

# CMO 1-01 | CMO 2-01

## DOCSIS/EuroDOCSIS Kabelmodem

### Betriebsanleitung



# Inhaltsverzeichnis

|       |  |    |
|-------|--|----|
| 1     | Produktbeschreibung .....                      | 4  |
| 1.1   | Verwendungsbereich .....                       | 4  |
| 1.1.1 | Typische Anwendung .....                       | 4  |
| 1.1.2 | Zusätzlicher Einsatzzweck .....                | 4  |
| 1.2   | Lieferumfang .....                             | 5  |
| 1.3   | Anforderungen .....                            | 5  |
| 1.4   | LEDs auf der Frontseite .....                  | 6  |
| 1.4.1 | CMO 1-01 .....                                 | 6  |
| 1.4.2 | CMO 2-01 .....                                 | 7  |
| 2     | Installation .....                             | 8  |
| 2.1   | Anschlüsse CMO 1-01 .....                      | 8  |
| 2.2   | Anschlüsse CMO 2-01 .....                      | 9  |
| 2.3   | WLAN-Verbindung zum CMO 2-01 herstellen: ..... | 9  |
| 3     | Konfiguration .....                            | 10 |
| 3.1   | TCP/IP-Konfiguration .....                     | 10 |
| 3.2   | Anmelden am CMO x-01 .....                     | 10 |
| 4     | Benutzeroberfläche des CMO 2-01 .....          | 11 |
| 4.1   | Status .....                                   | 11 |
| 4.1.1 | Connection .....                               | 11 |
| 4.1.2 | Software .....                                 | 12 |
| 4.1.3 | Security .....                                 | 12 |
| 4.1.4 | Diagnostics .....                              | 13 |
| 4.2   | Basic .....                                    | 14 |
| 4.2.1 | Setup .....                                    | 14 |
| 4.2.2 | DHCP .....                                     | 15 |
| 4.2.3 | DDNS .....                                     | 16 |
| 4.2.4 | Backup/Restore .....                           | 16 |
| 4.3   | Advanced .....                                 | 18 |
| 4.3.1 | Options .....                                  | 18 |
| 4.3.2 | IP Filtering .....                             | 19 |
| 4.3.3 | MAC Filtering .....                            | 20 |
| 4.3.4 | Port Filtering .....                           | 21 |
| 4.3.5 | Forwarding .....                               | 22 |
| 4.3.6 | Port Triggers .....                            | 23 |
| 4.3.7 | DMZ Host .....                                 | 24 |
| 4.4   | Firewall .....                                 | 24 |
| 4.4.1 | Basic .....                                    | 24 |
| 4.4.2 | Web Filtering .....                            | 25 |
| 4.4.3 | Local Log .....                                | 26 |
| 4.4.4 | Remote Log .....                               | 26 |
| 4.5   | Wireless .....                                 | 27 |
| 4.5.1 | Radio .....                                    | 27 |
| 4.5.2 | Primary Network .....                          | 28 |
| 4.5.3 | Guest Network .....                            | 28 |
| 4.5.4 | Access Control .....                           | 29 |
| 4.5.5 | WMM .....                                      | 30 |
| 4.5.6 | Bridging .....                                 | 30 |
| 5     | Technische Daten .....                         | 31 |
| 5.1   | CMO 1-01 .....                                 | 31 |
| 5.2   | CMO 2-01 .....                                 | 32 |



## WARNUNG

- Beachten Sie die dem Gerät beiliegenden Sicherheitshinweise! Diese sind auch unter der folgenden Internetadresse abrufbar: [https://download.axing.com/BAs/Sicherheitshinweise\\_9sprachig.pdf](https://download.axing.com/BAs/Sicherheitshinweise_9sprachig.pdf)
- Benutzen Sie das Gerät ausschließlich wie in dieser Betriebsanleitung beschrieben und insbesondere nach dem Stand der Technik. Wird das Gerät für andere Einsätze verwendet, wird keine Gewährleistung übernommen!



### EU-Konfirmationserklärung:

Hiermit erklärt die AXING AG, dass die gekennzeichneten Produkte den geltenden Richtlinien entsprechen.

CMO 2-01: Hiermit erklärt AXING AG, dass das Gerät den Anforderungen der Richtlinie 2014/53/EU entspricht. Die vollständige EU-Konformitätserklärung ist unter der folgenden Internetadresse abrufbar: <https://axing.com/downloads/ce/>



WEEE Nr. DE26869279 | Elektrische und elektronische Komponenten nicht mit dem Restmüll, sondern separat entsorgen.

# 1 Produktbeschreibung

## 1.1 Verwendungsbereich

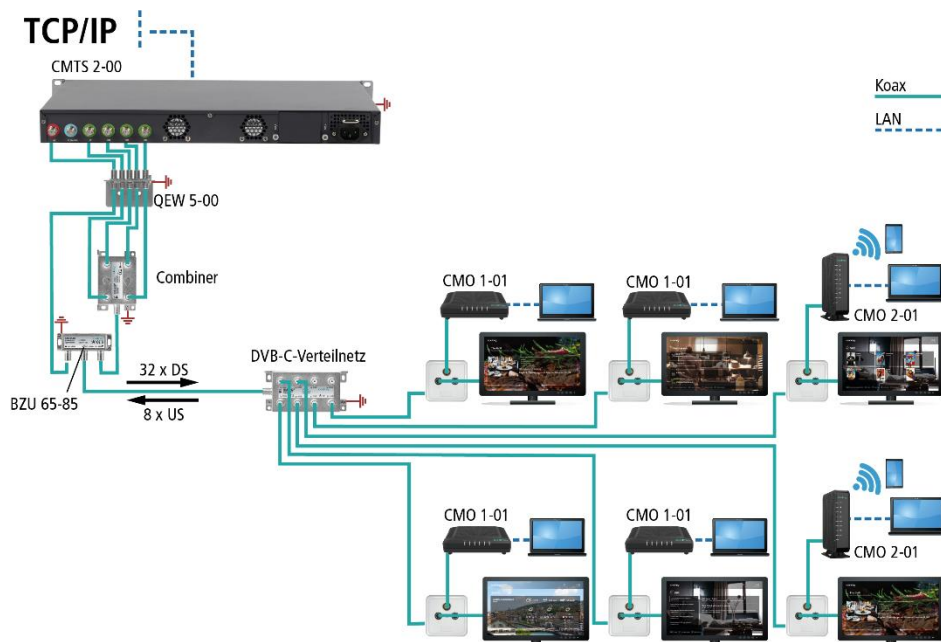
Die Kabelmodem CMO 1-01 und CMO 2-01 dienen dazu einen Internetzugang für die angeschlossenen Computer über den Kabelfernsehanschluss zu realisieren.

Das CMO 1-01/2-01 kann als Tischgerät verwendet werden.

Benutzen Sie die Geräte ausschließlich wie in der Betriebsanleitung vorgegeben. Werden die Geräte für andere Einsätze verwendet, wird keine Gewährleistung übernommen!

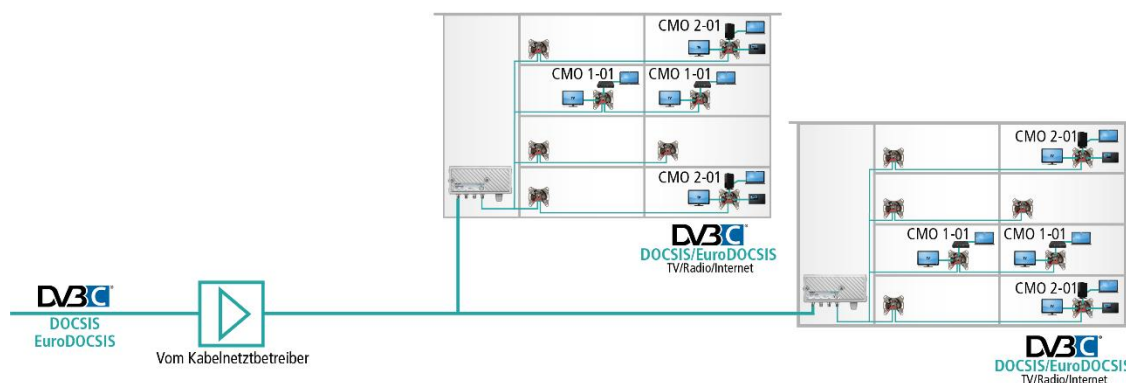
### 1.1.1 Typische Anwendung

Die Kabelmodems werden zusammen mit dem Mini CMTS 2-00 verwendet, um den Internetzugang in Krankenhäusern, Schulen, Wohnheimen oder Hotels über ein DVB-C-Netzwerk zu realisieren. Die Kabelmodems stellen dann über Ethernet und WLAN die Zugangspunkte für Internet und Datendienste zur Verfügung. Auch leistungsfähige WLAN-Access-Points, Switches und andere Netzwerktechnik können an ein solches Modem angeschlossen werden.



### 1.1.2 Zusätzlicher Einsatzzweck

Die Kabelmodems können auch eingesetzt werden, um Endkunden einen Breitband-Internetzugang über Kabel-TV-Anschlüsse zu ermöglichen. Voraussetzung dafür ist ein Internetzugang bei einem Kabelnetzbetreiber.



## 1.2 Lieferumfang

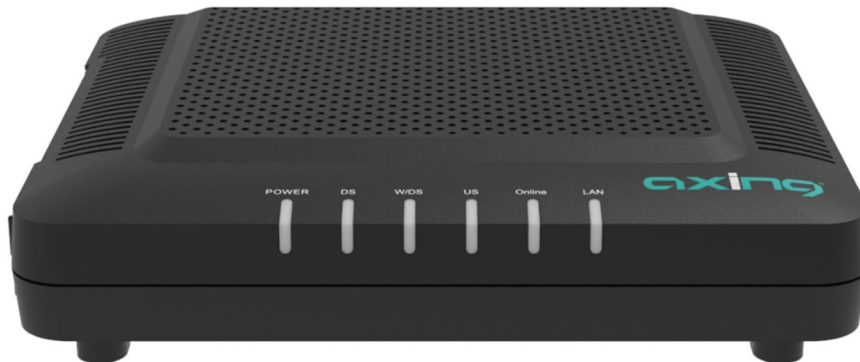
- Kabelmodem CMO 1-01 oder CMO 2-01
- Ethernet-Kabel
- 12 VDC Steckernetzteil zur Spannungsversorgung
- Quickstart-Anleitung

## 1.3 Anforderungen

- PC/Notebook, der das TCP/IP-Protokoll für die Konfiguration unterstützt.
- PC/Notebook mit einem Ethernet-Anschluss, der 10Base-T/100Base-TX und Gigabit-Ethernet unterstützt.





## 1.4 LEDs auf der Frontseite

### 1.4.1 CMO 1-01



| Name   | Farbe | Verhalten | Bedeutung  |
|--------|-------|-----------|--|
| POWER  | Grün  | An        | Gerät eingeschaltet                              |
|        |       | Aus       | Gerät ausgeschaltet oder Betriebsspannungsfehler |
| DS     | Grün  | Blinkt    | Downstream wird gescannt                         |
|        |       | An        | Downstream eingelockt                            |
|        |       | Aus       | Downstream ungenutzt oder Kanalbündelung aktiv   |
| W/DS   | Grün  | An        | Downstream eingelockt, Kanalbündelung aktiv      |
|        |       | Aus       | Kanalbündelung nicht aktiv                       |
| US     | Grün  | Blinkt    | Upstream wird gescannt                           |
|        |       | An        | Upstream eingelockt                              |
|        |       | Aus       | Upstream ungenutzt                               |
|        | Blau  | An        | Upstream eingelockt, Kanalbündelung aktiv        |
| Online | Grün  | Blinkt    | Kabelmodem wird provisioniert                    |
|        |       | An        | Kabelmodem online                                |
|        |       | Aus       | Kabelmodem offline                               |
| LAN    | Grün  | An        | Ethernet verbunden                               |
|        |       | Blinkt    | Datenverkehr aktiv                               |
|        |       | Aus       | Ethernet nicht verbunden                         |

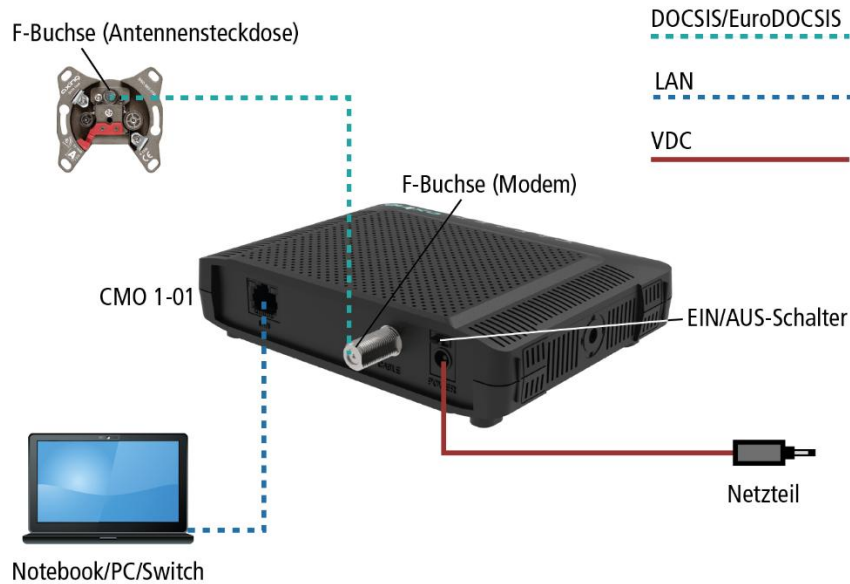
#### 1.4.2 CMO 2-01

| LED   | Name                       | Farbe            | Verhalten | Bedeutung   |
|---|----------------------------|------------------|-----------|---|
| <br><br>    | <b>POWER</b>               | Grün             | An        | Gerät eingeschaltet   |
|   |                            |                  | Aus       | Gerät ausgeschaltet oder Betriebsspannungsfehler                |
|   |                            |                  | Blinkt    | Downstream wird gescannt  |
|   | <b>DS</b>                  | Grün             | An        | Downstream eingelockt   |
|   |                            |                  | Aus       | Downstream ungenutzt  |
|   |                            | Orange           | An        | Kanalbündelung aktiv  |
|   |                            |                  | Aus       | Kanalbündelung nicht aktiv                                      |
| <br><br> | <b>US</b>                  | Grün             | Blinkt    | Upstream wird gescannt  |
|   |                            |                  | An        | Upstream eingelockt   |
|   |                            |                  | Aus       | Upstream ungenutzt  |
|   |                            | Orange           | An        | Kanalbündelung aktiv  |
|   |                            |                  | Aus       | Kanalbündelung nicht aktiv                                      |
|   |                            |                  | Blinkt    | Kabelmodem wird provisioniert                                   |
|   | <b>ONLINE</b>              | Grün             | An        | Kabelmodem online   |
|   |                            |                  | Aus       | Kabelschnittstelle ungenutzt                                    |
|   |                            | Grün oder Orange | An        | Ethernet verbunden<br>Grün = 1000-Mbit/s<br>Orange = 100-Mbit/s |
|   |                            |                  | Blinking  | Datenverkehr aktiv  |
| <b>LINK 1</b><br><b>LINK 2</b>  | <b>LAN1</b><br><b>LAN2</b> | Grün oder Orange | Aus       | Ethernet nicht verbunden  |
|   |                            |                  |           |   |
|   | <b>Wi-Fi</b>               | Grün             | An        | WLAN aktiviert  |
|   |                            |                  | Blinkt    | WLAN-Datenverkehr   |
|   |                            |                  | Aus       | WLAN nicht aktiviert  |
|   | <b>WPS</b>                 | Grün             | Blinkt    | WPS-Kopplung  |
|   |                            |                  | An        | WPS aktiviert   |
|   |                            |                  | Aus       | WPS nicht aktiviert   |



## 2 Installation

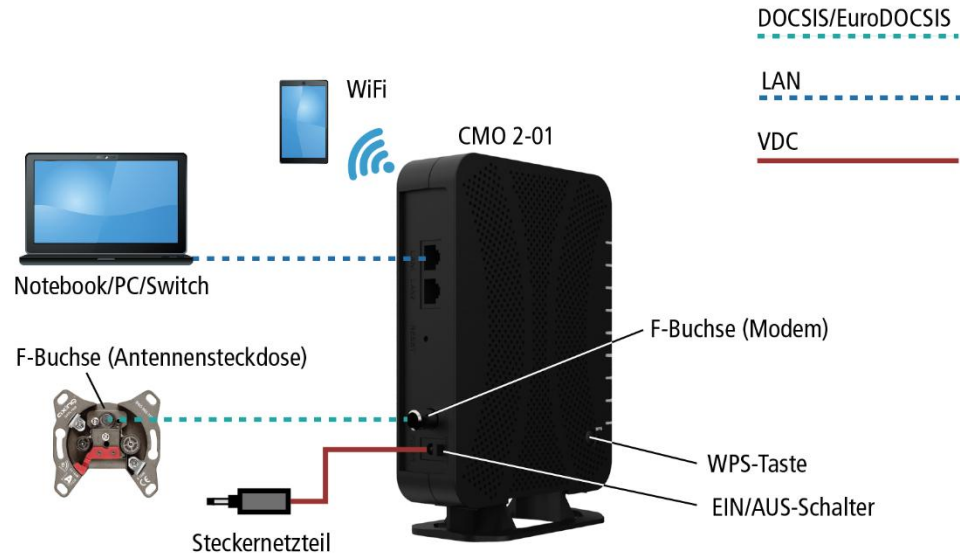
### 2.1 Anschlüsse CMO 1-01



- ➔ Verbinden Sie den DATA-Anschluss (F-Buchse) der Antennensteckdose mit der F-Buchse des CMO 1-01
- ➔ Verwenden Sie ein hochgeschirmtes Anschlusskabel mit F-Steckern.
- ➔ Verbinden Sie das mitgelieferte Steckernetzteil mit dem DC-Anschluss des Modems.
- ➔ Stecken Sie das Steckernetzteil in die Steckdose.
- ➔ Schalten Sie das Kabelmodem ein.
  - Die Power-LED leuchtet nun dauerhaft.
  - Während des Bootvorgangs blinken alle übrigen LEDs.
  - Nach dem Booten beginnt der Downstream-Kanalscan.



## 2.2 Anschlüsse CMO 2-01



- ➔ Verbinden Sie den DATA-Anschluss (F-Buchse) der Antennensteckdose mit der F-Buchse des CMO 2-01
- ➔ Verwenden Sie ein hochgeschirmtes Anschlusskabel mit F-Steckern.
- ➔ Verbinden Sie das mitgelieferte Steckernetzteil mit dem DC-Anschluss des Modems.
- ➔ Stecken Sie das Steckernetzteil in die Steckdose.
- ➔ Schalten Sie das Kabelmodem ein.
  - Die Power-LED leuchtet nun dauerhaft.
  - Während des Bootvorgangs blinken mehrere LEDs.
  - Nach dem Booten beginnt der Downstream-Kanalscan.

## 2.3 WLAN-Verbindung zum CMO 2-01 herstellen:

### 2.3.1.1 Per Eingabe von WLAN-Name und Passwort:

Auf dem Typenschild des Geräts ist der werkseitige WLAN-Name (SSID) und das Passwort (WPA Pre-Shared Key) aufgedruckt.

- ➔ Geben Sie SSID und Passwort am Notebook, Smartphones oder Tablets ein.

### 2.3.1.2 Über die WPS-Taste (WiFi Protected Setup, nicht kompatibel mit Apple®-Geräten):

- ➔ Melden Sie sich wie oben beschrieben an der Konfigurations-Oberfläche an (<http://192.168.100.1>).
- ➔ Gehen Sie auf die Seite Wireless > Primary Network.
- ➔ Wählen Sie rechts auf der Seite im Dropdown-Menü Automatic Security Configuration die Option WPS.
- ➔ Klicken Sie auf Apply, um die WPS-Funktion zu aktivieren.
- ➔ Drücken Sie die WPS-Taste am CMO 2-01 für weniger als 5 Sekunden<sup>1</sup>.
  - Die WPS-LED beginnt zu blinken.
- ➔ Verbinden Sie nun Ihr Gerät mit dem Kabelmodem. Beachten Sie ggf. die Bedienungsanleitung Ihres Gerätes.

<sup>1</sup> Drücken Sie die WPS-Taste länger als 5 Sekunden, um WiFi ein- oder auszuschalten

## 3 Konfiguration

### 3.1 TCP/IP-Konfiguration

Das TCP/IP-Protokoll muss auf Ihrem Computer korrekt installiert und konfiguriert sein.

- Wählen Sie Start und dann Einstellungen > Netzwerk und Internet aus.
- Wählen Sie Ethernet und dann das Ethernet-Netzwerk aus, mit dem Sie verbunden sind.
- Wählen Sie unter IP-Zuweisung die Option Bearbeiten aus.
- Wählen Sie unter IP-Einstellungen bearbeiten die Option Automatisch (DHCP).
- Verbinden Sie die Ethernet-Schnittstelle Ihres Computers mit der Ethernet-Schnittstelle des CMO x-01.  
Verwenden Sie das mitgelieferte Ethernet-Kabel oder ein vergleichbares Kabel mit RJ45-Steckern.

### 3.2 Anmelden am CMO x-01

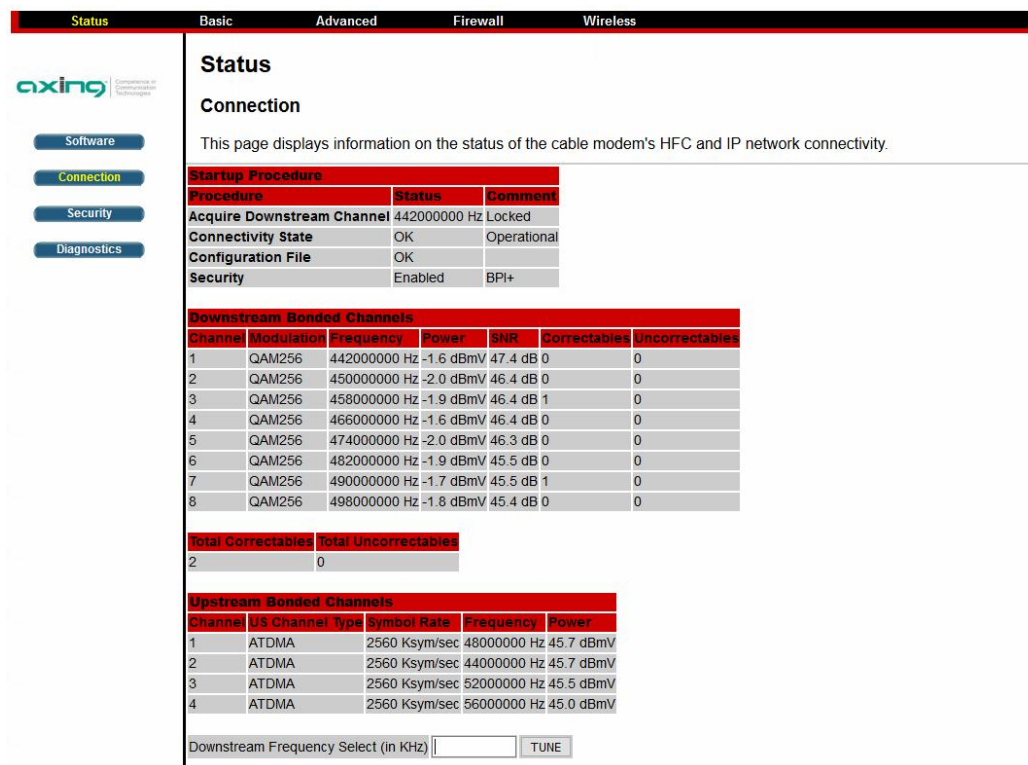
- Öffnen Sie Ihren Webbrowser.  
Sie erhalten möglicherweise eine Fehlermeldung, weil Ihr Computer nicht mit dem Internet verbunden ist.
- Geben Sie die Standard-IP-Adresse des CMO x-01 ein (z.B. 192.168.100.1) und drücken Sie die Eingabetaste.
- Geben Sie in der Eingabeaufforderung folgende Zugangsdaten ein:  
Benutzername: AXING\_USER  
Passwort: u\$erPassw0rd (0 = Null)
- Drücken Sie die Eingabetaste.  
Die Seite Status der GUI wird im Browser angezeigt (siehe 4.1.1 auf Seite 11).

## 4 Benutzeroberfläche des CMO 2-01

### 4.1 Status

#### 4.1.1 Connection

Diese Seite zeigt den Verbindungsstatus des Kabelmodems mit Downstream und Upstream



**Status**

**Connection**

This page displays information on the status of the cable modem's HFC and IP network connectivity.

**Startup Procedure**

| Procedure                  | Status              | Comment     |
|----------------------------|---------------------|-------------|
| Acquire Downstream Channel | 442000000 Hz Locked |             |
| Connectivity State         | OK                  | Operational |
| Configuration File         | OK                  |             |
| Security                   | Enabled             | BPI+        |

**Downstream Bonded Channels**

| Channel | Modulation | Frequency    | Power     | SNR     | Correctables | Uncorrectables |
|---------|------------|--------------|-----------|---------|--------------|----------------|
| 1       | QAM256     | 442000000 Hz | -1.6 dBmV | 47.4 dB | 0            | 0              |
| 2       | QAM256     | 450000000 Hz | -2.0 dBmV | 46.4 dB | 0            | 0              |
| 3       | QAM256     | 458000000 Hz | -1.9 dBmV | 46.4 dB | 1            | 0              |
| 4       | QAM256     | 466000000 Hz | -1.6 dBmV | 46.4 dB | 0            | 0              |
| 5       | QAM256     | 474000000 Hz | -2.0 dBmV | 46.3 dB | 0            | 0              |
| 6       | QAM256     | 482000000 Hz | -1.9 dBmV | 45.5 dB | 0            | 0              |
| 7       | QAM256     | 490000000 Hz | -1.7 dBmV | 45.5 dB | 1            | 0              |
| 8       | QAM256     | 498000000 Hz | -1.8 dBmV | 45.4 dB | 0            | 0              |

**Total Correctables** 2  
**Total Uncorrectables** 0

**Upstream Bonded Channels**

| Channel | US Channel Type | Symbol Rate   | Frequency   | Power     |
|---------|-----------------|---------------|-------------|-----------|
| 1       | ATDMA           | 2560 Ksym/sec | 48000000 Hz | 45.7 dBmV |
| 2       | ATDMA           | 2560 Ksym/sec | 44000000 Hz | 45.7 dBmV |
| 3       | ATDMA           | 2560 Ksym/sec | 52000000 Hz | 45.5 dBmV |
| 4       | ATDMA           | 2560 Ksym/sec | 56000000 Hz | 45.0 dBmV |

Downstream Frequency Select (in KHz)

Die Tabelle **Startup Procedure** zeigt die Prozesse an, die beim Startup des Kabelmodems erfolgt sind:

- **Acquire Downstream Channel:** Hier sollte die Frequenz des Downstreamkanals und Locked stehen. Das bedeutet, dass das Modem einen Downstreamkanal gefunden hat, mit dem Informationen aus dem Internet empfangen werden kann.
- **Connectivity State:** Sollte OK und Operational sein.
- **Configuration File:** Hier sollte OK stehen..
- **Security:** Hier sollte "Enabled" und "BPI+" stehen.

Die Tabelle **Downstream Bonded Channels** zeigt folgende Informationen zu den Downstream-Kanälen an:

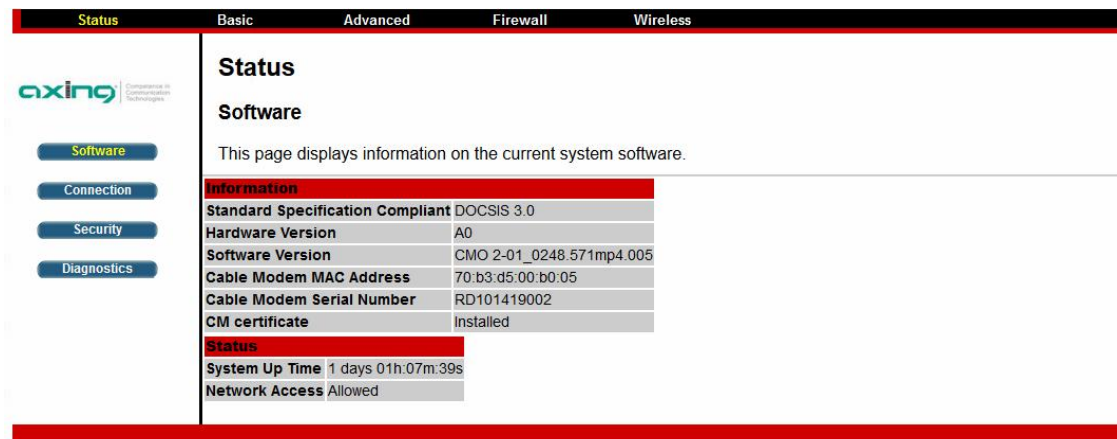
- Modulationsart in der Spalte **Modulation**
- Frequenz in der Spalte **Frequency**
- Pegel in der Spalte **Power**
- Signal-Rausch-Verhältnis (Signal to Noise Ratio) in der Spalte **SNR**
- In den Spalten **Correctables** und **Uncorrectables** stehen fehlerhafte Datenpakete, die während des Datenverkehrs korrigiert werden konnten bzw. nicht korrigiert werden konnten.

Die Tabelle **Upstream Bonded Channels** zeigt folgende Informationen zu den Upstream-Kanälen an:

- Multiplexverfahren innerhalb des Upstream-Kanals in der Spalte **US Channel Type**
- Die Symbolrate in der Spalte **Symbol Rate**
- Frequenz in der Spalte **Frequency**
- Pegel in der Spalte **Power**

## 4.1.2 Software

Diese Seite zeigt die Hardware- und Softwareversion des Kabelmodems in der folgenden Tabelle. Alle diese Informationen sind nur lesbar.



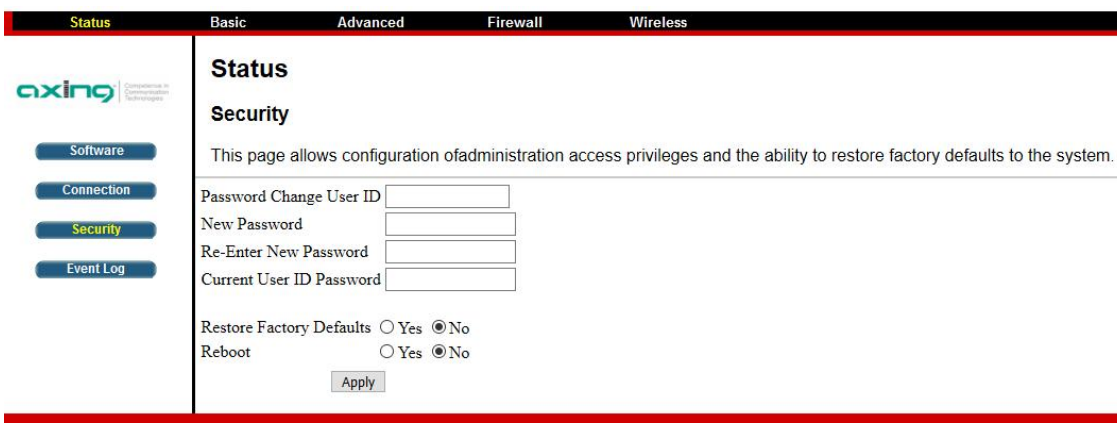
| Status   |                          |
|--|--------------------------|
| <b>Software</b>  |                          |
| This page displays information on the current system software. |                          |
| <b>Information</b>   |                          |
| Standard Specification Compliant                               | DOCSIS 3.0               |
| Hardware Version   | A0                       |
| Software Version   | CMO 2-01_0248.571mp4.005 |
| Cable Modem MAC Address  | 70:b3:d5:00:b0:05        |
| Cable Modem Serial Number                                      | RD101419002              |
| CM certificate   | Installed                |
| <b>Status</b>  |                          |
| System Up Time   | 1 days 01h:07m:39s       |
| Network Access   | Allowed                  |

### 4.1.2.1 Internetzugang bei einem Kabelnetzbetreiber

Wenn **Network Access** "Allowed" angezeigt wird, dann hat Ihr Kabelnetzbetreiber das CMO so konfiguriert, dass er über eine Internetverbindung verfügt. Wenn Netzwerkzugriff nicht erlaubt ist, haben Sie möglicherweise keinen Internetzugang. Wenden Sie sich bitte an Ihren Kabelnetzbetreiber, um Hilfe zu erhalten.

## 4.1.3 Security

Diese Seite ermöglicht die Konfiguration von Zugriffsrechten und bietet die Möglichkeit, die Werkseinstellungen des Systems wiederherzustellen.



**Security**

This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

Password Change User ID

New Password

Re-Enter New Password

Current User ID Password

Restore Factory Defaults ☐ Yes ☒ No

Reboot ☐ Yes ☒ No

- Geben Sie im Feld Password Change User ID den Benutzernamen ein, für den Sie das Passwort ändern möchten (z.B. AXING\_USER).
- Geben Sie im Feld New Password das neue Kennwort ein.
- Geben Sie im Feld Re-Enter New Password das neue Passwort erneut ein.
- Geben Sie im Feld Current User ID Password das bisherige Passwort ein.
- Klicken Sie anschließend auf **Apply**.

### 4.1.3.1 Werkseinstellungen wiederherstellen

- Aktivieren Sie bei Restore Factory Defaults die Option Yes.
- Klicken Sie anschließend auf **Apply**.

Die Konfiguration des Kabelmodems wird auf die Werkseinstellungen zurück gesetzt.

## 4.1.4 Diagnostics

Auf dieser Seite stehen zwei Diagnosewerkzeuge zur Verfügung:

- PING für das LAN
- Traceroute für das WAN

### 4.1.4.1 PING

The screenshot shows the 'Status' tab of the Axing web interface. The 'Diagnostics' section is active. The 'Utility' dropdown is set to 'Ping'. The 'Ping Test Parameter' section includes the following fields: 'Targets' (192.168.0.1), 'Ping Size' (64 bytes), 'No. of Pings' (3), and 'Ping Interval' (1000 ms). Below these fields are buttons for 'Start Test', 'Abort Test', and 'Clear Results'. A 'Results' section at the bottom shows 'Waiting for input...'.

→ Wählen Sie im Feld Utility das Diagnosewerkzeug Ping aus.

→ Geben Sie die Ping Test Parameters ein.

→ Klicken Sie auf Start Test.

Unter Results werden die Ergebnisse des Tests aufgelistet.

→ Sie können den Test mit Abort Test abbrechen oder mit Clear Results die Testergebnisse löschen.

### 4.1.4.2 Traceroute

The screenshot shows the 'Status' tab of the Axing web interface. The 'Diagnostics' section is active. The 'Utility' dropdown is set to 'Traceroute'. The 'Target Parameters' section includes the following fields: 'Targets' (192.168.0.1), 'Max Hops' (30), 'Data Size' (32 bytes), 'Base Port' (33434), and 'Resolve Host' (Off). Below these fields are buttons for 'Start Test' and 'Clear Results'. A 'Results' section at the bottom shows 'Waiting for input...'.

→ Wählen Sie im Feld Utility das Diagnosewerkzeug Traceroute aus.

→ Geben Sie die Target Parameters ein.

→ Klicken Sie auf **Start Test**.

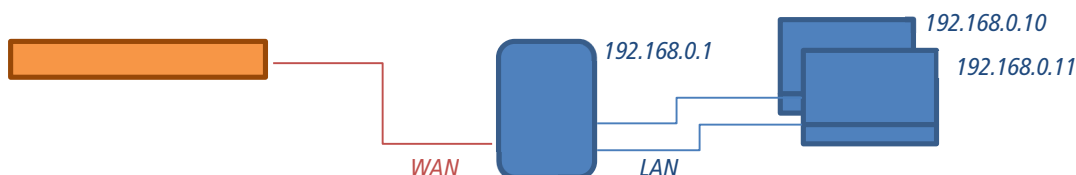
Unter **Results** werden die Ergebnisse des Tests aufgelistet.

→ Sie können mit **Clear Results** die Testergebnisse löschen.

## 4.2 Basic

Die Seite enthält die grundlegenden Funktionen des CMO 2-01 einschließlich Setup, DHCP und Backup.

### 4.2.1 Setup



Das WAN (Wide Area Network) ist das Netzwerk, das das CMO zum CMTS über die Koaxialleitung mit Hilfe des DOCSIS-Protokoll bildet.

Das LAN (Local Area Network) ist das Netzwerk, dass das CMO mit den angeschlossenen/verbundenen Ethernet- oder WLAN-Geräten mit Hilfe von TCP/IP bildet.

→ Im Bereich **LAN** kann die IP-Adresse des CMO im Local Area Network angepasst werden. Außerdem wird die MAC-Adresse angezeigt, die das CMO im LAN besitzt.

→ Wenn das CMO mit einem CMTS verbunden ist, wird im Bereich **WAN** die IP-Adresse des CMO im Wide Area Network angezeigt. Bei WAN Connection Type DHCP, wird diese vom DHCP-Server im CMTS vergeben. Außerdem wird die MAC-Adresse angezeigt, die das CMO im WAN besitzt.

→ Duration zeigt die Dauer der Verbindung zum CMTS an.

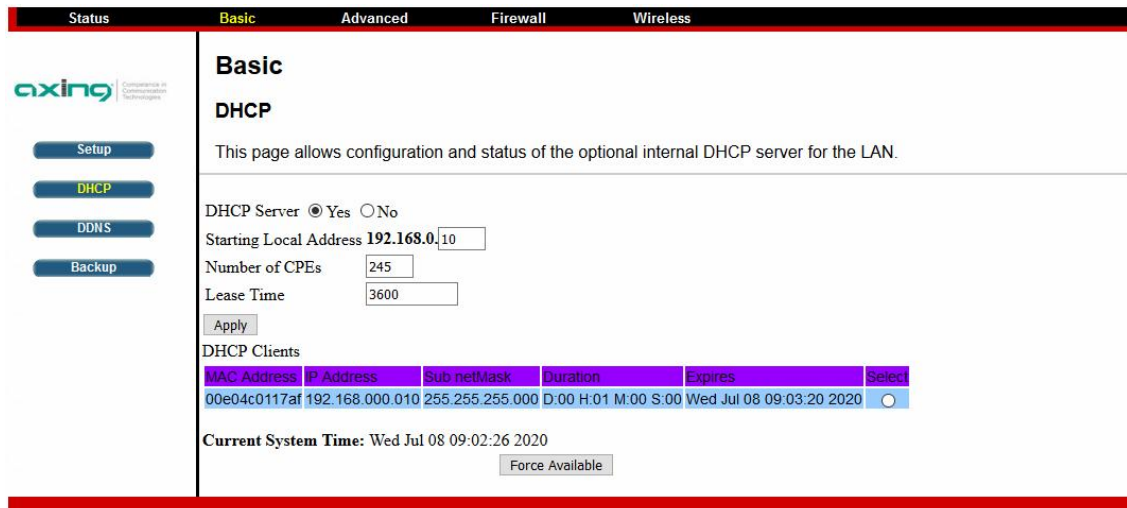
→ Das Feld Expires zeigt den Zeitpunkt, zu dem die Verbindung verfällt.

→ Mit **Release WAN Lease** wird die WAN-IP wieder als "verfügbar" freigegeben.

→ Mit **Renew WAN Lease** wird die Lease erneuert, also beim DHCP Server die Vergabe einer neuen IP Adresse angefragt.

## 4.2.2 DHCP

Auf der Seite können Sie die DHCP-Serverfunktion des CMO 2-01 aktivieren/deaktivieren. Wenn der DHCP-Server aktiviert ist, werden die von ihm vergebenen DHCP-Leases angezeigt.



**Status Basic Advanced Firewall Wireless**

**axing** Competence in Communication Technologies

**Setup DHCP DDNS Backup**

**Basic DHCP**

This page allows configuration and status of the optional internal DHCP server for the LAN.

DHCP Server ☒ Yes ☐ No

Starting Local Address

Number of CPEs

Lease Time

DHCP Clients

| MAC Address  | IP Address      | Sub netMask     | Duration            | Expires                  | Select                |
|--------------|-----------------|-----------------|---------------------|--------------------------|-----------------------|
| 00e04c0117af | 192.168.000.010 | 255.255.255.000 | D:00 H:01 M:00 S:00 | Wed Jul 08 09:03:20 2020 | <input type="radio"/> |

Current System Time: Wed Jul 08 09:02:26 2020

Der DHCP-Server des CMO stellt den angeschlossenen Geräten IP-Adressen zur Verfügung.

→ Diese IP-Adressen beginnen bei der Adresse, die Sie im Feld Starting Local Address festgelegt haben.

→ Um die maximale Anzahl von Geräten festzulegen, an die der CMO 2-01 IP-Adressen vergibt, geben Sie diese in das Feld Number of CPEs ein (Customer Premises Equipment).

Der DHCP-Server ordnet eine IP-Adresse mit einer Ablaufzeit zu. Standardmäßig sind im Feld Lease Time 3600 Sekunden eingetragen. Der DHCP-Server verfügt über einen automatischen Erneuerungsmechanismus, der ein Lease so lange verlängert, wie das zugehörige Gerät aktiv bleibt.

→ Klicken Sie anschließend auf Apply.

Die Tabelle DHCP Clients unten auf dieser Seite zeigt Informationen zu DHCP-Clients einschließlich deren IP- und MAC-Adressen für jeden PC. Da MAC-Adressen eindeutig und fest in der Hardware verankert sind, können Sie jedes aufgelistete Gerät anhand seiner MAC-Adresse identifizieren.

→ Um einen IP-Adressen-Lease zu kündigen, wählen Sie ihn in der Tabelle DHCP Clients aus und klicken Sie auf Force Available (Hinweis: Möglicherweise muss ein DHCP Renew auf diesem Gerät durchgeführt werden.)



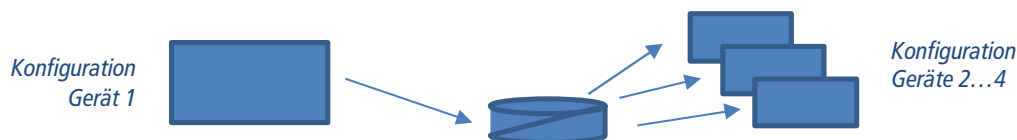
### 4.2.3 DDNS

Dynamisches DNS, DDNS oder DynDNS ist eine Technik, um Domains im Domain Name System (DNS) dynamisch zu aktualisieren. Um DDNS (Dynamisches Domains Name System) zu nutzen, müssen Sie bei einem DDNS Anbieter einen entsprechenden Dienst eingerichtet haben.

- Wählen Sie einen DDNS Service aus
- Geben Sie die Anmeldedaten für den DDNS Service in die Felder User Name und Password ein.
- Geben Sie den im Feld Host Name den Namen, den Sie beim DDNS-Service hinterlegt haben.
- Klicken Sie anschließend auf **Apply**.

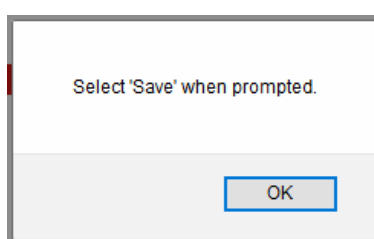
### 4.2.4 Backup/Restore

Die Konfiguration des CMO kann in eine Backup-Datei gespeichert werden. Dies kann als Sicherung der Daten verwendet werden oder zum Duplizieren einer Konfiguration auf mehrere Geräte.



#### 4.2.4.1 Backup

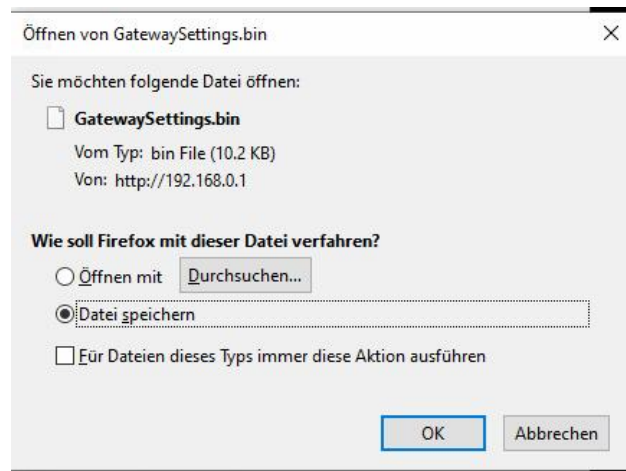
- Klicken sie auf **Backup**.
- Der folgende Dialog wird geöffnet.





→ Klicken Sie darin auf **OK**.

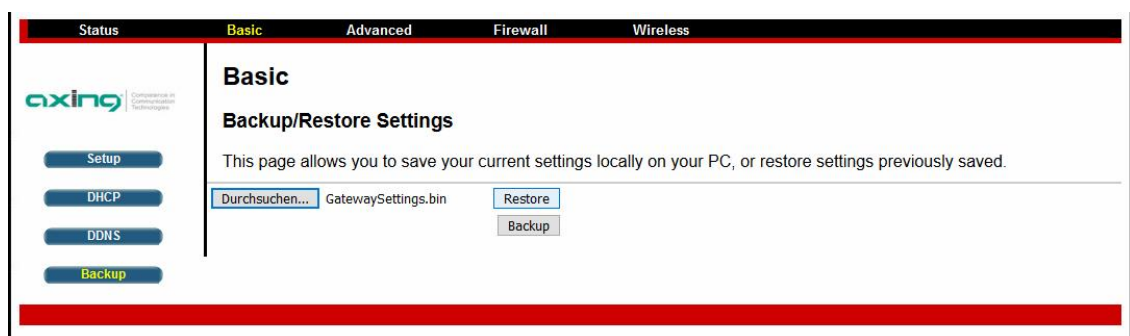
→ Wählen Sie anschließend Datei speichern und speichern Sie die Backup-Datei auf Ihrem PC.



→ Vergeben Sie einen sprechenden Namen, damit Sie die Datei später wiederfinden (Beispiel 20200716\_CMO\_Zimmer201.bin).

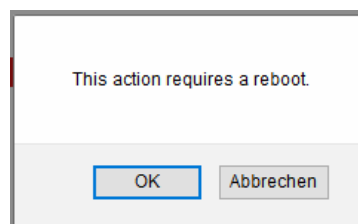
#### 4.2.4.2 Restore

→ Klicken Sie auf **Durchsuchen...** und wählen Sie eine Backup-Datei aus.



→ Klicken Sie auf **Restore**.

Die Folgende Meldung erscheint, die Sie darauf aufmerksam macht, dass das CMO anschließend neu gestartet wird.



→ Klicken Sie auf **OK**.

Die Backup-Konfiguration wird geladen und das CMO neu gestartet.

## 4.3 Advanced

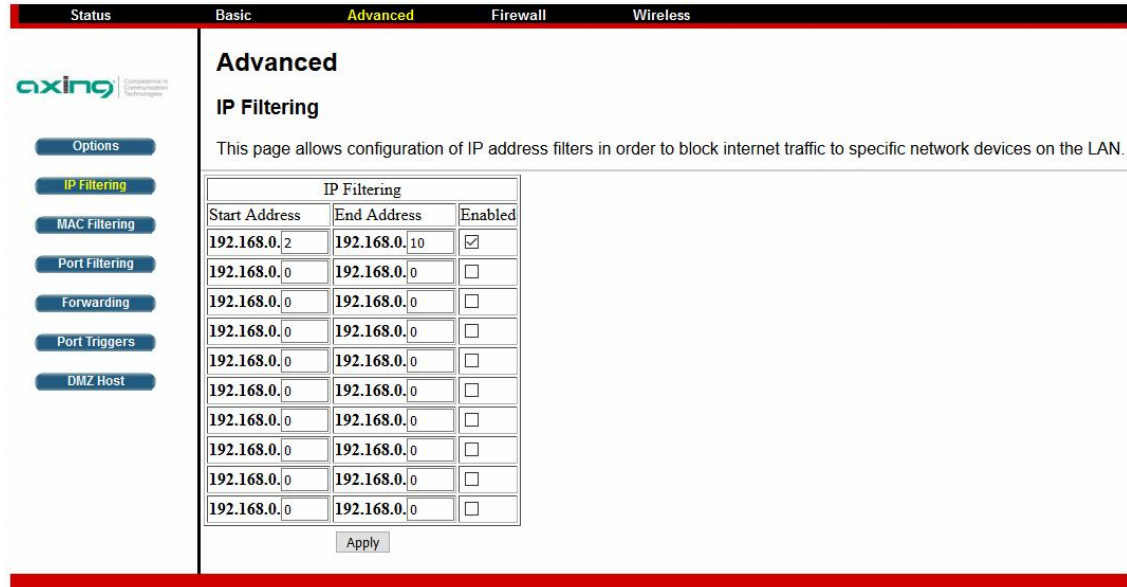
Auf der Seite können Sie einige erweiterte Funktionen des CMO 2-01 aktivieren/deaktivieren.

### 4.3.1 Options

- **WAN-Blocking:** Verhindert, dass andere auf der WAN-Seite in der Lage sind, Ihren CMO 2-01 anzupingen. Bei aktivierter WAN-Blockierung reagiert Ihr CMO 2-01 nicht auf empfangene Pings, wodurch Ihr Modem sozusagen "versteckt" wird.
  - **Isec PassThrough:** Ermöglicht den Durchlass von IPsec-Paketen zwischen WAN und LAN.
  - **PPTP PassThrough:** Ermöglicht den Durchgang von PPTP-Paketen zwischen WAN und LAN.
  - **Remote Config Management:** Um die Web-Management-Seiten Ihres CMO 2-01 von der WAN-Seite aus zugänglich zu machen. Der Zugriff auf die Seiten ist auf diejenigen beschränkt, die das Zugangspasswort des CMO 2-01 kennen, das Sie auf der Seite Status-Sicherheit festgelegt haben (siehe 4.1.3 auf Seite 12). Wenn Sie von einem Remote-Standort aus auf das CMO 2-01 zugreifen, müssen Sie den HTTP-Port 8080 und Ihre IP-Adresse verwenden. Dies ist die "WAN-IP-Adresse", die auf der Seite Basis-Setup angezeigt wird (siehe 4.2 auf Seite 14). Wenn diese IP-Adresse zum Beispiel 211.20.15.28 lautet, würden Sie `http:// 211.20.15.28:8080` eingeben, um die Web-Management-Seite des CMO 2-01 von einem anderen Standort aus zu erreichen.
  - **Multicast Enable:** Ermöglicht die Durchleitung von Multicast-Streams zwischen WAN und LAN. Möglicherweise müssen Sie dies aktivieren, um einige Arten von Broadcast-Streaming und -Inhalten im Internet zu sehen, wie z.B. die Web-Übertragung eines Live-Events.
  - **UPnP Enable:** UPnP (Universal Plug and Play) bietet umfassende Peer-to-Peer-Netzwerk-Konnektivität für PCs aller Art, intelligente Geräte und drahtlose Geräte.
- ➔ Aktivieren Sie die Option(en), die Sie verwenden möchten, und klicken Sie auf die Schaltfläche **Apply**.  
Bzw. deaktivieren Sie die Option(en), die Sie nicht verwenden möchten, und klicken Sie auf die Schaltfläche **Apply**.

### 4.3.2 IP Filtering

Die Seite ermöglicht es, PCs zu bestimmen, die keinen ausgehenden Zugriff auf das WAN (Internet) haben dürfen. Diese PCs können im LAN immer noch miteinander kommunizieren, aber Anfragen, die sie an Internet-Adressen senden, werden blockiert.



| IP Filtering  |              |                                     |
|---------------|--------------|-------------------------------------|
| Start Address | End Address  | Enabled                             |
| 192.168.0.2   | 192.168.0.10 | <input checked="" type="checkbox"/> |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |

Apply

Die PCs werden anhand von IP-Adressbereichen "herausgefiltert".

→ Geben Sie in die Felder Start Address und End Address den Adressbereiche ein.

→ Aktivieren Sie das Kontrollkästchen Enable.

→ Klicken Sie auf die Schaltfläche Apply.

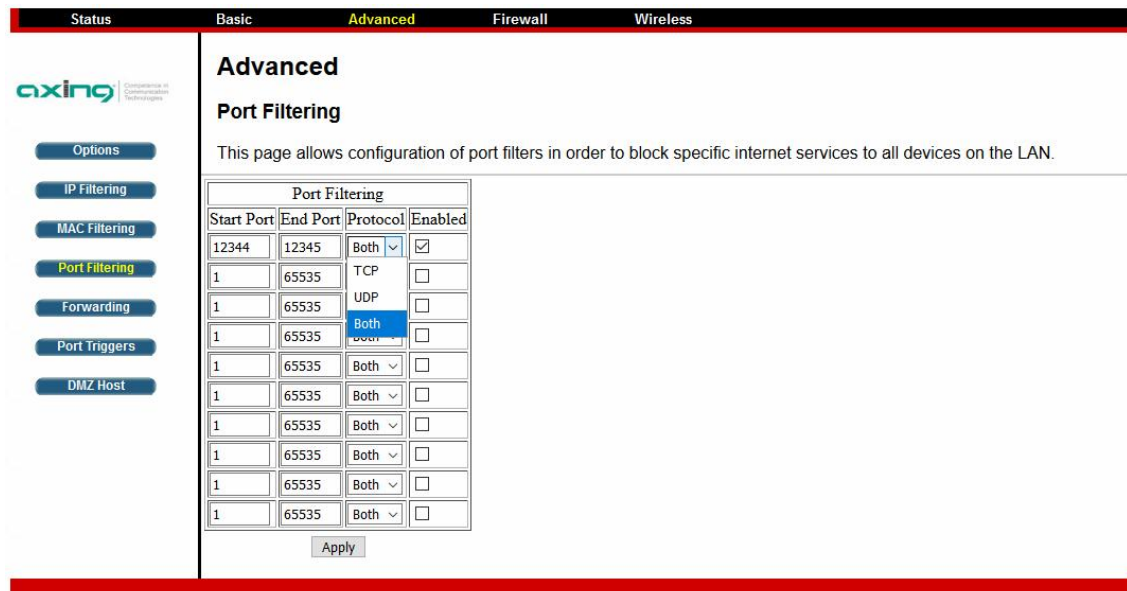
### 4.3.3 MAC Filtering

Die Seite ermöglicht es, PCs zu bestimmen, die keinen ausgehenden Zugriff auf das WAN (Internet) haben dürfen. Diese PCs können im LAN immer noch miteinander kommunizieren, aber Anfragen, die sie an WAN-Adressen senden, werden blockiert. Die PCs werden anhand ihrer MAC-Adresse "herausgefiltert".

- Geben Sie die MAC Address ein.
- Klicken Sie auf die Schaltfläche Add MAC Address.
- Um einem PC wieder Zugriff zu gewähren, markieren Sie dessen MAC Adresse und klicken Sie auf Remove MAC Address.
- Oder klicken Sie auf Clear All, um alle MAC-Adressen freizugeben.

#### 4.3.4 Port Filtering

Auf der Seite können Sie Ziel-Ports (Anwendungen) eingeben, mit denen Ihre LAN-PCs keine Verbindung aufbauen dürfen. Verbindungen, die Ihre LAN-PCs mit diesen Ports aufbauen wollen, werden blockiert. Sie könnten zum Beispiel den Zugang zum World Wide Web blockieren (HTTP-Port 80), aber trotzdem den E-Mail-Dienst zulassen (SMTP-Port 25 und POP3-Port 110).



The screenshot shows the Axing Firewall configuration interface. The top navigation bar includes tabs for Status, Basic, Advanced (selected), Firewall, and Wireless. On the left, a sidebar contains links for Options, IP Filtering, MAC Filtering, Port Filtering (selected), Forwarding, Port Triggers, and DMZ Host. The main content area is titled 'Advanced Port Filtering' and includes a description: 'This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.' Below this is a table for configuring port filters.

| Start Port | End Port | Protocol | Enabled                             |
|------------|----------|----------|-------------------------------------|
| 12344      | 12345    | Both     | <input checked="" type="checkbox"/> |
| 1          | 65535    | TCP      | <input type="checkbox"/>            |
| 1          | 65535    | UDP      | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |

An 'Apply' button is located at the bottom of the table.

- ➔ Um das Port-Filtering zu aktivieren, geben Sie den Start Port und den End Port für jeden Bereich ein (um nur einen Port zu blockieren, stellen Sie Start- und End Port gleich ein).
- ➔ Wählen Sie in der Dropdown-Liste sein Protokoll aus und aktivieren Sie das Kontrollkästchen in der Spalte Enable.
- ➔ Klicken Sie auf die Schaltfläche Apply.

### 4.3.5 Forwarding

Für die Kommunikation zwischen LAN und WAN erlaubt das CMO 2-01 normalerweise nur das Herstellen einer IP-Verbindung mit einem PC im WAN; Versuche eines PCs im WAN, eine Verbindung zu einem PC in Ihrem LAN herzustellen, werden ignoriert.

Manchmal kann es jedoch wünschenswert sein, dass jemand von außerhalb eine Verbindung zu einem bestimmten PC in Ihrem LAN herstellen kann, wenn der Zielpunkt (Anwendung) mit einem von Ihnen angegebenen Port übereinstimmt. Auf der Seite Forwarding können Sie bis zu 10 Regeln angeben.

Über die Forwarding-Seite können Sie lokale Dienste (Webserver, FTP-Server, Mailserver usw.) für Personen im Internet bereitstellen. Eine Tabelle mit häufig verwendeten Port-Nummern ist abgebildet.

**Advanced Forwarding**

This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Local IP: 192.168.0.2  
 Local Start Port: 12344  
 Local End Port: 12345  
 External Start Port: 12344  
 External End Port: 12345  
 Protocol: TCP  
 Description: Test  
 Enabled: On

Cancel Apply

| Application |  | Port |
|-------------|--|------|
| HTTP        |  | 80   |
| FTP         |  | 21   |
| TFTP        |  | 69   |
| SMTP        |  | 25   |
| POP3        |  | 110  |
| NNTP        |  | 119  |
| Telnet      |  | 23   |
| IRC         |  | 194  |
| SNMP        |  | 161  |
| Finger      |  | 79   |
| Gopher      |  | 70   |
| Whois       |  | 43   |
| rlogin      |  | 107  |
| LDAP        |  | 389  |
| UUCP        |  | 540  |

| Local       |            |          | External   |          |     | Protocol | Description | Enabled |        |
|-------------|------------|----------|------------|----------|-----|----------|-------------|---------|--------|
| IP Address  | Start Port | End Port | Start Port | End Port |     |          |             |         |        |
| 192.168.0.2 | 12344      | 12345    | 12344      | 12345    | TCP | Test     | Yes         | Edit    | Remove |

Remove All

→ Geben Sie die nötigen Parameter in die Felder Local IP bis Description für das Forwarding ein.

→ Setzen Sie Enable auf On.

→ Klicken Sie Apply.

Die Regel wird in die Tabelle am unteren Rand der Seite übernommen.

| Local       |            |          | External   |          | Protocol | Description | Enabled |      | Remove All |
|-------------|------------|----------|------------|----------|----------|-------------|---------|------|------------|
| IP Address  | Start Port | End Port | Start Port | End Port |          |             |         |      |            |
| 192.168.0.2 | 12344      | 12345    | 12344      | 12345    | TCP      | Test        | Yes     | Edit | Remove     |

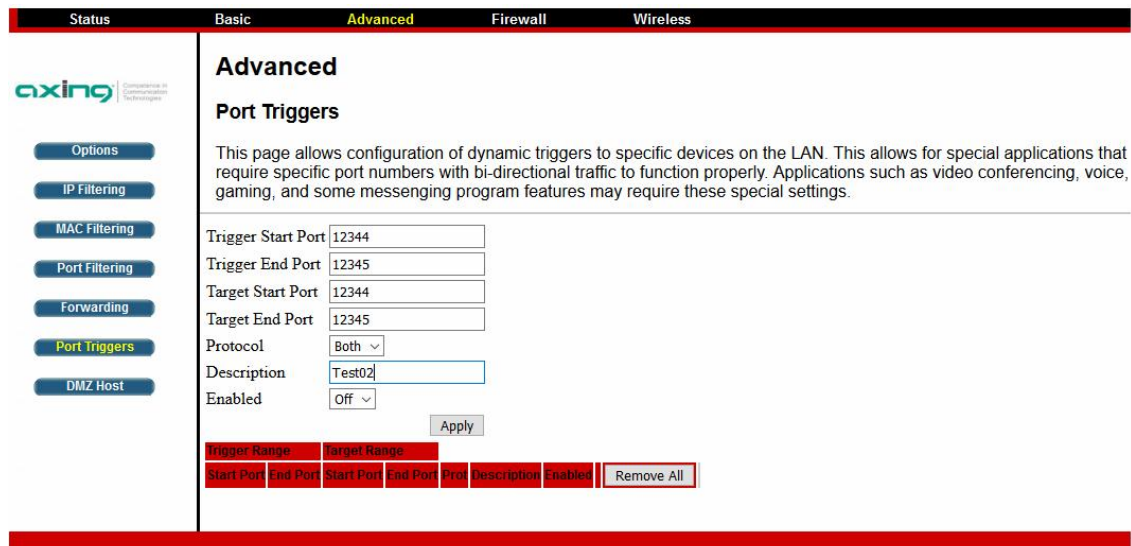
→ Klicken Sie in der Tabelle auf Edit, um eine Regel zu ändern.

→ Klicken Sie in der Tabelle auf Remove, um eine Regel zu löschen.

→ Klicken Sie in der Tabelle auf Remove All, um alle Regeln zu ändern.

### 4.3.6 Port Triggers

Die Seite ermöglicht es Ihnen, dynamische Trigger für bestimmte Geräte im LAN zu konfigurieren. Dies ermöglicht spezielle Anwendungen, die bestimmte Portnummern mit bidirektionalem Datenverkehr benötigen, um richtig zu funktionieren. Anwendungen wie Videokonferenzen, Sprache, Spiele und einige Messaging-Programmfunktionen erfordern möglicherweise diese speziellen Einstellungen.



**Advanced**

**Port Triggers**

This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Trigger Start Port: 12344  
 Trigger End Port: 12345  
 Target Start Port: 12344  
 Target End Port: 12345  
 Protocol: Both  
 Description: Test02  
 Enabled: Off

Apply

| Trigger Range |          | Target Range |          | Prot | Description | Enabled | Remove All  |
|---------------|----------|--------------|----------|------|-------------|---------|-------------|
| Start Port    | End Port | Start Port   | End Port |      |             |         |             |
| 12344         | 12345    | 12344        | 12345    | BOTH | Test02      | No      | Edit Remove |

→ Geben Sie die nötigen Parameter in die Felder Trigger Start Port bis Description für das Forwarding ein.

→ Setzen Sie Enable auf On.

→ Klicken Sie Apply.

Der Eintrag wird in die Tabelle am unteren Rand der Seite übernommen.

| Trigger Range |          | Target Range |          | Prot | Description | Enabled | Remove All |        |
|---------------|----------|--------------|----------|------|-------------|---------|------------|--------|
| Start Port    | End Port | Start Port   | End Port |      |             |         | Edit       | Remove |
| 12344         | 12345    | 12344        | 12345    | BOTH | Test02      | No      | Edit       | Remove |

→ Klicken Sie in der Tabelle auf Edit, um einen Eintrag zu ändern.

→ Klicken Sie in der Tabelle auf Remove, um einen Eintrag zu löschen.

→ Klicken Sie in der Tabelle auf Remove All, um alle Eintäge zu ändern.

### 4.3.7 DMZ Host

Auf der Seite können Sie ein bestimmtes Netzwerkgerät so konfigurieren, dass es direkt dem WAN (öffentliches Internet) zugänglich oder sichtbar ist. Wenn Sie einen Host in Ihrem lokalen Netzwerk als entmilitarisierte Zone (DMZ) einrichten, wird jeglicher Netzwerkverkehr, der nicht über die Portweiterleitungsfunktion an einen anderen Host umgeleitet wird, an die IP-Adresse dieses Hosts (PC) weitergeleitet. Damit wird ein PC in Ihrem LAN bezeichnet, der für alle PCs von der WAN-Seite aus für alle Ports erreichbar bleiben soll.

Wenn Sie zum Beispiel einen HTTP-Server auf diesem Rechner einrichten, kann jeder auf diesen HTTP-Server zugreifen, indem er die IP-Adresse Ihres CMO 2-01 als Ziel verwendet. Dies kann verwendet werden, wenn Anwendungen nicht mit Port-Triggern funktionieren. Die Einstellung "0" bedeutet NO DMZ PC.

## 4.4 Firewall

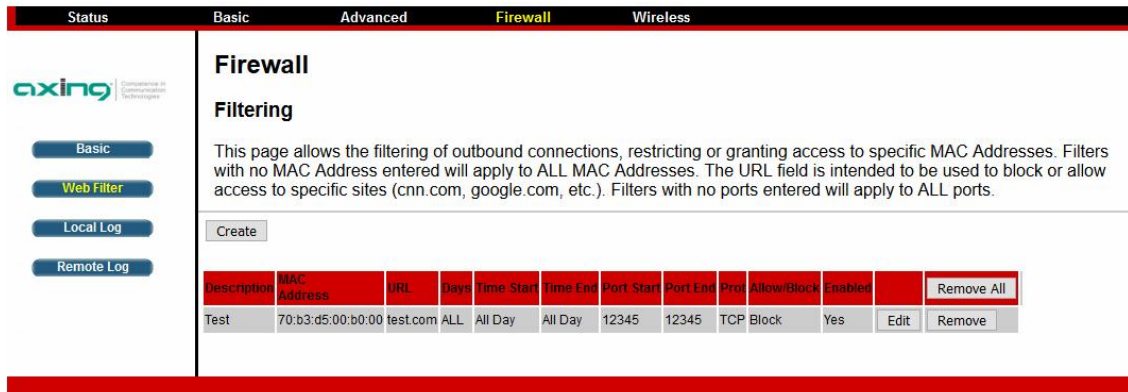
Der CMO 2-01 bietet eine integrierte Firewall-Funktion, mit der Sie das System vor Denial-of-Service (DoS)-Angriffen und anderen unerwünschten oder böswilligen Zugriffen auf Ihr LAN schützen können.

### 4.4.1 Basic



## 4.4.2 Web Filtering

Diese Seite erlaubt es, ausgehende Verbindungen zu filtern und den Zugriff auf bestimmte MAC-Adressen einzuschränken oder zu gewähren.



**Firewall Filtering**

This page allows the filtering of outbound connections, restricting or granting access to specific MAC Addresses. Filters with no MAC Address entered will apply to ALL MAC Addresses. The URL field is intended to be used to block or allow access to specific sites (cnn.com, google.com, etc.). Filters with no ports entered will apply to ALL ports.

Create

| Description | MAC Address       | URL      | Days | Time Start | Time End | Port Start | Port End | Prot | Allow/Block | Enabled |      |        |
|-------------|-------------------|----------|------|------------|----------|------------|----------|------|-------------|---------|------|--------|
| Test        | 70:b3:d5:00:b0:00 | test.com | ALL  | All Day    | All Day  | 12345      | 12345    | TCP  | Block       | Yes     | Edit | Remove |

→ Klicken Sie auf **Create**, um einen neuen Filter zu erstellen.

Die nachfolgend abgebildeten Felder werden eingeblendet.

Description

MAC Address

URL

Port Start

Port End

Protocol

Days

☐ Everyday ☒ Sunday ☐ Monday ☐ Tuesday

☐ Wednesday ☐ Thursday ☒ Friday ☒ Saturday

Time

☒ All day

Start:  (hour)  (min)

End:  (hour)  (min)

Allow/Block

Enabled

→ Geben Sie im Feld Description eine Beschreibung ein.

→ Geben Sie ggf. eine MAC-Adresse eines Geräts ein, für den der Filter gilt (z.B. Tablet eines Kindes).

Filter, in denen keine MAC-Adresse eingetragen ist, gelten für alle MAC-Adressen.

→ Geben Sie die URL ein, die blockiert oder zuzulassen werden soll.

→ Geben Sie einen Start- und einen End-Port ein.

Filter, in denen keine Ports angegeben sind, gelten für alle Ports.

→ Unter Days bzw. Time bestimmen Sie ggf. Wochentage oder Uhrzeiten, zu denen der Filter gültig ist.

→ Mit der Auswahl Allow/Block bestimmen Sie, ob der Filter einen Zugriff auf eine Website blockt oder zulässt.

→ Mit Enabled bestimmen Sie, ob der Filter aktiv (On) oder inaktiv (Off) ist.

→ Klicken Sie auf **Apply**.

Der Filter wird unten in die Tabelle übernommen.

**Bei bereits bestehenden Filter:**

→ Klicken Sie in der Tabelle auf **Edit**, um einen Filter zu ändern.

→ Klicken Sie in der Tabelle auf **Remove**, um einen Filter zu löschen.

→ Klicken Sie in der Tabelle auf **Remove All**, um alle Filter zu ändern.

#### 4.4.3 Local Log

Auf der Seite werden eventuelle Angriffe auf die Firewall protokolliert. Diese Angriffsaufzeichnungen sind in der Tabelle unten auf der Seite sichtbar.

**Firewall**

**Local Log**

This page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system.

Contact Email Address

SMTP Server Name

SMTP Username

SMTP Password

E-mail Alerts ☒ Enable

| Description  | Count | Last Occurrence | Target | Source |
|--|-------|-----------------|--------|--------|
| <input type="button" value="E-Mail Log"/> <input type="button" value="Clear Log"/> |       |                 |        |        |

- Geben Sie die E-Mail-Adresse und die SMTP-Zugangsdaten der Person an, die Benachrichtigungen über versuchte Firewall-Verletzungen erhalten soll.
- Geben Sie die Adressen im Standard-Internet-E-Mail-Adressformat ein, z. B. yourname@yourcompany.com. Aktivieren Sie dann das Kontrollkästchen Enable, um die Benachrichtigungsfunktion zu aktivieren.
- Klicken Sie auf E-Mail-Log, um das E-Mail-Protokoll sofort zu senden.
- Klicken Sie auf Clear Log, um die Tabelle mit den Einträgen zu löschen.

#### 4.4.4 Remote Log

Diese Seite ermöglicht optionale Konfigurationen von Ereignissen, die an einen lokalen SysLog-Server gesendet werden sollen.

- Aktivieren Sie unter Send selected events die Ereignisse, die protokolliert werden sollen.
- Geben Sie die IP-Adresse des SysLog-Servers in ihrem Netzwerk ein.
- Klicken Sie Apply.

**Firewall**

**Remote Log**

This page allows optional configuration of events to be sent to a local SysLog server.

Send selected events

☒ Permitted Connections

☒ Blocked Connections

☐ Known Internet Attacks


☐ Product Configuration Events

to SysLog server at 192.168.0.

## 4.5 Wireless

### 4.5.1 Radio

Auf der Seite werden die HF-Einstellungen für das WLAN-Funknetz vorgenommen.

| Status  | Basic | Advanced | Firewall | Wireless |
|---|-------|----------|----------|----------|
|    |       |          |          |          |
| <div> <div>Radio</div> <div>Primary Network</div> <div>Guest Network</div> <div>Access Control</div> <div>WMM</div> <div>Bridging</div> </div>  |       |          |          |          |
| <h3>Wireless</h3> <h4>802.11 Radio</h4> <p>This page allows configuration of the Wireless Radio including current channel number.</p> <div> <div>Wireless Interfaces:</div> <div>2.4 GHz (70:B3:D5:00:80:09)</div> </div> <div> <div>Wireless</div> <div>Enabled</div> </div> <div> <div>Country</div> <div>E0</div> </div> <div> <div>802.11 Band</div> <div>2.4 Ghz</div> <div>Current : 2.4 GHz</div> </div> <div> <div>802.11 n-mode</div> <div>Auto</div> </div> <div> <div>Bandwidth</div> <div>40 Mhz</div> <div>Current : 20MHz</div> </div> <div> <div>Sideband for Control Channel (40 Mhz only)</div> <div>Upper</div> <div>Current : None</div> </div> <div> <div>Control Channel</div> <div>Auto</div> <div>Current : 6 ***Interference Level: Acceptable</div> </div> <div> <div>Regulatory Mode</div> <div>Off</div> </div> <div> <div>TPC Mitigation (db)</div> <div>0 (Off)</div> </div> <div> <div>OBSS Coexistence</div> <div>1 (Enabled)</div> </div> <div> <div>STBC Tx</div> <div>Auto</div> </div> <div> <div>Apply</div> <div>Restore Wireless Defaults</div> <div>Scan Wireless APs</div> </div> |       |          |          |          |

## 4.5.2 Primary Network

Das 802.11 Primary Network ermöglicht die Konfiguration des primären drahtlosen Netzwerks und seiner Sicherheitseinstellungen.

**axing** Computer & Communications Technologies

**Wireless**

**802.11 Primary Network**

This page allows configuration of the Primary Wireless Network and its security settings.

CMO 2-01-B005-G (70:B3:D5:00:B0:09)

PrimaryNetwork: ☐ Enabled

Network Name (SSID):

Closed Network: ☐ Disabled

Mode Required:

AP Isolate: ☐ Disabled

Automatic Security Configuration: ☐ Disabled

WPA: ☐ Disabled

WPA-PSK: ☐ Enabled

WPA2: ☐ Disabled

WPA2-PSK: ☐ Enabled

WPA/WPA2 Encryption:

WPA Pre-Shared Key:  ☐ Show Key

RADIUS Server:

RADIUS Port:

RADIUS Key:

Group Key Rotation Interval:

WPA/WPA2 Re-auth Interval:

WEP Encryption: ☐ Disabled

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Current Network Key:

PassPhrase:

→ Wenn AP-Isolation aktiviert ist, können Geräte im selben drahtlosen Netzwerk nicht miteinander kommunizieren.

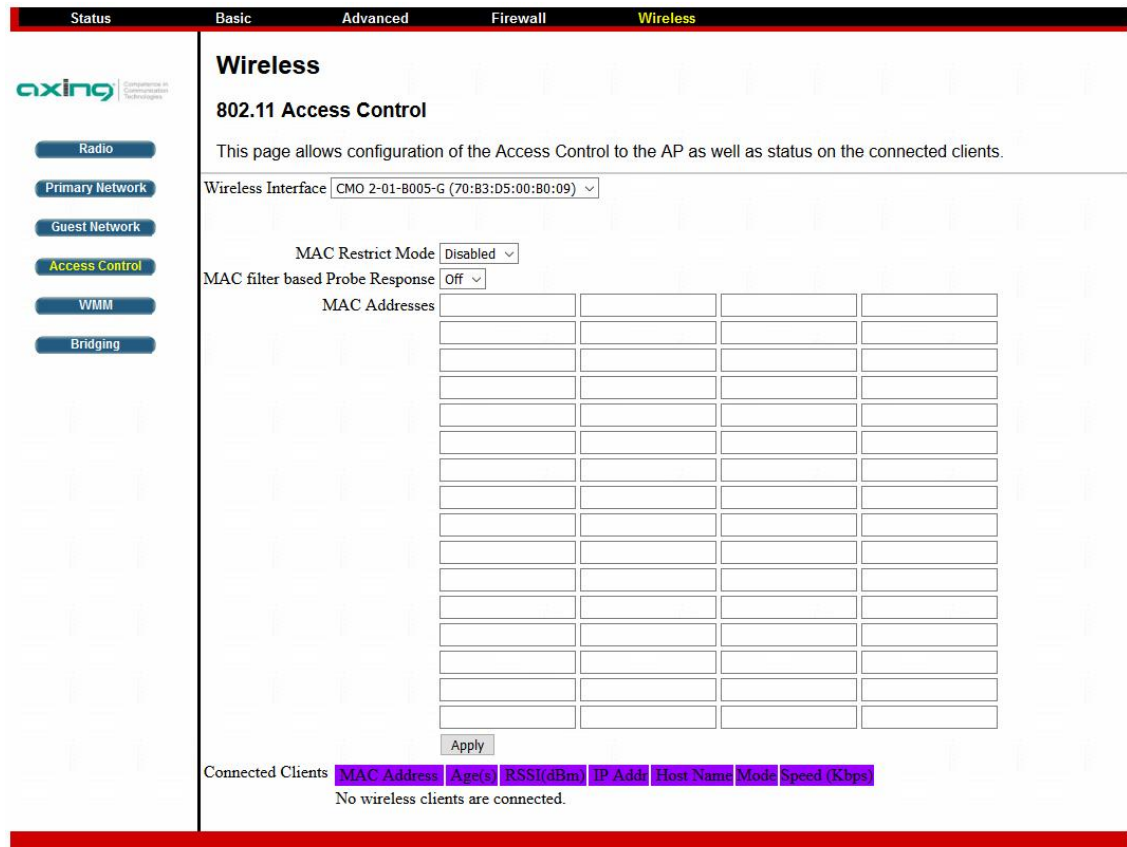
## 4.5.3 Guest Network

Diese Seite ermöglicht die Konfiguration eines Gastnetzwerks.

Die Einstellungen sind die selben, wie beim Primary Network.

## 4.5.4 Access Control

Diese Seite ermöglicht die Konfiguration einer Zugriffskontrolle und zeigt die aktuell verbundenen Geräte (Clients) an.



**Wireless**

**802.11 Access Control**

This page allows configuration of the Access Control to the AP as well as status on the connected clients.

Wireless Interface: CMO 2-01-8005-G (70:B3:D5:00:B0:09) ▼

MAC Restrict Mode: Disabled ▼

MAC filter based Probe Response: Off ▼

MAC Addresses

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Apply

Connected Clients

| MAC Address                        | Age(s) | RSSI(dBm) | IP Addr | Host Name | Mode | Speed (Kbps) |
|------------------------------------|--------|-----------|---------|-----------|------|--------------|
| No wireless clients are connected. |        |           |         |           |      |              |

### 4.5.4.1 MAC Restrict Mode

→ Wählen Sie zunächst ob Sie Mit Hilfe des MAC-Filterings Geräte den Zugriff erlauben oder verweigern wollen.

- Disabled: Schaltet die MAC-Filterung aus.
- Allow: Erlaubt den Zugriff für Geräte mit den angegebenen MAC-Adressen.
- Deny: Verweigert den Zugriff für Geräte mit den angegebenen MAC-Adressen.

→ Geben Sie dann die MAC-Adressen der Geräte ein und klicken Sie **Apply**.

→ Klicken Sie auf **Remove**, um das entsprechende Gerät aus der Liste zu entfernen.

### 4.5.4.2 Connected Clients

In der Tabelle Connected Clients sind die Geräte aufgeführt, die momentan mit dem CMO 2-01 über WLAN verbunden sind.

#### 4.5.5 WMM

Diese Seite ermöglicht die Konfiguration der Wi-Fi Multimedia-QoS. Wi-Fi Multimedia Quality of Service (WMM QoS) priorisiert Sprach- und Videodatenverkehr über das WLAN.

- Wählen Sie im Feld WMM Support die Option On, um Wireless Multimedia zu ermöglichen.  
Die WMM-Unterstützung hilft bei verschiedenen Arten des Datenverkehrs wie Sprach-, Video- und Hintergrunddiensten.
- No Acknowledgement: Dies ist ein Funktionsmerkmal, das die Fehlerfreiheit der übertragenen Daten verbessert. Diese Option ist im Allgemeinen nur notwendig, wenn sich viele weitere WLAN-Netzwerke in Umgebung befinden.
- Power Save Support: Der Sinn dieser Einstellung besteht darin, dass der Router die Daten in eine Warteschlange stellt, während sich Ihre mobilen Geräte im Energiesparmodus befinden. Der Zweck besteht darin, die Akkus für die Geräte zu schonen, die auf Akkustrom angewiesen sind.

#### 4.5.6 Bridging

Diese Seite ermöglicht die Konfiguration von WDS-Funktionen (Wireless Distribution System).

Mithilfe eines Wireless Distribution Systems lassen sich WLANs durch die funkbasierte Verbindung von WLAN-Accesspoints erweitern und größere Bereiche abdecken, ohne dass eine Kabelverbindung zwischen den Accesspoints notwendig ist.

- Wählen Sie im Auswahlfeld Wireless Bridging die Option Enabled.
- Tragen Sie als Remote Bridges die WLAN-MAC-Adresse der Geräte ein.  
Sie können bis zu 4 Bridge-Geräte eingeben
- Klicken Sie Apply.

## 5 Technische Daten

### 5.1 CMO 1-01

|   |  |
|---|--|
| <b>Downstream</b>                               |  |
| Datenrate                                       | Max. 320 Mbps @ DOCSIS<br>Max. 400 Mbps @ EuroDOCSIS                                       |
| Frequenzbereich                                 | 108...1002 MHz   |
| Kanalbandbreite                                 | 6 MHz @ DOCSIS<br>8 MHz @ EuroDOCSIS   |
| Kanalbündelung                                  | ≤8   |
| Eingangspegel                                   | -15 dBmV...+15 dBmV  |
| Demodulation                                    | QAM64, QAM256  |
| <b>Upstream</b>                                 |  |
| Datenrate                                       | 120 Mbps @ TDMA<br>160 Mbps @ S-CDMA   |
| Frequenzbereich                                 | 5...42 MHz @ DOCSIS<br>5...65 MHz @ EuroDOCSIS   |
| Kanalbandbreite                                 | 200/400/800/1600/3200/6400 KHz   |
| Ausgangspegel                                   | 8...58 dBmV @ QPSK<br>8...54 dBmV @ 64 QAM<br>8...54 dBmV @ 32 QAM<br>8...53 dBmV @ S-CDMA |
| Kanalbündelung                                  | ≤4   |
| Modulation                                      | QPSK, QAM8, QAM16, QAM32, QAM64, QAM128<br>(SCDMA)   |
| <b>Schnittstellen</b>                           |  |
| Ethernet-Anschlüsse (LAN)                       | 1 × RJ 45  |
| Ethernet-Standards                              | IEEE 802.3 10Base-T   802.3u 100Base-TX   802.3ab<br>1000Base-T (GigE)                     |
| Unterstützte Transportprotokolle                | IP, TCP, UDP, ARP  |
| Unterstützte Anwendungsprotokolle               | HTTP, ICMP, DHCP, TFTP, SNMP   |
| DOCSIS  | F-Buchse (75 Ohm)  |
| <b>Allgemein</b>                                |  |
| Betriebsspannung                                | 12 VDC   |
| Betriebstemperaturbereich                       | 0...40 °C  |
| Lagertemperaturbereich                          | -20...70 °C  |
| Betriebs-Luftfeuchtigkeit (nicht kondensierend) | 10...90%   |
| Maße (B × H × T) ca.                            | 160 × 125 × 32,5 mm  |
| Gewicht   | 200 g  |
| <b>Externes Zubehör</b>                         |  |
| Steckernetzteil                                 | 100...240 V/50...60 Hz   12 V=1 A  |

## 5.2 CMO 2-01

|  |  |
|--|--|
| <b>Downstream</b>                                  |  |
| Datenrate  | Max. 320 Mbps @ DOCSIS<br>Max. 400 Mbps @ EuroDOCSIS                                       |
| Frequenzbereich                                    | 108...1002 MHz   |
| Kanalbandbreite                                    | 6 MHz @ DOCSIS<br>8 MHz @ EuroDOCSIS   |
| Kanalbündelung                                     | ≤8   |
| Eingangspegel                                      | -15 dBmV...+15 dBmV  |
| Demodulation                                       | QAM64, QAM256  |
| <b>Upstream</b>                                    |  |
| Datenrate  | 120 Mbps @ TDMA<br>160 Mbps @ S-CDMA   |
| Frequenzbereich                                    | 5...42 MHz @ DOCSIS<br>5...65 MHz @ EuroDOCSIS   |
| Kanalbandbreite                                    | 200/400/800/1600/3200/6400 KHz   |
| Ausgangspegel                                      | 8...58 dBmV @ QPSK<br>8...54 dBmV @ 64 QAM<br>8...54 dBmV @ 32 QAM<br>8...53 dBmV @ S-CDMA |
| Kanalbündelung                                     | ≤4   |
| Modulation   | QPSK, QAM8, QAM16, QAM32, QAM64, QAM128 (SCDMA)  |
| <b>Schnittstellen</b>                              |  |
| Ethernet-Anschlüsse (LAN)                          | 2 × RJ 45  |
| Ethernet-Standards                                 | IEEE 802.3 10Base-T   802.3u 100Base-TX   802.3ab 1000Base-T (GigE)                        |
| WLAN-Standard                                      | IEEE 802.11b/g/n   |
| WLAN-Band  | 2.4 GHz single-band  |
| WLAN-Signalrate                                    | 300 Mbps   |
| WLAN-Verschlüsselung                               | WPA/WPA2   |
| Unterstützte Transportprotokolle                   | IP, TCP, UDP, ARP, TR-069  |
| Unterstützte Anwendungsprotokolle                  | HTTP, ICMP, DHCP, TFTP, SNMP   |
| DOCSIS   | F-Buchse (75 Ohm)  |
| <b>Allgemein</b>                                   |  |
| Betriebsspannung                                   | 12 VDC   |
| Betriebstemperaturbereich                          | 0...40 °C  |
| Lagertemperaturbereich                             | -10...60 °C  |
| Betriebs-Luftfeuchtigkeit<br>(nicht kondensierend) | 10...90%   |
| Maße (B × H × T) ca.                               | 167 × 125 × 38 mm  |
| Gewicht  | 320 g  |
| <b>Externes Zubehör</b>                            |  |
| Steckernetzteil                                    | 110...240 V/50...60 Hz   12 V=1,5 A  |







# CMO 1-01 | CMO 2-01

## DOCSIS/EuroDOCSIS cable modem

### Operation instructions



## Table of contents

|       |                                      |    |
|-------|--------------------------------------|----|
| 1     | Product description .....            | 4  |
| 1.1   | Field of application .....           | 4  |
| 1.1.1 | Typical application.....             | 4  |
| 1.1.2 | Additional Application.....          | 4  |
| 1.2   | Scope of delivery.....               | 5  |
| 1.3   | Requirements.....                    | 5  |
| 1.4   | LEDs on the front panel .....        | 6  |
| 1.4.1 | CMO 1-01.....                        | 6  |
| 1.4.2 | CMO 2-01.....                        | 7  |
| 2     | Installation .....                   | 8  |
| 2.1   | Connections CMO 1-01.....            | 8  |
| 2.2   | Connections CMO 2-01.....            | 9  |
| 2.3   | WiFi connection to CMO 2-01:.....    | 9  |
| 3     | Configuration .....                  | 10 |
| 3.1   | TCP/IP configuration .....           | 10 |
| 3.2   | Login to the CMO x-01 .....          | 10 |
| 4     | User Interface of the CMO 2-01 ..... | 11 |
| 4.1   | Status.....                          | 11 |
| 4.1.1 | Connection .....                     | 11 |
| 4.1.2 | Software.....                        | 12 |
| 4.1.3 | Security.....                        | 12 |
| 4.1.4 | Diagnostics .....                    | 13 |
| 4.2   | Basic.....                           | 14 |
| 4.2.1 | Setup .....                          | 14 |
| 4.2.2 | DHCP.....                            | 15 |
| 4.2.3 | DDNS.....                            | 15 |
| 4.2.4 | Backup/Restore.....                  | 16 |
| 4.3   | Advanced.....                        | 17 |
| 4.3.1 | Options.....                         | 17 |
| 4.3.2 | IP Filtering .....                   | 18 |
| 4.3.3 | MAC Filtering .....                  | 19 |
| 4.3.4 | Port Filtering.....                  | 19 |
| 4.3.5 | Forwarding .....                     | 20 |
| 4.3.6 | Port Triggers.....                   | 21 |
| 4.3.7 | DMZ Host .....                       | 22 |
| 4.4   | Firewall .....                       | 22 |
| 4.4.1 | Basic.....                           | 22 |
| 4.4.2 | Web Filtering.....                   | 23 |
| 4.4.3 | Local Log .....                      | 24 |
| 4.4.4 | Remote Log .....                     | 24 |
| 4.5   | Wireless .....                       | 25 |
| 4.5.1 | Radio .....                          | 25 |
| 4.5.2 | Primary Network .....                | 26 |
| 4.5.3 | Guest Network .....                  | 26 |
| 4.5.4 | Access Control .....                 | 27 |
| 4.5.5 | WMM .....                            | 28 |
| 4.5.6 | Bridging.....                        | 28 |
| 5     | Technical data .....                 | 29 |
| 5.1   | CMO 1-01 .....                       | 29 |
| 5.2   | CMO 2-01 .....                       | 30 |



## WARNING

- Observe the safety instructions supplied with the device! They are also available at the following Internet address: [https://download.axing.com/BAs/Sicherheitshinweise\\_9sprachig.pdf](https://download.axing.com/BAs/Sicherheitshinweise_9sprachig.pdf)
- Use the device only as described in these operating instructions and in particular in accordance with the state of the art. If the device is used for other purposes, no warranty will be assumed!



### EU Declaration of Conformity:

Hereby AXING AG declares that the marked products comply with the valid guidelines.

CMO 2-01: Hereby AXING AG declares that the device is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: <https://axing.com/en/downloads/ce/>



WEEE Nr. DE26869279 | Electrical and electronic components must not be disposed of as residual waste, it must be disposed of separately.



## 1.2 Scope of delivery

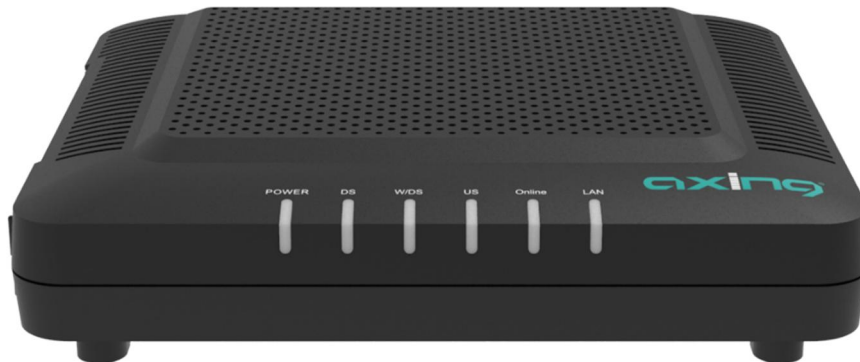
- Cable modem CMO 1-01 or CMO 2-01
- Ethernet cable
- 12 VDC power adapter for power supply
- Quick start guide

## 1.3 Requirements

- PC/Notebook which supports TCP/IP protocol for Configuration.
- PC/Notebook with an Ethernet port supports 10Base-T/100Base-TX and Gigabit Ethernet.

## 1.4 LEDs on the front panel






### 1.4.1 CMO 1-01



| Name          | Colour | Behavior | Meaning                                      |
|---------------|--------|----------|--|
| <b>POWER</b>  | Green  | On       | Device switched on                           |
|               |        | Off      | Device switched off or power failure         |
| <b>DS</b>     | Green  | Blinking | Downstream scanning                          |
|               |        | On       | Downstream locked                            |
|               |        | Off      | Downstream idle or channel bonding active    |
| <b>W/DS</b>   | Green  | On       | Downstream locked,<br>channel bonding active |
|               |        | Off      | Channel bonding not active                   |
| <b>US</b>     | Green  | Blinking | Upstream scanning                            |
|               |        | On       | Upstream locked                              |
|               |        | Off      | Upstream idle                                |
|               | Blue   | On       | Upstream locked,<br>channel bonding active   |
| <b>Online</b> | Green  | Blinking | Cable modem provisioning                     |
|               |        | On       | Cable modem online                           |
|               |        | Off      | Cable modem offline                          |
| <b>LAN</b>    | Green  | On       | Ethernet connected                           |
|               |        | Blinking | Data in traffic                              |
|               |        | Off      | Ethernet disconnected                        |



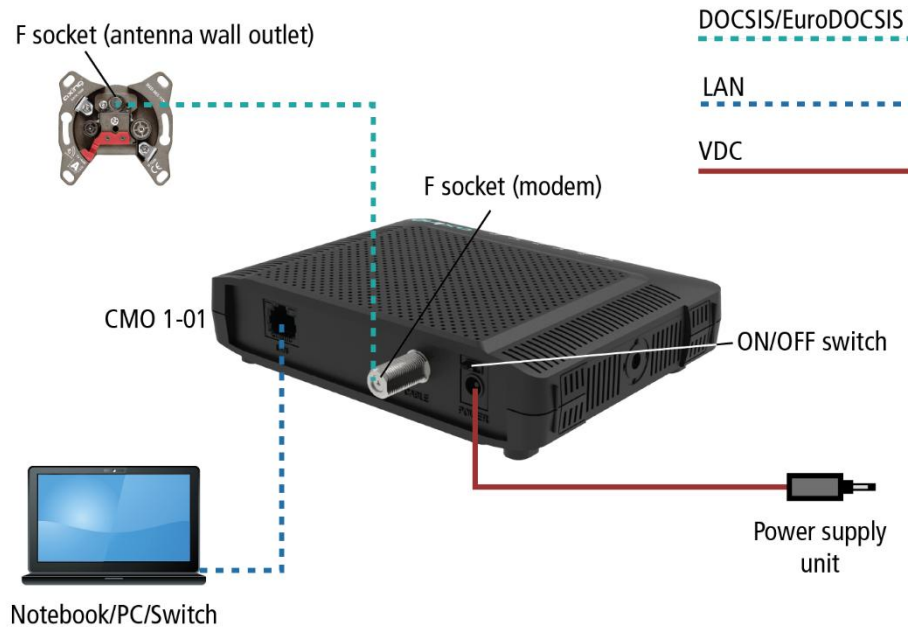
### 1.4.2 CMO 2-01

| LED   | Name         | Colour          | Behavior | Meaning  |
|---|--------------|-----------------|----------|--|
| <br><br>    | POWER        | Green           | On       | Device switched on   |
|   |              |                 | Off      | Device switched off or power failure                             |
|   |              |                 | Blinking | Downstream scanning  |
|   | DS           | Green           | On       | Downstream locked  |
|   |              |                 | Off      | Downstream idle  |
|   |              | Orange          | On       | Channel bonding active   |
|   |              |                 | Off      | Channel bonding not active                                       |
| <br><br> | US           | Green           | Blinking | Upstream scanning  |
|   |              |                 | On       | Upstream locked  |
|   |              |                 | Off      | Upstream idle  |
|   | ONLINE       | Green           | On       | Channel bonding active   |
|   |              |                 | Off      | Channel bonding not active                                       |
|   |              |                 | Blinking | Cable modem provisioning   |
| <b>LINK 1</b><br><b>LINK 2</b>  | LAN1<br>LAN2 | Green or Orange | On       | Cable modem online   |
|   |              |                 | Off      | Cable interface idle   |
|   |              |                 | On       | Ethernet connected<br>Green = 1000-Mbit/s<br>Orange = 100-Mbit/s |
|   |              |                 | Blinking | Data in traffic  |
|   |              |                 | Off      | Ethernet not connected   |
| <br><br><b>WPS</b>   | Wi-Fi        | Green           | On       | WiFi enabled   |
|   |              |                 | Blinking | WiFi data in traffic   |
|   |              |                 | Off      | WiFi disabled  |
|   | WPS          | Green           | Blinking | WPS in paring  |
|   |              |                 | On       | WPS enabled  |
|   |              |                 | Off      | WPS disabled   |



## 2 Installation

### 2.1 Connections CMO 1-01



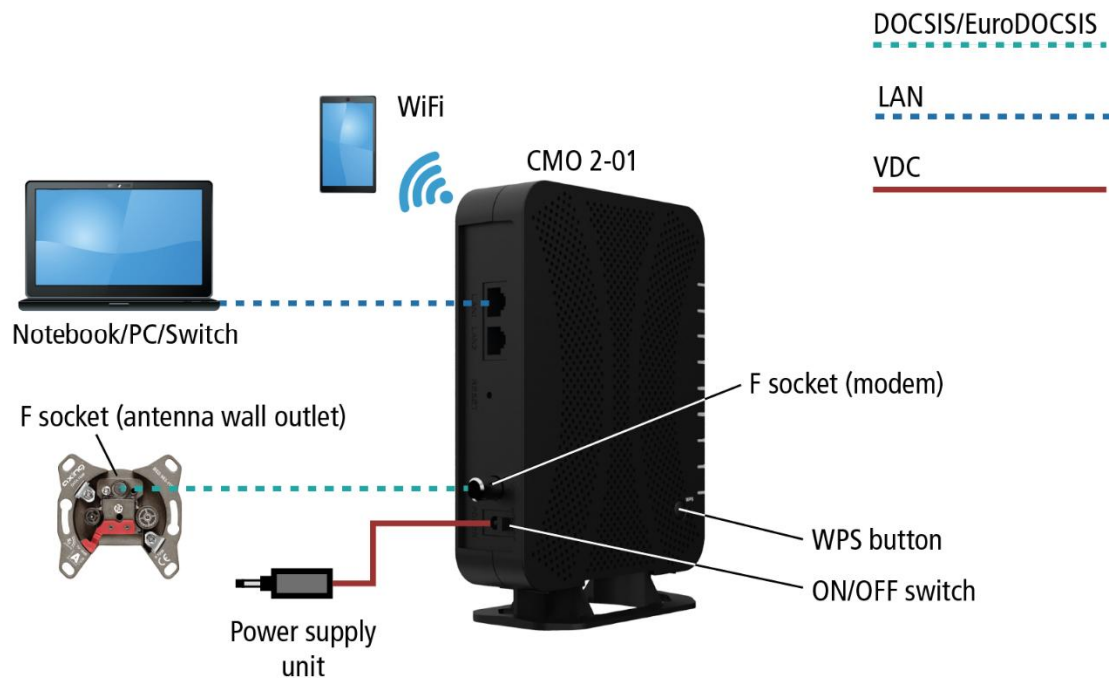
- ➔ Connect the DATA connector (F-female) of the antenna wall outlet to the F connector of the CMO 1-01.
- ➔ Use a highly shielded connection cable with F plugs.
- ➔ Connect the supplied AC adapter to the DC connector of the modem.
- ➔ Plug the power supply unit into the mains socket.
- ➔ Switch on the cable modem.

The power LED lights up permanently.

During the boot process, all other LEDs are blinking.

After booting, the downstream channel scan starts.

## 2.2 Connections CMO 2-01



- ➔ Connect the DATA connector (F-female) of the antenna wall outlet to the F connector of the CMO 2-01.
  - ➔ Use a highly shielded connection cable with F plugs.
  - ➔ Connect the supplied AC adapter to the DC connector of the modem.
  - ➔ Plug the power supply unit into the mains socket.
  - ➔ Switch on the cable modem.
- The power LED lights up permanently.
- During the boot process, several other LEDs are blinking.
- After booting, the Downstream channel scan starts.

## 2.3 WiFi connection to CMO 2-01:

### 2.3.1.1 By entering WiFi name and password:

The factory WiFi name (SSID) and password (WPA Pre-Shared Key) are printed on the unit's nameplate.

- ➔ Enter the SSID and password on your notebook, smartphone, or tablet.

### 2.3.1.2 By WPS button (WiFi Protected Setup, not compatible with Apple® devices):

- ➔ Log in to the configuration interface as described later (<http://192.168.100.1>).
  - ➔ Go to the page **Wireless** > **Primary Network**.
  - ➔ On the right side of the page select in the drop down menu Automatic Security Configuration the option WPS.
  - ➔ Click Apply to enable the WPS function.
  - ➔ Press the WPS button on the CMO 2-01 for less than 5 seconds<sup>1</sup>.
- The WPS LED starts to blink.
- ➔ Connect your device to the cable modem. If necessary, follow the operating instructions of your device.

<sup>1</sup> Press the WPS button more than 5 seconds will turn on or turn off WiFi.

## 3 Configuration

### 3.1 TCP/IP configuration

The TCP/IP protocol must be correctly installed and configured on your computer.

- ➔ Select Start, then select Settings > Network and Internet.
- ➔ Select Ethernet, then select the Ethernet network you are connected to.
- ➔ Under IP Assignment, select Edit.
- ➔ Under Edit IP Settings, select Automatic (DHCP).
- ➔ Connect the Ethernet interface of your computer to the Ethernet interface of the CMO x-01. Use the supplied Ethernet cable or a similar cable with RJ45 connectors.

### 3.2 Login to the CMO x-01

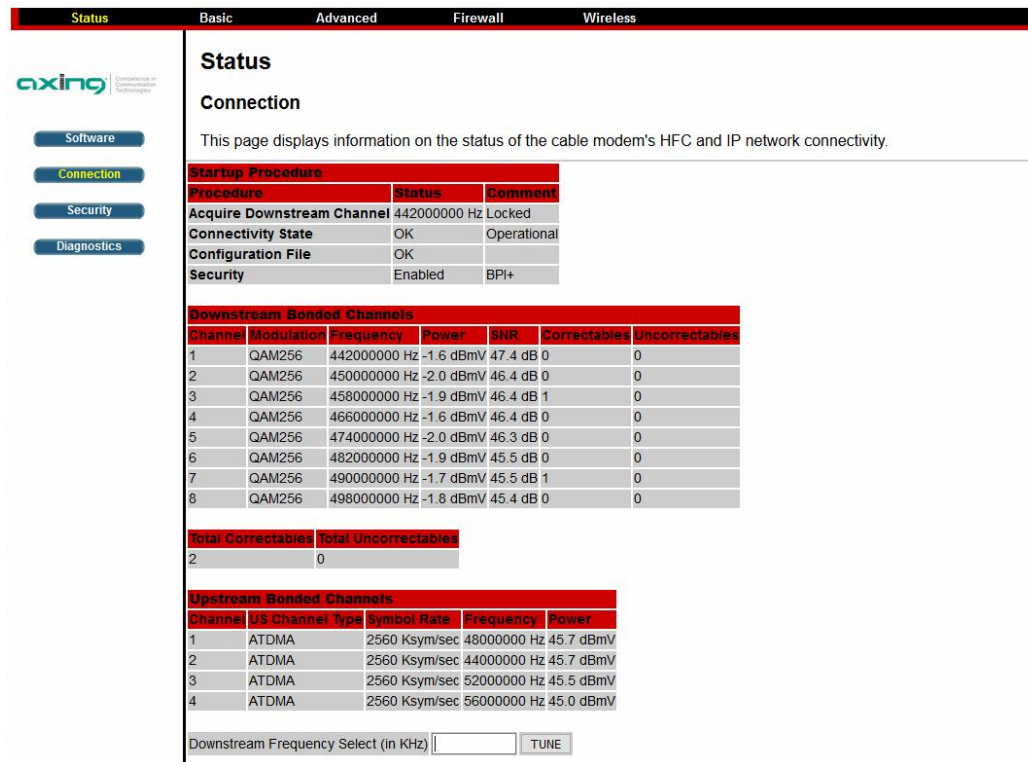
- ➔ Open your web browser.
  - You may receive an error message because your computer is not connected to the Internet.
- ➔ Type the default IP address of the CMO `http://192.168.100.1` and press Enter.
- ➔ Enter the following access data at the prompt:
  - Username: `AXING_USER`
  - Password: `u$erPassw0rd` (0 = zero)
- ➔ Press Enter.
- ➔ The Status page of the GUI is shown in the Browser (see 4.1.1 on page 11).

## 4 User Interface of the CMO 2-01

### 4.1 Status

#### 4.1.1 Connection

This page shows the cable modem connection status including Downstream and Upstream.



The screenshot shows the 'Status' page of the axing interface. The 'Connection' tab is selected. The page displays information about the cable modem's HFC and IP network connectivity.

**Startup Procedure**

| Procedure                  | Status              | Comment     |
|----------------------------|---------------------|-------------|
| Acquire Downstream Channel | 442000000 Hz Locked |             |
| Connectivity State         | OK                  | Operational |
| Configuration File         | OK                  |             |
| Security                   | Enabled             | BPI+        |

**Downstream Bonded Channels**

| Channel | Modulation | Frequency    | Power     | SNR     | Correctables | Uncorrectables |
|---------|------------|--------------|-----------|---------|--------------|----------------|
| 1       | QAM256     | 442000000 Hz | -1.6 dBmV | 47.4 dB | 0            | 0              |
| 2       | QAM256     | 450000000 Hz | -2.0 dBmV | 46.4 dB | 0            | 0              |
| 3       | QAM256     | 458000000 Hz | -1.9 dBmV | 46.4 dB | 1            | 0              |
| 4       | QAM256     | 466000000 Hz | -1.6 dBmV | 46.4 dB | 0            | 0              |
| 5       | QAM256     | 474000000 Hz | -2.0 dBmV | 46.3 dB | 0            | 0              |
| 6       | QAM256     | 482000000 Hz | -1.9 dBmV | 45.5 dB | 0            | 0              |
| 7       | QAM256     | 490000000 Hz | -1.7 dBmV | 45.5 dB | 1            | 0              |
| 8       | QAM256     | 498000000 Hz | -1.8 dBmV | 45.4 dB | 0            | 0              |

**Total Correctables**: 2  
**Total Uncorrectables**: 0

**Upstream Bonded Channels**

| Channel | US Channel Type | Symbol Rate   | Frequency   | Power     |
|---------|-----------------|---------------|-------------|-----------|
| 1       | ATDMA           | 2560 Ksym/sec | 48000000 Hz | 45.7 dBmV |
| 2       | ATDMA           | 2560 Ksym/sec | 44000000 Hz | 45.7 dBmV |
| 3       | ATDMA           | 2560 Ksym/sec | 52000000 Hz | 45.5 dBmV |
| 4       | ATDMA           | 2560 Ksym/sec | 56000000 Hz | 45.0 dBmV |

Downstream Frequency Select (in KHz):

The Startup Procedure table shows the processes that took place when the modem was started:

- **Acquire Downstream Channel**: This should show the frequency of the downstream channel and Locked. This means that the modem has found a downstream channel that can be used to receive information from the Internet.
- **Connectivity State**: Should be OK and Operational.
- **Configuration File**: This should read OK.
- **Security**: This should read "Enabled" and "BPI+".

The **Downstream Bonded Channels** table shows the following information about the downstream channels:

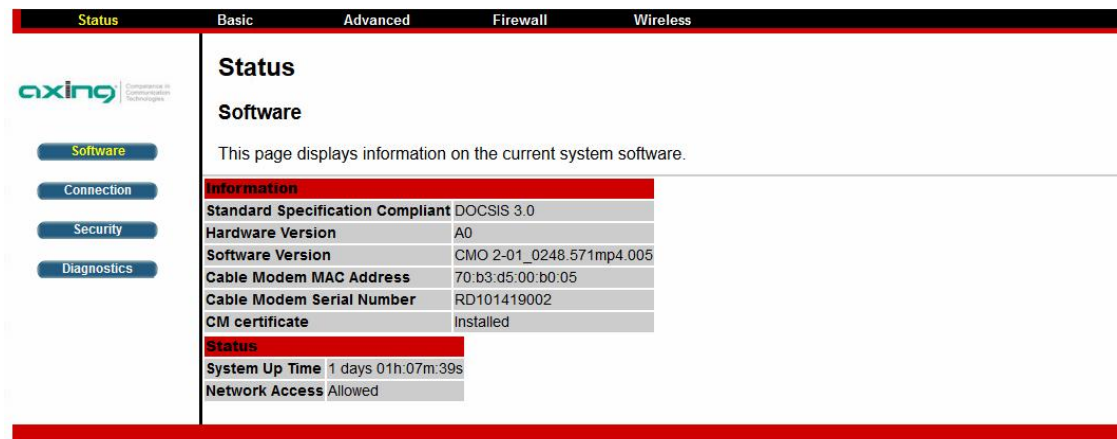
- Modulation type in the **Modulation** column
- Frequency in the **Frequency** column
- Level in the **Power** column
- Signal to Noise Ratio in the **SNR** column
- The **Correctables** and **Uncorrectables** columns contain incorrect data packets that could or could not be corrected during the data traffic.

The table **Upstream Bonded Channels** displays the following information about the upstream channels:

- Multiplexing within the upstream channel in the **US Channel Type** column
- The symbol rate in the **Symbol Rate** column
- Frequency in the **Frequency** column
- Level in the **Power** column

## 4.1.2 Software

This page shows the cable modem hardware and software version as the following table. All those information are read only.



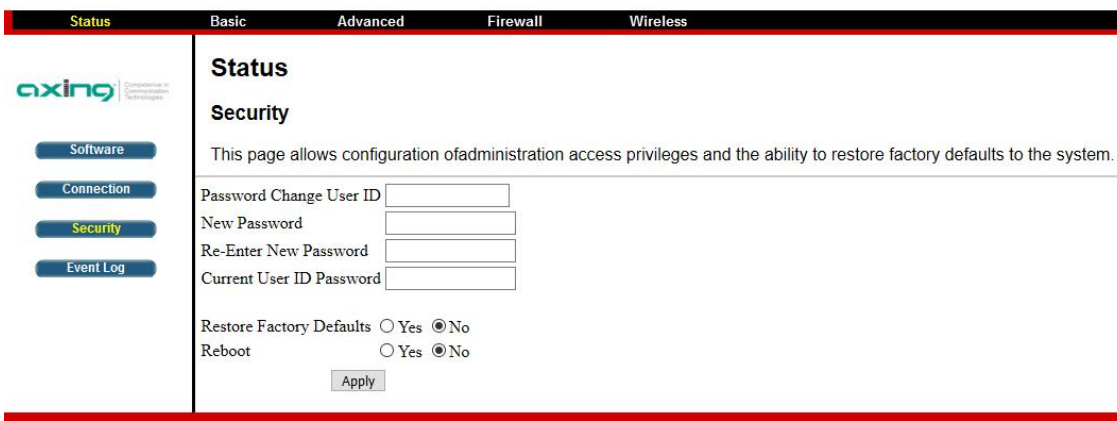
| Status   |                          |
|--|--------------------------|
| <b>Software</b>  |                          |
| This page displays information on the current system software. |                          |
| <b>Information</b>   |                          |
| Standard Specification Compliant                               | DOCSIS 3.0               |
| Hardware Version   | A0                       |
| Software Version   | CMO 2-01_0248.571mp4.005 |
| Cable Modem MAC Address  | 70:b3:d5:00:b0:05        |
| Cable Modem Serial Number                                      | RD101419002              |
| CM certificate   | Installed                |
| <b>Status</b>  |                          |
| System Up Time   | 1 days 01h:07m:39s       |
| Network Access   | Allowed                  |

### 4.1.2.1 Internet access with a cable network operator

If Network Access shows "Allowed," then your cable network operator has configured the CMO 2-01 to have Internet connectivity. If Network Access shows otherwise, you may not have Internet access, and please contact your cable network operator for assistance.

## 4.1.3 Security

This page allows the configuration of access privileges and offers the possibility to restore the factory settings of the system.



**Security**

This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

Password Change User ID

New Password

Re-Enter New Password

Current User ID Password

Restore Factory Defaults ☐ Yes ☒ No

Reboot ☐ Yes ☒ No

- In the Password Change User ID field, enter the user name for which you want to change the password (for example, AXING\_USER).
- In the New Password field, enter the new password.
- In the Re-Enter New Password field, enter the new password again.
- In the Current User ID Password field, enter the previous password.
- Then click Apply.

### 4.1.3.1 Restore factory settings

- For Restore Factory Defaults, enable the Yes option.
- Then click Apply.

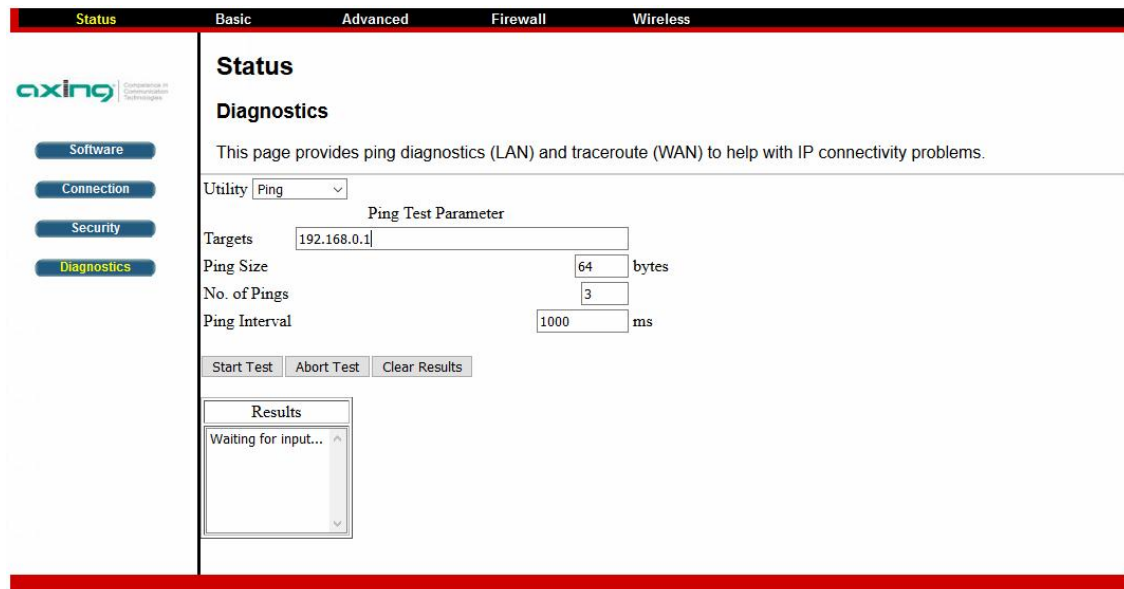
The gateway configuration is reset to the factory defaults.

## 4.1.4 Diagnostics

Two diagnostic tools are available on this page:

- PING for the LAN
- Traceroute for the WAN

### 4.1.4.1 PING



The screenshot shows the 'Status' tab of the axing interface. The 'Diagnostics' section is active, displaying the 'Ping' utility. The 'Ping Test Parameter' section includes fields for 'Targets' (192.168.0.1), 'Ping Size' (64 bytes), 'No. of Pings' (3), and 'Ping Interval' (1000 ms). Below these are buttons for 'Start Test', 'Abort Test', and 'Clear Results'. A 'Results' section at the bottom shows 'Waiting for input...'.

→ In the Utility field, select the Ping diagnostic tool.

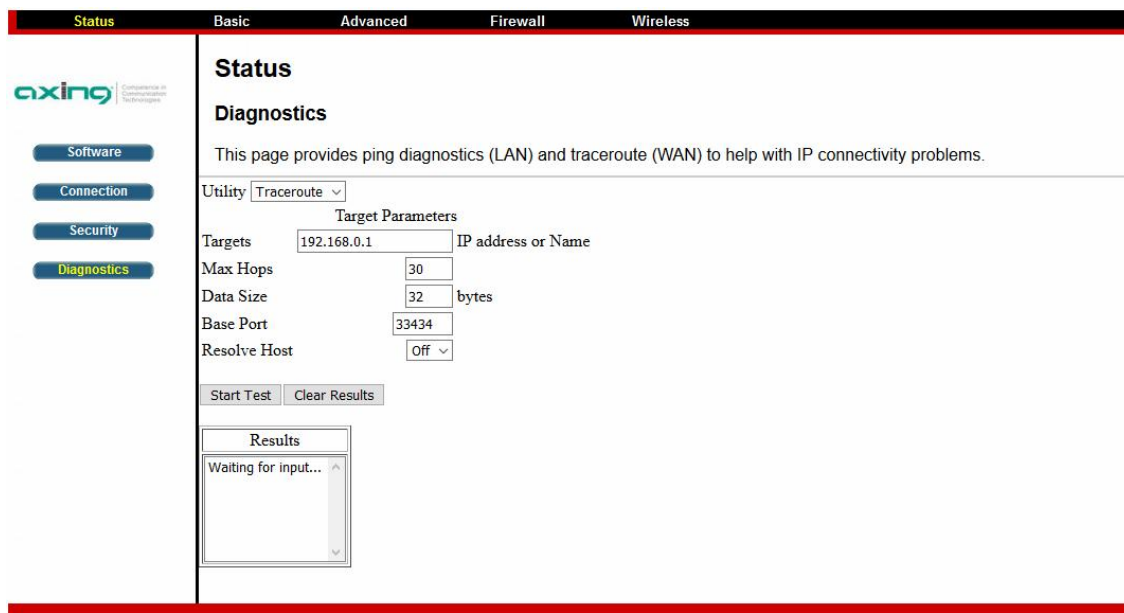
→ Enter the Ping Test Parameters.

→ Click Start Test.

→ The results of the test are listed under Results.

→ You can abort the test with Abort Test or clear the test results with Clear Results.

### 4.1.4.2 Traceroute



The screenshot shows the 'Status' tab of the axing interface. The 'Diagnostics' section is active, displaying the 'Traceroute' utility. The 'Target Parameters' section includes fields for 'Targets' (192.168.0.1), 'Max Hops' (30), 'Data Size' (32 bytes), 'Base Port' (33434), and 'Resolve Host' (Off). Below these are buttons for 'Start Test' and 'Clear Results'. A 'Results' section at the bottom shows 'Waiting for input...'.

→ In the Utility field, select the Traceroute diagnostic tool.

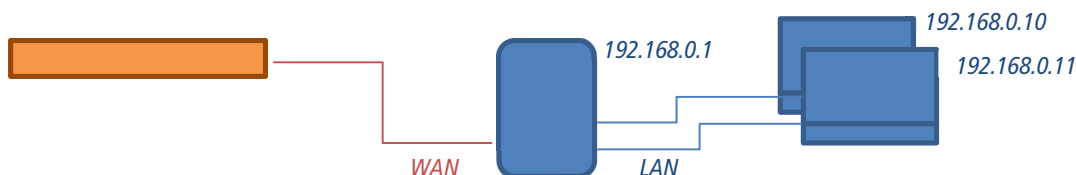
→ Enter the Target Parameters.

- Click Start Test.
- The results of the test are listed under Results.
- You can delete the test results by clicking Clear Results.

## 4.2 Basic

The Basic page contains the basic features of CMO 2-01 including Setup, DHCP and Backup.

### 4.2.1 Setup



The WAN (Wide Area Network) is the network that establishes the CMO to the CMTS over the coaxial line using the DOCSIS protocol.

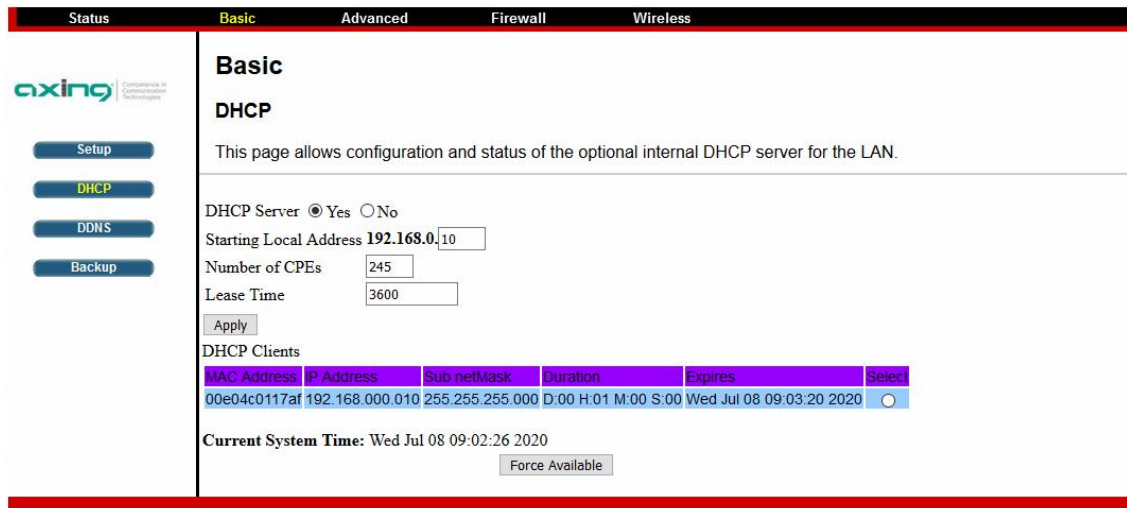
The LAN (Local Area Network) is the network that the CMO establishes with the attached/connected Ethernet or WiFi devices using TCP/IP.

- In the LAN section, the IP address of the CMO in the Local Area Network can be adjusted. The MAC address that the CMO has in the LAN is also displayed.
- In the WAN section, if the CMO is connected to a CMTS, the IP address of the CMO in the Wide Area Network is displayed. For WAN Connection Type DHCP, this is assigned by the DHCP server in the CMTS. The MAC address that the CMO has in the WAN is also displayed.
- Duration shows the duration of the connection to the CMTS.
- The Expires field shows the time at which the connection expires.
- With Release WAN Lease the WAN IP is released as "available" again.
- With Renew WAN Lease the lease is renewed, i.e. the DHCP server is requested to assign a new IP address.



## 4.2.2 DHCP

The **DHCP** page allows you to activate/deactivate the DHCP server function of the CMO 2-01. If the DHCP server is activated, the DHCP leases it has provided are displayed.



The screenshot shows the axing DHCP configuration page. The left sidebar has buttons for Setup, DHCP (highlighted), DDNS, and Backup. The main content area is titled 'Basic DHCP' and includes a description: 'This page allows configuration and status of the optional internal DHCP server for the LAN.' Below this, there are fields for 'DHCP Server' (Yes/No radio buttons), 'Starting Local Address' (192.168.0.10), 'Number of CPEs' (245), and 'Lease Time' (3600). An 'Apply' button is present. A table titled 'DHCP Clients' shows one client with MAC address 00e04c0117af, IP address 192.168.0.10, and a 'Select' button. At the bottom, it shows 'Current System Time: Wed Jul 08 09:02:26 2020' and a 'Force Available' button.

The DHCP server of the CMO provides the IP addresses of the connected devices.

→ This IP addresses start at the address you set in **Starting Local Address** field.

→ To set the maximum number of devices to which the CMO 2-01 will issue IP addresses, enter it in the Number of CPEs (Customer Premises Equipment).

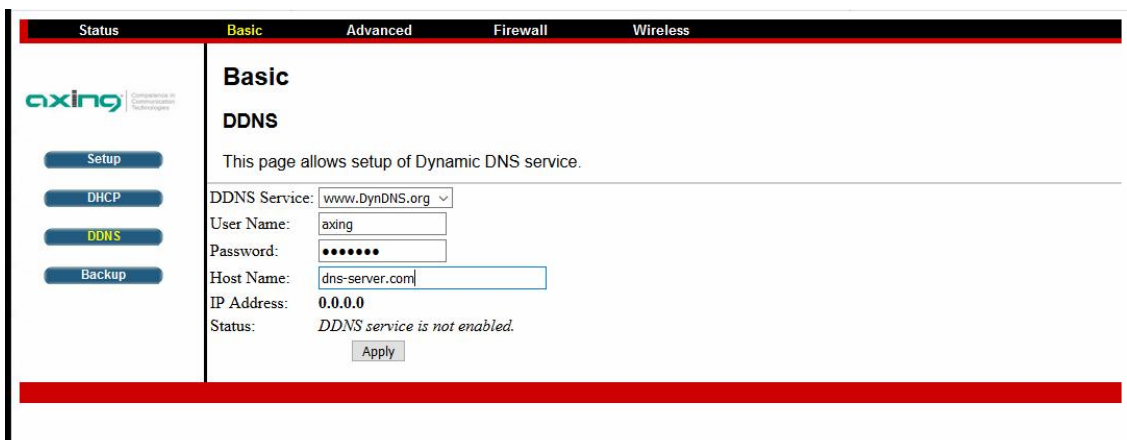
The DHCP server leases an IP address with an expiration time. The CMO 2-01 provides leases for 3600 seconds (default), and has an automatic renewal mechanism that will keep extending a lease as long as the associated device remains active.

The table DHCP Clients on the bottom of this page shows the information of DHCP clients including the IP and MAC addresses of each PC. Since MAC addresses are unique and permanently fixed into hardware, you can identify any device listed by its MAC address.

→ To cancel an IP address lease, **Select** it in the DHCP Clients table and click the **Force Available** button (Note: It may be necessary to perform a DHCP Renew on this device)

## 4.2.3 DDNS

Dynamic DNS, DDNS or DynDNS is a technique for dynamically updating domains in the Domain Name System (DNS). To use DDNS (Dynamic Domains Name System), you must have set up an appropriate service with a DDNS provider.



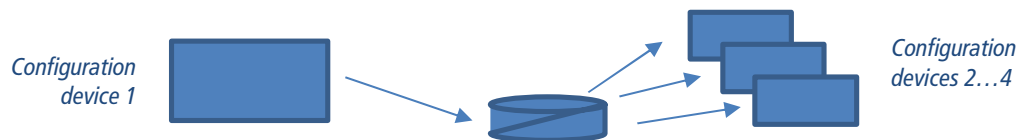
The screenshot shows the axing DDNS configuration page. The left sidebar has buttons for Setup, DHCP, DDNS (highlighted), and Backup. The main content area is titled 'Basic DDNS' and includes a description: 'This page allows setup of Dynamic DNS service.' Below this, there are fields for 'DDNS Service' (www.DynDNS.org), 'User Name' (axing), 'Password' (masked), 'Host Name' (dns-server.com), and 'IP Address' (0.0.0.0). The status is 'DDNS service is not enabled.' and there is an 'Apply' button.

→ Select a DDNS service

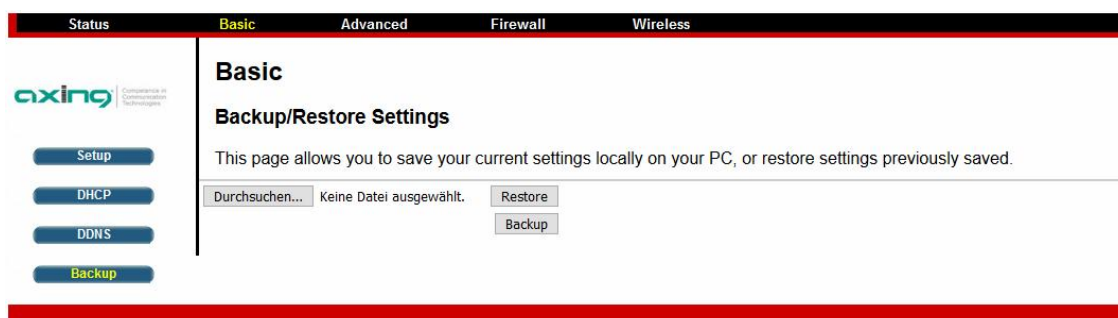
- ➔ Enter the DDNS service credentials in the User Name and Password fields.
- ➔ In the Host Name field, enter the name that you have specified in the DDNS service.

#### 4.2.4 Backup/Restore

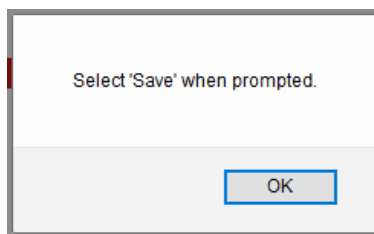
The configuration of the CMO can be saved to a backup file. This can be used as a backup of the data or to duplicate a configuration to multiple devices.



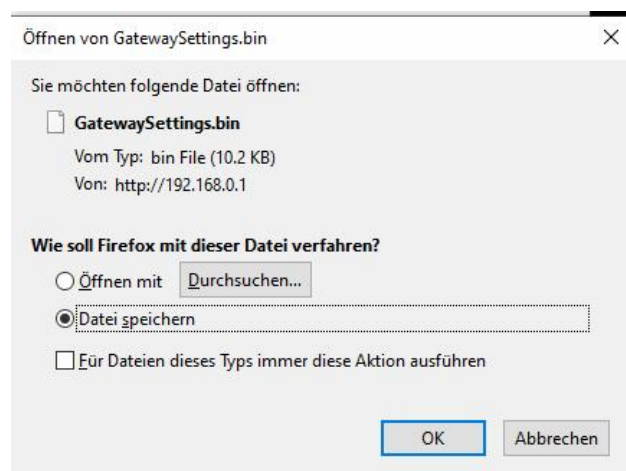
##### 4.2.4.1 Backup



- ➔ Click on Backup.
- The following dialog will open.



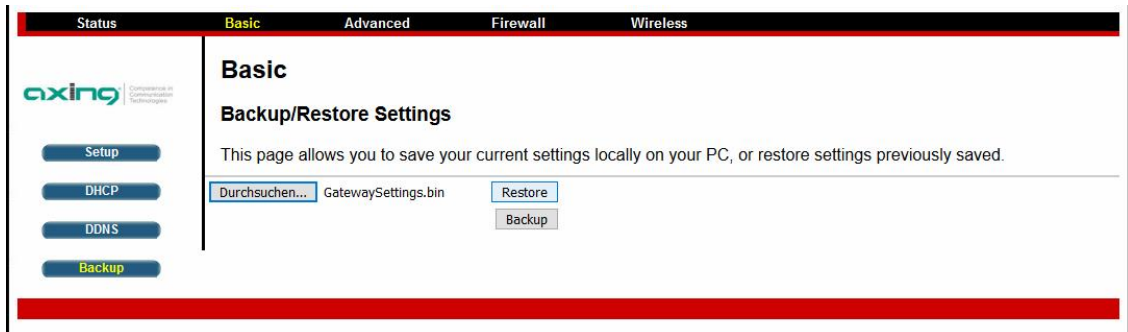
- ➔ Click OK in it.
- ➔ Then select Save file and save the backup file on your PC.



- ➔ Assign a descriptive name so that you can find the file later (example 20200716\_CMO\_room201.bin).

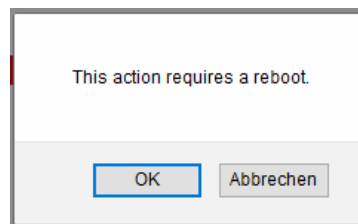
#### 4.2.4.2 Restore

→ Click Browse... and select a backup file.



→ Click on Restore.

The following message appears, informing you that the CMO will be restarted afterwards



→ Click on OK.

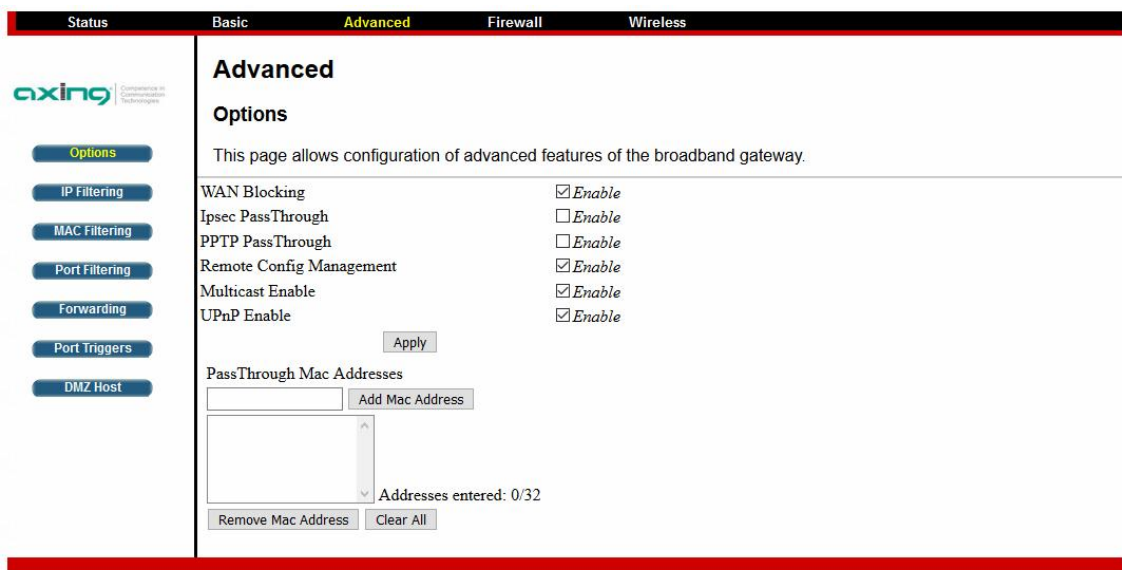
→ The backup configuration is loaded and the CMO is restarted.

### 4.3 Advanced

The Advanced page allows you to enable/disable some advanced features of the CMO 2-01.

Auf der Seite **Advanced** können Sie einige erweiterte Funktionen des CMO 2-01 aktivieren/deaktivieren.

#### 4.3.1 Options



- WAN Blocking: To prevent others on the WAN side from being able to ping your CMO 2-01. With WAN Blocking on, your CMO 2-01 will not respond to pings it receives, "hiding" your modem.
- Isec PassThrough: To enable IpSec type packets to pass through between WAN and LAN.
- PPTP PassThrough: To enable PPTP type packets to pass through between WAN and LAN.

- Remote Config Management: To make the Web Management pages of your CMO 2-01 accessible from the WAN side. Page access is limited to only those who know the CMO 2-01 access password you set in the Status-Security page (see 4.1.3 on page 12).

When accessing the CMO 2-01 from a remote location, you must use HTTP port 8080 and your IP address. This is the "WAN IP address" that appears at the Basic-Setup page. For example, if this IP address were 211.20.15.28, you would enter `http:// 211.20.15.28:8080` to reach the CMO 2-01's Web Management page from a remote location.

- Multicast Enable: To enable multicast streams to pass through between WAN and LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet, such as webcasting of a live event.
- UPnP Enable: UPnP (Universal Plug and Play) offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices.

→ Check the option(s) you want to use and click **Apply**.

Or, uncheck the option(s) you do not want to use and click Apply.

### 4.3.2 IP Filtering

The IP Filtering page allows you to specify PCs that must not have outgoing access to the WAN (Internet). These PCs can still communicate with each other on the LAN, but requests sent to WAN addresses will be blocked. The PCs are "filtered out" based on IP address ranges.

The screenshot shows the Axing CMO 2-01 Web Management interface. The top navigation bar includes Status, Basic, Advanced (highlighted), Firewall, and Wireless. The left sidebar contains a list of configuration options: Options, IP Filtering (highlighted), MAC Filtering, Port Filtering, Forwarding, Port Triggers, and DMZ Host. The main content area is titled "Advanced IP Filtering" and includes a description: "This page allows configuration of IP address filters in order to block internet traffic to specific network devices on the LAN." Below the description is a table for configuring IP filters.

| IP Filtering  |              |                                     |
|---------------|--------------|-------------------------------------|
| Start Address | End Address  | Enabled                             |
| 192.168.0.2   | 192.168.0.10 | <input checked="" type="checkbox"/> |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |
| 192.168.0.0   | 192.168.0.0  | <input type="checkbox"/>            |

Below the table is an "Apply" button.

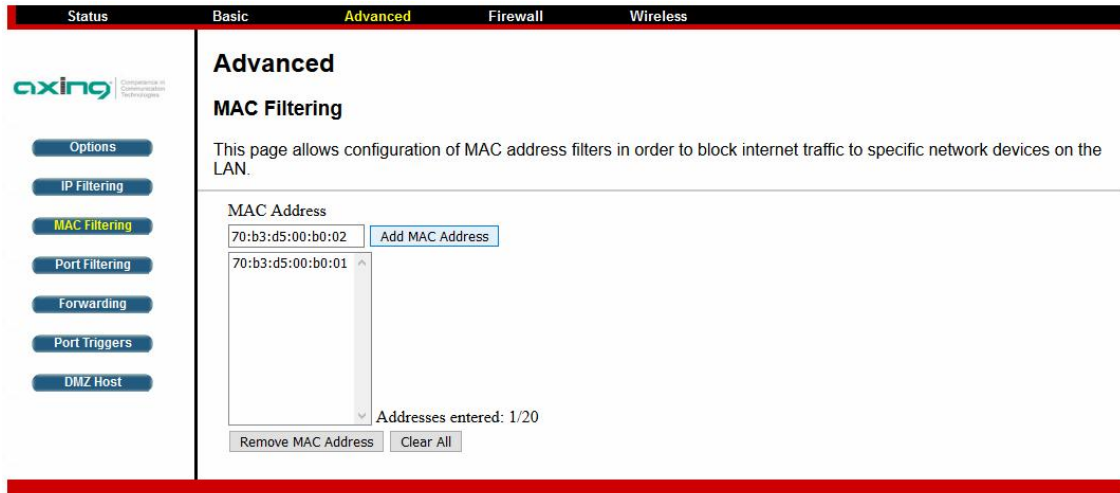
→ Enter the address ranges in the Start Address and End Address fields.

→ Select the Enable check box.

→ Click the Apply button.

### 4.3.3 MAC Filtering

The MAC Filtering page allows you to specify PCs that must not have outgoing access to the WAN (Internet). These PCs can still communicate with each other on the LAN, but requests sent to WAN addresses will be blocked. The PCs are "filtered out" based on their MAC address.



**Advanced**

**MAC Filtering**

This page allows configuration of MAC address filters in order to block internet traffic to specific network devices on the LAN.

MAC Address

70:b3:d5:00:b0:02 [Add MAC Address](#)

70:b3:d5:00:b0:01

Addresses entered: 1/20

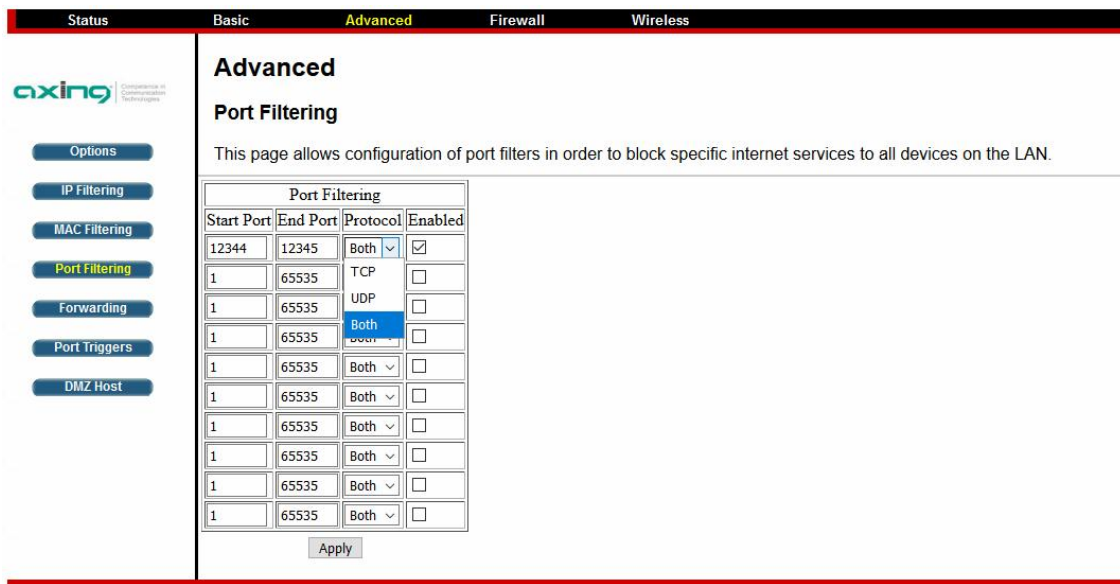
[Remove MAC Address](#) [Clear All](#)

➔ Enter the MAC Address.

➔ Click the Add MAC Address button.

### 4.3.4 Port Filtering

On the Port Filtering page you can enter destination ports (applications) to which your LAN PCs should not connect. Connections that your LAN PCs want to establish with these ports are blocked. For example, you could block access to worldwide web browsing (HTTP port 80) but still allow email service (SMTP port 25 and POP3 port 110).



**Advanced**

**Port Filtering**

This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.

| Start Port | End Port | Protocol | Enabled                             |
|------------|----------|----------|-------------------------------------|
| 12344      | 12345    | Both     | <input checked="" type="checkbox"/> |
| 1          | 65535    | TCP      | <input type="checkbox"/>            |
| 1          | 65535    | UDP      | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |
| 1          | 65535    | Both     | <input type="checkbox"/>            |

[Apply](#)

➔ To enable port filtering, enter the **Start port** and **End port** for each range (to block only one port, set both Start and End ports the same).

➔ Select its **Protocol** from the drop-down list and check the **Enable** box.

➔ Click the **Apply** button.

### 4.3.5 Forwarding

For communications between LAN and WAN, the CMO 2-01 normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one port you specify. The Forwarding page allows you to specify up to 10 rules. The Forwarding page allows you to provide local services (web server, FTP server, mail server, etc.) to people on the Internet. A table with frequently used port numbers is shown.

| Application | Port |
|-------------|------|
| HTTP        | 80   |
| FTP         | 21   |
| TFTP        | 69   |
| SMTP        | 25   |
| POP3        | 110  |
| NNTP        | 119  |
| Telnet      | 23   |
| IRC         | 164  |
| SNMP        | 161  |
| Finger      | 79   |
| Gopher      | 70   |
| Whois       | 43   |
| rdlnet      | 107  |
| LDAP        | 389  |
| UUCP        | 540  |

| Local       |            |          | External   |          |     | Protocol | Description | Enabled |        |
|-------------|------------|----------|------------|----------|-----|----------|-------------|---------|--------|
| IP Address  | Start Port | End Port | Start Port | End Port |     |          |             |         |        |
| 192.168.0.2 | 12344      | 12345    | 12344      | 12345    | TCP | Test     | Yes         | Edit    | Remove |

→ Enter the necessary parameters for forwarding.

→ Click Apply.

The rule is added to the table at the bottom of the page.

| Local       |            |          | External   |          |     | Protocol | Description | Enabled | Remove All |  |
|-------------|------------|----------|------------|----------|-----|----------|-------------|---------|------------|--|
| IP Address  | Start Port | End Port | Start Port | End Port |     |          |             |         |            |  |
| 192.168.0.2 | 12344      | 12345    | 12344      | 12345    | TCP | Test     | Yes         | Edit    | Remove     |  |

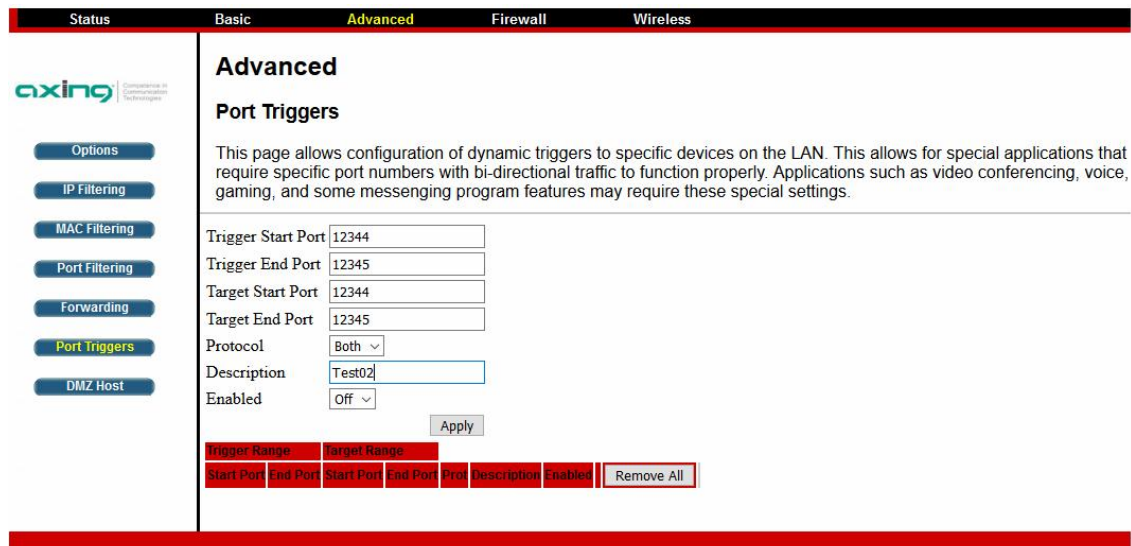
→ Click Edit in the table to change a rule.

→ Click Remove in the table to delete a rule.

→ Click Remove All in the table to change all rules.

### 4.3.6 Port Triggers

The **Port Triggers** page allows you to configure dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.



| Trigger Range |          | Target Range |          | Prot | Description | Enabled |             |
|---------------|----------|--------------|----------|------|-------------|---------|-------------|
| Start Port    | End Port | Start Port   | End Port |      |             |         | Remove All  |
| 12344         | 12345    | 12344        | 12345    | BOTH | Test02      | No      | Edit Remove |

→ Enter the necessary parameters for port triggering.

→ Click Apply.

The entry is added to the table at the bottom of the page.

| Trigger Range |          | Target Range |          | Prot | Description | Enabled |      |        |
|---------------|----------|--------------|----------|------|-------------|---------|------|--------|
| Start Port    | End Port | Start Port   | End Port |      |             |         | Edit | Remove |
| 12344         | 12345    | 12344        | 12345    | BOTH | Test02      | No      | Edit | Remove |

→ Click Edit in the table to change an entry.

→ Click Remove in the table to delete an entry.

→ Click Remove All in the table to change all entries.



### 4.3.7 DMZ Host

The **DMZ** page allows you to configure a specific network device to be exposed or visible directly to the WAN (public Internet). Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the port forwarding feature to the IP address of these host (PC). This designates one PC on your LAN that should be left accessible to all PCs from the WAN side for all ports. For example, if you locate a HTTP server on this machine, anyone will be able to access that HTTP server by using your CMO 2-01's IP address as the destination. This may be used when problem applications do not work with port triggers. The setting of "0" indicates NO DMZ PC.

The screenshot shows the Axing CMO 2-01 web interface. The top navigation bar includes Status, Basic, Advanced (highlighted), Firewall, and Wireless. On the left, a sidebar lists various configuration options: Options, IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers, and DMZ Host (highlighted). The main content area is titled 'Advanced' and 'DMZ Host'. It contains a description: 'This page allows configuration of a specific network device to be exposed or visible directly to the WAN (public internet). ; This may be used when problem applications do not work with port triggers. Entering a "0" means there are no exposed hosts.' Below this, there is a text input field for 'DMZ Address' with the value '192.168.0.2' and an 'Apply' button.

## 4.4 Firewall

The CMO 2-01 provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other unwelcome or malicious accesses to your LAN.

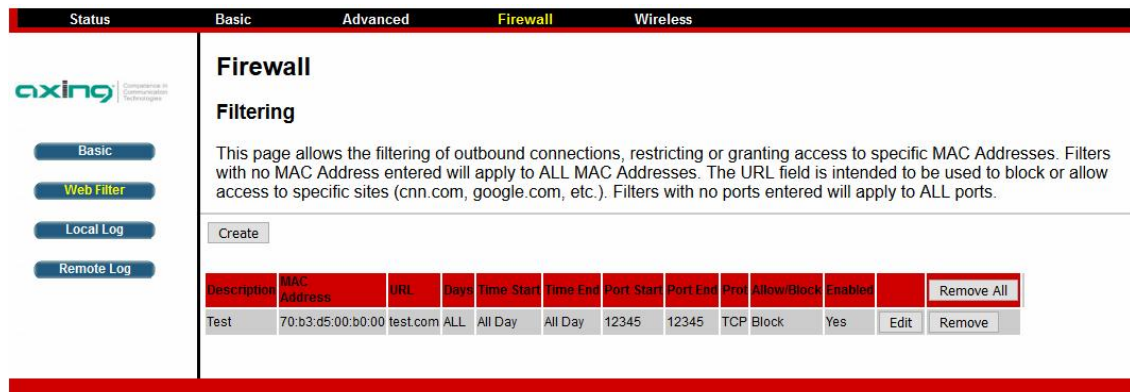
### 4.4.1 Basic

The screenshot shows the Axing CMO 2-01 web interface. The top navigation bar includes Status, Basic (highlighted), Advanced, Firewall, and Wireless. On the left, a sidebar lists various configuration options: Basic (highlighted), Web Filter, Local Log, and Remote Log. The main content area is titled 'Firewall' and 'Web Content Filter'. It contains a description: 'This page allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. A list of "trusted computers" can also be defined that are not subject to any filters configured. Specific Firewall features can also be enabled. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks. Go to the Parental Control page to block internet access to specific sites.' Below this, there is a section for 'Allowed Services' with a text box containing 'No Ports Restricted.' and an 'Apply' button. To the left of the 'Allowed Services' box, there are several settings: 'IPv4 Firewall Protection' set to 'Low', 'Block Fragmented IP Packets' with an 'Enable' checkbox, 'Port Scan Detection' with an 'Enable' checkbox, and 'IP Flood Detection' with an 'Enable' checkbox.



## 4.4.2 Web Filtering

This page allows the filtering of outbound connections, restricting or granting access to specific MAC addresses.



→ Click Create to create a new filter.

The fields shown below will appear.

Description   
 MAC Address   
 URL   
 Port Start   
 Port End   
 Protocol   
 Days  
☐ Everyday ☒ Sunday ☐ Monday ☐ Tuesday  
☐ Wednesday ☐ Thursday ☒ Friday ☒ Saturday  
 Time  
☒ All day  
 Start:  (hour)  (min) AM ▼  
 End:  (hour)  (min) AM ▼  
 Allow/Block   
 Enabled

→ Enter a description in the Discription field.

→ If necessary, enter a MAC address of a device to which the filter applies (for example, a child's tablet).

Filters in which no MAC address is entered apply to all MAC addresses.

→ Enter the URL that you want to block or allow.

→ Enter a start port and an end port.

Filters in which no ports are specified apply to all ports.

→ Under Days or Time, you can specify weekdays or times when the filter is valid.

→ Use the Allow/Block field to determine whether the filter blocks or allows access to a website.

→ With Enabled you determine whether the filter is active (On) or inactive (Off).

→ Click Apply.

The filter is added to the table below.

→ Click Edit in the table to change a filter.

→ Click Remove in the table to delete a filter.

→ Click Remove All in the table to change all filters.

### 4.4.3 Local Log

The Local Log page logs any attacks on the firewall. These attack records are visible in the table at the bottom of the page.

- Specifies the e-mail address and its SMTP of the person who should receive notices of any attempted firewall violations.
- Type the addresses in standard Internet e-mail address format, for example, yourname@onecompany.com. Then check the Enable box to enable the alert feature.
- Click E-mail Log to immediately send the email log.
- Click Clear Log to clear the table of entries for a fresh start.

### 4.4.4 Remote Log

This page allows optional configurations of events to be sent to a local SysLog server.

- Activate the events to be logged.
- Enter the IP address of the SysLog server in your network.
- Click Apply.

## 4.5 Wireless

### 4.5.1 Radio

The **Wireless** Connection Stage Configuration of the Wireless Radio includes current country and channel number.

Status

Basic

Advanced

Firewall

Wireless

axing

Competence in  
Communication  
Technologies

Radio

Primary Network

Guest Network

Access Control

WMM

Bridging

### Wireless

#### 802.11 Radio

This page allows configuration of the Wireless Radio including current channel number.

Wireless Interfaces:

2.4 GHz (70:B3:D5:00:80:09)

Wireless

Enabled

Country

E0

802.11 Band

2.4 Ghz

Current : 2.4 GHz

802.11 n-mode

Auto

Bandwidth

40 Mhz

Current : 20MHz

Sideband for Control Channel (40 Mhz only)

Upper

Current : None

Control Channel

Auto

Current : 6 \*\*\*Interference Level: Acceptable

Regulatory Mode

Off

TPC Mitigation (db)

0 (Off)

OBSS Coexistence

1 (Enabled)

STBC Tx

Auto

Apply

Restore Wireless Defaults


Scan Wireless APs

Auf der Seite Radio werden die HF-Einstellungen für das WiFi-Funknetz vorgenommen.

## 4.5.2 Primary Network

The 802.11 Primary Network allows configuration of the Primary Wireless Network and its security settings.

| Status | Basic | Advanced | Firewall | Wireless |
|--------|-------|----------|----------|----------|
|--------|-------|----------|----------|----------|



Radio  
**Primary Network**  
Guest Network  
Access Control  
WMM  
Bridging

### Wireless

#### 802.11 Primary Network

This page allows configuration of the Primary Wireless Network and its security settings.

CMO 2-01-B005-G (70:B3:D5:00:B0:09)

PrimaryNetwork 
Automatic Security Configuration

Network Name (SSID)

Closed Network

Mode Required

AP Isolate

WPA

WPA-PSK

WPA2

WPA2-PSK

WPA/WPA2 Encryption

WPA Pre-Shared Key  ☐ Show Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

WEP Encryption

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

→ When AP Isolation is enabled, devices on the same wireless network cannot communicate with each other.

## 4.5.3 Guest Network

This page allows configuration of a guest network.


The settings are the same as for the Primary Network.

#### 4.5.4 Access Control

This page allows configuration of the Access Control to the AP as well as on the connected clients.

**Status**    **Basic**    **Advanced**    **Firewall**    **Wireless**

---

 axing  
Communications &  
Information Technology

## Wireless

### 802.11 Access Control

This page allows configuration of the Access Control to the AP as well as status on the connected clients.

---

Wireless Interface CMO 2-01-8005-G (70:B3:D5:00:80:09) ▾

MAC Restrict Mode Disabled ▾

MAC filter based Probe Response Off ▾

MAC Addresses

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Apply

Connected Clients

| MAC Address                        | Age(s) | RSSI(dBm) | IP Addr | Host Name | Mode | Speed (Kbps) |
|------------------------------------|--------|-----------|---------|-----------|------|--------------|
| No wireless clients are connected. |        |           |         |           |      |              |

#### 4.5.4.1 MAC Restrict Mode

➔ First select whether you want to allow or deny access to devices using MAC filtering.

- Disabled: Turns off MAC filtering.
- Allow: Permits access to a specified MAC address.
- Deny: Rejects access to a specified MAC address.

➔ Then enter the MAC addresses and click Apply.

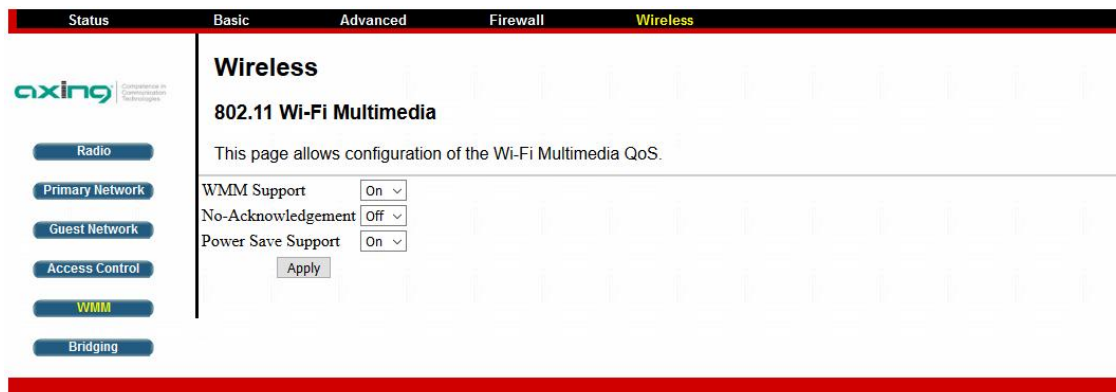
➔ Click Remove to remove the client device from the list.

#### 4.5.4.2 Connected Clients

The Connected Clients table lists the devices that are currently connected to the CMO 2-01 via WiFi.

#### 4.5.5 WMM

This page allows configuration of the Wi-Fi Multimedia QoS. Wi-Fi Multimedia Quality of Service (WMM QoS) prioritizes voice and video data traffic over the WLAN



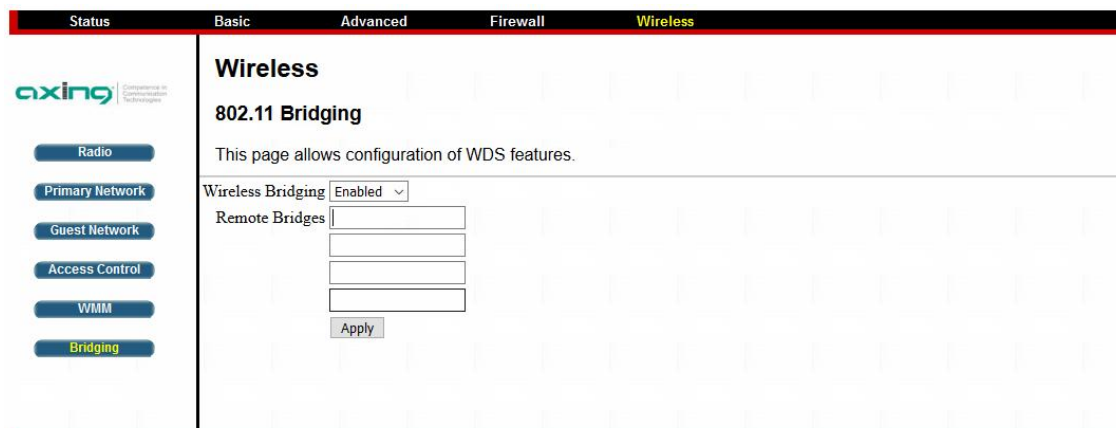
The screenshot shows the Axiom router's web interface. The top navigation bar includes Status, Basic, Advanced, Firewall, and Wireless. The left sidebar has buttons for Radio, Primary Network, Guest Network, Access Control, WMM (highlighted), and Bridging. The main content area is titled 'Wireless' and '802.11 Wi-Fi Multimedia'. It contains the text: 'This page allows configuration of the Wi-Fi Multimedia QoS.' Below this, there are three settings: 'WMM Support' set to 'On', 'No-Acknowledgement' set to 'Off', and 'Power Save Support' set to 'On'. An 'Apply' button is at the bottom.

- In the WMM Support field, select On to enable wireless multimedia.  
WMM support helps with various types of traffic such as voice, video, and background services.
- No Acknowledgement: This is a feature that improves the accuracy of the transmitted data. This option is generally only necessary if there are many other WiFi networks in the same area.
- Power Save Support: The purpose of this setting is for the router to queue the data while your mobile devices are in power save mode. The purpose is to conserve battery power for devices that rely on battery power.

#### 4.5.6 Bridging

This page allows configuration of WDS features (Wireless Distribution System).

With the help of a wireless distribution system, WLANs can be expanded by wirelessly connecting WLAN access points and covering larger areas without the need for a cable connection between the access points.



The screenshot shows the Axiom router's web interface. The top navigation bar includes Status, Basic, Advanced, Firewall, and Wireless. The left sidebar has buttons for Radio, Primary Network, Guest Network, Access Control, WMM, and Bridging (highlighted). The main content area is titled 'Wireless' and '802.11 Bridging'. It contains the text: 'This page allows configuration of WDS features.' Below this, there is a 'Wireless Bridging' dropdown menu set to 'Enabled'. Underneath, there are four empty text boxes for 'Remote Bridges'. An 'Apply' button is at the bottom.

- In the Wireless Bridging selection box, select Enabled.
- Enter the WLAN MAC address of the devices as Remote Bridges.  
You can enter up to 4 bridges

## 5 Technical data

### 5.1 CMO 1-01

|                                     |  |
|-------------------------------------|--|
| <b>Downstream</b>                   |  |
| Data rate                           | Max. 320 Mbps @ DOCSIS<br>Max. 400 Mbps @ EuroDOCSIS                                       |
| Frequency range                     | 108...1002 MHz   |
| Channel bandwidth                   | 6 MHz @ DOCSIS<br>8 MHz @ EuroDOCSIS   |
| Channel bonding                     | ≤8   |
| Input level                         | -15 dBmV...+15 dBmV  |
| Demodulation                        | QAM64, QAM256  |
| <b>Upstream</b>                     |  |
| Data rate                           | 120 Mbps @ TDMA<br>160 Mbps @ S-CDMA   |
| Frequency range                     | 5...42 MHz @ DOCSIS<br>5...65 MHz @ EuroDOCSIS   |
| Channel bandwidth                   | 200/400/800/1600/3200/6400 KHz   |
| Output level                        | 8...58 dBmV @ QPSK<br>8...54 dBmV @ 64 QAM<br>8...54 dBmV @ 32 QAM<br>8...53 dBmV @ S-CDMA |
| Channel bonding                     | ≤4   |
| Modulation                          | QPSK, QAM8, QAM16, QAM32, QAM64, QAM128 (SCDMA)  |
| <b>Interfaces</b>                   |  |
| Ethernet connectors (LAN)           | 1 × RJ 45  |
| Ethernet standards                  | IEEE 802.3 10Base-T   802.3u 100Base-TX   802.3ab 1000Base-T (GigE)                        |
| Supported transport protocols       | IP, TCP, UDP, ARP  |
| Supported application protocols     | HTTP, ICMP, DHCP, TFTP, SNMP   |
| DOCSIS                              | F-female (75 Ohm)  |
| <b>General</b>                      |  |
| Operating voltage                   | 12 VDC   |
| Operating temperature range         | 0...40 °C  |
| Storage temperature range           | -20...70 °C  |
| Operating humidity (non-condensing) | 10...90%   |
| Dimensions (W × H × D) appr.        | 160 × 125 × 32,5 mm  |
| Weight                              | 200 g  |
| <b>External accessories</b>         |  |
| Plug-in power supply                | 100...240 V/50...60 Hz   12 V=1 A  |

## 5.2 CMO 2-01

|                                     |  |
|-------------------------------------|--|
| <b>Downstream</b>                   |  |
| Data rate                           | Max. 320 Mbps @ DOCSIS<br>Max. 400 Mbps @ EuroDOCSIS                                       |
| Frequency range                     | 108...1002 MHz   |
| Channel bandwidth                   | 6 MHz @ DOCSIS<br>8 MHz @ EuroDOCSIS   |
| Channel bonding                     | ≤8   |
| Input level                         | -15 dBmV...+15 dBmV  |
| Demodulation                        | QAM64, QAM256  |
| <b>Upstream</b>                     |  |
| Data rate                           | 120 Mbps @ TDMA<br>160 Mbps @ S-CDMA   |
| Frequency range                     | 5...42 MHz @ DOCSIS<br>5...65 MHz @ EuroDOCSIS   |
| Channel bandwidth                   | 200/400/800/1600/3200/6400 KHz   |
| Output level                        | 8...58 dBmV @ QPSK<br>8...54 dBmV @ 64 QAM<br>8...54 dBmV @ 32 QAM<br>8...53 dBmV @ S-CDMA |
| Channel bonding                     | ≤4   |
| Modulation                          | QPSK, QAM8, QAM16, QAM32, QAM64, QAM128 (SCDMA)  |
| <b>Interfaces</b>                   |  |
| Ethernet connectors (LAN)           | 2 × RJ 45  |
| Ethernet standards                  | IEEE 802.3 10Base-T   802.3u 100Base-TX   802.3ab 1000Base-T (GigE)                        |
| WiFi standard                       | IEEE 802.11b/g/n   |
| WIFI band                           | 2.4 GHz single-band  |
| Wifi signal rate                    | 300 Mbps   |
| WiFi encryption                     | WPA/WPA2   |
| Supported transport protocols       | IP, TCP, UDP, ARP, TR-069  |
| Supported application protocols     | HTTP, ICMP, DHCP, TFTP, SNMP   |
| DOCSIS                              | F-female (75 Ohm)  |
| <b>General</b>                      |  |
| Operating voltage                   | 12 VDC   |
| Operating temperature range         | 0...40 °C  |
| Storage temperature range           | -10...60 °C  |
| Operating humidity (non-condensing) | 10...90%   |
| Dimensions (W × H × D) appr.        | 167 × 125 × 38 mm  |
| Weight                              | 320 g  |
| <b>External accessories</b>         |  |
| Plug-in power supply                | 110...240 V/50...60 Hz   12 V=1,5 A  |





