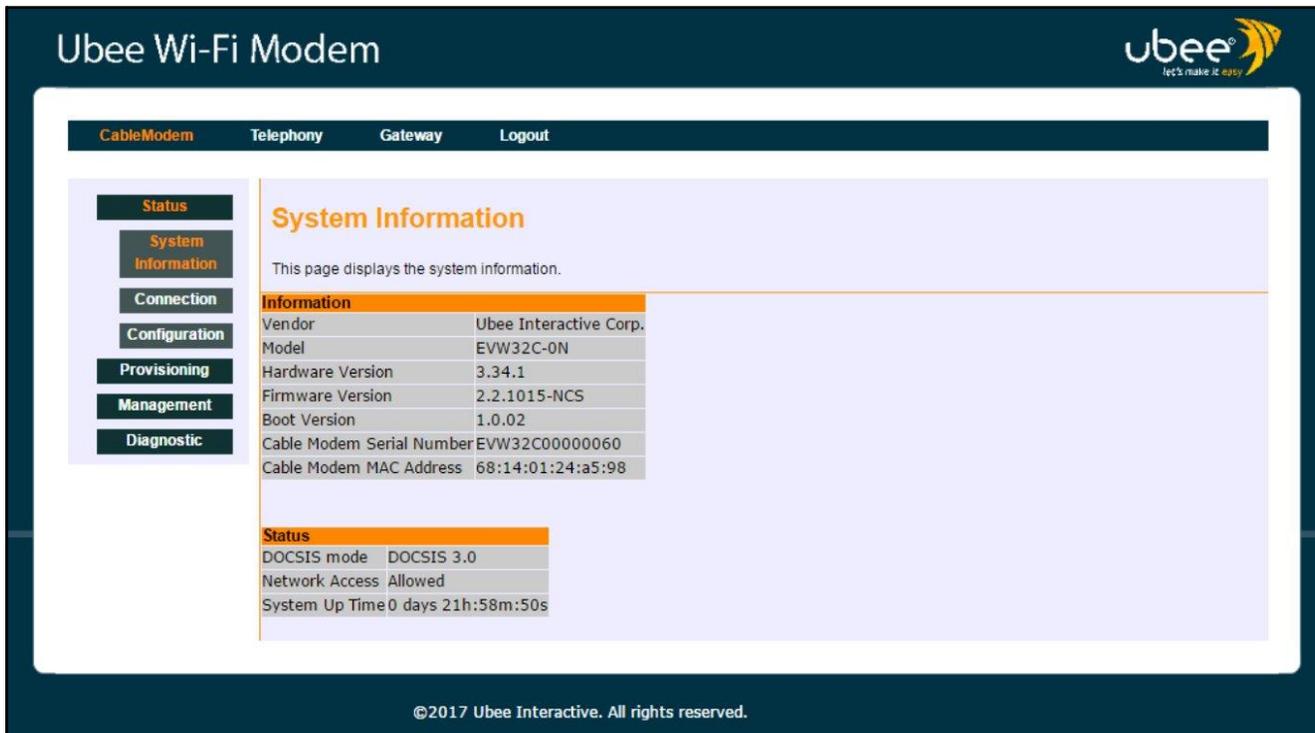
The screenshot shows the 'Ubee Wi-Fi Modem' web interface. At the top right is the Ubee logo with the tagline 'let's make it easy'. The main heading is 'Ubee Wi-Fi Modem'. Below it, the section is titled 'Create User Name and Password'. A message reads: 'Please enter username and password for first time login.' There are three input fields: 'Create Username' with the value 'newusername', 'New Password' with a masked password '\*\*\*\*\*', and 'Retype the Password' with a masked password '\*\*\*\*\*'. An 'Apply' button is located below the fields.

5. Nach dem Klicken des Kommandos **Übernehmen** erscheint der Standard-Anmelde-Bildschirm. Geben Sie den im letzten Schritt erstellten Benutzernamen und das Passwort ein und klicken Sie dann auf **Anmelden**.



The screenshot shows the 'Ubee Wi-Fi Modem' web interface. At the top right is the Ubee logo with the tagline 'let's make it easy'. The main heading is 'Ubee Wi-Fi Modem'. Below it, the section is titled 'Log in'. A message reads: 'Please enter the username and password to login.' There are two input fields: 'Username' with the value 'newusername' and 'Password' with a masked password '\*\*\*\*\*'. A 'Login' button is located below the fields.

Es erscheint der u. g. Bildschirm mit Grundinformationen über das EVW32C. Siehe [Option: Systeminformationen auf S. 22](#) für Beschreibungen der Bildschirmfelder.



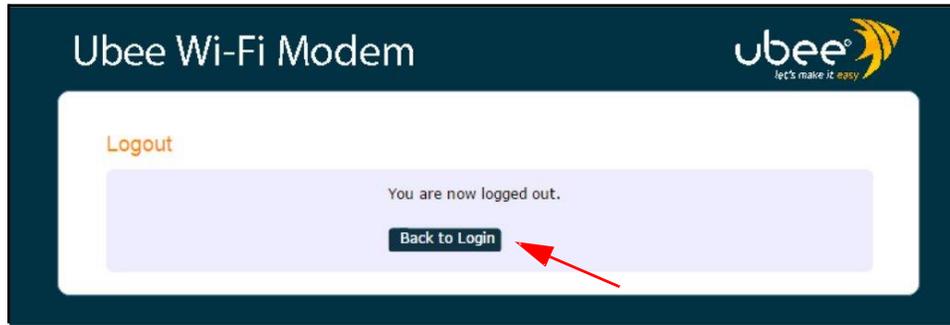
Nachdem Sie **Login** angeklickt haben, erscheint der u. g. Bildschirm mit Grundinformationen über das EVW32C. Siehe [Option: Systeminformationen auf S. 22](#) für Beschreibungen der Bildschirmfelder.

### 3.2 Von der web-basierten Nutzeroberfläche abmelden

Um sich von der web-basierten Nutzeroberfläche abzumelden, klicken Sie auf „Abmelden“ oben rechts in der Menüleiste.



Der folgende Bildschirm erscheint und bestätigt Ihre Abmeldung - mit der Option, den Bildschirm zum „Anmelden“ wieder aufzurufen.



## 4 Kabelmodem-Menü

Das **Kabelmodem-Menü** der web-basierten Nutzeroberfläche ermöglicht den Zugriff auf Geräteinformationen, wie Softwareversion, Verbindungsstatus (vor-/nachgeschaltet). Ebenfalls lassen sich von hier aus Benutzername und Passwort ändern und Informationen über die Bereitstellung des Kabelmodems abfragen.



### Themen:

#### Schlagen Sie hier nach:

- [Status-Option, S. 23](#)
  - [Option: Systeminformationen, S. 24](#)
  - [Verbindungs-Option, S. 25](#)
  - [Konfigurations-Option, S. 26](#)
- [Bereitstellungs-Option, S. 27](#)
- [Management-Option, S. 29](#)
- [Diagnose-Option, S. 30](#)

#### Zugriff auf Kabel-Modem-Optionen:

1. Rufen Sie die web-basierte Nutzeroberfläche auf. Siehe [Lokaler Zugriff auf die Nutzeroberfläche des lokalen Netzwerks auf S. 19](#).
2. Klicken Sie auf **Kabel-Modem** im Hauptmenü.



### 4.1 Status-Option

Die **Status**-Option zeigt die interne Gerätekonfiguration der Software und Hardware an sowie den Verbindungsstatus (vor-/nachgeschaltet). Ebenfalls kann die Anfangs-Scanfrequenz eingestellt, das Gerät neu gestartet oder auf die Werkseinstellungen zurückgestellt werden.

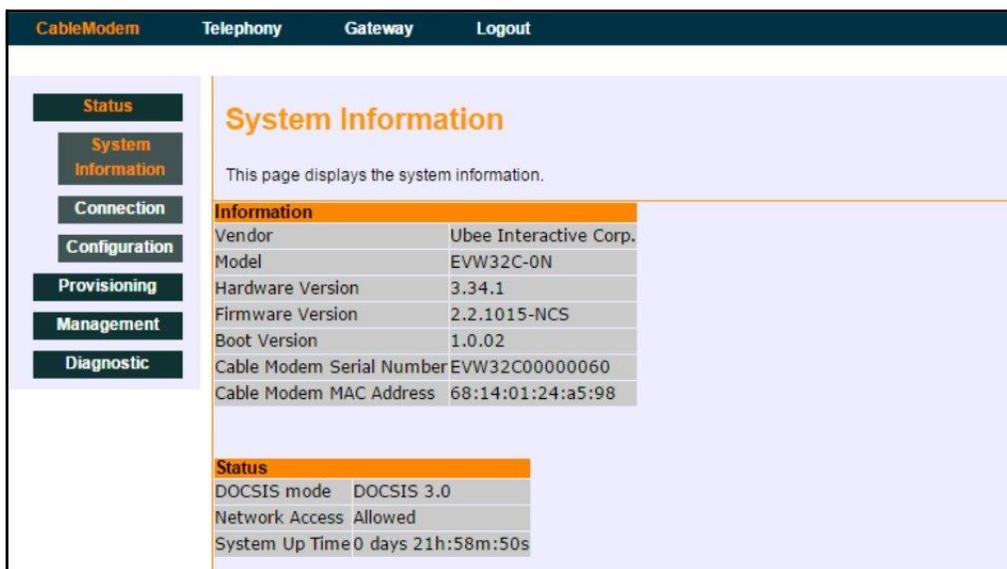
#### Abfrage der Status-Daten:

1. Klicken Sie auf **Kabel-Modem** im Hauptmenü.
2. Wählen Sie **Status** im linken Menü.
3. Folgende Untermenüs sind verfügbar:
  - Systeminformationen

- Verbindung
- Konfiguration

### 4.1.1 Option: Systeminformationen

Der Bildschirm „Systeminformationen“ zeigt die interne Gerätekonfiguration der Software und Hardware an. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Information</b>	
<b>Anbieter</b>	Zeigt den Gerätehersteller an (Ubee Interactive Corp.)
<b>Modell</b>	Zeigt die Gerätenummer an.
<b>Hardware-Version</b>	Zeigt die interne Versionsnummer an, die das Hardware-Design identifiziert.
<b>Firmware-Version</b>	Zeigt die Firmware-Version des Geräts an.
<b>Boot-Version</b>	Zeigt die Bootloader-Version an.
<b>Seriennummer des Kabelmodems</b>	Zeigt die nur einmal vergebene Geräteseriennummer an.
<b>Kabelmodem-MAC-Adresse</b>	Zeigt die nur einmal vergebene Medienzugangskontroll-Hardware-Adresse des Geräts an.
<b>Status</b>	
<b>DOCSIS-Modus</b>	Zeigt die DOCSIS-Version des Geräts an.
<b>Netzwerkzugang</b>	Zeigt Genehmigungsstatus des Netzwerkzugangs an. In positivem Falle besteht eine Freigabe für den Benutzer.
<b>Systemverbindungszeit</b>	Zeigt an, wie lange das Gerät schon verbunden ist.

### 4.1.2 Verbindungs-Option

Der Bildschirm **Verbindung** ermöglicht es einem Nutzer, die bevorzugte Anfangs-Scanfrequenz einzustellen. Ferner werden hier Daten über den Verbindungsstatus sowie über die Kabelbündelung (nachgeschaltetet/vorgeschaltetet) angezeigt.

- **Nachgeschaltetet** zeigt Detailinformationen über die Netzwerkauslastung auf dem Weg vom Dienstanbieter **zum** lokalen Computer (nachgeschaltete Kanäle).
- **Vorgeschaltetet** zeigt Detailinformationen über die Netzwerkauslastung auf dem Weg **vom** lokalen Computer zu entfernten Zielnetz-Computern (vorgeschaltete Kanäle).

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.

**Connection**

This page displays the connection information.

**Initial Scan**

Favorite Frequency (MHz)

**Downstream Bonded Channels**

Channel	Lock	Status	Modulation	Frequency	Power	SNR	Symbol Rate	Correctables	Uncorrectables
1	Locked		QAM256	711000000 Hz	8.1 dBmV	45.4 dB	5360 Ksym/sec	0	0
2	Locked		QAM256	717000000 Hz	8.1 dBmV	45.2 dB	5360 Ksym/sec	0	0
3	Locked		QAM256	723000000 Hz	8.1 dBmV	45.1 dB	5360 Ksym/sec	0	0
4	Locked		QAM256	729000000 Hz	7.9 dBmV	44.8 dB	5360 Ksym/sec	0	0
5	Locked		QAM256	735000000 Hz	7.7 dBmV	44.6 dB	5360 Ksym/sec	0	0
6	Locked		QAM256	741000000 Hz	7.6 dBmV	44.4 dB	5360 Ksym/sec	0	0
7	Locked		QAM256	747000000 Hz	7.3 dBmV	44.3 dB	5360 Ksym/sec	0	0
8	Locked		QAM256	753000000 Hz	7.4 dBmV	44.3 dB	5360 Ksym/sec	0	0
9	Locked		QAM256	759000000 Hz	8.0 dBmV	44.5 dB	5360 Ksym/sec	0	0
10	Locked		QAM256	765000000 Hz	7.8 dBmV	44.2 dB	5360 Ksym/sec	0	0
11	Locked		QAM256	771000000 Hz	7.4 dBmV	43.5 dB	5360 Ksym/sec	0	0
12	Locked		QAM256	777000000 Hz	7.4 dBmV	43.7 dB	5360 Ksym/sec	0	0
13	Locked		QAM256	783000000 Hz	7.7 dBmV	44.5 dB	5360 Ksym/sec	0	0
14	Locked		QAM256	789000000 Hz	7.8 dBmV	44.2 dB	5360 Ksym/sec	0	0
15	Locked		QAM256	795000000 Hz	7.9 dBmV	44.0 dB	5360 Ksym/sec	0	0
16	Locked		QAM256	801000000 Hz	8.2 dBmV	44.2 dB	5360 Ksym/sec	0	0
17	Locked		QAM256	807000000 Hz	11.0 dBmV	47.1 dB	5360 Ksym/sec	0	0
18	Locked		QAM256	813000000 Hz	11.1 dBmV	47.3 dB	5360 Ksym/sec	0	0
19	Locked		QAM256	819000000 Hz	11.4 dBmV	47.4 dB	5360 Ksym/sec	0	0
20	Locked		QAM256	825000000 Hz	11.7 dBmV	47.4 dB	5360 Ksym/sec	0	0
21	Locked		QAM256	831000000 Hz	11.6 dBmV	47.3 dB	5360 Ksym/sec	0	0
22	Locked		QAM256	837000000 Hz	11.4 dBmV	46.8 dB	5360 Ksym/sec	0	0
23	Locked		QAM256	843000000 Hz	11.6 dBmV	47.3 dB	5360 Ksym/sec	0	0
24	Locked		QAM256	885000000 Hz	10.2 dBmV	46.3 dB	5360 Ksym/sec	0	0

**Upstream Bonded Channels**

Channel	Lock	Status	US Channel	Type	Symbol Rate	Frequency	Power
1				ATDMA	5120 Ksym/sec	32000000 Hz	47.3 dBmV
2				ATDMA	5120 Ksym/sec	186000000 Hz	44.8 dBmV
3				ATDMA	5120 Ksym/sec	252000000 Hz	51.0 dBmV
4				ATDMA	2560 Ksym/sec	390000000 Hz	43.8 dBmV
5	Not Locked	Unknown			0 Ksym/sec	0 Hz	0.0 dBmV
6	Not Locked	Unknown			0 Ksym/sec	0 Hz	0.0 dBmV
7	Not Locked	Unknown			0 Ksym/sec	0 Hz	0.0 dBmV
8	Not Locked	Unknown			0 Ksym/sec	0 Hz	0.0 dBmV

Bezeichnung	Beschreibung
<b>Anfangs-Scan</b>	
<b>Bevorzugte Frequenz (MHz)</b>	Nutzer kann eine bevorzugte Frequenz (in MHz) für den Anfangs-Scan eingeben
<b>Übernehmen</b>	Änderungen zur bevorzugten Frequenz werden gespeichert.
<b>Downstream Bonded Channels - nachgeschaltete, gebündelte Kanäle</b>	
<b>Kanal</b>	Anzahl der nachgeschalteten, gebündelten Kanäle.
<b>Verbindungsstatus</b>	Zeigt an, ob ein Gerät erfolgreich an einen nachgeschalteten Kanal angeschlossen ist.
<b>Modulation</b>	Zeigt die für die nachgeschalteten, gebündelten Kanäle notwendige Modulations-Methode für dieses Gerät an. Diese Methode wird durch den Serviceanbieter festgelegt.
<b>Frequenz</b>	Zeigt die Frequenz des nachgeschalteten, gebündelten Kanals an.
<b>Leistung</b>	Zeigt die Empfangsleistung in dBmV nach dem Anordnungsverfahren an.
<b>SNR</b>	Zeigt das Signal-Rausch-Verhältnis (SNR) in dB des erwünschten Signals gegenüber des Hintergrundsignals an.
<b>Schrittgeschwindigkeit</b>	Zeigt die Schrittgeschwindigkeit an (1000 Schritte/s).
<b>Korrekturmöglichkeiten</b>	Zeigt die Menge der korrigierbaren Codewords an.
<b>Korrektursperre</b>	Zeigt die Menge der nicht-korrigierbaren Codewords an.
<b>Upstream Bonded Channels - vorgeschaltete, gebündelte Kanäle</b>	
<b>Kanal</b>	Anzahl der vorgeschalteten, gebündelten Kanäle
<b>Verbindungsstatus</b>	Anzeige, ob das EVW32C an einen vorgeschalteten, gebündelten Kanal angeschlossen wurde.
<b>US Kanal-Typ</b>	Zeigt den Kanaltyp an.
<b>Schrittgeschwindigkeit</b>	Zeigt die Schrittgeschwindigkeit an (1000 Schritte/s).
<b>Frequenz</b>	Zeigt die Frequenz des vorgeschalteten, gebündelten Kanals in Hertz an.
<b>Leistung</b>	Zeigt die Übertragungsleistung des vorgeschalteten, gebündelten Kanals in dBmV an.

### 4.1.3 Konfigurations-Option

Der Bildschirm **Konfiguration** ermöglicht den Neustart des Geräts oder dessen Zurückstellung auf die Werkseinstellungen. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Neustart/zurück auf Werkseinstellungen</b>	
<b>Neustart</b>	Zum Neustarten, Ein-/und Ausschalten des EVW32C klicken Sie auf <b>Ja</b> und <b>Übernehmen</b> .
<b>Werkseinstellungen</b>	Zum Zurückstellen auf die Werkseinstellungen klicken Sie auf <b>Ja</b> und <b>Übernehmen</b> .

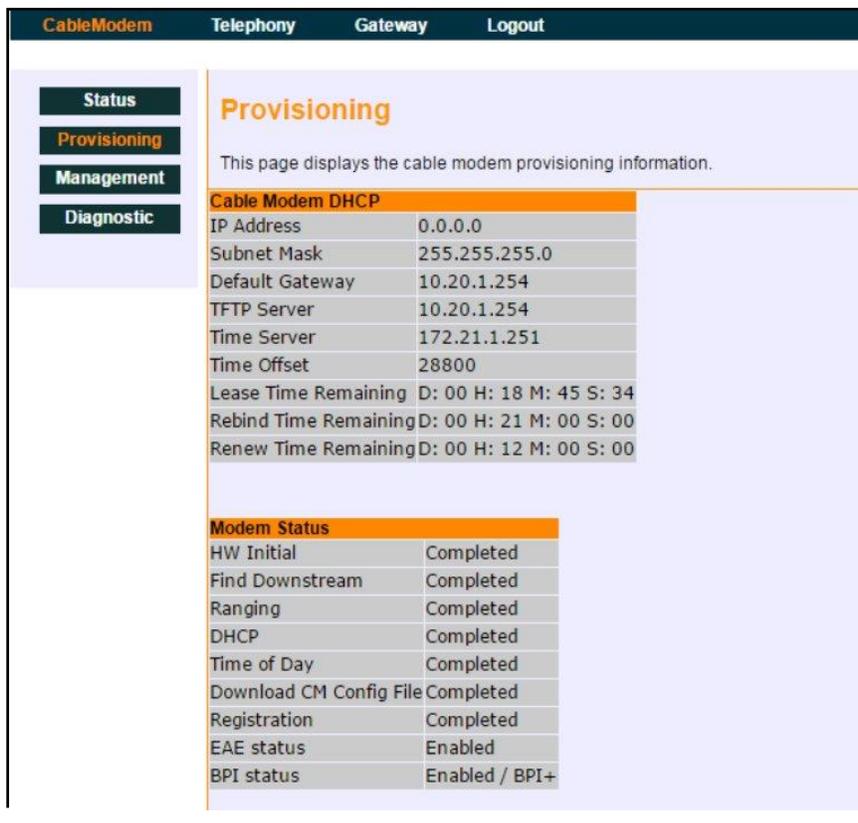
## 4.2 Bereitstellungs-Option

Die **Bereitstellungs**-Option zeigt die Bereitstellungsoptionen des Kabelmodems an, u. a. das Dynamic Host Configuration Protocol (DHCP) und die Daten des Modem-Status.

### Bereitstellungs-Menü abrufen:

1. Klicken Sie auf **Kabel-Modem** im Hauptmenü.
2. Wählen Sie **Bereitstellung** im linken Menü.

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Kabelmodem-DHCP</b>	
<b>IP-Adresse</b>	Zeigt die IP-Adresse des Kabelmodems (DHCP) an.
<b>Subnetzmaske</b>	Zeigt die IP-Adresse der Subnetzmaske an.
<b>Standardgateway</b>	Zeigt die IP-Adresse des Standardgateways an.
<b>TFTP-Server</b>	Zeigt die IP-Adresse des TFTP-Servers an.
<b>Zeitserver</b>	Zeigt die IP-Adresse des Zeitserver an.
<b>Zeitlicher Versatz</b>	Zeigt den zeitlichen Versatz an.
<b>Verbleibende Freigabezeit</b>	Definiert die verbleibende DHCP-Freigabezeit in Minuten (von 1 bis 71582788). Dem PC eines DHCP-Nutzers wird eine IP-Adresse mit einer Freigabezeit zugewiesen. Wenn diese abläuft, muss der PC mit dem DHCP-Server verbunden sein und es wird eine neue, noch nicht belegte IP-Adresse eingesetzt.
<b>Verbleibende Rebind-Zeit</b>	Die verbleibende Rebind-Zeit wird in Tagen, Stunden, Minuten und Sekunden angezeigt.
<b>Verbleibende Renew-Zeit</b>	Die verbleibende Renew-Zeit wird in Tagen, Stunden, Minuten und Sekunden angezeigt.
<b>Modem-Status</b>	
<b>HW Initial</b>	Zeigt an, ob die Hardware vollständig initialisiert wurde.

Bezeichnung	Beschreibung
DHCP	Zeigt an, ob das DHCP abgeschlossen wurde.
Tageszeit	Zeigt an, ob die Tageszeit abgelaufen ist.
CM-Konfigurationsdatei herunterladen	Zeigt den Namen der Konfigurationsdatei sowie den Download-Status an.
Registrierung	Zeigt an, ob das Gerät vollständig registriert wurde.
EAE Status	Zeigt an, ob die EAE (Frühzeitige Authentifizierungsverschlüsselung) aktiviert ist.
BPI Status	Zeigt an, ob die BPI (Baseline Datenschutz-Benutzeroberfläche) aktiviert ist.

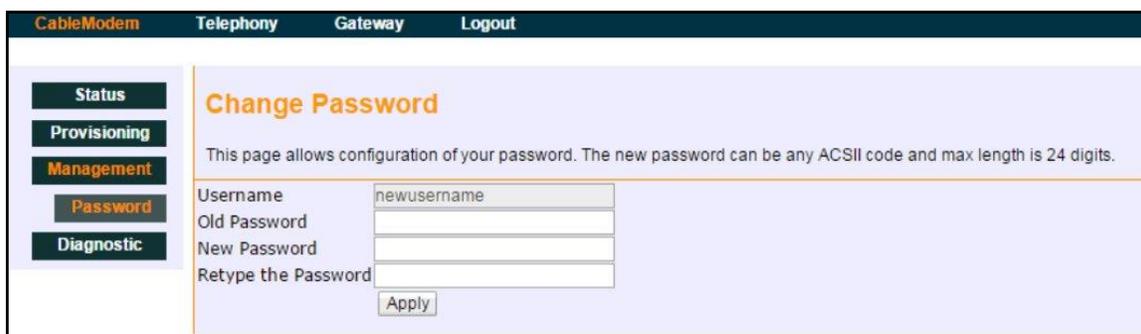
### 4.3 Management-Option

Diese Option ermöglicht es, den Gerätebenutzernamen und das Passwort festzulegen.

#### Management-Menü abrufen:

1. Klicken Sie auf **Kabel-Modem** im Hauptmenü.
2. Wählen Sie **Management** im linken Menü.

Der Bildschirm zur **Passwort**-Eingabe lässt die Änderung des Benutzernamens und des Passworts für das EVW32C zu. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
Benutzername	Neuen Benutzernamen eingeben.
Altes Passwort	Altes Passwort eingeben.
Neues Passwort	Neues Passwort eingeben.
Passwort wiederholen	Passwort durch Wiederholen bestätigen.
Übernehmen	Speichert Änderungen.

## 4.4 Diagnose-Option

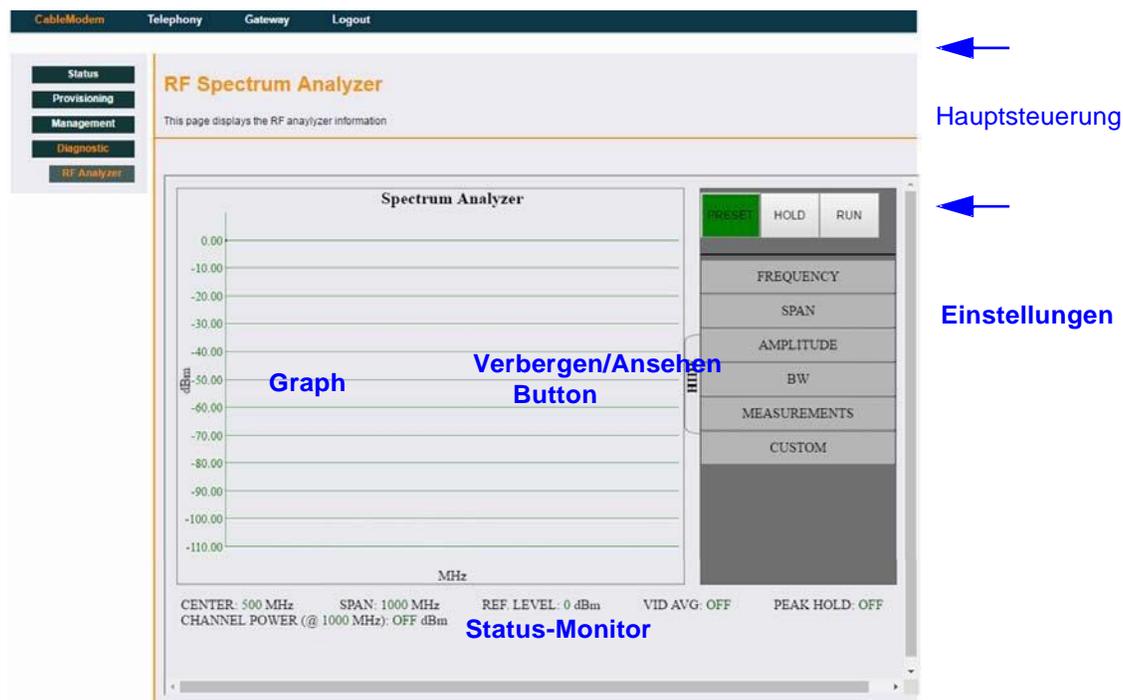
Die Diagnose-Option ermöglicht den Abruf der RF-Spektralanalysedaten. Auf diese Art kann unbemerkt die gesamte 1-GHz-Kabel-Anlage in Echtzeit überwacht werden, ohne dass die Abruffunktionen des Nutzers oder die Lieferung von Breitband-Datendiensten auf Video oder anderen Datenkanälen beeinträchtigt werden. Dieses Tool kann durch Kabelbetreiberfirmen zur Verminderung von Kundenanrufen hinsichtlich der technischen Betreuung zur Fehlerbehebung bei Installationen eingesetzt werden. Danach können sie RF-Diagnosedaten von jeder Einheit zur Analyse und Auswertung der Netzwerkbedinglichkeiten auf diese Weise erheben, analysieren und auswerten.

**Hinweis:** Zum Abrufen der Spektralanalysedaten muss ein Browser HTML5 und Websockets unterstützen. Geeignet dafür sind Chrome und Safari, jedoch nicht der Internet Explorer.

### Diagnose-Menü abrufen:

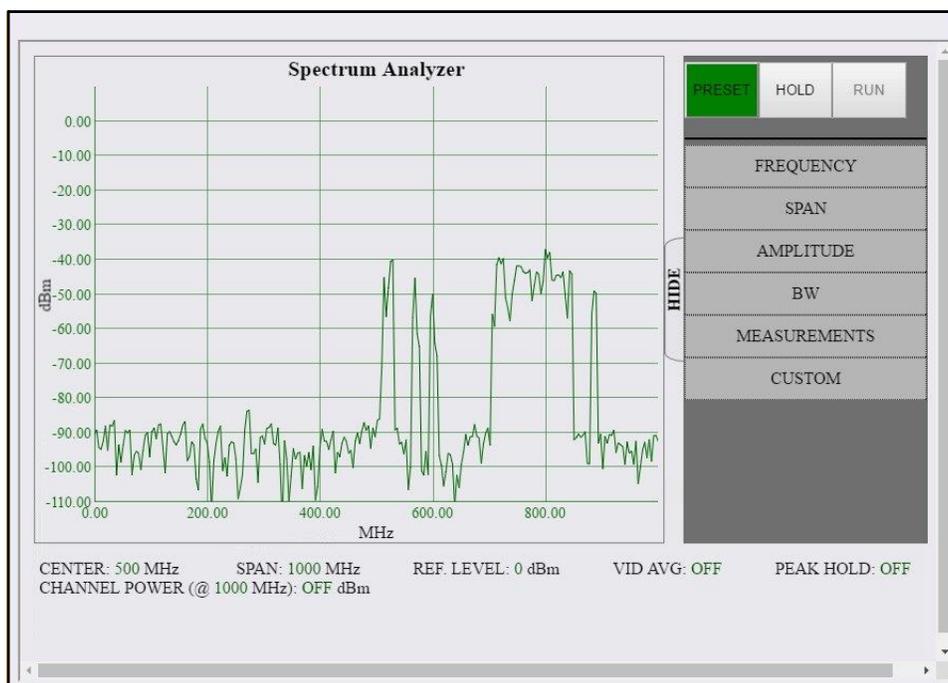
1. Klicken Sie auf **Kabel-Modem** im Hauptmenü.
2. Wählen Sie **Diagnose** im linken Menü.

Am Bildschirm wird nun der **RF-Analysator** angezeigt. Feldbeschreibungen siehe unterhalb des Screenshots.



Bezeichnung	Beschreibung
<b>Graph</b>	Dieser Abschnitt stellt den Hauptbereich des Spektralanalysators dar - hier werden die Daten angezeigt.
<b>VERBERGEN/ ANSEHEN Button</b>	Klicken Sie auf VERBERGEN, um die Kontrollanzeigen rechts zu verkleinern und die graphische Darstellung in voller Größe anzuzeigen. Klicken Sie auf ANSEHEN und die Kontrollanzeigen rechts werden vollständig angezeigt.
<b>Hauptsteuerung</b>	Dieser Abschnitt enthält die Haupt-Buttons zum Starten/Anhalten des Spektrumanalysators und zum Zurückstellen auf die Standardeinstellungen. <ul style="list-style-type: none"> <li>• ZURÜCKSTELLEN: Die Standardeinstellungen werden wiederhergestellt.</li> <li>• HALTEN: Hält den Spektrumanalysator an.</li> <li>• STARTEN: Startet den Spektrumanalysator.</li> </ul>
<b>Einstellungen</b>	Dieser Abschnitt enthält sämtliche unterstützten Einstellungen der Anpassung des Hauptbereichs oder der Funktionsaktivierung. <ul style="list-style-type: none"> <li>• FREQUENZ: Spezifiziert die Frequenz (Mitte, Start, Stop) der Überwachung in Hz.</li> <li>• SPANNBREITE: Spezifiziert die Spannbreite für den Abruf (Hz).</li> <li>• AMPLITUDE: Stellt den Referenzbereich (Offset) des Eingabebereichs ein.</li> <li>• BW: Bandbreite</li> <li>• MESSUNGEN:</li> </ul>
<b>Status-Monitor</b>	Dieser Abschnitt enthält sämtliche Felder für die unterstützten Messungen und aktuellen Einstellungen. <ul style="list-style-type: none"> <li>• MITTEL</li> <li>• SPANNBREITE</li> <li>• REFERENZBEREICH: Referenzbereich</li> <li>• VID AVG: Videomittelung (de-)aktivieren:</li> <li>• KANALLEISTUNG: Spezifiziert die Spannbreite des Kanals im Verhältnis zur Mittelfrequenz zur entsprechenden Leistungsmessung.</li> </ul>

Der folgende Screenshot zeigt wie der Analysator läuft.



## 5 Telefonie-Menü

Das Telefonie-Menü liefert Daten über die Bereitstellung und den Verbindungsstatus des EVW32C.



### Themen:

#### Schlagen Sie hier nach:

- [Status-Option, S. 32](#)

#### Telefonie-Menü abrufen:

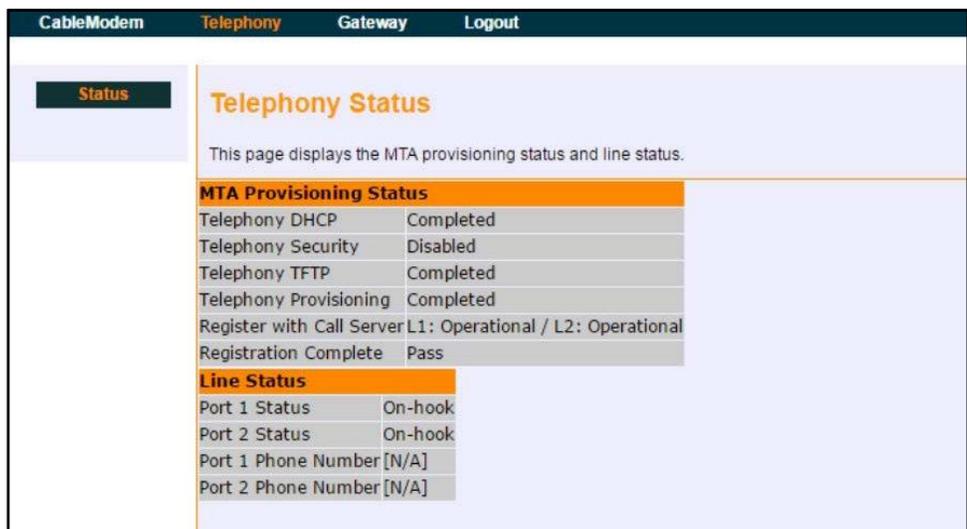
1. Rufen Sie die web-basierte Nutzeroberfläche auf. Siehe [Lokaler Zugriff auf die Nutzeroberfläche des lokalen Netzwerks auf S. 19](#).
2. Klicken Sie auf **Telefonie** im Hauptmenü.



3. Die Statusseite wird angezeigt.

### 5.1 Status-Option

Der **Status**-Bildschirm zeigt den Fortschritt der Bereitstellung und des MTA-Verbindungsstatus an. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>MTA Bereitstellungsstatus</b>	
<b>Telefonie - DHCP</b>	Zeigt an, ob die DHCP-IP-Adresse registriert wurde.
<b>Telefonie-Sicherheit</b>	Zeigt an, ob der Status des Sicherheitsmodus des MTA aktiviert ist.
<b>Telefonie - TFTP</b>	Zeigt an, ob die TFTP-Serverregistrierung des MTA abgeschlossen ist.
<b>Telefonie-Bereitstellung</b>	Zeigt an, ob die Telefonie-Bereitstellung vollständig ist.
<b>Mit Call Server registrieren</b>	Zeigt den Status der Registrierung der MTA gegenüber dem Call-Server des Serviceanbieters pro Leitung wird an (nicht verbunden, betriebsbereit).
<b>Registrierung abgeschlossen</b>	Zeigt an, ob die MTA-Registrierung abgeschlossen ist.
<b>Verbindungsstatus</b>	
<b>Port 1 Status</b>	Zeigt an, ob das dem Port 1 zugewiesene Telefon angeschlossen ist.
<b>Port 2 Status</b>	Zeigt an, ob das dem Port 2 zugewiesene Telefon angeschlossen ist.
<b>Port 1 Telefonnummer</b>	Zeigt die Telefonnummer des dem Port 1 zugewiesenen Telefons an.

## 6 Gateway-Menü

Über das Gateway-Menü können die meisten Konfigurationen für das EVW32C eingestellt werden. Es werden hier die Menüpunkte LAN, WAN, VPN, Elternzugangskontrolle behandelt.



### Themen:

#### Schlagen Sie hier nach:

- [LAN-Option, S. 35](#)
  - [Setup-Option, S. 35](#)
  - [DHCP-Option, S. 36](#)[Static-Lease-Option, S. 37](#)
- [S. 38](#)
- [WLAN-Option, S. 39](#)
  - [Basic-Option, S. 39](#)
  - [Sicherheits-Option, S. 42](#)
  - [WPS-Option, S. 43](#)
  - [Zugangskontroll-Option, S. 44](#)
  - [Drahtloses Netzwerk: Inbetriebnahme und Fehlerbehebung, S. 46](#)
- [Erweiterte Option, S. 51](#)
  - [Option verbundener Geräte, S. 52](#)
  - [Options-Option, S. 53](#)
  - [Port-Weiterleitungs-Option, S. 54](#)
  - [IP-Filter-Option, S. 59](#)
  - [MAC-Filter-Option, S. 59](#)
  - [S. 60](#)
  - [Option: Port auslösen, S. 61](#)
  - [Firewall-Option, S. 64](#)
  - [DMZ-Option, S. 65](#)
  - [DDNS-Option, S. 66](#)
- [Management-Option, S. 67](#)
  - [Datensicherungs-Option, S. 67](#)
- [VPN-Option, S. 70](#)
  - [Basic-Option, S. 71](#)
  - [IPsec-Option, S. 72](#)
- [Elternkontroll-Option, S. 75](#)
  - [Basic-Option, S. 71](#)
  - [IPsec-Option, S. 72](#)
  - [Benutzer-Setup-Option, S. 76](#)

### Gateway-Menü abrufen:

1. Rufen Sie die web-basierte Nutzeroberfläche auf. Siehe [Lokaler Zugriff auf die Nutzeroberfläche des lokalen Netzwerks auf S. 19.](#)
2. Klicken Sie auf **Gateway** im Hauptmenü.



3. Folgende Untermenüs sind verfügbar:

- LAN
- WAN
- WLAN
- Erweiterte
- Verwaltung
- VPN
- Elternkontrolle

## 6.1 LAN-Option

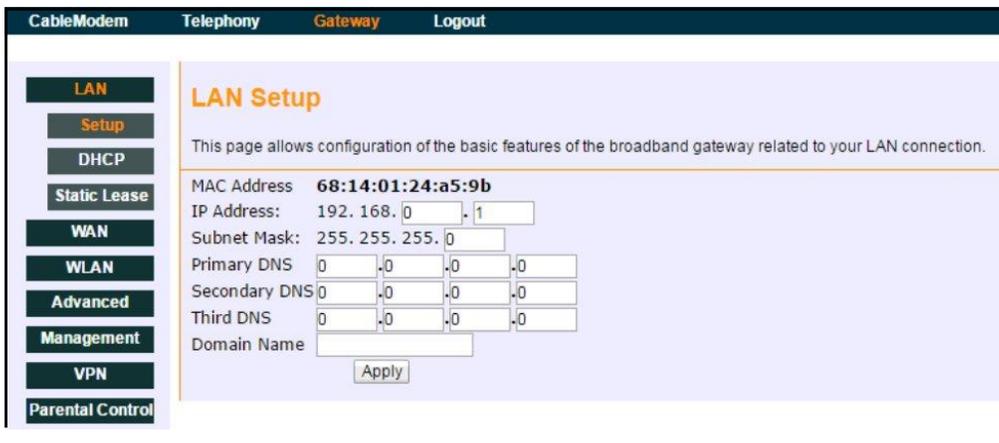
Über die **LAN**-Option lassen sich übliche Gateway-Parameter und DHCP (Dynamic Host Configuration Protocol)-Funktionalitäten konfigurieren.

### Konfiguration der LAN-Parameter:

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **LAN** im linken Menü.
3. Folgende Untermenüs sind verfügbar:
  - Setup
  - DHCP

### 6.1.1 Setup- Option

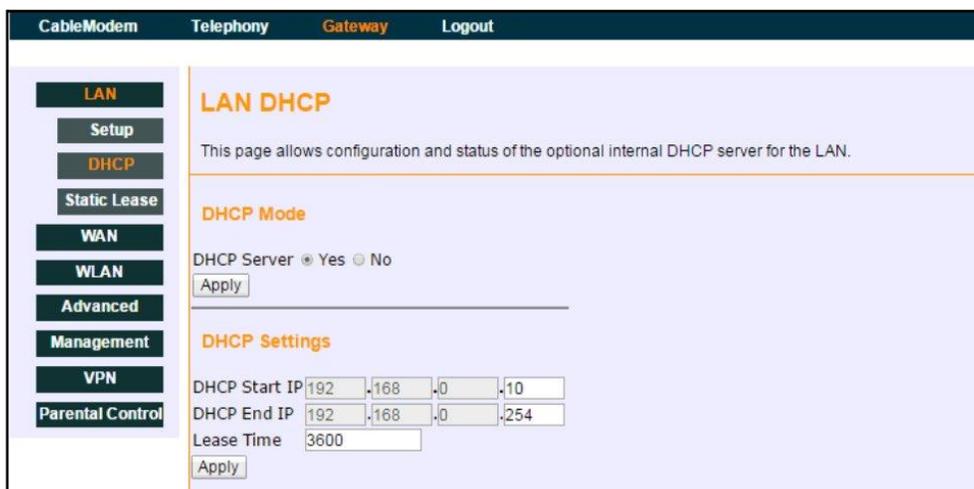
Der LAN-Setup-Bildschirm dient zur Konfiguration der Grundfunktionen der LAN-Verbindung. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
MAC-Adresse	Zeigt die Hardware-Adresse der LAN-Schnittstelle an.
IP-Adresse	Definiert die lokale IP-Adresse, bei der es sich um die Standard-Gateway-Adresse für sämtliche mit dem EVW32C durch Kabel verbundenen LAN-Hosts handelt.
Subnetzmaske	Zeigt die Subnetz-Maske für die LAN-Schnittstelle an.
Primärer DNS	Ermöglicht Ihnen den primären DNS (Domain Name Server) für das geroutete Subnetz einzugeben.
Sekundärer DNS	Ermöglicht Ihnen den sekundären DNS (Domain Name Server) für das geroutete Subnetz einzugeben.
Drittrangiger DNS	Ermöglicht Ihnen den drittrangigen DNS (Domain Name Server) für das geroutete Subnetz einzugeben.
Domain-Name	Es handelt sich hier um ein System, welches Internet-Web-Servern Adressen zuweist. Dies wird ggf. durch Domain-Namen-Serviceanbieter vorgegeben.
Übernehmen	Speichert Änderungen.

### 6.1.2 DHCP- Option

Die DHCP-Option dient zur Konfiguration der DHCP-Funktionalitäten des Geräts. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



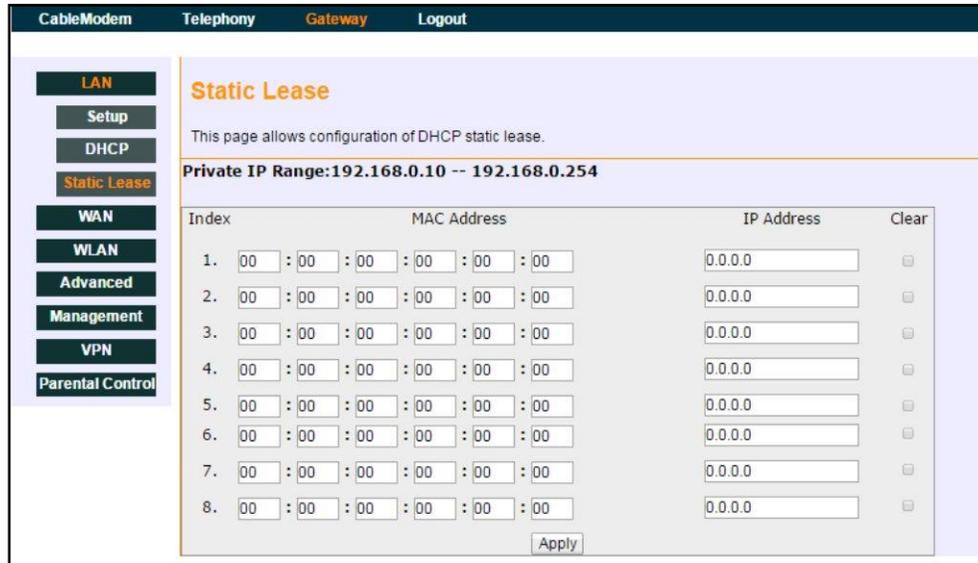
Bezeichnung	Beschreibung
<b>DHCP-Modus</b>	
<b>DHCP Server</b>	DHCP wird auf dem EVW32C aktiviert (Ja) oder deaktiviert (Nein). Bei „Nein“ werden sämtliche statischen DHCP-Einstellungen auf diesem Bildschirm ignoriert.
<b>Übernehmen</b>	Speichert Änderungen.
<b>DHCP-Einstellungen</b>	
<b>DHCP Start IP</b>	Definiert die anfängliche IP-Adresse für den Pool der IP-Adressen, die zur Verbindung von Clients genutzt werden können.
<b>DHCP End IP</b>	Definiert die letzte IP-Adresse zur Verbindung von Clients.
<b>Freigabezeit</b>	Definiert die verbleibende DHCP-Freigabezeit in Minuten (von 1 bis 71582788). Dem PC eines DHCP-Nutzers wird eine IPv4-Adresse mit einer Freigabezeit zugewiesen. Wenn diese abläuft, muss der PC mit dem DHCP-Server verbunden sein und es wird eine neue, noch nicht belegte IPv4-Adresse eingesetzt.  <b>Hinweis:</b> Die im Vorfeld programmierte Lease-Time beträgt 3600 Sekunden und sollte auf <b>86400</b> Sekunden (24 Stunden) geändert werden. So lassen sich Verbindungsprobleme mit einigen Mac-/Windows 7-Geräten lösen, die die Nutzeroberfläche für das Netzwerk abschalten, sofern der Bereitschaftsmodus aktiviert wird. Dadurch verlangsamt sich die Geschwindigkeit beim Internetsurfen, bis dem Gerät per DHCP eine neue IPv4-Adresse zugewiesen wird.
<b>Übernehmen</b>	Speichert Änderungen.

### 6.1.3 Static-Lease-Option

Die **Static-Lease**-Option dient zur Zuweisung von IP-Adressen an Clients Ihres Netzwerks, die sich nicht verändern. Damit wird gewährleistet, dass einem bestimmten Gerät immer dieselbe IP-Adresse zugewiesen wird, insbesondere, wenn Geräte ein- und ausgeschaltet bzw. Verbindungstrennungen unterworfen werden. Dies kann sich bei Netzwerken als hilfreich erweisen, in denen eine breitere Kontrolle über das Netzwerk und die verbundenen Clients erforderlich ist. Beispiele für den Einsatz einer Static-Lease-Option beinhalten:

- [IP-Filter-Option, S. 59](#)
- [S. 60](#)
- [DMZ-Option, S. 65](#)

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



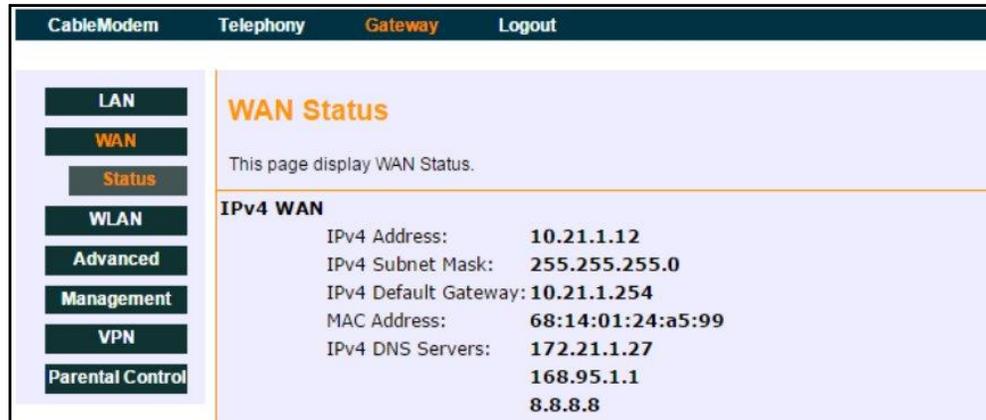
Bezeichnung	Beschreibung
<b>Index</b>	Stellt eine Index-Nummer für jeden Client bereit, der mit Ihrem Netzwerk verbunden wird.
<b>MAC-Adresse</b>	Ermöglicht Ihnen die MAC-Adresse des Client einzugeben, dem Sie eine Static-Lease zuweisen wollen.
<b>IP-Adresse</b>	Ermöglicht Ihnen die IP-Adresse des Client einzugeben.
<b>Löschen</b>	Löscht die Static Lease, wenn das Feld „Löschen“ angekreuzt ist und <b>Übernehmen</b> gewählt wird.
<b>Übernehmen</b>	Speichert Änderungen.

## 6.2 WAN-Option

Mit der **WAN-Option** lassen sich Daten hinsichtlich der WAN-Nutzeroberfläche des EVW32C abrufen.

### Zum Abrufen der Daten der WAN-Nutzeroberfläche:

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **WAN** im linken Menü.
3. Der **WAN-Status** wird angezeigt. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>IPv4 WAN</b>	
<b>IPv4 Adresse</b>	Zeigt die aktuelle WAN-Adresse (öffentlich, IPv4) an, wie sie vom Serviceanbieter eingeholt wird.
<b>IPv4 Subnetzmaske</b>	Zeigt die IPv4-Subnetzmaske an.
<b>IPv4 Standardgateway</b>	Zeigt den IPv4-Standardgateway an.
<b>MAC-Adresse</b>	Zeigt die Hardware-Adresse der WAN-Nutzeroberfläche an.
<b>IPv4 DNS Server</b>	Listet die IPv4-DNS-Server auf, wie sie im Netzwerk verfügbar sind.

## 6.3 WLAN-Option

Mit dieser Option (WLAN - Wireless Local Area Network) können WiFi-Netzwerkeinstellungen konfiguriert werden. Für Hilfe bei der Inbetriebnahme und Fehlerbehebung des drahtlosen Netzwerks, siehe [Drahtloses Netzwerk: Inbetriebnahme und Fehlerbehebung auf S. 46](#).

### Konfiguration der WiFi-Netzwerkeinstellungen:

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **WLAN** im linken Menü.
3. Folgende Untermenüs sind verfügbar:
  - Basic
  - Sicherheit
  - WPS
  - Zugangskontrolle

#### 6.3.1 Basic-Option

Mit der **Basic**-Option werden beide Funkbänder (2,4 GHz und 5 GHz) einschließlich Kanalnummer, sowie die Bandbreitensteuerung konfiguriert.

**WICHTIGER HINWEIS:** Das EVW32C ist ein Zwei-Band-Gateway mit simultaner, drahtloser Übertragung. Beide Funkbänder (2,4 GHz, 5 GHz) lassen sich gleichzeitig betreiben. Beide Funkbänder sind standardgemäß betriebsbereit.

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.

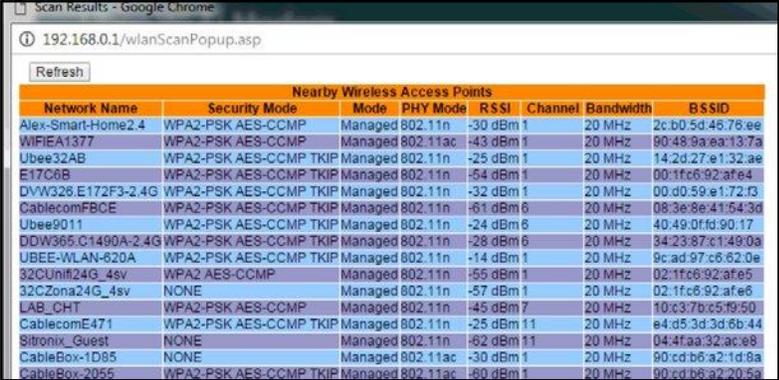
The screenshot displays the web management interface for the Ubee EVW32C. At the top, there are navigation tabs: CableModem, Telephony, Gateway (highlighted), and Logout. On the left side, there is a vertical menu with options: LAN, WAN, WLAN (highlighted), Basic (highlighted), Security, WPS, Access Control, Advanced Management, VPN, and Parental Control.

The main content area is divided into two sections:

- Wireless 2.4G Basic:** This section allows configuration of the 2.4 GHz wireless network. It includes settings for:
  - Wireless: Enabled
  - Network Name (SSID): 24A598
  - Hidden SSID: Disabled
  - 802.11 mode: G/N-mix
  - WMM Support: On
  - Output Power: 100%
  - Control Channel: 1 (Current: 1, Interference Level: Acceptable)
  - Bandwidth: 20 MHz (Current: 20MHz)
  - Sideband for Control Channel (40 MHz only): None
- Wireless 5G Basic:** This section allows configuration of the 5 GHz wireless network. It includes settings for:
  - Wireless: Enabled
  - Network Name (SSID): 24A598
  - Hidden SSID: Disabled
  - 802.11 mode: A/N/AC-mix
  - WMM Support: On
  - Output Power: 100%
  - Control Channel: 40 (Current: 100, Interference Level: Acceptable (This is a DFS channel))
  - Bandwidth: 40 MHz (Current: 20MHz)
  - Sideband for Control Channel (40 MHz only): Upper (Current: Lower)

Buttons for 'Apply' and 'Restore Wireless Defaults' are present at the bottom of each configuration section. A 'Scan Wireless APs' button is also visible between the two sections.

Bezeichnung	Beschreibung
<b>Die folgenden Felder stehen zur Konfiguration beider Funkbänder (2,4/5 GHz) zur Verfügung:</b>	
<b>WiFi</b>	Ermöglicht Ihnen, das WiFi ein- und auszuschalten. Beide Funkbänder (2,4/5 GHz) sind standardgemäß betriebsbereit.
<b>Netzwerkname (SSID)</b>	<p>Zeigt den primären Netzwerknamen (SSID) an, mit dem sich die Client-Geräte verbinden. Entweder wird eine Standard-SSID oder eine nutzerdefinierte SSID angezeigt.</p> <p>Standard-SSID = Die letzten 6 Zeichen der Kabel-Modem-MAC-Adresse.</p> <p>Um die SSID in einen personalisierten Netzwerk-Namen zu ändern, markieren Sie den Netzwerknamen im Textfeld, löschen Sie ihn und geben einen personalisierten Namen ein. Klicken Sie <b>Übernehmen</b>.</p>
<b>Verborgene SSID</b>	Bei ihrer Aktivierung ist die SSID WiFi-Clients gegenüber nicht sichtbar, sofern sie nicht dort manuell angelegt wird. Bei ihrer Deaktivierung ist die SSID WiFi-Clients gegenüber sichtbar, die eine Verbindung zum EVW32C herstellen wollen.
<b>802.11 Modus</b>	<p>Richtet den WiFi-Netzwerk-Standard ein. Wählen Sie "Auto", um den 802.11 n-Modus zu verwenden, wenn möglich. Dieser Modus erhöht signifikant die maximale Übertragungsrate der nicht aufgearbeiteten Daten in der physischen Schicht (OSI) von 54 Mbit/s auf ein Maximum von 600 Mbit/s mit dem Einsatz vier spatialer Ströme bei einer Kanalbreite von 40 MHz.</p> <p>Optionen:</p> <ul style="list-style-type: none"> <li>• 2,4GHz: B/G/N-mix, G/N-mix, B/G-mix, N-only</li> <li>• 5GHz: A/N/AC-mix, N/AC-mix, AC-only, A-only</li> </ul>
<b>WMM Support</b>	Bei eingeschaltetem WMM (WiFi Multimedia) ist der QoS-Dienst (Quality of Service) aktiviert, um den besten Service in Ihrem WiFi-Netzwerk zu gewährleisten.
<b>Ausgangsleistung</b>	Hier können Sie die Ausgangsleistung per Drop-Down-Menü auswählen. Optionen: 25%, 50%, 75%, 100%.
<b>Kontrollkanal</b>	<p>Auswahl eines konkreten Kanals, um das drahtlose Netzwerk zu nutzen. Auf diese Weise können Sie die Betriebsfrequenz/den Betriebskanal je nach Region auswählen. Die Kanalauswahl kann sich auf die Leistung des drahtlosen Netzwerks auswirken. Die Standardeinstellung ist: <b>Auto</b>. Für weitere Informationen siehe <a href="#">WiFi-Kanal auswählen auf S. 50</a>.</p> <p>Optionen:</p> <ul style="list-style-type: none"> <li>• 2,4GHz: Auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13</li> <li>• 5GHz: Auto, 40, 48, 56, 64, 104, 112, 120, 128, 136</li> </ul>
<b>Bandbreite</b>	<p>Setzt die Bandbreite auf 20 MHz oder 40 MHz. Für 40 MHz setzen Sie die Seitenbandbreite auf einen Wert, der größer oder kleiner 20 MHz ist. 40 MHz-Kanäle verdoppeln die Kanalbreite. So kann die PHY-Datenrate mittels eines einzigen 20 MHz-Kanals verdoppelt werden.</p> <p>Optionen:</p> <ul style="list-style-type: none"> <li>• 2,4GHz: 20MHz, 40MHz</li> <li>• 5GHz: 20MHz, 40MHz, 80MHz</li> </ul>
<b>Seitenband für Kontrollkanal</b>	Nur bei 40 MHz Bandbreite sollten Sie einen Wert größer oder kleiner als 20 MHz wählen.

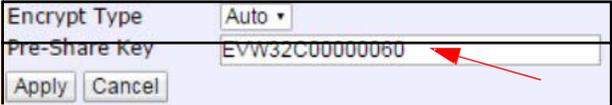
Bezeichnung	Beschreibung
Übernehmen	Speichert alle Bildschirmänderungen.
WiFi-Standardwerte wiederherstellen	Stellt Werkseinstellungen für WiFi-Konfigurationen wieder her.
WiFi-APs-Scan (2,4 und 5)	<p>Beim Anklicken des Buttons <b>WiFi AP scannen</b> erscheint ein Dialogfenster mit Informationen über nahegelegene WiFi-Zugangsstellen (Beispiel unten).</p> 

### 6.3.2 Sicherheits-Option

Die **Sicherheits**-Option ermöglicht die Konfiguration einer Bandbreite an Sicherheitseinstellungen für beide Funkbänder (2,4 und 5 GHz). Für weitere Informationen über WiFi-Voreinstellungswerte siehe [Standardvorgaben und Anmeldevorgänge auf S. 10](#).

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Die folgenden Felder stehen zur Konfiguration der Sicherheitseinstellungen beider Funkbänder (2,4/5 GHz) zur Verfügung:</b>	
<b>Sicherheitsmodus</b>	Ermöglicht Ihnen die Auswahl des Sicherheitsmodus. Optionen: <ul style="list-style-type: none"> <li>• Deaktivierung</li> <li>• WEP 128</li> <li>• WEP 64</li> <li>• WPA Personal (Standardvorgaben)</li> <li>• WPA Enterprise</li> </ul>
<b>WPA Version</b>	Ermöglicht Ihnen die Auswahl der WPA-Version. Optionen: <ul style="list-style-type: none"> <li>• Version 1</li> <li>• Version 2</li> <li>• v1/v2 Mix (Standardvorgaben)</li> </ul>
<b>Verschlüsselungstyp</b>	Ermöglicht Ihnen die Auswahl des Verschlüsselungstyps. Optionen: <ul style="list-style-type: none"> <li>• TKIP</li> <li>• AES</li> <li>• Auto (Standardvorgabe)</li> </ul>
<b>Netzwerk-Schlüssel</b>	<p>Zeigt Netzwerkschlüssel an, wenn WPA- oder 802.1-Netzwerkauthentifizierung eingesetzt wird. Der Netzwerkschlüssel ist ein nur einmal pro Gerät vergebener Schlüssel, auch bezeichnet als „Pre-Share Key“, WiFi-Schlüssel, oder WiFi-Passwort. Der Netzwerkschlüssel für das EVW32C entspricht den 14 Zeichen der Geräte-Seriennummer. Beispiel: <b>EVW32C00000060</b>.</p> <p><b>Hinweis:</b> der Netzwerkschlüssel wird sichtbar, wenn Sie den Mauszeiger über das Feld daneben halten.</p>  <p>Um diesen Netzwerkschlüssel (WiFi-Passwort) in ein persönliches Passwort zu ändern, markieren Sie das aktuelle Passwort in dem entsprechenden Feld, löschen Sie es und geben Sie ein persönliches Passwort ein. Klicken Sie <b>Übernehmen</b>.</p>
<b>Übernehmen</b>	Speichert Änderungen.
<b>Abbrechen</b>	Änderungen ignorieren.

### 6.3.3 WPS-Option

Die **WPS**-Option dient zur automatischen Sicherheitskonfiguration für Geräte, die mit dem WiFi-Netzwerk über WPS (WiFi Protected Setup) verbunden werden, ohne dass der Verschlüsselungstyp, der Netzwerkname, oder das WiFi-Netzwerkpasswort eingesetzt wird. Diese Bildschirmanzeige ermöglicht die Konfiguration für beide Funkbänder (2,4 und 5 GHz). Für eine Beschreibung von WiFi-Standardvorgaben siehe [Standardvorgaben und Anmeldevorgänge auf S. 10](#).

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.

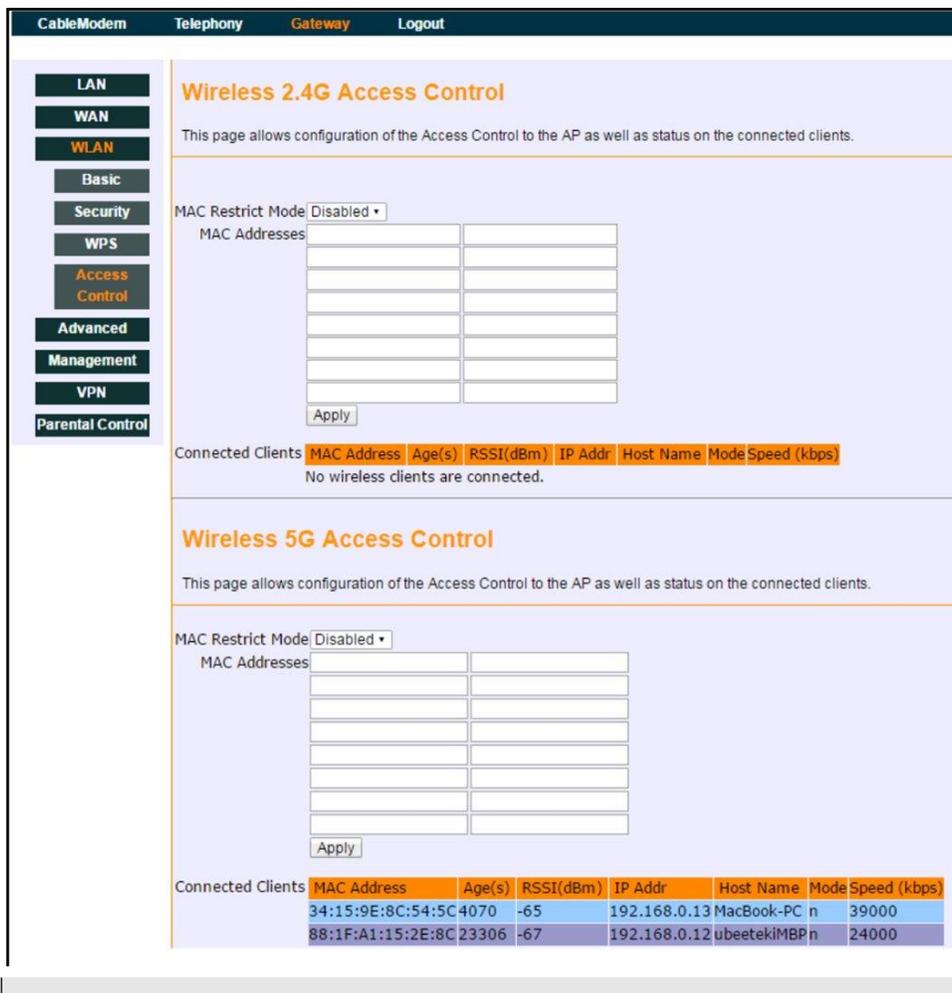


Bezeichnung	Beschreibung
<b>Die folgenden Felder stehen zur Konfiguration der WPS-Einstellungen beider Funkbänder (2,4/5 GHz) zur Verfügung:</b>	
<b>WPS aktivieren</b>	Klicken Sie auf <b>AN</b> oder <b>AUS</b> , um die WPS-Option zu (de-)aktivieren.
<b>WPS-Modus</b>	Ermöglicht Ihnen die Auswahl zwischen 2 WPS-Modi: 1. PIN: Nutzer wird zur Eingabe der WPS-PIN aufgefordert. <b>Hinweis:</b> Bei Auswahl „PIN“ erscheint die Eingabeaufforderung für die WPS Client Pin. 2. PBC (Push Button Configuration) - (Buttonfunktionskonfiguration): Sowohl am EVW32C also auch beim WiFi-Client, der mit dem Netzwerk verbunden werden soll, wird ein Software-bzw. Hardwarebutton betätigt. Beide Geräte befinden sich dann im Registrierungs-Modus. Dies ist voreingestellt.
<b>WPS Client PIN</b>	Dieses Feld wird nur sichtbar, wenn PIN als WPS-Modus ausgewählt wird. Die WPS-Pin-Nummer des Client, der verbunden werden soll, muss in das angezeigte Feld eingegeben werden, bevor das Feld „Verbinden“ betätigt wird.
<b>WPS Auslöser</b>	Löst Verbindung zum Client per WPS aus. Die WPS-Pin-Nummer des Client muss in das angezeigte Feld eingegeben werden, bevor das Feld „Verbinden“ betätigt wird.
<b>Übernehmen</b>	Speichert Änderungen.

### 6.3.4 Zugangskontroll-Option

Die **Zugangskontroll**-Option konfiguriert den Zugriff von Clients (Komponenten) auf die Funkbänder (2,4 GHz oder 5 GHz). Außerdem wird der Status der aktuell verbundenen Clients (Netzwerkkomponenten) angezeigt.

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<p><b>Die folgenden Felder stehen zur Konfiguration der Zugangskontroll-Einstellungen beider Funkbänder (2,4/5 GHz) zur Verfügung:</b></p>	
<p><b>MAC Beschränkungs-modus</b></p>	<p>Kontrolliert den WiFi-Zugang zu Ihrem Netzwerk über die MAC-Adresse.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> MAC-Beschränkungen werden abgeschaltet und Zugang/Verbindungsbereitstellung zu WiFi-Clients wird gewährt. Nutzen Sie andere Sicherheitsmechanismen für den Zugang zum WiFi-Netzwerk, sind die Clients immer noch technisch von diesen Beschränkungen abhängig. "Deaktiviert" ist voreingestellt.</li> <li>• <b>Aktiviert:</b> Liste von WiFi-Clients wird erstellt, die mit dem WiFi-Netzwerk verbunden werden können. Geben Sie die MAC-Adressen dieser Clients in die entsprechenden Felder ein. Nicht gelistete MAC-Adressen haben keine Zugangsberechtigung.</li> <li>• <b>Zugriff verweigert:</b> Liste von WiFi-Clients wird erstellt, die keinen Zugang zum WiFi-Netzwerk haben sollen. Geben Sie die MAC-Adressen dieser Clients in die entsprechenden Felder ein.</li> </ul>

Bezeichnung	Beschreibung
MAC-Adressen	Zeigt MAC-Adressen an. Hinweis: Sie können MAC-Adressen der verbundenen Client-Listen vom unteren Bildschirmrand ausschneiden und kopieren.
Übernehmen	Speichert Änderungen bei Betätigung.
Verbundene Clients	<p>Listet derzeit verbundene WiFi-Clients nach MAC-Adressen geordnet auf.</p> <ul style="list-style-type: none"> <li>• <b>MAC Address</b> – MAC Adresse – Zeigt MAC-Adressen an, die im entsprechenden Feld eingegeben sind (siehe oben).</li> <li>• <b>Dauer</b> – Zeigt an, ab welchem Zeitpunkt die abgefragten Werte des WiFi-Client an das Gerät gesendet wurden (Zeitdauerwert). Die Werte enthalten sämtliche Daten, die auf diesem Bildschirm angezeigt werden. Je kleiner der Wert, desto aktueller sind die Daten. <ul style="list-style-type: none"> <li>• <b>RSSI(dBm)</b> – Zeigt die Empfangssignalstärke des Geräts gegenüber dem WiFi-Kabelmodem an. Dieser Wert kommt üblicherweise im Rahmen der Fehlerbehebung bei WiFi-Leistungsproblemen zum Einsatz. Eine Signalstärke zwischen 0 dBm und -65 dBm gilt als optimal. Werte von -66 dBm und darunter (-70,-80 usw.) sind nachteilig für den WiFi-Datendurchsatz. Siehe <a href="#">Empfangssignalstärke auf S. 46</a> für weitere Informationen.</li> </ul> </li> <li>• <b>IP Addr</b> – Zeigt die diesem WiFi-Client zugewiesene IP-Adresse an.</li> <li>• <b>Host Name</b> – Zeigt den Host-Namen des WiFi-Client an.</li> <li>• <b>Mode</b> – zeigt den anwendbaren 802.11a/b/g/n-Standard an, der für das verbundene Client-Gerät gilt.</li> <li>• <b>Geschwindigkeit (kbps)</b> – Zeigt die maximale theoretische Link-Geschwindigkeit an, die sich zwischen dem WiFi-Gateway und dem Client ergibt, ohne zusätzlich Verschlüsselungszeiträume usw. zu berücksichtigen. Zum Beispiel ergeben sich tatsächliche Geschwindigkeitswerte bei WEP-Verschlüsselung als typischerweise geringer als 50% der theoretischen Link-Geschwindigkeit. TKIP-Verschlüsselung kann ebenfalls die Leistung beeinträchtigen. AES hat die höchste Effizienz, höchste Sicherheit, und den höchsten Datendurchsatz. WMM kann deaktiviert werden, wenn der Durchsatz auf manchen Client-Adaptern beeinträchtigt wird.</li> </ul>

### 6.3.5 Drahtloses Netzwerk: Inbetriebnahme und Fehlerbehebung

Der Inhalt dieses Kapitels verweist auf die Inbetriebnahme und die Fehlerbehebung im Rahmen des WiFi-Netzwerks:

- [Empfangssignalstärke, S. 46](#)
- [Berechnung des Abstands zwischen WiFi-Kabelmodem und WiFi-Client, S. 47](#)
- [Funkbänder \(2,4GHz und 5GHz\), S. 49](#)
- [WiFi-Kanal auswählen, S. 50](#)

#### 6.3.5.1 Empfangssignalstärke

Die Empfangssignalstärke (Received Signal Strength - RSSI) wird zwischen dem verbundenen WiFi-Client und dem WiFi-Kabelmodem gemessen. Dieser Wert kann sich erheblich auf die WiFi-Übertragungsgeschwindigkeit/Leistung auswirken. Durch folgende Faktoren bestimmt sich dieser Wert:

- Materialien (z.B. im Freien, Beton, Bäume)
- Abstand zwischen WiFi-Clients und WiFi-Kabelmodem
- WiFi-Kapazitäten der Client-Geräte

Zur Festlegung der Empfangssignalstärke siehe [Zugangskontrolloption auf S. 44](#) und prüfen Sie den **RSSI**-Wert. Eine Empfangssignalstärke zw. 0 u. -64 dBm gilt als optimal. Werte von -67 dBm und darunter (z.B. -70,-80 usw.) sind nachteilig für den WiFi-Datendurchsatz.

### 6.3.5.2 Berechnung des Abstands zwischen WiFi-Kabelmodem und WiFi-Client

In diesem Kapitel erfahren Sie, in welchem Abstand eine WiFi-Zugangsstelle (nämlich das EVW32C) von WiFi-Clients-Geräten positioniert werden kann. Umgebungsvariablen sind u. a. die Kapazitäten der WiFi-Clients sowie die Materialien, durch die das WiFi-Signal dringen muss. Wenn das EVW32C und die WiFi-Clients einen gewissen Abstandswert überschreiten, verringert sich die Leistung des Netzwerks.

#### Festlegung des Standortes des Kabelmodems:

1. Schließen Sie einen WiFi-Client an das EVW32C an. Siehe [Geräte mit dem Netzwerk verbinden auf S. 15](#), wenn nötig.
2. Stellen Sie den WiFi-Client in einem Abstand von ca. einem Meter zum EVW32C auf.
3. Ermitteln Sie den **RSSI**-Wert für den verbundenen Client. Siehe [Zugangskontroll-Option auf S. 44](#). Dieser Wert gilt für die unten angegebene Formel.
4. Legen Sie anhand der folgenden Tabelle fest, welche Materialien das WiFi-Signal durchdringt, um die erwünschte WiFi-Abdeckung zu erzielen.

Leistungsdämpfung		
Materialien	Leistungsdämpfung	
	2.4GHZ	5GHz
Freiraum	0,24dB / 0,30 m	0,3dB / 0,30 m
Innenwand aus Gipskartonplatten	3 dB bis 4 dB	3 dB bis 5 dB
Verstärkte Wände	2 dB bis 5 dB	4 dB bis 9 dB
Holztür (hohl/massiv)	3 dB bis 4 dB	6 dB bis 7 dB
Ziegel/Betonwand (Hinweis 1)	6 dB bis 18 dB	10 dB bis 30 dB
Glasfenster (nicht getönt)	2 dB bis 3 dB	6 dB bis 8 dB
Fenster mit Doppelscheiben bzw. beschichtetem Glas	13 dB	20 dB
Schusssicheres Glas	10 dB	20 dB
Stahl/Notausgangstür	13 dB bis 19 dB	25 dB bis 32 dB
Menschlicher Körper	3 dB	6 dB
Bäume (Hinweis 2)	0,15 dB / 0,30 m	0,3dB / 0,30 m
<p><b>Hinweis 1:</b> Beton ist in jedem Land unterschiedlich beschaffen. Die Stärke (Dicke) und Beschichtung dieses Materials unterscheidet sich danach, ob es in Fußböden, Innen- oder Außenwänden verarbeitet wurde.</p> <p><b>Hinweis 2:</b> Die Signalschwächung durch Bäume hängt entscheidend von Form und Dicke des Laubwerks ab.</p>		

5. Übertragen Sie die Materialabschwächungswerte aus der Tabelle oben in die folgende Formel:

**Formel:**

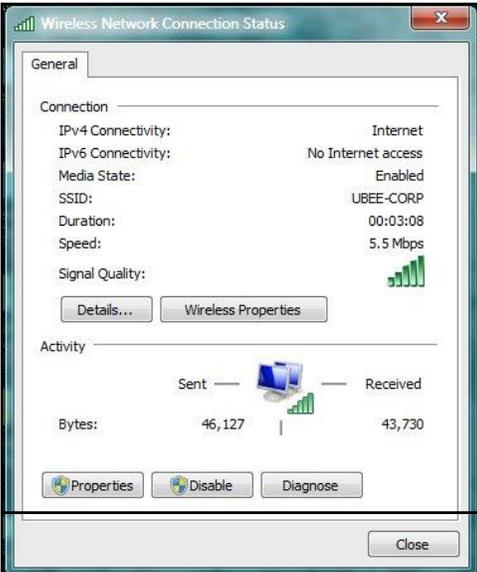
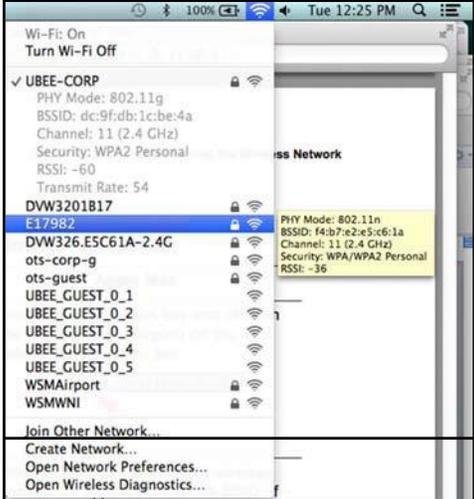
(Übertragungsleistung: **-30dBm**) – (Empfängersensibilität: **RSSI-Wert**) =  
Zulässiger Verlust im freien Raum  
Zulässiger Verlust im freien Raum ÷ Materialabschwächungswert =  
Optimaler Abstand zwischen EVW32C und WiFi-Client (in ft, 1 ft = 0,30 cm)

**Beispiel:**

$(-30\text{dBm}) - (-67\text{dBm}) = 37\text{dBm}$  (zulässiger Verlust im freien Raum für eine 54Mbps-Verbindung)

$37\text{dBm} \div 24\text{db/ft (im Freien)} = 154,16 \text{ ft} = 46,98 \text{ m}$

6. Wenn Sie den optimalen Abstand zwischen EVW32C und einem WiFi-Client kennen, können Sie Leistungsschwächen beheben und ihnen vorbeugen.
7. Prüfen Sie die WiFi-Signalstärke und -Übertragungsgeschwindigkeit des per WiFi mit dem EVW32C verbundenen Computers. Anweisungen zur Geschwindigkeitsprüfung für einen Windows bzw. Mac Computer sind in der untenstehenden Tabelle zu finden. Falls der drahtlose Computer nicht verbunden ist, siehe [Ein drahtloses Gerät \(WiFi\) anschließen auf S. 16](#).

<b>WiFi-Signalstärke und -Übertragungsgeschwindigkeit prüfen</b>	
<b>Windows PC</b>	<b>Apple Mac</b>
<p>1. Klicken Sie auf das WiFi-Netzwerk-Symbol in der Systemleiste. Es wird Ihnen eine Liste verfügbarer WiFi-Netzwerke angezeigt.</p> 	<p>1. Halten Sie „Optionen“ gedrückt und klicken Sie auf das WiFi-Icon (Flughafen) auf der rechten Seite der oberen Menüleiste.</p> 
<p>2. Klicken Sie auf „Offen zugängliche, gemeinsam genutzte Netzwerke“ und dann auf „WiFi-Verbindung“.</p>	<p>2. Daten der aktuellen WiFi-Verbindung erscheinen unterhalb der SSID. Wenn Sie „Optionen“ gedrückt halten und den Mauszeiger über andere Netzwerke bewegen, werden deren Daten sichtbar.</p>
<p>3. Prüfen Sie die Geschwindigkeit und die Signalstärke im Status-Fenster.</p> 	

### 6.3.5.3 Funkbänder (2,4 GHz und 5 GHz)

Das EVW32C arbeitet mit beiden Funkbändern (2,4 GHz und 5 GHz) gleichzeitig. So können Sie das beste Funkband für Ihr Gerät zur Gewährleistung der Stabilität Ihrer lokalen Vernetzung sowie Ihrer Internetverbindung wählen.

Die Tabelle unten vergleicht die beiden Funkbänder (2,4 GHz und 5 GHz).

Band	2.4GHz	5GHz
<b>Kanäle</b>	In den USA werden die Kanäle 1 – 11 verwendet. Es gibt 3 Kanäle, die sich nicht überschneiden (1, 6 und 11). Wählen Sie die „Auto-Kanal“-Funktion. So wird der Kanal mit der geringsten Störungsanfälligkeit genutzt.	23 Kanäle überschneiden sich nicht.
<b>Standards</b>	802.11b,g,n	802.11a,n,ac
<b>Netzwerk bereich</b>	Höhere Reichweite	Geringere Reichweite
<b>Interferenz</b>	Höhere Interferenz - da viele drahtlos betriebene Geräte , wie drahtlose Telefone, Mikrowellen, und Computer auf 2,4 GHz betrieben werden.	Geringere Interferenz, da nur wenige drahtlos betriebene Geräte auf 5 GHz betrieben werden.
<b>Anwendung</b>	Empfohlen für die einfache Internetbedienung und den E-Mail-Zugang, weil solche Anwendungen eine eher geringe Bandbreite in Anspruch nehmen und bei höherem Abstand optimal betrieben werden können.	Empfohlen für Anwendungen mit ununterbrochenem Datendurchsatz, wie „Streaming“ von Audio-/Video-Medien. Das breitere Spektrum lässt eine höhere Leistung zu.
<b>Hinweis:</b> Wählen Sie 5 GHz, müssen sämtliche WiFi-Client-Adapter diese Frequenz unterstützen.		

### 6.3.5.4 WiFi-Kanal auswählen

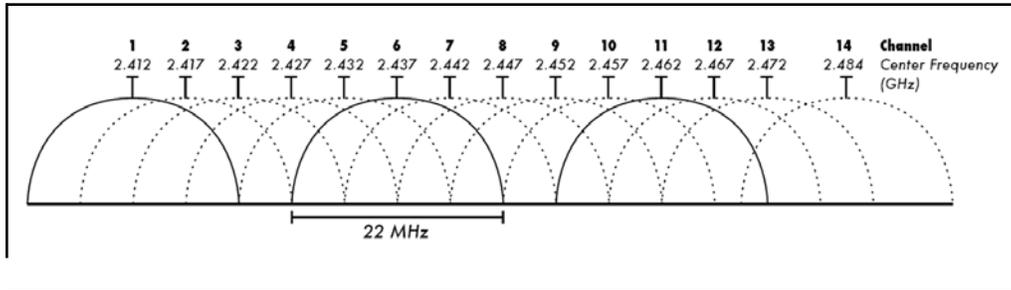
Sie könnten den WiFi-Kanal, mit dem das EVW32C arbeitet, wechseln müssen, sofern in der Umgebung ggf. Computer, Testgeräte und mehrere WiFi-Zugangsstellen ggf. im 2,4-GHz-Bereich arbeiten.

In Einzelfällen lässt sich der WiFi-Datenverkehr segmentieren, wobei verschiedene Gerätegruppen jeweils anderen Kanälen zugeordnet sind. Dies wird durch die Kanalkonfiguration jeder einzelnen Zugangsstelle ermöglicht (falls mehrere zur Verfügung stehen). Wenn Sie nur ein WiFi-Gerät in einer Umgebung von mehreren Geräten steuern können, nutzen Sie für Ihr Gerät einen nicht häufig genutzten Kanal.

**HINWEIS:** Zur Änderung des WiFi-Kanals siehe [Basic-Option auf S. 39](#).

#### 2,4 GHz Kanäle

Dem folgenden Diagramm können Sie die Kanäle entnehmen, denen auf dem amerikanischen Kontinent die Frequenz 2,4 GHz zugewiesen ist. Jeder Kanal hat eine Bandbreite von 22 MHz. Wählen Sie Kanäle mit der geringsten Überschneidungswahrscheinlichkeit (amerikanischer Kontinent: 1, 6 und 11 und in Europa: 1, 5, 9 und 13). Kanäle, die sich überschneiden, lösen ggf. WiFi-Netzwerkleistungsprobleme aus.



Quelle: Wikipedia.org und IEEE-Artikel IEEE 802.11n-2009

### 5 GHz Kanäle

Die folgende Tabelle listet die 5 GHz Kanäle und die entsprechenden Frequenzen auf.

Kanal	GHz	Kanal	GHz
36	5,180	108	5,540
40	5,200	112	5,560
44	5,220	116	5,580
48	5,240	136	5,680
52	5,260	140	5,700
56	5,280	149	5,745
60	5,300	153	5,765
64	5,320	157	5,785
100	5,500	161	5,805
104	5,520	165	5,825

## 6.4 Erweiterte Option

Die **Erweiterte** Option gewährt die Konfiguration von zusätzlichen Einstellungen, wie z. B. MAC-Filter und Port-Weiterleitung.

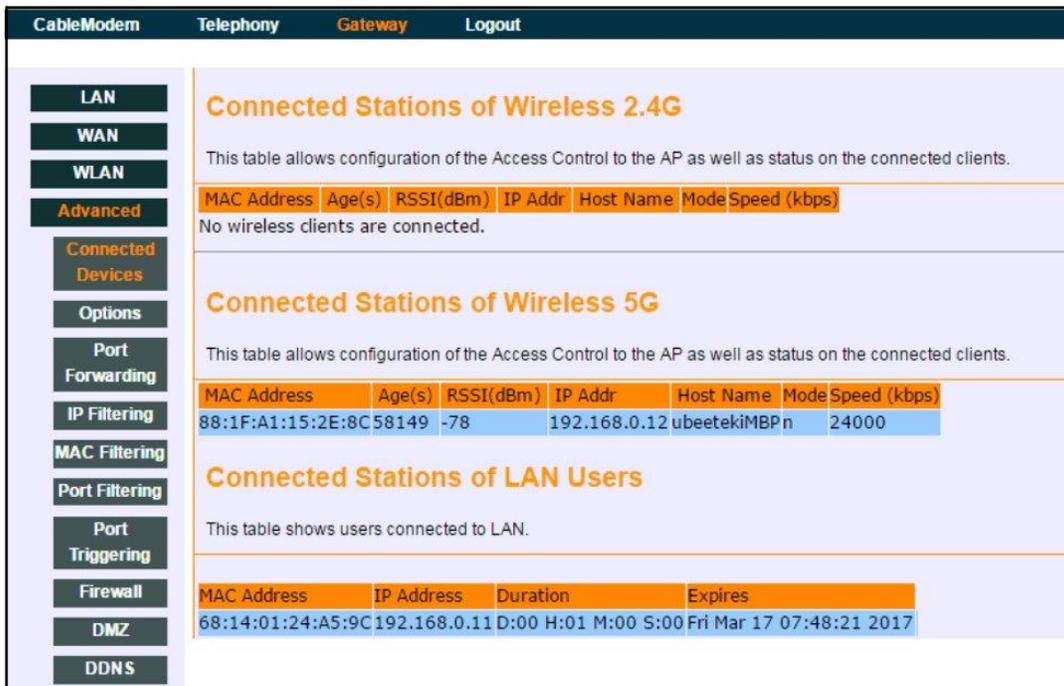
Konfigurieren erweiterter Optionen:

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **Erweiterte Option** auf der linken Seite.
3. Folgende Untermenüs sind verfügbar:
  - Verbundene Geräte
  - Optionen
  - Port-Weiterleitung
  - IP-Filterung
  - MAC-Filterung
  - Port-Filterung

- Auslösen des Ports
- Firewall
- DMZ
- DDNS

### 6.4.1 Option: Angeschlossene Geräte

Die Bildschirmanzeige dieser Option zeigt Daten über derzeit mit dem EVW32C verbundene Geräte an. Felddesreibungen siehe unterhalb des Bildschirmbeispiels.

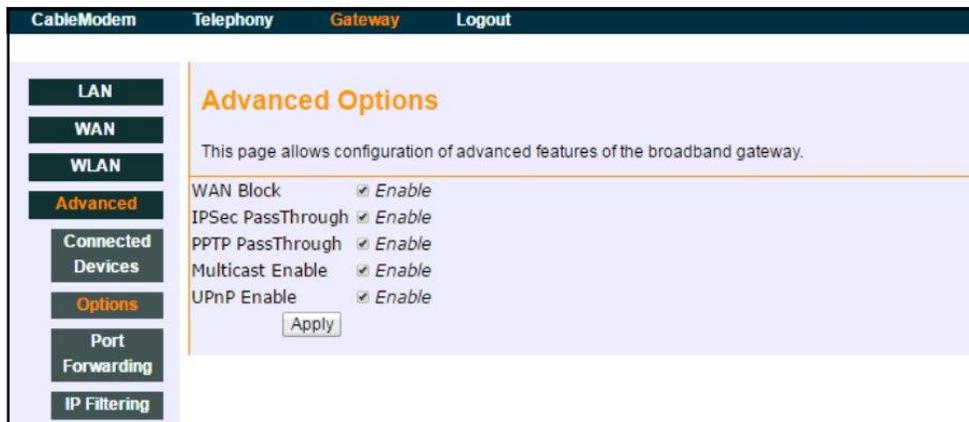


Bezeichnung	Beschreibung
Verbundene Stationen von WiFi-Nutzern (2,4 GHz)	Zeigt Daten über aktuell mit dem 2,4-GHz-Funkband verbundene Clients an.
MAC-Adresse	Zeigt MAC-Adressen des/der verbundenen Client(s) an.
Dauer	Zeigt an, ab welchem Zeitpunkt die abgefragten Werte der WiFi-Clients an das Gerät gesendet wurden. Werte enthalten sämtliche Daten, die auf diesem Bildschirm angezeigt werden. Je kleiner der Wert, desto aktueller sind die Daten.
RSSI (dBm)	Zeigt die Empfangssignalstärke des Geräts gegenüber dem WiFi-Kabelmodem an. Dieser Wert kommt üblicherweise im Rahmen der Fehlerbehebung bei WiFi-Leistungsproblemen zum Einsatz. Eine Signalstärke zwischen 0 dBm und -65 dBm gilt als optimal. Werte von -66 dBm und darunter (-70,-80 usw.) sind nachteilig für den WiFi-Datendurchsatz. Siehe <a href="#">Empfangssignalstärke auf S. 46</a> für weitere Informationen.
IP Addr	Zeigt die diesem WiFi-Client zugewiesene IP-Adresse an.
Host Name	Zeigt den Host-Namen des WiFi-Client an.
Modus	Zeigt den anwendbaren 802.11a/b/g/n-Standard an, der für das verbundene Client-Gerät gilt.

Bezeichnung	Beschreibung
<b>Geschwindigkeit (kbps)</b>	Zeigt die maximale theoretische Link-Geschwindigkeit zwischen dem WiFi-Gateway und dem Client an, nicht zzgl. der Zeitdauer, die durch Verschlüsselungsvorgänge o. ä. in Anspruch genommen werden. Zum Beispiel ergeben sich tatsächliche Geschwindigkeitswerte bei WEP-Verschlüsselung typischerweise geringer als 50% der theoretischen Link-Geschwindigkeit. TKIP-Verschlüsselung kann ebenfalls die Leistung beeinträchtigen. AES hat die höchste Effizienz, höchste Sicherheit, und den höchsten Datendurchsatz. WMM kann deaktiviert werden, wenn der Durchsatz auf manchen Client-Adaptoren beeinträchtigt wird.
<b>Verbundene Stationen von WiFi-Nutzern (5 GHz)</b>	Zeigt Daten über aktuell mit dem 5-GHz-Funkband verbundene Clients an.
<b>MAC-Adresse</b>	Zeigt MAC-Adressen des/der verbundenen Client(s) an.
<b>Dauer</b>	Zeigt an, ab welchem Zeitpunkt die abgefragten Werte der WiFi-Clients an das Gerät gesendet wurden. Werte enthalten sämtliche Daten, die auf diesem Bildschirm angezeigt werden. Je kleiner der Wert, desto aktueller sind die Daten.
<b>RSSI (dBm)</b>	Zeigt die Empfangssignalstärke des Geräts gegenüber dem WiFi-Kabelmodem an. Dieser Wert kommt üblicherweise im Rahmen der Fehlerbehebung bei WiFi-Leistungsproblemen zum Einsatz. Eine Signalstärke zwischen 0 dBm und -65 dBm gilt als optimal. Werte von -66 dBm und darunter (-70,-80 usw.) sind nachteilig für den WiFi-Datendurchsatz. Siehe <a href="#">Empfangssignalstärke auf S. 46</a> für weitere Informationen.
<b>IP Addr</b>	Zeigt die diesem WiFi-Client zugewiesene IP-Adresse an.
<b>Host Name</b>	Zeigt den Host-Namen des WiFi-Client an.
<b>Modus</b>	Zeigt den anwendbaren 802.11a/b/g/n-Standard an, der für das verbundene Client-Gerät gilt.
<b>Geschwindigkeit (kbps)</b>	Zeigt die maximale theoretische Link-Geschwindigkeit zwischen dem WiFi-Gateway und dem Client an, nicht zzgl. der Zeitdauer, die durch Verschlüsselungsvorgänge o. ä. in Anspruch genommen werden. Zum Beispiel ergeben sich tatsächliche Geschwindigkeitswerte bei WEP-Verschlüsselung typischerweise geringer als 50% der theoretischen Link-Geschwindigkeit. TKIP-Verschlüsselung kann ebenfalls die Leistung beeinträchtigen. AES hat die höchste Effizienz, höchste Sicherheit, und den höchsten Datendurchsatz. WMM kann deaktiviert werden, wenn der Durchsatz auf manchen Client-Adaptoren beeinträchtigt wird.
<b>Verbundene Stationen von LAN-Nutzern</b>	Zeigt mit dem LAN verbundene Benutzer an.
<b>MAC-Adresse</b>	Zeigt MAC-Adressen des/der verbundenen Geräts/Geräte an.
<b>IP-Adresse</b>	Zeigt IP-Adressen des/der verbundenen Geräts/Geräte an.
<b>Laufzeit</b>	Zeigt die Zeitdauer ab dem Zeitpunkt an, zu welchem die IP-Adresse diesem Client zugeordnet wurde
<b>Abgelaufen</b>	Zeigt die Zeitdauer bis zu dem Zeitpunkt an, zu welchem die IP-Adresse in ihrer Gültigkeit abläuft und wiederverwendet werden muss. Ist eine IP-Adresse einem bestimmten Host zugeordnet, werden die Werte STATISCHER IP-ADRESSE angezeigt.

### 6.4.2 Options-Option

Der Options-Bildschirm ermöglicht die Aktivierung/Deaktivierung von Netzwerkprotokollen für das Gerät. Die Anwendung der Übersetzung der Einstellungen der Netzwerkadresse (NAT ALG) bietet zusätzliche Sicherheit über die Firewall hinaus. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>WAN-Block</b>	Bei Aktivierung blockiert der WAN-Block den PING-Zugriff auf die öffentliche Gateway-IP-Adresse, die dem Internet offengelegt wird. Bei Deaktivierung ist der PING -Zugriff zulässig, was für die Fernkonfiguration von VoIP-Telefonie bei manchen Anbietern erforderlich ist (z. B. Cisco, Polycom usw.).
<b>IPsec Datendurchsatz</b>	Bei Aktivierung ist der verschlüsselte IPsec-VPN-Verkehr durch den Router zwischen der IPsec-VPN-Client-Anwendung des PC/Mac und des IPsec-VPN-Konzentrator (z. B. Barracuda, Cisco, Juniper u. a.) für den Zugang auf die Firmen-VPN zulässig.
<b>PPTP Datendurchsatz</b>	Bei Aktivierung ist der verschlüsselte PPTP-VPN-Verkehr durch den Router zwischen der PPTP-VPN-Client-Anwendung des PC/Mac und des PPTP-VPN-Servers (z. B. Windows Server 2013) für den Zugang auf die Firmen-VPN zulässig.
<b>Aktivierung d. Multicast</b>	Optimiert die Bandbreitennutzung im Vergleich mit Unicast (insbesondere bei Video-Streaming-Anwendungen).
<b>Aktivierung von UPnP</b>	Aktiviert Universal Plug and Play (UPnP). Bei Aktivierung kann ein UPnP-Gerät dynamisch Teil eines Netzwerks werden, eine IP-Adresse erhalten, seine Kapazitäten übertragen und Daten von anderen Geräten des Netzwerks übermittelt bekommen. Ebenso kann ein solches Gerät reibungslos und automatisch nach Gebrauch vom Netzwerk abgetrennt werden. Spielekonsolen und Webkameras sind Beispiele für Geräte, für die UPnP nützlich ist.
<b>Übernehmen</b>	Speichert Änderungen.

### 6.4.3 Port-Weiterleitungs-Option

Mit der Port-Weiterleitungs-Option wird dem EVW32C mitgeteilt, an welchen Computer des LAN Daten gesendet werden sollen. Bei Kommunikationsproblemen der Systeme oder Anwendungen mit dem Internet kann diese Option zur Lösung der folgenden Fehler gewählt werden:

- Daten werden von einem lokalen Host an das Internet gesendet, jedoch wird die Rückverfolgung der erwarteten Daten von diesem nicht empfangen.
- Eine Anwendung oder ein Dienst Ihres LAN (oder lokalen Hosts) ist nicht direkt vom Internet zugänglich (z. B.: Abfrage eines lokalen Audio-Servers).
- Beispiele sind:
  - Xbox/PlayStation – Spiele/Anwendungen
  - Gebäudesicherheitssysteme, die auf das Internet zugreifen

- Audio Servers/VoIP – Audio-und-VoIP-Anwendungen und -Dienste

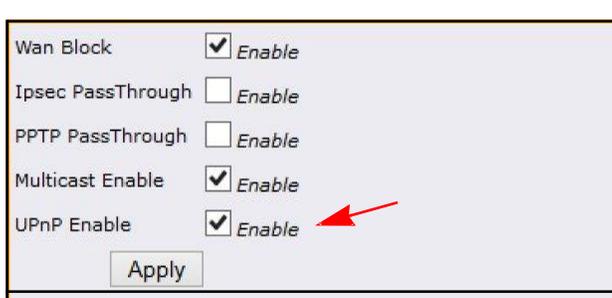
### Schlagen Sie hier nach:

- [Vor der Einrichtung der Weiterleitung, S. 55](#)
- [Einrichtung der Weiterleitung, S. 55](#)
- [Einrichtung der Port-Weiterleitung \(Beispiel: Xbox\), S. 58](#)

#### 6.4.3.1 Vor der Einrichtung der Weiterleitung

Vor der Zuweisung von Weiterleitungs-Regeln sind die folgenden Optionen zu beachten:

1. Aktivieren Sie das Universal Plug and Play (UPnP). Dies löst möglicherweise Problemstellungen ohne Weiterleitungs-Regeln.
  - a. Zugriff auf webbasierte Nutzeroberfläche des EVW32C, siehe [Lokaler Zugriff auf die webbasierte Nutzeroberfläche auf S. 19](#).
  - b. Klicken Sie auf **Gateway** im Hauptmenü.
  - c. Wählen Sie **Erweiterte Option** im linken Menü.
  - d. Wählen Sie **Optionen** im Untermenü.
  - e. Prüfen Sie das Feld **UPnP aktivieren**.



- f. Klicken Sie auf **Übernehmen**.
  - g. Testen Sie Ihren lokalen Host bzw. Ihre lokale Anwendung (etwa: Xbox) auf ordnungsgemäße Funktionalität. Setzen Sie mit der Port-Weiterleitung fort, sofern der Host bzw. die Anwendung nicht ordnungsgemäß kommuniziert.
2. Ordnen Sie eine statische IP-Freigabe dem Client/Host zu, an den Sie eine Weiterleitung einrichten. Auf diese Weise ändert sich die IP nicht und stört nicht Ihre Weiterleitungsregeln. Zum Beispiel, wenn Sie Hosting-Provider eines Web-Servers in Ihrem internen Netzwerk sind und eine Weiterleitungs-Regel hierfür einrichten wollen, ordnen Sie eine statische IP-Freigabe diesem System zu, sodass sich die IP nicht ständig ändert und die Weiterleitung stört.

**HINWEIS:** Für den Zugriff auf eine VPN müssen Nutzer den WAN-Block deaktivieren und IPsec PassThrough und PPTP PassThrough aktivieren.

#### 6.4.3.2 Einrichtung der Weiterleitung

Löste sich Ihr Problem nicht gemäß dem Kapitel [Vor der Einrichtung der Weiterleitung auf S. 55](#), richten Sie eine Port-Weiterleitung ein.

Sie benötigen die folgenden Daten, um die Port-Weiterleitung einzustellen.

- **IP-Adresse** jedes lokalen Hostsystems (etwa: Xbox), für die eine Port-Weiterleitung erforderlich ist.
- **Port-Zahlen** - die Anwendung des lokalen Hosts wartet auf eingehende Anfragen/Daten (z. B. Spiele oder andere Dienste). Diese Port-Zahlen sind den Unterlagen des jeweiligen Anwendungsgeräts zu entnehmen.

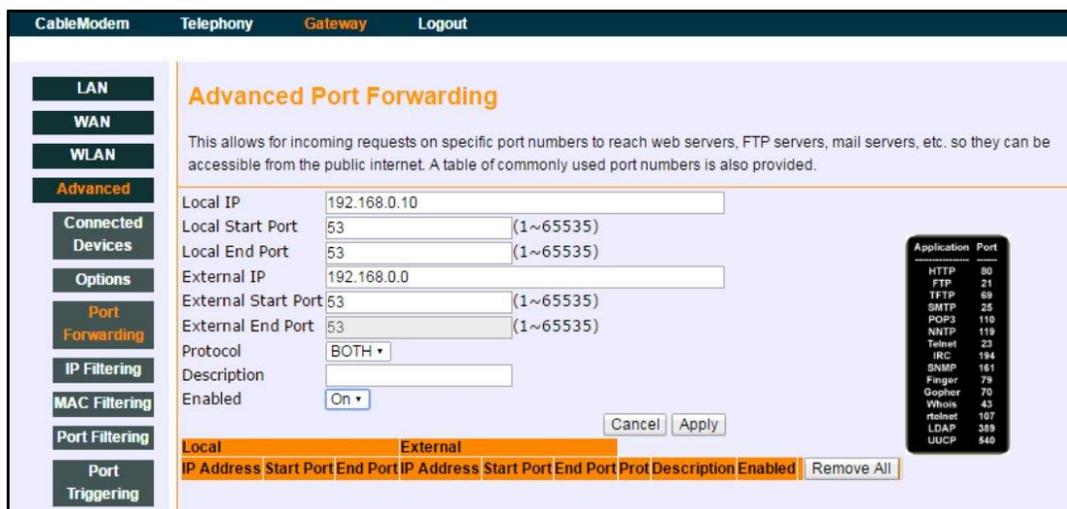
**HINWEIS:** Detaillierte Informationen zum Thema „Port-Weiterleitung“ bzw. darüber, dies bei bestimmten Anwendungen mit konkreten Netzwerkgeräten durchzuführen (z. B. Kabelmodems) sind wie folgt abzurufen: <http://portforward.com>. Alternativ liefern die Bedienungsanleitungen der einzelnen Geräte weitere Informationen.

**Einrichtung der Port-Weiterleitung:**

1. Wird der Bildschirm zur Port-Weiterleitung angezeigt, klicken Sie auf **Create IPv4**.

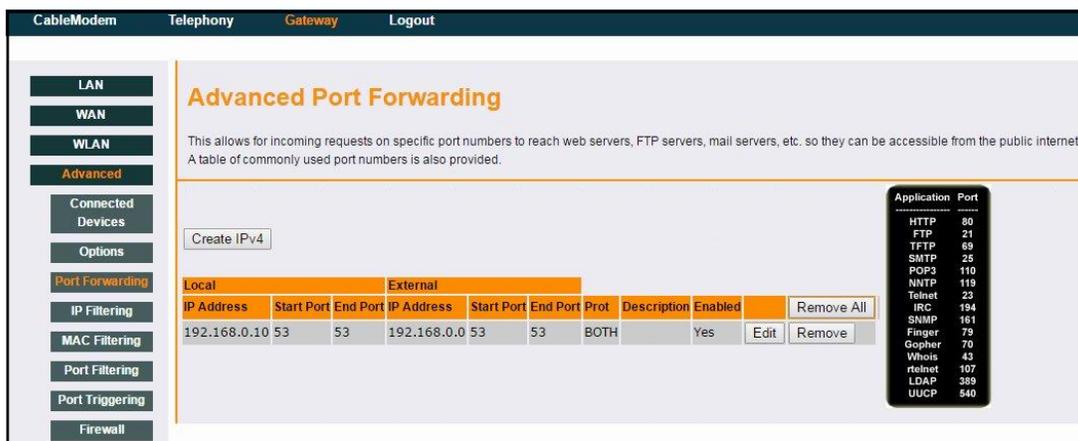


2. Geben Sie Daten in das Textfeld der Weiterleitung ein (siehe Screenshot unten). Beschreibungen der Textfelder folgen.



Bezeichnung	Beschreibung
<b>Lokale IP</b>	Definiert die IP-Adresse des lokalen LAN-Geräts, dem die Weiterleitungsregel zugeordnet wird, wie z.B. Xbox oder PC.
<b>Lokaler Start-Port</b>	Definiert die Nummer des Start-Ports, die der Server-Host in Ihrem LAN erwartet.
<b>Lokaler End-Port</b>	Definiert die Nummer des End-Ports, die der Server-Host in Ihrem LAN erwartet.
<b>Externe IP</b>	Designiert die IP-Adresse eines anderen Routers im Netzwerk, durch die Daten weiterzuleiten sind.
<b>Externer Start-Port</b>	Definiert die Port-Nummer, mit der die Port-Reihe beginnt, die dem Internet gegenüber angezeigt wird.
<b>Externer End-Port</b>	Definiert die Port-Nummer, mit der die Port-Reihe endet, die dem Internet gegenüber angezeigt wird. <b>Hinweis:</b> Vorsicht bei der Anordnung von Ports. Ports innerhalb eines Anordnungsbereichs sind ggf. nicht durch andere Anwendungen abzurufen, für die sie erforderlich sein könnten. Es ist üblich und sicherer, dieselbe Nummer als Start- und End-Port eines Bereichs zu verwenden.
<b>Protokoll</b>	Wählt Protokolltyp aus. Optionen sind UDP, TCP oder BEIDE.
<b>Beschreibung</b>	Spezifiziert den Namen der Weiterleitungsregel.
<b>Aktiviert</b>	Aktiviert (An) / Deaktiviert (Aus) die Weiterleitungsregel.
<b>Abbrechen</b>	Unterbricht den Erstellungsvorgang der Weiterleitungsregel und führt Sie zurück zum vorherigen Bildschirm.
<b>Übernehmen</b>	Speichert Änderungen.
<b>Port-Map</b>	Zeigt eine Liste allgemein üblicher Anwendungen und ihrer Ports an.
<b>Weiterleitungs-Tabelle</b> – Listet Weiterleitungsregeln auf.	
<b>Alle löschen</b>	Löscht alle Einträge der Weiterleitungstabelle.

3. Klicken Sie **Übernehmen**. Die Weiterleitungsregel wird erstellt und als Tabellenwert angezeigt (siehe Abbildung unten). Zusätzliche Feldbeschreibungen folgen.



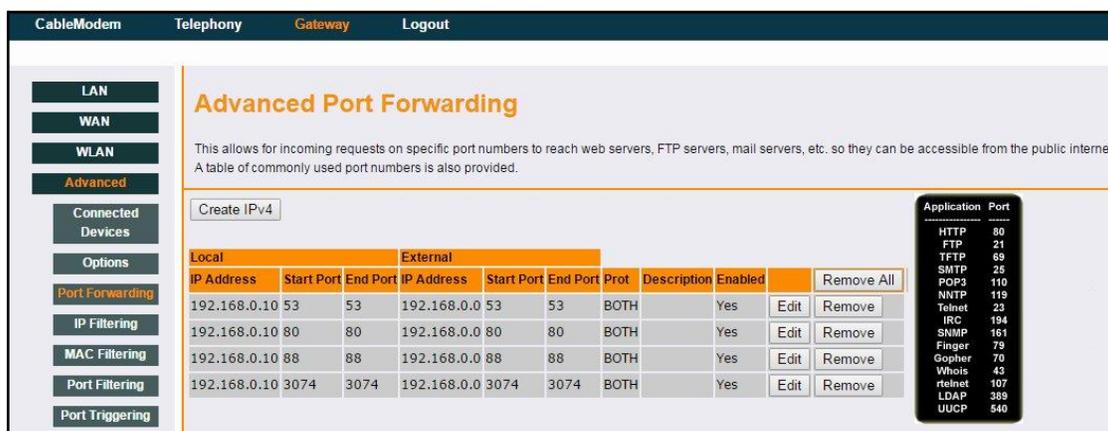
Bezeichnung	Beschreibung
<b>Alle löschen</b>	Löscht alle Einträge der Weiterleitungstabelle.
<b>Bearbeiten</b>	Zeigt Felder für die ausgesuchten Regeln an, so dass Werte geändert werden können.
<b>Löschen</b>	Löscht die ausgewählte Regel.

### 6.4.3.3 Einrichtung der Port-Weiterleitung am Beispiel der Xbox

Es folgt das Beispiel der Einrichtung einer Xbox mit dem Spiel Modern Warfare 2. Es werden mehrere Ports für die Xbox und Modern Warfare 2 benötigt, weshalb eine separate Weiterleitungsregel für jeden Port eingerichtet werden muss. Mehrere Ports und Weiterleitungsregeln sind für andere Anwendungen möglicherweise nicht erforderlich.

#### Einrichtung der Port-Weiterleitung für die Xbox:

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **Erweiterte Optionen** im linken Menü.
3. Klicken Sie auf **Port-Weiterleitung** im Untermenü.
4. Geben Sie die Xbox-IP-Adresse in das Feld **Local IP** ein.
5. Definieren Sie die Ports der Xbox in den folgenden Feldern: **Local Start Port** und **Local End Port**. Definieren Sie diese Ports der Xbox in den folgenden Feldern: **External Start Port** und **External End Port**.
6. Erstellen Sie die Weiterleitung separat für jeden Port. Eine Regel, die für Port 53 erstellt wird, funktioniert nur für Port 53. Nicht mehr als ein Programm kann zu einem Zeitpunkt auf einen Port zugreifen.



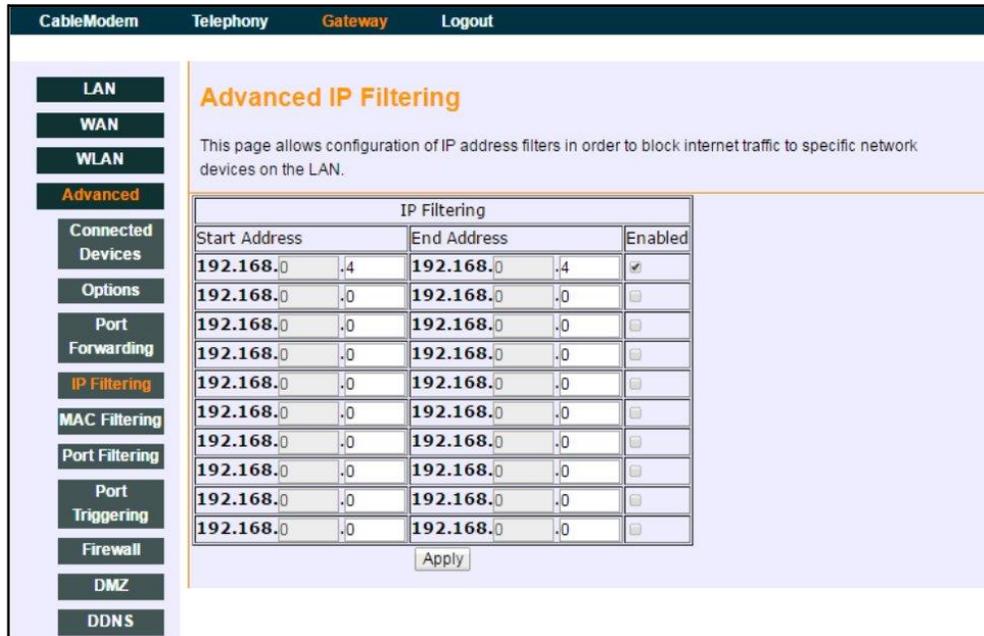
**HINWEIS:** Sie können Anwendungen/Dienste so einrichten, dass diese Daten von einem internen Port erwarten. Externe Internetnutzer, die auf diese Anwendung zugreifen wollen, führen dies durch die Adressgebung eines externen Ports durch, wie etwa einen Audio-Server. Interne Ports sind Ports, von denen lokale Server Daten erwarten und empfangen. Externe Ports sind Ports, von denen das Kabelmodem Daten über das WAN erwartet und empfängt.

### 6.4.4 IP-Filter-Option

Die **IP-Filter**-Option dient zur Filterung bestimmter IP-Adressen, sodass bestimmte an das Netzwerk angeschlossene Geräte im LAN vom Internetverkehr abgeschirmt werden. Hosts auf dieser Liste sind vom Internetverkehr abgeschirmt.

**HINWEIS:** Eine Filterung kann auch über MAC-Adressen erfolgen, die nicht die Einrichtung einer statischen Freigabe erfordern. Siehe [MAC-Filter-Option auf S. 59](#).

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Start-Adresse</b>	Definiert die erste IP-Adresse, die vom Internet abgeschirmt wird.
<b>End-Adresse</b>	Definiert die letzte IP-Adresse, die vom Internet abgeschirmt wird.
<b>Aktiviert</b>	Aktiviert die Regel, wenn das Feld „aktiviert“ angekreuzt wird.
<b>Übernehmen</b>	Speichert Änderungen.

### 6.4.5 MAC Filter-Option

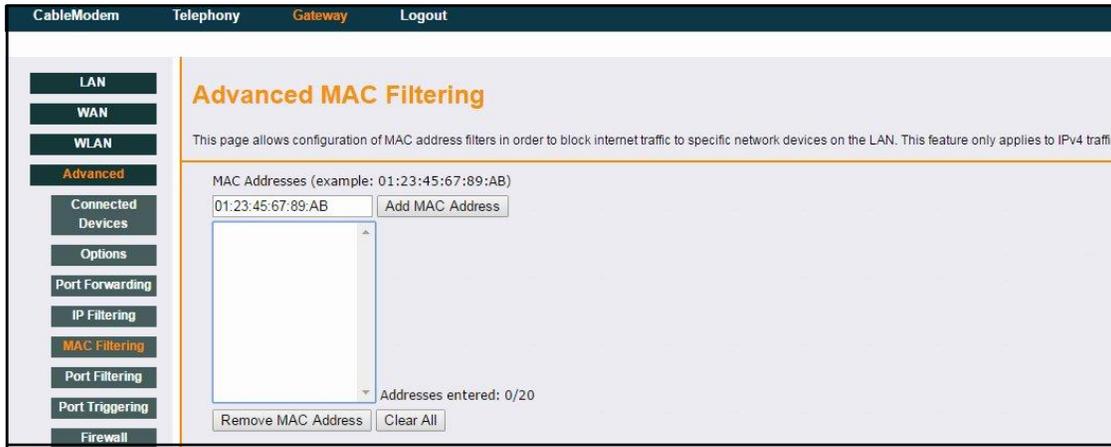
Die **MAC Filter**-Option dient zur Filterung bestimmter MAC-Adressen, sodass bestimmte an das Netzwerk angeschlossene Geräte im LAN vom Internetverkehr abgeschirmt werden. Es wird eine Liste mit Hosts erstellt, die nicht durch den EVW32C auf das Netzwerk zugreifen können.

1. Notieren Sie die MAC-Adressen der Geräte, die Sie vom Internet abschirmen wollen.

Wichtig: Alle Geräte, die ggf. vom Internet abgeschirmt werden sollen, müssen mit dem EVW32C-Netzwerk verbunden sein.

2. Geben Sie die MAC-Adresse in das Textfeld links vom Button **MAC Adresse hinzufügen** ein.

3. Klicken Sie auf den Button **MAC Adresse hinzufügen**. Die MAC-Adresse wird in der Liste der gefilterten MAC-Adressen angezeigt. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>MAC-Adressen</b>	Spezifiziert die MAC-Adressen, die gesperrt werden sollen. Geben Sie die MAC-Adresse in das Textfeld ein.
<b>MAC-Adresse hinzufügen</b>	Fügt MAC-Adresse der Liste der zu sperrenden Adressen hinzu.
<b>Eingegebene Adressen: n/20</b>	Zeigt die MAC-Adressen an, die gesperrt werden sollen. Die Anzahl der eingegebenen MAC-Adressen wird als n/20 angezeigt, wobei n die Listenposition einer solchen Adresse anzeigt. Sie können bis zu 20 MAC-Adressen zugleich filtern.
<b>MAC-Adresse löschen</b>	Löscht die ausgewählte MAC-Adresse aus der Liste der zu sperrenden Adressen.
<b>Alle löschen</b>	Löscht alle MAC-Adressen von der Liste.

### 6.4.6 Port-Filter-Option

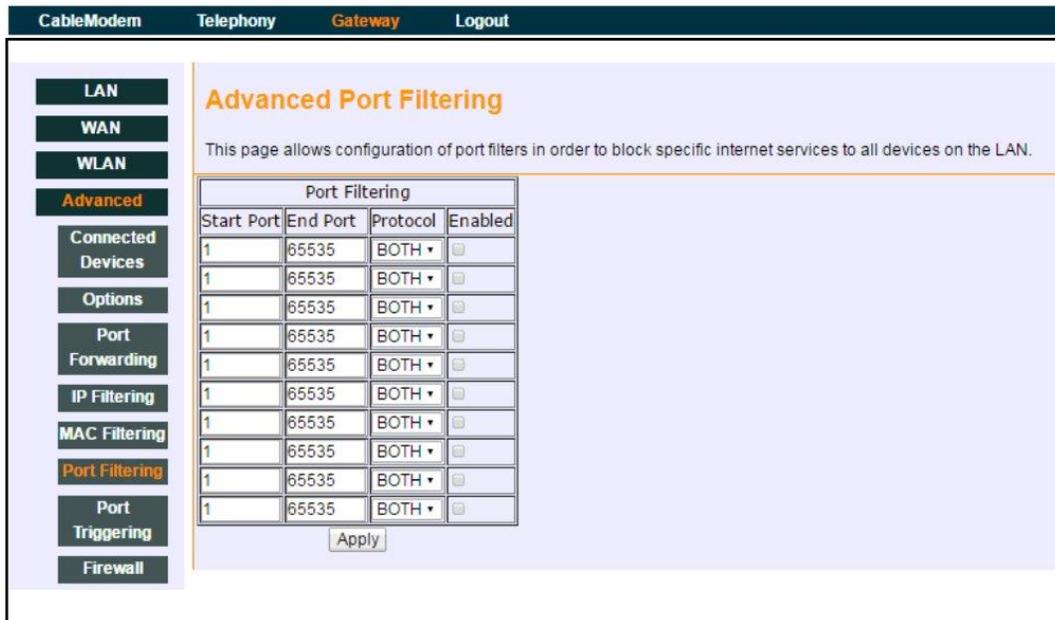
Die **Port-Filter**-Option dient zum Konfigurieren der Port-Filter, um sämtliche an die LAN-Internet-Dienste angeschlossenen Geräte zu blockieren, die die konkret benannten Ports bezeichnen.

Beispiel:

#### Zugriffsverweigerung für Telnet auf und innerhalb Ihres LAN einstellen:

1. Geben Sie als **Start-** und **End-Port** 23 ein.
2. Wählen Sie **Beide** bei Protokoll, um TCP und UDP miteinzubeziehen.
3. Haken Sie **Aktiviert** an.
4. Klicken Sie **Übernehmen**. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.

**HINWEIS:** Vorsicht bei der Port-Filterzuweisung gemäß des Portbereichs. Versehentlich können Sie Internetverkehr abschirmen, der eigentlich für Ihr Netzwerk bestimmt ist, wie http oder E-Mail. Im Voraus zugewiesene Anwendungs-Ports werden auf der Bildschirmanzeige zur Weiterleitung angezeigt. Siehe [Port-Weiterleitungs-Option auf S. 54](#).



Bezeichnung	Beschreibung
<b>Start-Port</b>	Definiert die Nummer des Start-Ports
<b>End-Port</b>	Definiert die Nummer des End-Ports.
<b>Protokoll</b>	Wählt Protokolltyp aus. Optionen sind: UDP, TCP oder BEIDE.
<b>Aktiviert</b>	Aktiviert die Regel und filtert allen Datenverkehr an den benannten Ports heraus.
<b>Übernehmen</b>	Speichert Änderungen.

### 6.4.7 Option: Port Auslösen

Die Option **Port Auslösen** definiert dynamische Auslöser für konkrete Geräte im Netzwerk. So funktioniert bei besonderen Anwendungen, denen spezifische Port-Nummern zugewiesen werden müssen, der Datenverkehr in beide Richtungen ordnungsgemäß. Anwendungen wie Videokonferenzen, Stimmenübertragung, Internetspiele und einige Chatprogrammeigenschaften u. a. könnten diese besonderen Einstellungen benötigen.

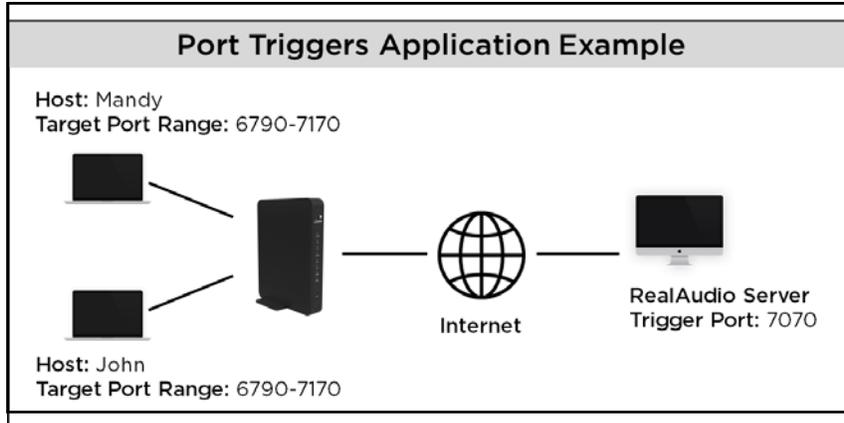
Einige Dienste bedienen sich eines konkreten Portbereichs auf der Seite des Client und eines konkreten Portbereichs auf der Seite des Servers. Zwischen Port-Weiterleitung und Auslösen besteht der folgende Unterschied:

- Port-Weiterleitung erstellt eine Regel, um einen Dienst an eine einzelne LAN-IP-Adresse weiterzuleiten.
- Port-Auslösen definiert zwei Arten von Ports: Auslöser-Port und Ziel-Port. Der Auslöser-Port sendet eine Dienstanforderung von einem LAN-Host an eine spezifische Ziel-Port-Nummer. Der Port, dessen Übertragung der LAN-Host nach Anforderung der Anwendung erwartet, ist der sogenannte Ziel-Port. Der Server sendet Antworten an diese Ports.

Beispiel:

1. John fordert eine Datei vom Real-Audio-Server (Port 7070) an. Port 7070 ist ein Auslöser-Port und löst aus, dass das Gerät die IP-Adresse von Johns Computer aufzeichnet. Der EVW32C erkennt Johns IP-Adresse als Ziel-Portbereich zwischen 6970 und 7170 an.

2. Der Real-Audio-Server reagiert auf eine Port-Nummer zwischen 6970 und 7170.
3. Der EVW32C leitet den Datenverkehr an die IP-Adresse von Johns Computer weiter.
4. Nur John kann mit dem Real-Audio-Server Verbindung aufnehmen, bis diese geschlossen wird oder nicht mehr wirksam ist.



**Einrichtung des Port-Auslösevorgangs:**

1. Wird der Bildschirm zum Port-Auslösevorgang angezeigt, klicken Sie auf **Erstellen**.



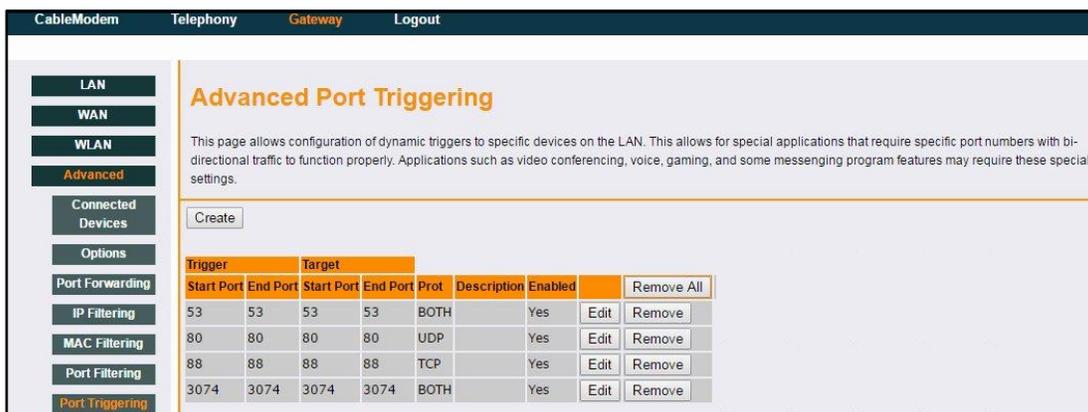
2. Geben Sie Daten in das Textfeld der Weiterleitung ein (siehe Screenshot unten). Beschreibungen der Textfelder folgen.



Bezeichnung	Beschreibung
<b>Auslösevorgang: Start-Port</b>	Ermöglicht die Eingabe einer Port-Nummer oder der Start-Port-Nummer eines Bereichs von Port-Nummern.
<b>Auslösevorgang: End-Port</b>	Ermöglicht die Eingabe einer Port-Nummer oder der End-Port-Nummer eines Bereichs von Port-Nummern.
<b>Ziel: Start-Port</b>	Ermöglicht die Eingabe einer Port-Nummer oder der Start-Port-Nummer eines Bereichs von Port-Nummern.
<b>Ziel: End-Port</b>	Ermöglicht die Eingabe einer Port-Nummer oder der End-Port-Nummer eines Bereichs von Port-Nummern.
<b>Protokoll</b>	Ermöglicht die Eingabe des Protokoll-Typs für diese Regel: UDP, TCP oder BEIDE.
<b>Beschreibung</b>	Ermöglicht die Eingabe des Namens der Auslöse-Regel.
<b>Aktiviert</b>	Deaktiviert (Aus) oder Aktiviert (An) die Auslöse-Regel
<b>Übernehmen</b>	Speichert Änderungen.
<b>Alle löschen</b>	Löscht alle Einträge der Weiterleitungstabelle.

3. Klicken Sie **Übernehmen**. Die Auslöse-Regel wird erstellt und als Tabellenwert angezeigt (siehe Abbildung unten). Zusätzliche Feldbeschreibungen folgen.

Im folgenden Beispiel wird die Port-Auslöse-Option für eine duale Xbox-Konfiguration angezeigt.



Bezeichnung	Beschreibung
Alle löschen	Löscht alle Einträge der Weiterleitungstabelle.
Bearbeiten	Zeigt Felder für die ausgesuchte Regel an, so dass Werte geändert werden können.
Löschen	Löscht die ausgewählte Regel.

### 6.4.8 Firewall-Option

Folgen Sie diesen Anleitungen zur Konfiguration der EVW32C-Firewall-Einstellungen zur Kontrolle der erlaubten Datenverkehrs-Typen in Ihrem Netzwerk. Die Firewall kann bestimmte weborientierte Cookies, Java-Scripts sowie Dialogfenster blockieren. Es wird dringend empfohlen, die Firewall immer zu aktivieren. So schützen Sie sich vor Dienstverweigerungs-Angriffen (Denial of Service, DoS).



Bezeichnung	Beschreibung
IPv4 Firewall Schutz	Definiert den Grad der IPv4-Abschirmung. Optionen sind: Aus, Gering, Mittel, Hoch. Der Standard ist Gering. Dienste basieren auf dem Abschirmungsgrad und werden im Fenster „Erlaubte Dienste“ angezeigt.
Blockierte fragmentierte IP-Pakete	Erkennt fragmentierte IP-Pakete und blockiert diese.
Port-Scan-Erkennung	Erkennt Port-Scans, die verfügbare Ports prüfen und potentiell als Schwachstellen des Netzwerks erkennen.
IP-Flood-Erkennung	Erkennt IP-Flood-Angriffe, die unverhältnismäßige Informationsmengen an das Gerät senden und Bandbreite in Anspruch nehmen.
Übernehmen	Speichert Änderungen.

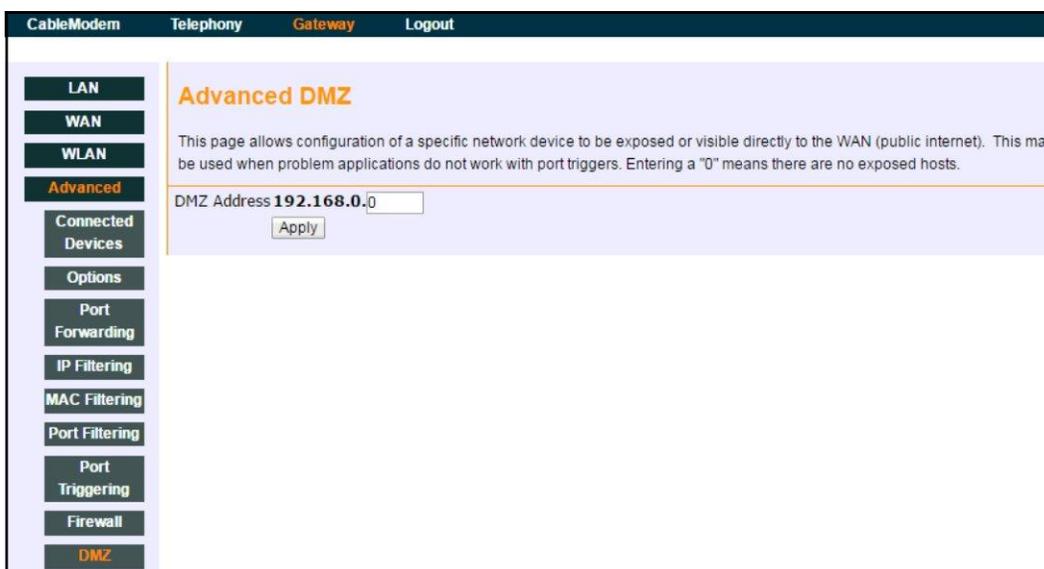
## 6.4.9 DMZ-Option

Die **DMZ**-Option (Demilitarized Zone) legt eine Host-IP-Adresse gegenüber dem WAN (öffentlichen Internet) offen. Indem ein Host in die DMZ jenseits der Firewall versetzt wird, kann schnell und leicht ein Fernzugriff und eine Gerätefunktionalität hergestellt werden, die sich auf Router, Webkameras, VoIP-Telefonie, Spielekonsolen u. a. bezieht. Dies erfolgt hier im Besonderen ohne Einrichtung von Port-Weiterleitungs-/Port-Auslöse-Konfigurationen.

### DMZ-Host einrichten

1. Verbinden Sie einen PC mit dem Ethernet-Port des EVW32C. Beide Geräte sollen funktionsfähig und eingeschaltet sein.
2. Verbinden Sie ein Home-Gateway (oder andere für die DMZ erwünschte Geräte) mit dem Ethernet-Port des EVW32C.
3. Melden Sie sich bei der web-basierten Nutzerschnittstelle des EVW32C an.
4. Klicken Sie auf **Gateway** im Hauptmenü.
5. Wählen Sie **Erweiterte Optionen** im linken Menü.
6. Wählen Sie **DMZ** unter den Erweiterten Optionen.
7. Geben Sie die IP-Adresse des Home-Gateway oder anderer Geräte ein, die für den WAN sichtbar werden sollen.
8. Testen Sie das Gerät, um den Internetzugang sowie die Gerätefunktionalität zu gewährleisten. Beispiel: Internetverbindung von einem PC aus herstellen, der mit dem Home-Gateway verbunden ist, oder Anruf vom VoIP-Telefon.

Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
DMZ-Adresse	Definiert die IP-Adresse des Host-Geräts, welches gegenüber dem WAN sichtbar wird.
Übernehmen	Speichert Änderungen.

### 6.4.10 DDNS-Option

Die **DDNS**-Option gewährt die Nutzung des dynamischen Domain-Namen-Systems (Dynamic Domain Name System), um eine IP-Adresse, die sich ändert, einem konstanten, vordefinierten Host-Namen zuzuweisen. Der Host kann dann von anderen Hosts aus dem Internet kontaktiert werden, auch wenn sich dessen IP-Adresse ändert.

Der DDNS-Dienst für das EVW32C wird durch Dritte bereitgestellt und kann über die Firma Dynamic Network Services Inc. unter [www.dynDNS.com](http://www.dynDNS.com) erworben werden.



Bezeichnung	Beschreibung
DDNS Service	Ermöglicht die (De-)Aktivierung des DDNS-Services. Bei Aktivierung ist dieser Service unter <a href="http://www.dynDNS.org">www.dynDNS.org</a> verfügbar.
Benutzername	Ermöglicht die Eingabe des Namens des DDNS-Kontos.
Passwort	Geben Sie das Passwort für das DDNS-Konto ein.
Host Name	Ermöglicht die Eingabe des Hostnamens des DDNS-Kontos.

Bezeichnung	Beschreibung
IP-Adresse	Zeigt die IP-Adresse des DDNS-Kontos an.
Status	Zeigt den Aktivierungsstatus des DDNS-Dienstes an.
Übernehmen	Speichert Änderungen.

## 6.5 Management-Option

Das Management-Menü bietet Ihnen eine Datensicherung der EVW32C-Konfiguration wie auch eine Zurückstellung auf vorherige Konfigurationen.

### Management-Menü abrufen:

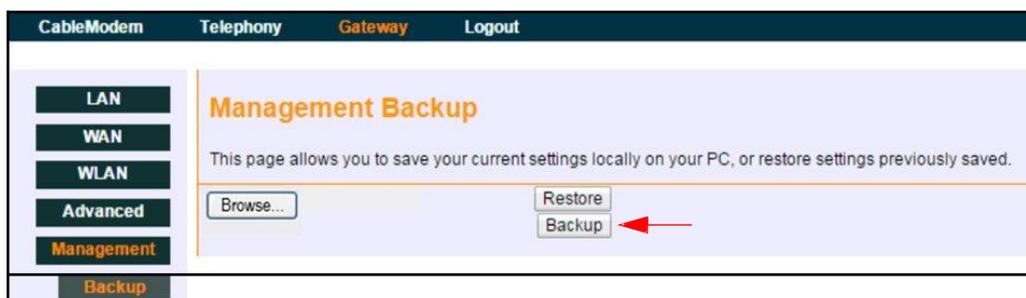
1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **Management** im linken Menü.
3. Folgende Untermenüs sind verfügbar:
  - Datensicherung

### 6.5.1 Datensicherungs-Option

Die Konfigurationsdaten des EVW32C können hier sicherungsgespeichert oder auf den Stand einer vorherigen Einstellung zurückgestellt werden.

#### 6.5.1.1 Aktuelle Konfiguration des Modems speichern

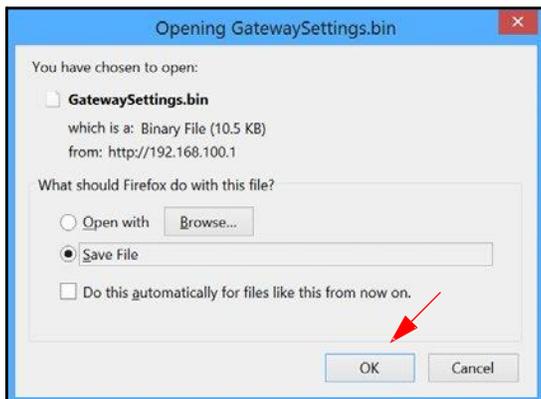
Zum Sichern und Speichern der aktuellen Modem-Konfiguration klicken Sie auf den Button „Backup“.



Ein Dialogfenster öffnet sich mit der Aufforderung „Speichern“. Klicken Sie auf „**OK**“.



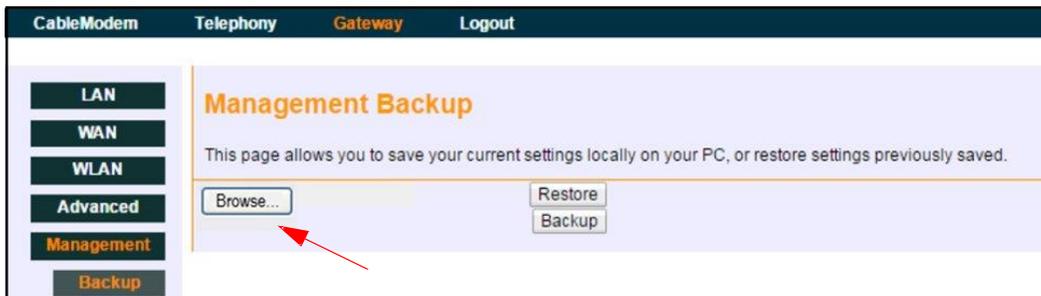
Das folgende Fenster erscheint. Sie haben die Option, die Datei zu speichern. Klicken Sie auf „Datei speichern“ und dann „OK“.



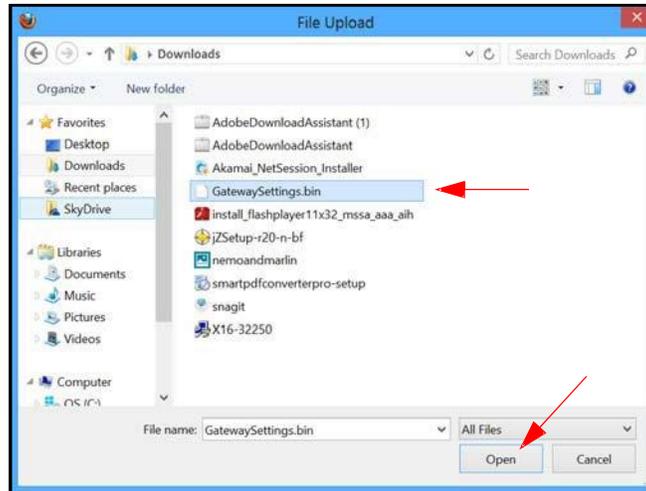
Die Datei wird in Ihrem Download-Folder als Binärdatei (.bin) unter dem Dateinamen „GatewaySettings.bin“ gespeichert.

### 6.5.1.2 Zurückstellung des EVW32C auf vorherige Gerätekonfiguration

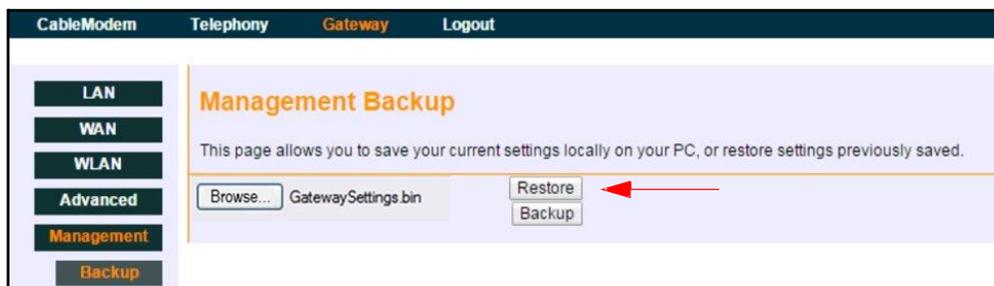
Um das Gerät auf eine zuvor gespeicherte Konfiguration zurückzusetzen, klicken Sie auf den Button „Browse“.



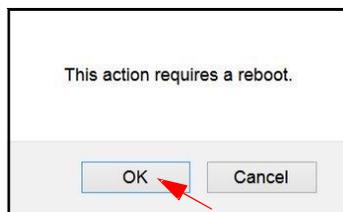
Das Dialogfenster „Datei hochladen“ erscheint. Sie können nun eine früher gespeicherte Sicherungsdatei auswählen. Markieren Sie die Datei und klicken Sie auf „Öffnen“.



Die Sicherungsdatei erscheint rechts neben dem Button „Browse“. Klicken Sie auf „Wiederherstellen“.



Es erscheint die Meldung, dass Sie Ihren Computer neu starten müssen. Klicken Sie „OK“.



Es erscheint die Meldung, dass Ihr Gerät zurückgestellt wurde. Klicken Sie „Reload“.



Es erscheint der Anmeldebildschirm für den EVW32C. Geben Sie Ihren Nutzernamen und Ihr Passwort ein, um zur Nutzeroberfläche des Modems zurückzukehren.



## 6.6 VPN-Option

Mit der **VPN**-Option konfigurieren Sie virtuelle private Tunnel (VPN) für den EVW32C.

Bei VPN handelt es sich um ein Computernetzwerk zwischen Netzknoten offener Verbindungen (Internet) oder virtueller Schaltkreise anstelle von physischen, elektrischen Verbindungen. Eine verbreitete Verwendung eines VPN ist, wenn Sie zwischen zwei ortsunabhängigen Computern eine konkrete Verbindung herstellen wollen, wie beispielsweise von einer Niederlassung zu einem Hauptsitz, um private Daten zu übertragen.

- **Internet Protocol Security (IPsec)** – Standardprotokollsuite zur Sicherung von IP-Kommunikationen. IPsec wird in der Internetschicht (TCP/IP) zur Authentifizierung und Verschlüsselung eines jeden IP-Pakets für die Dauer eines Datenaustauschs betrieben.
- **VPN Tunnel** – Eine private Datenübertragung nutzt die Kapazitäten des öffentlichen Netzwerks. Daten werden so übertragen, dass die Routingpunkte eines öffentlichen Netzwerks diesen Vorgang nicht einem privaten Netzwerk zuordnen.

### Ein VPN-Tunnel wird in zwei Phasen errichtet:

- Phase 1 - Errichten Sie eine Internet Key Exchange (IKE) Security Association (SA) zwischen einem Computer und einem ortsfernen IPsec-Router.
- Phase 2 - Richten Sie unter Verwendung der IKE SA eine IPsec SA ein, über die Ihr Computer und der ortsferne IPsec-Router abgesichert Daten zwischen Computern des lokalen und eines entfernten Netzwerks übertragen.
- **SA** – Eine „Security Association“ ist eine vertragliche Vereinbarung über Sicherheitsparameter, die zwischen Computer und dem ortsfernen IPsec-Router für jede Phase eingesetzt werden. Die SA begründet eine IPsec-VPN-Konfiguration.
- **IPsec Algorithmen** – Die AH- und ESP-Protokolle bilden die Grundlage des Authentifizierungsvorgangs, mit dem eine Security Association gegründet wird. Nach der SA-Errichtung können Sie abgesichert Daten übertragen.
  - **AH** – Das Authentication Header Protocol (RFC 2402) ist konzipiert für Integrität, Authentifizierung und die Vermeidung von Wiederholungssignalen. Bei Anwendungen ohne gesetzliche Verschwiegenheitsverpflichtung durch Regierungsverschlüsselungsbeschränkungen, kann ein AH zur Gewährleistung der (Daten-)Integrität eingesetzt werden. Ein AH prüft die Datenintegrität und authentifiziert den Urheber, doch es blockiert die Datenverbreitung nicht.

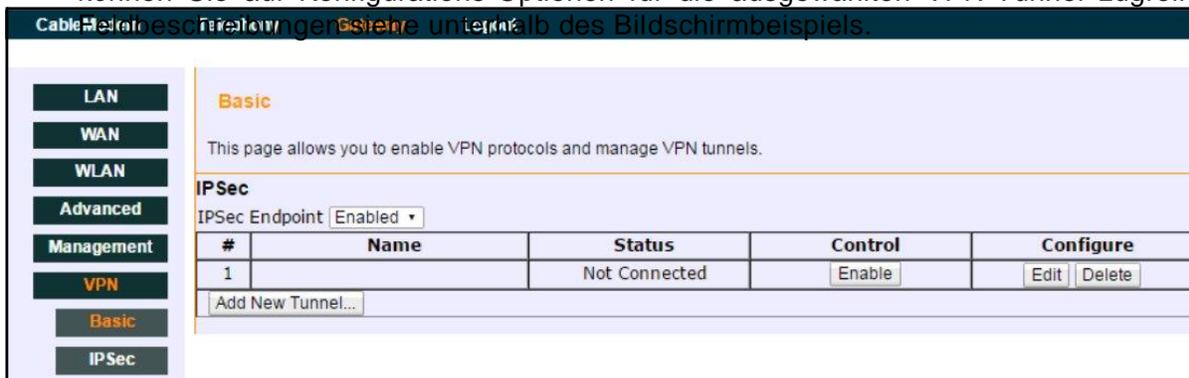
- **ESP** – Das Encapsulating Security Payload Protocol - ESP - (RFC 2406) dient der Verschlüsselung und leistet ebenso AH-Dienste. Die Authentifizierungsfunktionen des ESP beziehen sich nicht auf die IP-Header-Informationen während des Authentifizierungsvorgangs, im Gegensatz zum AH-Protocol. Es genügt, das ESP einzusetzen, wenn nur die oberen Protokoll-Schichten authentifiziert werden müssen. Eine Funktion des ESP besteht ebenso darin, für die maximale Nutzlast noch einen Spielraum anzulegen (Payload Padding). Die Größe der Pakete, die zur weiteren Absicherung von Kommunikationen übermittelt werden, wird hierdurch verdeckt.

**VPN-Optionen konfigurieren:**

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **VPN** im linken Menü.
3. Folgende Untermenüs sind verfügbar:
  - Basic
  - IPsec

**6.6.1 Basic-Option**

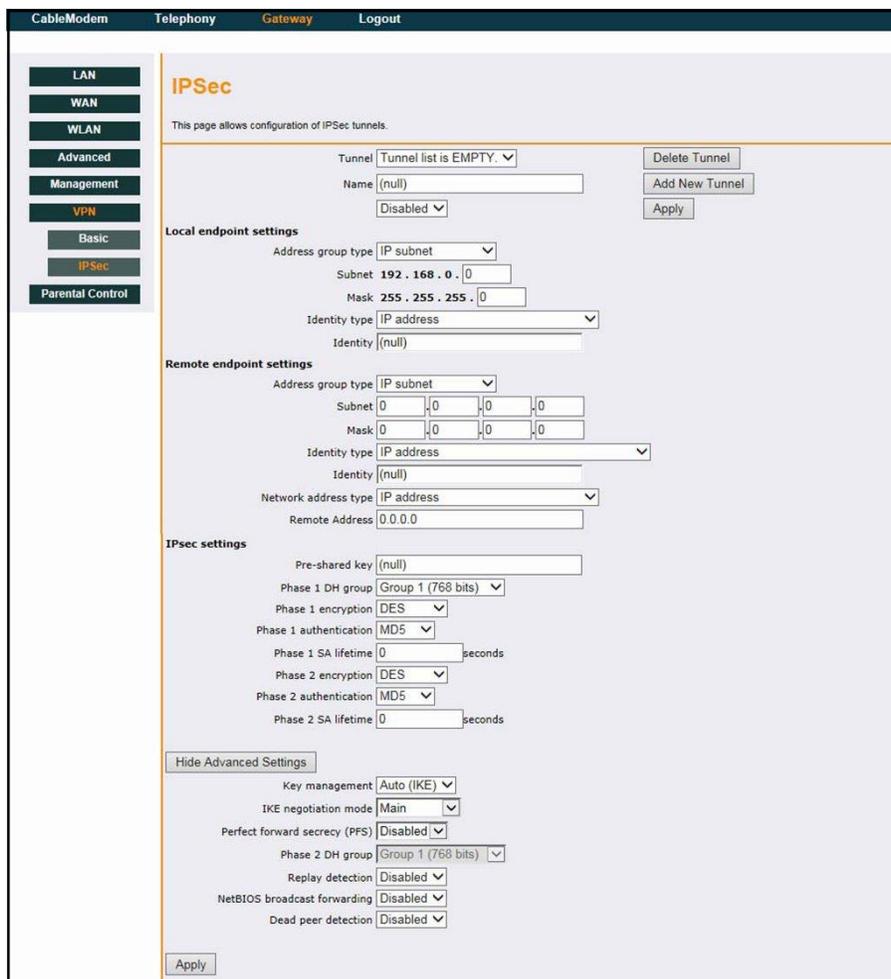
Die **Basic**-Option zeigt im Überblick die VPN-Einstellungen an. Über diesen Bildschirm können Sie auf Konfigurations-Optionen für die ausgewählten VPN-Tunnel zugreifen.



Bezeichnung	Beschreibung
<b>IPsec Endpunkt</b>	(De-)Aktiviert das IPsec (Internet Protocol Security) für den VPN-Dienst.
<b>#</b>	Zeigt ID-Nummer für bestehende IPsec-VPN-Tunnel an.
<b>Name</b>	Zeigt Namen des IPsec-VPN-Tunnels an.
<b>Status</b>	Zeigt Status des IPsec an. Nach erfolgreicher Verbindung eines IPsec-VPN wird der Status auf „Verbunden“ geändert. Sonst wird der Status als „nicht verbunden“ angezeigt.
<b>Steuerung</b>	Zeigt an, wenn der Nutzer manuell eine IPsec-VPN-Verbindungsanforderung an den ortsfernen VPN-Gateway auslöst.
<b>Konfigurieren</b>	Ermöglicht die Bearbeitung und Löschung der IPsec-Konfiguration. <ul style="list-style-type: none"> <li>• <b>Bearbeiten</b> – IPsec-VPN-Parameter dieses Tunnels können geändert werden.</li> <li>• <b>Löschen</b> –IPsec-VPN-Tunnel kann gelöscht werden.</li> </ul>
<b>Neuen Tunnel hinzufügen</b>	Erstellt einen neuen IPsec-VPN-Tunnel und fügt ihn zu der IPsec-Liste hinzu. Klicken Sie auf <b>Bearbeiten</b> , um dessen Parameter zu verändern.

### 6.6.2 IPsec-Option

Die IPsec-Option dient zur Konfiguration eines vollständigen VPN. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Tunnel</b>	Listet die Anzahl der zur Bearbeitung verfügbaren VPN-Tunnel auf. Ist kein Tunnel vorhanden, wird die Liste als LEER angezeigt.
<b>Name</b>	Zeigt Namen des Tunnels an.
<b>(De-)Aktivieren</b>	(De-)aktiviert den VPN-Tunnel.
<b>Tunnel löschen</b>	Löscht den ausgewählten VPN-Tunnel.
<b>Neuen Tunnel hinzufügen</b>	Fügt neuen Tunnel hinzu nachdem der Name eingegeben wurde.
<b>Übernehmen</b>	(De-)aktiviert Tunnel nach Klicken auf „Übernehmen“, um Änderungen zu speichern.
<b>Lokale Einstellungen des Endpunkts</b>	

Bezeichnung	Beschreibung
<b>Gruppentyp der Adresse</b>	Konfiguriert das lokale Netzwerk, welches durch die IPsec-VPN im LAN Ihres Geräts geschützt wird. Wählen Sie den lokalen Adresstyp: <ul style="list-style-type: none"> <li>• IP Subnet - Schutz des gesamten Subnetzes (Standardvorgabe).</li> <li>• Single IP address - Schutz eines Computers.</li> <li>• IP address range - Schutz mehrerer Computer.</li> </ul>
<b>Subnetz</b>	Definiert Subnetz.
<b>Maske</b>	Definiert Subnetz-Maske.
<b>Identitätstyp</b>	Definiert Identitätstyp für dieses Gerät: <ul style="list-style-type: none"> <li>• Automatisch wird die WAN IP-Adresse eingesetzt</li> <li>• IP-Adresse eingesetzt (Standardvorgabe).</li> <li>• Vollständig qualifizierter Domäne-Name (Fully qualified domain name (FQDN)) E-Mail-Adresse (USER FQDN)</li> </ul> Im Hauptmodus (siehe <a href="#">IKE-Negotiations-Modus, S. 75</a> ) werden Identitätstyp und Inhalte zur Identitätsabsicherung verschlüsselt. Der VPN-Konzentrator kann bis zu 30 eingehende SAs voneinander unterscheiden, sofern sie über dynamische WAN-IP-Adressen verfügen und sich mit ortsfernen IPsec-Routern verbinden. Sie können zwischen fünf Verschlüsselungsalgorithmen wählen (DES, 3DES, AES-128, AES-192 und AES-256), zwei Authentifizierungsalgorithmen (MD5 und SHA1) sowie drei Schlüsselgruppen (DH1 und DH2, DH5), sofern Sie eine VPN-Regel konfigurieren. Der Identitätstyp und -inhalt stellen einen zusätzlichen Grad der Identifikation für eingehende SAs dar.  Im Aggressiv-Modus (siehe <a href="#">IKE-Negotiation, S. 75</a> ) ordnet der VPN-Concentrator eingehende, nicht verschlüsselte SAs nach Identitätstyp und -inhalt, um zwischen mehrfachen Regeln für SAs zu unterscheiden, die sich von ortsfernen IPsec-Routern mit dynamischen WAN-IP-Adressen verbinden.
<b>Identität</b>	Definiert Werte entsprechend des ausgewählten Identitätstyps.
<b>Fernbediente Einstellungen des Endpunkts</b>	
<b>Gruppentyp der Adresse</b>	Definiert Adressgruppentyp: <ul style="list-style-type: none"> <li>• IP Subnet – schützt gesamtes Subnetz.</li> <li>• Single IP address - Schutz eines Computers.</li> <li>• IP address range - Schutz mehrerer Computer.</li> </ul>
<b>Subnetz</b>	Definiert Subnetz.
<b>Maske</b>	Definiert Subnetz-Maske.
<b>Identitätstyp</b>	Definiert Identitätstyp für dieses Gerät, das nun wie folgt erkannt wird: <ul style="list-style-type: none"> <li>• Automatisch wird die WAN IP-Adresse eingesetzt</li> <li>• IP-Adresse</li> <li>• Vollständig qualifizierter Domäne-Name (Fully qualified domain name (FQDN))</li> <li>• E-Mail-Adresse (USER FQDN)</li> </ul>
<b>Identität</b>	Definiert Werte entsprechend des ausgewählten Identitätstyps.
<b>Netzwerk-Adresstyp</b>	Definiert den Netzwerk-Adresstyp: <ul style="list-style-type: none"> <li>• IP-Adresse: üblicherweise für statische öffentliche IP-Adressen geeignet (Standardvorgabe).</li> <li>• Vollqualifizierter Domäne-Name (FQDN) - üblicherweise geeignet für flexible öffentliche Adressen.</li> </ul>

Bezeichnung	Beschreibung
<b>Ortsferne Adresse</b>	<p>Identifiziert den spezifizierten ortsfernen IPsec-VPN-Gateway, über den Ihr Gerät die IPsec-VPN-Verbindung aufbaut.</p> <ul style="list-style-type: none"> <li>• Verwenden Sie den IP-Adressenwert, wenn eine IP-Adresse dem Netzwerk-Adressen-Typ entspricht.</li> <li>• Verwenden Sie FQDN, wenn dies ausgewählt ist.</li> </ul>
<b>IP-Einrichtung</b>	
<b>Netzwerk-Schlüssel</b>	<p>Definiert Ihren Netzwerk-Schlüssel. Ein Netzwerkschlüssel identifiziert eine kommunizierende Partei während einer Phase 1 - IKE-Negotiation. Der Netzwerkschlüssel muss mit der anderen Partei geteilt werden, bevor mit dieser über eine geschützte Verbindung kommuniziert werden kann.</p>
<b>Phase 1 - DH-Gruppe</b>	<p>Definiert, welche Diffie-Hellman-Schlüssel-Gruppe (DHx) Sie für die Verschlüsselung einsetzen:</p> <ul style="list-style-type: none"> <li>• <b>DH1</b> – eine 768-bit Zufallszahl (Standardvorgabe)</li> <li>• <b>DH2</b> – eine 1024-bit Zufallszahl</li> <li>• <b>DH5</b> – eine 1536-bit Zufallszahl</li> </ul>
<b>Phase 1 – Verschlüsselung</b>	<p>Definiert, welche Schlüsseldimension und welcher Verschlüsselungsalgorithmus für Datenkommunikationen zur Verfügung stehen.</p> <ul style="list-style-type: none"> <li>• <b>DES</b> – ein 56-bit Schlüssel mit dem DES-Verschlüsselungsalgorithmus (Standardvorgabe).</li> <li>• <b>3DES</b> – ein 168-bit Schlüssel mit dem DES-Verschlüsselungsalgorithmus. Das EVW32C und der ortsf</li> </ul> <p>IPsec-Router müssen dieselben Algorithmen/Schlüssel einsetzen - zur Ver- /Entschlüsselung der Nachrichten oder zur Generierung und zur Verifizierung eines Nachrichtenauthentifizierungscodes. Längere Schlüssel erfordern eine höhere Bearbeitungsleistung, wodurch sich eine erhöhte Latenz und ein verminderter Datendurchsatz ergeben.</p> <p><b>AES</b> –der erweiterte Verschlüsselungsstandard (Advanced Encryption Standard) setzt ebenfalls einen</p>
<b>Phase 1 - Authentifizierung</b>	<p>Definiert, welcher Hash-Algorithmus für die Authentifizierung der Paket-Daten in der IKE SA zur Verfügung steht.</p> <ul style="list-style-type: none"> <li>• <b>MD5</b> (message digest 5) erzeugt einen 128-bit Digest zur Authentifizierung der Paketdaten (Standardv</li> <li>• <b>SHA1</b> (secure hash algorithm) erzeugt einen 160-bit Digest zur Authentifizierung der Paketdaten. SHA gegenüber MD5 generell als stärker, doch es ist auch langsamer.</li> </ul>
<b>Phase 1 - SA Lifetime</b>	<p>Definiert die Zeitdauer (120 - 86400 Sekunden), bevor ein IKE SA-Vorgang einen neuen Schlüssel aushandelt. Eine kurze SA-Dauer erhöht die Sicherheit, weil beide VPN-Gateways zur Aktualisierung der Verschlüsselungs- und Authentifizierungsschlüssel aufgefordert werden. Jedes Mal, wenn der VPN-Tunnel neue Schlüssel aushandelt, wird die Verbindung der Fernzugriffsnutzer vorübergehend getrennt.</p>
<b>Phase 2 – Verschlüsselung</b>	<p>Definiert, welche Schlüsseldimension und welcher Verschlüsselungsalgorithmus für Datenkommunikationen zur Verfügung stehen.</p> <ul style="list-style-type: none"> <li>• <b>DES</b> – ein 56-bit Schlüssel mit dem DES-Verschlüsselungsalgorithmus (Standardvorgabe).</li> <li>• <b>3DES</b> – ein 168-bit Schlüssel mit dem DES-Verschlüsselungsalgorithmengerät und dem ortsfernen IPsec-Router müssen dieselben Algorithmen/Schlüssel einsetzen - zur Ver-/Entschlüsselung der Nachrichten oder zur Generierung und zur Verifizierung eines Nachrichtenauthentifizierungscodes. Längere Schlüssel erfordern eine höhere Bearbeitungsleistung, wodurch sich eine erhöhte Latenz und ein verminderter Datendurchsatz ergeben.</li> <li>• <b>AES</b> – der erweiterte Verschlüsselungsstandard (Advanced Encryption Standard) setzt ebenfalls einen Schlüssel ein.</li> </ul> <p>Diese Umsetzung der AES passt einen 128-bit-Schlüssel jeweils 128-bit-Datenblöcken an. AES funktioniert schneller als 3DES. Zur Auswahl stehen: <b>AES-128, AES-192, AES-256</b>.</p>
<b>Phase 2 - Authentifizierung</b>	<p>Definiert, welcher Hash-Algorithmus für die Authentifizierung der Paket-Daten in der IKE SA zur Verfügung steht. Die Auswahl besteht zwischen <b>SHA1</b> und <b>MD5</b> (Standardvorgabe). <b>SHA1</b> gilt gegenüber <b>MD5</b> generell als stärker, doch ist es auch langsamer.</p>
<b>Phase 2 - SA Lifetime</b>	<p>Definiert die Zeitdauer (120 - 86400 Sekunden), bevor ein IKE SA-Vorgang einen neuen Schlüssel aushandelt.</p>

**Erweiterte Einstellungen**

Bezeichnung	Beschreibung
<b>Schlüsselmanagement</b>	Definiert die automatische (IKE) oder manuelle Schlüsselkonfiguration zur Einrichtung eines VPN. Standardvorgabe ist Automatisch.
<b>IKE Negotiations-Modus</b>	Legt fest, wie die Security Association (SA) für jede Verbindung durch IKE-Negotiationen errichtet wird. Zur Auswahl stehen: <b>Hauptmodus</b> – Höchster Sicherheitsgrad, sofern die Kommunikationsparteien eine Authentifizierung verhandeln (Phase 1). Dies ist voreingestellt. <b>Aggressiver Modus</b> – Eliminiert mehrere Schritte, wenn die Kommunikationsparteien eine Authentifizierung verhandeln (Phase 1). Schneller als Hauptmodus.
<b>Perfect forward secrecy (PFS)</b>	(De-)Aktiviert die PFS-Option. Sie ist per Standard in Phase 2, IPsec-SA-Einrichtung deaktiviert, um eine schnellere IPsec-Einrichtung zu ermöglichen, aber dies ist nicht unbedingt sicher. Wählen Sie DH1, DH2 oder DH5, um PFS zu aktivieren.
<b>Phase 2 - DH-Gruppe</b>	Definiert, welche Diffie-Hellman-Schlüssel-Gruppe (DHx) Sie für die Verschlüsselung einsetzen: <ul style="list-style-type: none"> <li>• <b>DH1</b> – eine 768-bit Zufallszahl</li> <li>• <b>DH2</b> – eine 1024-bit Zufallszahl</li> <li>• <b>DH5</b> – eine 1536-bit Zufallszahl</li> </ul>
<b>Wiedereinspielungs-Erkennung</b>	(De-)Aktiviert die Wiedereinspielungs-Erkennung. Während der VPN-Einrichtung ist das System möglicherweise anfällig für Dienstverweigerungs- (DOS-) Angriffe. Der IPsec-Empfänger kann nicht mehr gültige oder doppelte Pakete erkennen und abweisen, um Wiedereinspielungs-Angriffe abzuwehren.
<b>NetBIOS Broadcast-Weiterleitung</b>	Ermöglicht das Versenden von NetBIOS-Paketen über die VPN-Verbindung. NetBIOS (Netzwerk Basic Eingabe/Ausgabe System) sind TCP-/UDP-Pakete, die einem Computer das Erkennen anderer Computer ermöglichen. Gelegentlich ist das zulässige Versenden von NetBIOS-Paketen durch VPN-Tunnel erforderlich, um lokalen Computern die Erkennung anderer Computer des ortsfernen Netzwerks zu ermöglichen und umgekehrt.
<b>Dead peer detection</b>	(De-)Aktiviert die Option "Dead peer detection". Ist die Option aktiviert, prüft das Gerät periodisch, ob der ortsferne IPsec-Gateway verfügbar ist.
<b>Übernehmen</b>	Speichert Änderungen.

## 6.7 Elternkontrolle

Diese Funktion dient zur Kontrolle des Benutzerzugriffs auf das EVW32C-Netzwerk. Die Elternkontrolle hat folgende Funktionen:

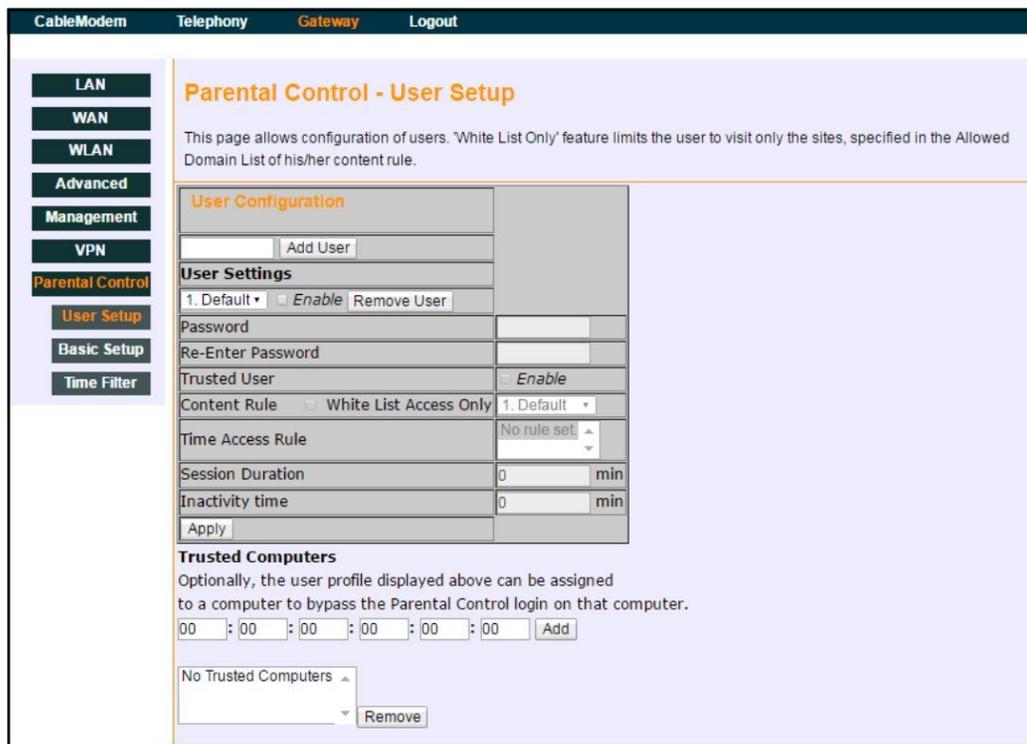
- Zugriff nur nach Eingabe von Nutzernamen und Passwort möglich.
- Keyword-definierte Webseiten können für Nutzer gesperrt werden.
- Zeitdauer der Internetnutzung kann für Nutzer tages- und stundenweise begrenzt werden.

### Zugriff auf das Elternkontroll-Menü:

1. Klicken Sie auf **Gateway** im Hauptmenü.
2. Wählen Sie **Elternkontrolle** im linken Menü.
3. Folgende Untermenüs sind verfügbar:
  - Einrichtung Nutzerdaten
  - Einrichtung Grunddaten
  - Zeitfilter

### 6.7.1 Benutzereinrichtung

Die Option **Benutzereinrichtung** dient zur Konfiguration der Nutzerkonten hinsichtlich der jeweiligen Zugriffsberechtigung auf das WiFi-/kabelgeleitete Netzwerk sowie hinsichtlich der Parameter jeder Verbindungsmöglichkeit. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.

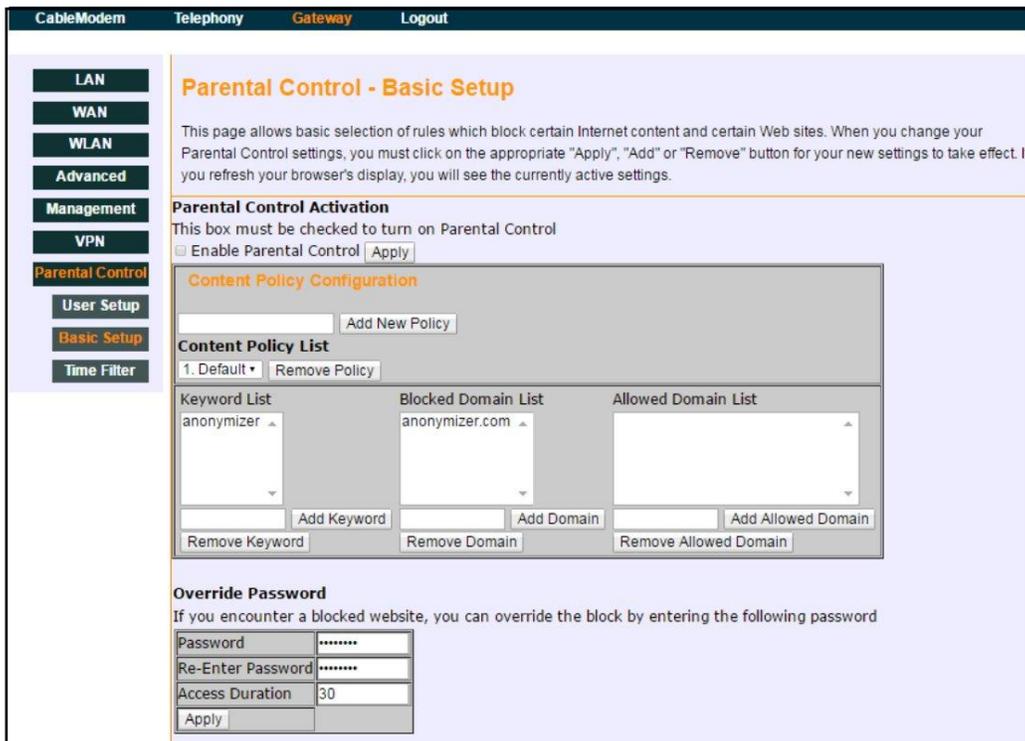


Bezeichnung	Beschreibung
<b>Nutzerkonfiguration</b>	
<b>Nutzer hinzufügen Nutzer löschen Aktivieren</b>	Definiert Nutzerkonten: <ul style="list-style-type: none"> <li>• Zur Auswahl eines Bestandsnutzers wählen Sie diesen aus dem Drop-Down-Menü Nutzereinstellungen.</li> <li>• Zum Hinzufügen eines neuen Nutzers geben Sie den Nutzernamen ein und klicken Sie auf „Nutzer hinzufügen“. Nutzernamen dürfen keine Leerzeichen enthalten.</li> <li>• Zur Aktivierung des ausgewählten Nutzers markieren Sie „Aktivieren“.</li> <li>• Zum Löschen eines Nutzers wählen Sie diesen aus dem Drop-Down-Menü aus und klicken Sie auf „Nutzer löschen“.</li> </ul>
<b>Passwort</b>	Definiert das Passwort für den ausgewählten Nutzer. Nur per Passwort-Eingabe kann der Nutzer über den EVW32C auf das Internet zugreifen.
<b>Passwort wiederholt eingeben</b>	Passwort durch wiederholte Eingabe bestätigen.
<b>Vertrauenswürdiger Nutzer</b>	Jedem Nutzer kann der Status "Vertrauenswürdiger Nutzer" zugewiesen werden. Dies verleiht ihm übergeordnete und filterunabhängige Internetzugriffsrechte. Hier ankreuzen, um einem Nutzer vollen Zugriff zu gewähren. Gleichzeitig jedoch bleiben alle vorher eingerichteten Einstellungen gespeichert und verfügbar.
<b>Inhaltsregel</b>	Listet Drop-Down-Liste bestehender Inhaltsregeln auf, die definieren, welche Zugriffsrechte/-verweigerungen bestimmte Nutzer auf bestimmten Webseiten haben.

Bezeichnung	Beschreibung
<b>Zugriffsrechte nur für Whitelist</b>	Aktiviert die Option "Zugriffsrechte nur für Whitelist". Nach der Erstellung einer Inhaltsregel, die eine Blacklist/Whitelist definiert, markieren Sie das Textfeld dieser Option, so dass der EVW32C diese Regel für die entsprechend ausgewählten Nutzer anwendet.
<b>Zeitlich definierter Zugriff</b>	Dem ausgewählten Nutzer wird eine zeitlich definierte Zugangsregel zugewiesen.
<b>Sitzungsdauer</b>	Begrenzt die Sitzung eines Nutzers durch die Eingabe eines Minutenwerts. Nach Ablauf dieser Zeitdauer kann der Nutzer sich erneut für dieselbe Sitzungsdauer anmelden.
<b>Zeitdauer der Inaktivität</b>	Erlaubt die Eingabe eines Wertes für die Zeitabschaltung, wenn ein Nutzer keine Internetaktivität ausübt. Wird dieser Wert überschritten, schaltet sich die Nutzeroberfläche für den Internetzugriff aus.
<b>Übernehmen</b>	Speichert alle Bildschirmänderungen.
<b>Vertrauenswürdige Computer</b>	Definiert vertrauenswürdige Hosts, die die Elternkontrollbeschränkungen umgehen können.
<b>Hinzufügen</b>	Geben Sie die MAC-Adresse der vertrauenswürdigen Hosts ein, und klicken Sie auf „Hinzufügen“, um einem Gerät diesen Status zuzuweisen.
<b>Löschen</b>	Entfernt einen vertrauenswürdigen Computer von der Liste, wenn er in der Liste markiert wird und dann auf „Löschen“ geklickt wird.

### 6.7.2 Grundeinstellungen

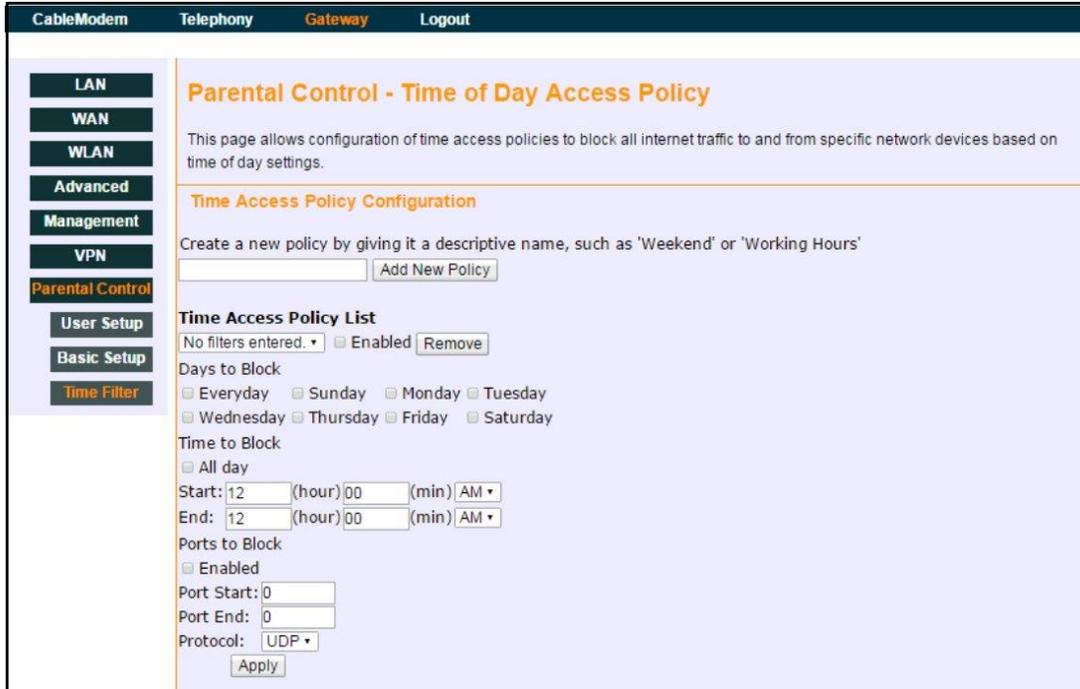
Diese Option aktiviert die Elternkontrolle und ermöglicht die Zugriffsverweigerung auf bestimmte Internetinhalte und Webseiten. Nach der Änderung der Einstellungen klicken Sie auf „Übernehmen“ sowie „Hinzufügen“ oder „Löschen“, sodass Ihre Einstellungen wirksam werden. Aktualisieren Sie Ihren Browser, um die aktuellen und aktiven Einstellungen abzurufen. Feldbeschreibungen siehe unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Elternkontrolle aktivieren</b>	Aktiviert die Elternkontrolle, wenn das Feld markiert ist und auf „Übernehmen“ geklickt wird.
<b>Übernehmen</b>	Speichert in den Bildschirm eingegebene Änderungen und aktiviert die Elternkontrolle, sofern das entsprechende Feld markiert wurde.
<b>Konfiguration der inhaltsbedingten Internetzugriffsrechte</b>	
<b>Neue Regel hinzufügen</b>	Neue Regel wird der Liste hinzugefügt. Geben Sie den Namen der Regel ein und klicken Sie auf „Neue Regel hinzufügen“. Beachten Sie, dass der Name der Regel keine Leerzeichen enthalten darf.
<b>Liste der inhaltsbedingten Internetzugriffsrechte</b>	Listet bestehende Regeln auf, die zur Aktivierung ausgewählt werden können.
<b>Regel löschen</b>	Löscht Regel aus der Liste der inhaltsbedingten Internetzugriffsrechte. Wählen Sie die Regel aus und klicken Sie auf „Regel löschen“.
<b>Keyword-Liste</b>	Zeigt Keywords zur Blockierung von Webseitenadressen (URLs) an, die dort enthalten sind.
<b>Keyword hinzufügen</b>	Neues Keyword wird der Liste hinzugefügt. Geben Sie das Keyword in das Textfeld ein und klicken Sie auf „Keyword hinzufügen“. Das Keyword wird der Liste hinzugefügt.
<b>Keyword löschen</b>	Keyword wird aus Liste gelöscht. Wählen Sie das Keyword aus und klicken Sie auf „Keyword löschen“.
<b>Liste blockierter Domains</b>	Zeigt Web-Domains an (z. B. unwanted.com), die per Konfiguration gesperrt werden können.
<b>Domain hinzufügen</b>	Neue Domain wird der Liste gesperrter Domains hinzugefügt. Geben Sie die Domain in das Textfeld ein und klicken Sie auf „Domain hinzufügen“. Die Domain wird hinzugefügt.
<b>Domain löschen</b>	Domain wird von der Liste gesperrter Domains gelöscht. Wählen Sie die Domain aus und klicken Sie auf „Domain löschen“.
<b>Liste zulässiger Domains</b>	Zeigt Web-Domains an (z. B. safe.com), die für bestimmte Nutzer ausschließlich zugelassen werden können.
<b>Zulässige Domain hinzufügen</b>	Neue Domain wird der Liste zulässiger Domains hinzugefügt. Geben Sie die Domain in das Textfeld ein und klicken Sie auf „Zulässige Domain hinzufügen“. Die Domain wird hinzugefügt.
<b>Zulässige Domain löschen</b>	Domain wird von der Liste zulässiger Domains gelöscht. Wählen Sie die Domain aus und klicken Sie auf „Zulässige Domain löschen“.
<b>Sonderzugangs-Passwort</b>	Die Sperrung blockierter Webseiten kann durch Eingabe dieses Passworts umgangen werden.
<b>Passwort</b>	Definieren Sie ein Passwort zur Umgehung der Sperrung blockierter Webseiten.
<b>Passwort wiederholt eingeben</b>	Passwort durch wiederholte Eingabe bestätigen.
<b>Zugriffszeitraum</b>	Erlaubt die Definition eines Zeitraums (in Minuten) für den Zugriff auf eine blockierte Seite, wenn die Sperrung durch Eingabe des Passworts umgangen wurde.
<b>Übernehmen</b>	Speichert Änderungen des Passworts und des Zugriffszeitraums.

### 6.7.3 Zeitfilter

Der Internetzugang kann auf bestimmte Uhrzeiten beschränkt werden. Beschreibungen der Felder folgen unterhalb des Bildschirmbeispiels.



Bezeichnung	Beschreibung
<b>Konfiguration Zugriffszeitregel</b>	
<b>Neue Regel hinzufügen</b>	Fügt eine neue Zugriffszeitregel hinzu. Geben Sie den Namen der Regel ein und klicken Sie auf „Neue Regel hinzufügen“.
<b>Liste Zugriffszeitregeln</b>	Zeigt bestehende Zugriffszeitregeln als Drop-Down-Menü an.
<b>Aktiviert</b>	Aktiviert eine Regel. Wählen Sie die Regel aus dem Drop-Down-Menü und markieren Sie „Aktivieren“.
<b>Löschen</b>	Löscht die Regel. Wählen Sie die Regel aus dem Drop-Down-Menü und markieren Sie „Löschen“.
<b>Internetsperrtage</b>	Ermöglicht tageweise Zugriffsverweigerung auf das Internet.
<b>Zeitfenstersperre Internet: Ganztägig oder Zeitfenster</b>	Zeitangaben zur Internetsperre werden festgelegt. <ul style="list-style-type: none"> <li>• Markieren Sie „Ganztägssperre“, um den Internetzugriff während ausgewählter Tage zu sperren.</li> <li>• Geben Sie „Start-/Endzeit“ für eine Zeitfenstersperre an den ausgewählten Tagen ein. AM = vormittags, PM = nachmittags.</li> </ul>
<b>Portsperr</b>	Definiert den Portbereich, dem bei Markierung des Feldes „Aktivieren“ der Internetzugriff verwehrt wird. <ul style="list-style-type: none"> <li>• Port Start: Geben Sie die Port-Start-Nummer, die blockiert werden soll.</li> <li>• End-Port: Geben Sie die Port-End-Nummer, die blockiert werden soll.</li> <li>• Protokoll: Wählt Protokolltyp aus. Optionen sind: UDP, TCP oder BEIDE.</li> </ul>
<b>Übernehmen</b>	Speichert alle Bildschirmänderungen.