

power
SPEED privat
das Glasfasernetz der Energie AG



Benutzerhandbuch

PM520 LWL Router



ENERGIE AG
Telekom

Wir denken an morgen

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
Über das Handbuch.....	3
Einleitung	3
Vorsichtsmaßnahmen.....	4
Energie AG – FTTH Kundengerät.....	5
PM520 Vorderseite.....	5
PM520 Rückseite	6
Einrichten der Anschlüsse	7
Wandmontage des Gerätes	7
Ethernet-Eigenschaften	8
VoIP-Eigenschaften.....	8
WLAN Eigenschaften	9
Allgemeines	9
Login am Heimrouter	10
LAN IPv4 DHCP Einstellungen.....	11
Wireless Einstellungen (WLAN).....	12
Wireless Sicherheitseinstellungen	13
Advanced Wireless Einstellungen	14
User Management.....	16
URL Filter	17
Firewall	18
MAC Filter.....	19
Security Filter	20
UPnP.....	21
NAT ALG Settings	22
NAT DMZ Settings	23
NAT Virtual Server Settings	24

Über das Handbuch

Dieses Handbuch beschreibt, wie das FTTH Kundenendgerät PM520 installiert und konfiguriert wird. Das Handbuch richtet sich speziell an Personen, die über Grundkenntnisse im Netzwerkbereich verfügen.

• **Bitte beachten Sie, dass nicht alle Einstellungen geändert werden können.**

Einleitung

Die neueste Light Link® PM520 Series P2MP ONU ermöglicht eine zukunftsweisende Bandbreite bis 1000 Mbps, maßgeschneidert für FTTH Dienstleistungen. Die kompakte Bauweise berücksichtigt speziell jene Aspekte der Sicherheit und Einfachheit der Installation.

Nachfolgend werden spezielle Aspekte beim Betrieb des LWL Routers herausgegriffen, um so den Benutzer bestmöglich im Betrieb des Routers zu unterstützen und möglichen Fragen vorzubeugen.

Vorsichtsmaßnahmen



General Warning

ACHTUNG!

Das Gerät ist für die Anwendung im Innenbereich ausgerichtet. Um Feuer, Stromschlag oder eine Beschädigung des Gerätes zu vermeiden, darf das Gerät weder Wasser noch Feuchtigkeit ausgesetzt werden.

- Es muss für ausreichende Kühlung und Lüftung, wie angegeben, gesorgt werden.
- Die Bedienungsanleitung des Produktes muss gelesen und verstanden werden, bevor das Gerät in Betrieb genommen wird.
- Setzen Sie stets die Schutzkappen wieder auf die optischen Anschlüsse, wenn sie nicht verwendet werden.
- Der typische Anschluss ist SC/APC 8 °.
Hinweis: Ein 8° Grad polierter Stecker muss verwendet werden.
- Gefährliche Spannungen sind innerhalb des Netzteils immer vorhanden.
- Das Gerät darf nicht betrieben werden, sofern nicht alle Abdeckungen und Panels ordnungsgemäß installiert wurden.

Reinigung

Für die Reinigung der Vorderseite verwenden Sie lediglich ein feuchtes Tuch. Verwenden Sie ein weiches, trockenes Tuch, um die Oberseite des Gerätes zu reinigen. Verwenden Sie keine Reinigungssprays jeglicher Art.

Überlastung

Eine Überlastung der Steckdosen und Verlängerungskabel erhöht die Gefahr von Bränden oder elektrischen Schlägen. Verwenden Sie das empfohlene Netzteil mit dem richtigen Kabel und dem richtigen Stecker für den Einsatz des Gerätes.

Schäden mit Reparaturbedarf

Trennen Sie das Gerät und lassen Sie dieses nur von dafür qualifiziertem Servicepersonal von Pacific Broadband Networks warten bzw. reparieren. Versuchen Sie nicht, dieses Gerät selber zu warten.



Laser Radiation

ACHTUNG!

Eine Gefährdung durch Laserstrahlung der Klasse 1M ist möglich. Zugang sollte nur einem beschränkten und entsprechend geschulten Personal gewährt werden. Freiliegende Fasern oder aber auch Stecker sollen beim Umgang mit optischen Geräten nicht näher inspiziert werden.

Energie AG – FTTH Kundengerät

PM520 Vorderseite



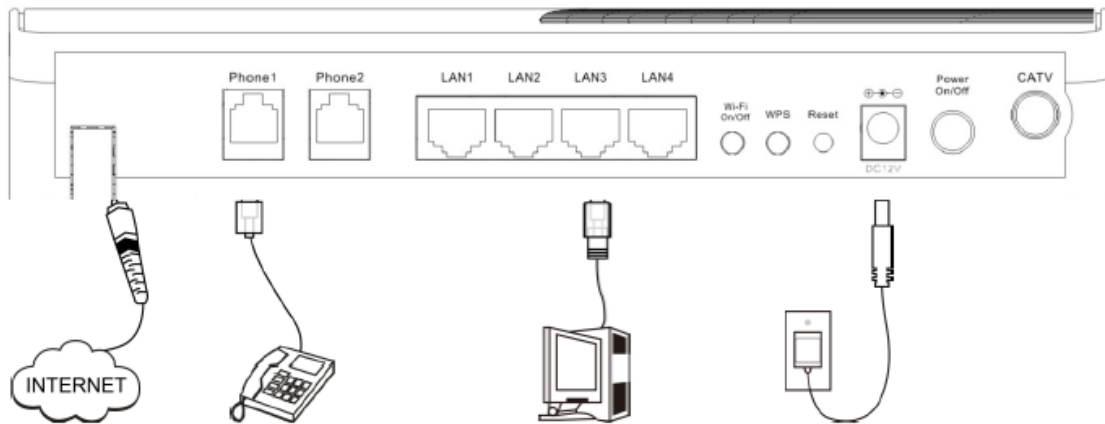
LED	Funktion	
WPS	AUS	WLAN Protected Setup nicht aktiv
	Blinken	WLAN Protected Setup läuft
Wi-Fi	AUS	WLAN aktiv
	EIN	WLAN ist konfiguriert und aktiv
	Blinken	WLAN entdeckt
Power	AUS	Keine Stromversorgung des Gerätes
	EIN	Stromversorgung des Gerätes funktioniert korrekt
Fiber Link	AUS	Router ist nicht an der Zentrale registriert.
	EIN	Router ist an der Zentrale registriert.
	Blinken	Router wurde nicht korrekt bei der Zentrale registriert
Alarm	AUS	Kein Alarm
	Rot	Keine Glasfaserverbindung hergestellt
LAN 1-4	AUS	Keine Ethernet-Verbindung hergestellt.
	EIN	Grün = 1000 Mbps, Orange = 100 Mbps, Gelb = 10 Mbps
	Blinken	Die Datenübertragung läuft (bei jeder Geschwindigkeit).
Phone 2	AUS	Phone 2 ist nicht beim SIP Server registriert.
	EIN	Phone 2 ist beim SIP Server registriert.
	Blinken	Phone 2 ist derzeit abgehoben oder in Verwendung.
Phone 1	AUS	Phone 1 ist nicht beim SIP Server registriert.
	EIN	Phone 1 ist beim SIP Server registriert.
	Blinken	Phone 1 ist derzeit abgehoben oder in Verwendung.
System	Blinken	System bereit

PM520 Rückseite



Element	Beschreibung
Phone 1	Telefon 1 – RJ11 Anschluss
Phone 2	Telefon 2 – RJ11 Anschluss
LAN 1-4	Gigabit Ethernet Ports, 4xRJ45 – 10/100/1000 Mbps
WPS Button	Drücken und halten Sie die WLAN-Taste für 3 Sekunden, um das WLAN zu aktivieren / deaktivieren
Reset Button	Die Reset-Taste nur nach Aufforderung des EnergieAG Serviceteams benutzen!
DC12V Power Port	Netzbuchse für 11 bis 15V DC Netzteil
Power On/Off	An-/Aus-Schalter für PM520

Einrichten der Anschlüsse



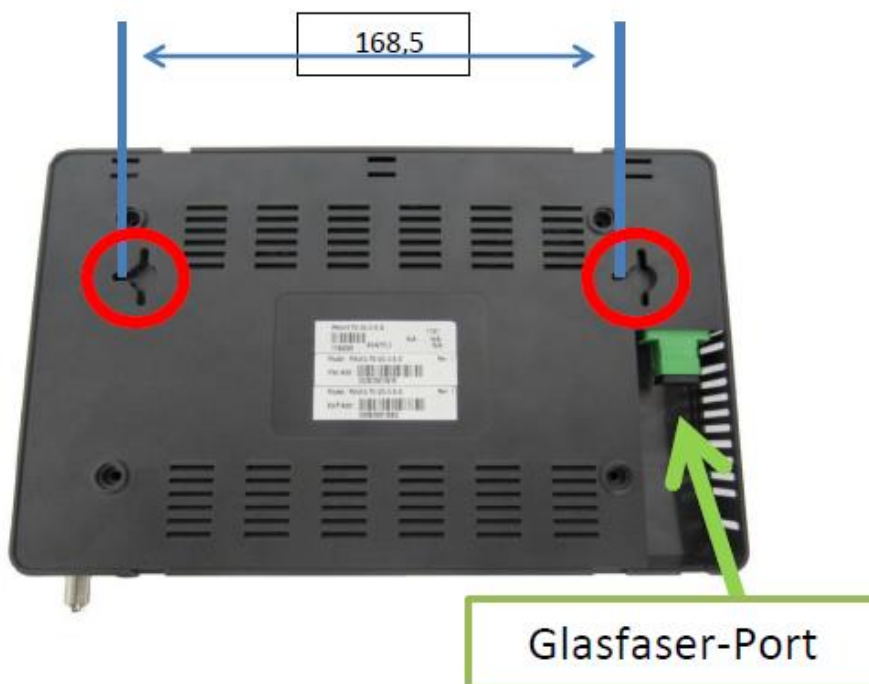
Schließen Sie ihr Gerät gemäß folgenden Schritten an, um Ihr Glasfasernetz zu nutzen:

1. Verbinden Sie den „PON Port“ mit dem Lichtwellenleiter-Anschluss vom Typ SC
2. Verbinden Sie das Telefon mit dem „FXS Port“ mittels RJ-11 Telefonanschlusskabel.
3. Verbinden Sie den PC mit dem Ethernet Port mittels RJ-45 Cat5/Cat6 Kabel
4. Verbinden Sie den Gerätenetzanschluss mittels des Netzteils. Drücken sie den Knopf „Power On/Off“ um das Gerät zu starten.

Wandmontage des Gerätes

Sie können das Gerät auf einer senkrechten Fläche mit Hilfe der vorgeformten Montagelöcher auf der Unterseite des Gerätes und den zwei Plattenkopf-Holzschrauben befestigen.

- Befestigen Sie die Schrauben in der Wand. Die Position der Schrauben muss in der gleichen horizontalen Linie sein und den gleichen Mittenabstand wie die Befestigungslöcher haben. Lassen Sie die Schraubenköpfe mindestens 6 mm aus der Wand herausstehen. Hängen Sie das Gerät durch die Befestigungslöcher an die Schrauben.



Ethernet-Eigenschaften

Schnittstelle	4x10/100/1000 Mbps auf RJ45, Full/Half-Duplex, Auto-Negotiation, Auto MDI/MDIX
VLAN	IEEE802.1Q, QinQ unterstützt
Spanning Tree Protocol	IEEE802.1D unterstützt, > 64 MAC pro Gerät (RSTP standardmäßig aktiviert)
QoS	IEEE802.1p, DiffServ Unterstützung, 4 Queues pro Port
Framegröße	64 bis 1522 Bytes
IGMP	IGMP (v1, v2) Snooping Support
Security	Broadcast / Multicast Storm Unterdrückung, Accesslisten und -filter

VoIP-Eigenschaften

VoIP	SIPv2
SIP Codecs	G.711,G.723.1,G.726_24, G.726_32,G.729A
Eigenschaften	Anrufweiterleitung Anruf halten/ abgeben Anklopfen Anrufer-ID Echo-Unterdrückung (LEC) Adaptiver Jitter-Puffer Paketverlustverschleierung Comfort Noise Generator
DHCP	Option 66 & 67, Auto-Provisioning Unterstützung
Telefonanschlüsse	2 x RJ11 (POTS)

WLAN Eigenschaften

Standards	802.11 b/g/n
Konfigurationsoptionen	1) 2 x 2 (2.4 GHz) – minimaler Durchsatz 40 Mbps
WLAN-Security	WLAN Verschlüsselung: WPA2-PSK; WPA-PSK; WEP; Open Weitere Security Features: WLAN MAC Adressenfilter
QoS	WMM-QoS (für Multimediaapplikationen)
Setup/ Konfiguration	WPS Unterstützung (WLAN geschütztes Setup) Webkonfiguration
Mehrere SSIDs	Unterstützt bis zu 4 SSIDs Standard SSID ist vorkonfiguriert.
WLAN Kanal Konfiguration	Standard: Automatische Kanalwahl (basierend auf Congestion Scan) Manuelle Auswahl
Konfigurierbare Parameter	DTIM Intervall Fragmentierungsschwelle RTS Schwelle 802.11n-Übertragungsrate CTS Schutzmodus SSID Broadcast aktivieren/ deaktivieren
Antennen	Interne Antenne

Allgemeines

Eingangsspannung	11-15V DCdc
Netzstromgerät	100~240V AC, 50~60 Hz, 0.5 A max.
Leistungsaufnahme	< 8.5 W (Vollbeladen)
Dimension (H x W x D)	46 mm x 207 mm x 147 mm
Nettogewicht	0.55 kg

Login am Heimrouter

Sie können Ihren WLAN Router ganz einfach über die Weboberfläche Ihrer Browser bedienen und konfigurieren.

Gehen Sie wie folgt vor:

1. Starten Sie ihren Webbrowser (Internet Explorer, Firefox, Chrome, usw.)
2. Geben Sie die IP Adresse des Routers ein: **http://10.0.0.10**
3. Es erscheint ein Anmeldefenster Ihres Routers.
 - a. Default-Login: **user / changeme** (Wir weisen darauf hin dieses Passwort umgehend zu ändern)
4. Klicken Sie auf "**Submit**" um in den Konfigurationsmodus zu gelangen.

Sie können diese Einstellungen auch von Ihrem Smartphone, Tablet oder per WLAN verbundenen PC aus konfigurieren. Sie müssen hierzu nur mit Ihrem WLAN-Netz verbunden sein!

The screenshot shows the login interface for the PBN PM520 Web Management Interface. At the top, there is a blue header with the text "PBN PM520 Web Management Interface". Below the header, on the left, is the PBN logo (Pacific Broadband Networks). To the right of the logo, there are two input fields: "Username" and "Password". Below these fields are two buttons: "Submit" and "Cancel". At the bottom of the interface, there is a blue footer with the text "Copyright © 2013 - Pacific Broadband Networks. All rights reserved."

LAN IPv4 DHCP Einstellungen

Im Webinterface Ihres Routers, klicken Sie auf "**Network**" in der obersten Reihe, dann auf "**LAN**" und schließlich "**LAN**" auf der linken Seite.

Die LAN-Einstellungen erscheinen.

PBN PM520 Web Management [Logout]

Network | Status | Network | Security | Application | Management | Diagnose

Internet | **LAN** | WLAN | QoS | Time Server

LAN
IPv6 DHCP

LAN Settings

Configure the IP address and subnet mask of the LAN access ports of the CPE. Click "Save/Apply" button to save the LAN configuration.

IP Address:
Subnet Mask:

Disable DHCP server
 Enable DHCP server
Beginning IP Address:
Ending IP Address:
Subnet Mask:
Lease Time:

Enable DHCP server relay
DHCP server IP address:

Reserved IP address

Select "Add" or "Del" to configure reserved IP allocations in the DHCP server.
Note: A maximum of 10 reserved IP address are allowed.

MAC Address	IP Address	Del
<input type="text"/>	<input type="text"/>	<input type="text"/>

Auf dieser Seite können Sie folgende Parameter einstellen:

- LAN IP Adresse und Subnet (IP Adresse des Routers = Default Gateway)
- Enable/Disable DHCP Server
- IPv4 Lease-Dauer
- IP/MAC address assignment

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

Wireless Einstellungen (WLAN)

Auf dem Webinterface des Routers, klicken Sie auf "**Network**" im oberen Reiter, dann den "**WLAN**" Button, und dann auf "**WLAN Basic**" auf der linken Seite.

Die Wireless- oder WLAN Einstellungen erscheinen.



Das Wireless-LAN ist bei Auslieferung aktiviert! Dies können Sie ändern, indem Sie den Haken bei „**Enable Wireless**“ entfernen und anschließend "**Save/Apply**" klicken

Auf dieser Seite können Sie die Basiseinstellungen Ihres WLAN (WIFI) ändern. Hier haben Sie die Möglichkeit, unter anderem die SSID (WLAN-Name) zu ändern, die Ländereinstellung vorzunehmen, die maximale Teilnehmeranzahl pro SSID einzustellen, das WIFI-Multicast-Forwarding (WMF) zu konfigurieren sowie User-Isolationen durchzuführen.

Stellen Sie sicher, dass Ihr WLAN durch Aktivieren des Punktes „Enable Wireless“ eingeschaltet und eine SSID (WLAN-Name) eingetragen ist!

VERWENDEN SIE BITTE KEINE SONDERZEICHEN BEI DER SSID (WLAN-Name)!

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern!

PBN PM520 Web Management [Logout]

Network | Status | **Network** | Security | Application | Management | Diagnose

Internet | LAN | **WLAN** | QoS | Time Server

WLAN Basic | Security | WLAN Advanced | Station Info

Wireless -- Basic

This page is used to configure basic features of Wireless LAN interface. Including enabling or disabling the wireless radio. Click on "Save/Apply" for the adjustment to take effect, the Wirelesses interface(s) will restart before changes take effect.

Enable Wireless

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 00:0B:05:62:19:79

Country:

Max Clients:

Wireless - Virtual Interface:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="Pbn2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	00:0B:05:62:19:7A
<input type="checkbox"/>	<input type="text" value="Pbn3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	00:0B:05:62:19:7B
<input type="checkbox"/>	<input type="text" value="Pbn4"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	00:0B:05:62:19:7C

Wireless Sicherheitseinstellungen

Auf dem Webinterface des Routers, klicken Sie auf "**Network**" im oberen Reiter, dann den "**WLAN**" Button, und dann auf "**Security**" auf der linken Seite. Auf dieser Seite können Sie die Sicherheitseinstellungen Ihres WLAN (WIFI) einstellen.



Das Standardpasswort ist auf der Unterseite ihres WLAN-Routers aufgeklebt. Dieses Passwort wird auch nach einem Werksreset wieder hergestellt!

PBN PM520 Web Management

Network | Status | Network | Security | Application | Management | Diagnose

Internet | LAN | WLAN | QoS | Time Server

WLAN Basic | **Security** | WLAN Advanced | Station Info

WLAN Config -- Security

This page is used to configure the wireless LAN interface security settings. Including WPS on/off and authentication methods etc. Click on "Save/Apply" for the adjustments to take effect.

WPS Setup

Enable WPS: Enabled

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

Push-Button | PIN | Add Enrollee

00000000 Help

Set WPS AP Mode: Configured

Setup AP (Configure all security settings with an external registrar)

Push-Button | PIN | Config AP

Device PIN: 0 Help

Manual Setup AP

Select SSID: Pbn1

Network Authentication: WPA2-PSK

WPA/WAPI passphrase: ***** Click here to display

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

Save/Apply

In dem "WPS Setup" Bereich können Sie die Wi-Fi Protected Setup (WPS) Funktion einschalten. Durch Drücken der WPS Taste auf der Rückseite des Routers oder durch Eingabe des WPS Codes ihres Endgerätes, können Sie einfach neue Geräte in Ihr Wirelessnetzwerk mitaufnehmen.

Im "Manual Setup AP" Bereich, können Sie die Sicherheitseinstellungen manuell für jede einzelne Ihrer SSID ändern.

Nach dem Auswählen der SSID, die Sie ändern wollen, können Sie die Einstellung für die Art der Verschlüsselung, das Passwort (**WPA/WAPI Passphrase**) sowie die Encryption Methode wählen. Wir empfehlen die Einstellung: WPA2-PSK, AES sowie ein sicheres Passwort.

Klicken Sie "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

Advanced Wireless Einstellungen

Auf dem Webinterface des Routers, klicken Sie auf **"Network"** im oberen Reiter, dann den **"WLAN"** Button, und dann auf **"WLAN Advanced"** auf der linken Seite.

Auf dieser Seite können Sie weitere Einstellungen für Ihr Wireless-Netzwerk vornehmen. Wir empfehlen diese Einstellungen nur durch geschultes Personal ändern zu lassen.

Klicken Sie **"Save/Apply"** um Ihre Einstellungen dauerhaft zu speichern.

PBN PBN PM520 Web Management [Logout]

Network | Status | **Network** | Security | Application | Management | Diagnose

Internet | LAN | **WLAN** | QoS | Time Server

WLAN Basic
Security
WLAN Advanced
Station Info

Wireless -- Advanced

This page is used to configure advanced features of wireless LAN port. Including speed, TRS, power-saving mode, access point beacons, XPress mode and so on.
Click "Save/Apply" to take effect advanced configurations of wireless.

Band: 2.4GHz
Channel: 1 Current: 1 (interference: acceptable)
Auto Channel Timer(min): 0
802.11n/EWC: Auto
Bandwidth: 20MHz in 2.4G Band and 40MHz in 5G Band Current: 20MHz
Control Sideband: Lower Current: None
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
RIFS Advertisement: Off
OBSS Co-Existence: Disable
RX Chain Power Save: Disable
Power Save status: Full Power
RX Chain Power Save Quiet Time: 10
RX Chain Power Save PPS: 10
54g™ Rate: 1 Mbps
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 16
XPress™ Technology: Disabled
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enabled
WMM No Acknowledgement: Disabled
WMM APSD: Enabled

Save/Apply

DDNS Einstellungen

Auf dem Webinterface des Routers, klicken Sie auf " **Network** " im oberen Reiter und dann auf den " **DDNS** " Button.

Die Dynamic DNS Einstellungen erscheinen.

Der Dynamische DNS(DDNS)-Dienst ermöglicht es Ihnen, eine dynamische IP-Adresse auf einen statischen Hostnamen zu verweisen. Somit ist es möglich, trotz sich ändernder IP-Adresse, Geräte im Heimnetzwerk vom Internet zu erreichen. Die benötigten Port-Forwards müssen separat eingestellt werden, diese Anleitung finden Sie auf Seite 24 (NAT Virtual Server Settings)

Um den DDNS-Dienst nutzen zu können benötigen Sie ein Benutzerkonto bei einem der folgenden Anbieter:

www.dyndns.com/account/create.html

www.noip.com/sign-up

Wählen Sie den Anbieter, bei dem ein aktives DDNS-Konto besteht, aus der Liste aus und tragen Sie Ihren „**Hostnamen**“ sowie Ihren „**Usernamen**“ und „**Passwort**“ in die dafür vorgesehenen Felder ein. Bitte ändern Sie das Interface auf „**43_INTERNET_R_VID_401/epon0.3**“

The screenshot shows the 'PBN PM520 Web Management' interface. The 'Network' menu is active, and the 'DDNS' sub-menu is selected. The main content area is titled 'Add Dynamic DNS'. Below the title, there is a brief instruction: 'This page allows you to add a Dynamic DNS address from DynDNS.org or TZO, NOIP.' The configuration form includes:

- 'D-DNS provider': A dropdown menu currently showing 'DynDNS.org'.
- 'Hostname': An empty text input field.
- 'Interface': A dropdown menu showing '43_INTERNET_R_VID_401/epon0.3'.
- 'DynDNS Settings': A section containing 'Username' and 'Password' text input fields.
- 'Apply/Save': A button located at the bottom right of the form.

Sie können unter „**Status**“ -> „**DDNS**“ kontrollieren ob sich das Modem bei Ihrem DDNS-Anbieter angemeldet hat und somit Ihr Modem über den Hostnamen erreichbar ist.

User Management

Auf dem Webinterface des Routers, klicken Sie auf "**Management**" im oberen Reiter, dann den "**User Manage**" Button und dann auf "**User Manage**" auf der linken Seite.

Die User Management Einstellungen erscheinen.



Wir bitten Sie, das Standardpasswort umgehend zu ändern!!!

DER USERNAME KANN NICHT GEÄNDERT WERDEN! Dieser wird bei Änderung nicht gespeichert!

The screenshot shows the 'PBN PM520 Web Management' interface. The top navigation bar includes 'Management', 'Status', 'Network', 'Security', 'Application', 'Management', and 'Diagnose'. Under 'Management', there are sub-menus for 'User Manage', 'Device Manage', 'Log File', and 'LOID'. The left sidebar has 'User Manage' and 'User Config' options. The main content area is titled 'Access Control -- Password' and contains the following text:

The CPE can be accessed by the following three User level accounts: Admin, Support and User.

The Admin account is able to access and modify all settings of the CPE. ISP technicians can use the Support account to maintain or test the CPE. The User account can only be used to view configurations and the CPE status. The user account can also update software.

Passwords are limited to 16 characters. Click "Save/Apply" to modify or create a password. Note: Passwords are not allowed to contain spaces.

User level	Username
Admin	Admin
Support	support
User	user

Below the table, there are input fields for:

- Select User level: Admin (dropdown menu)
- Username: Admin (text field)
- Old password: (text field)
- New username name: (text field) (If the user name is to remain unchanged please leave the field blank)
- New Password: (text field)
- Password Confirm: (text field)

A 'Save/Apply' button is located at the bottom right of the form.

Sie können auf dieser Seite das PASSWORT ihres Routers ändern.

Default User: **user**

Default Passwort: **changeme**

Klicken Sie "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

URL Filter

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**URL Filter**"

Die URL-Filter Einstellungen erscheinen.

PBN PM520 Web Management

Security | Status | Network | Security | Application | Management | Diagnose

URL Filter | Firewall | MAC Filter | Security Filter

URL Filter

URL Filter -- Please select the list type and set the rules. 100 rules supported at most.

Enable URL Filter

URL List Mode : Black List White List

URL Address	Port	Del
http://sampleblockpage.com	80	<input type="checkbox"/>

Add Del

Auf dieser Seite können Sie den URL-Filter für Ihr Heimnetzwerk aktivieren bzw. deaktivieren.

Sie haben 2 Möglichkeiten Webseiten zu sperren:

1. Black List
 - a. Mit dieser Einstellung können Sie den **Zugriff auf einzelne Webseiten sperren**.
 - b. Klicken Sie auf „Add“ und geben Sie die Adressen der Webseiten ein (IP-Adresse oder URL), auf die von Ihrem Heimnetzwerk aus nicht zugegriffen werden soll.
 - c. Alle anderen Webseiten bleiben von Ihrem Heimnetzwerk **erreichbar**.
2. White List
 - a. Mit dieser Einstellung können Sie den Zugriff auf einzelne Webseiten erlauben.
 - b. Klicken Sie auf „Add“ und geben Sie die Adressen der Webseiten ein (IP-Adresse oder URL), auf die von Ihrem Heimnetzwerk aus zugegriffen werden darf.
 - c. Alle anderen Webseiten sind von Ihrem Heimnetzwerk **gesperrt**.

Firewall

Im Webinterface Ihres Routers, klicken Sie auf **"Security"** in der obersten Reihe und schließlich auf **"Firewall"**

Die Firewall-Einstellungen erscheinen.

The screenshot shows the 'PBN PM520 Web Management' interface. The 'Security' menu is expanded, and the 'Firewall' sub-menu is selected. The main content area is titled 'Security Level' and contains the following text:

Select the Firewall Level:

Low: Protect nothing;

Medium: Denial of Service protections;

High: Forbid ICMP Input, Forbid Port Scan, Denial of Service protections;

Below this text, there is a 'Firewall Level:' label followed by a dropdown menu currently set to 'Low'. At the bottom of the configuration area is a 'Save/Apply' button.

Sie können aus 3 vordefinierten Sicherheitslevel wählen:

Sicherheitslevel	WAN (eingehende Pakete aus dem Internet)	LAN (ausgehende Pakete aus dem LAN)
Low	Keine Sicherheitseinstellungen; sämtliche Verbindungen aus dem Internet sind erlaubt!	Unbeschränkter Zugriff von Ihrem Heimnetzwerk ins World Wide Web
Medium	Schutz vor „Denial of Service“ Attacken; Ausnahmen können in den Port-Forwarding und DMZ Einstellungen vorgenommen werden!	Unbeschränkter Zugriff von Ihrem Heimnetzwerk ins World Wide Web
High	Sämtliche Ports sind von außen gesperrt! Schutz vor „Denial of Service“ und „ICMP“-Attacken; Ausnahmen können in den Port-Forwarding und DMZ Einstellungen vorgenommen werden!	Unbeschränkter Zugriff von Ihrem Heimnetzwerk ins World Wide Web

Klicken Sie nach dem Ändern auf **"Save/Apply"**, um Ihre Einstellungen dauerhaft zu speichern.

MAC Filter

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**MAC Filter**"

Die MAC Filter Einstellungen erscheinen.

PBN PM520 Web Management

Security | Status | Network | Security | Application | Management | Diagnose

URL Filter | Firewall | **MAC Filter** | Security Filter

MAC Filter

Add MAC Address Filter Rules

MAC Address Filter: Enable Disable

Filter Mode: Black List White List

MAC Address:

MAC Address	Del
00:11:22:aa:bb:cc	<input type="checkbox"/>

Auf dieser Seite können Sie folgende Einstellungen vornehmen:

- Enable/Disable MAC Address Filter
- Filter-Modus per Black- oder White List
- MAC Adressen für Filtereinstellungen

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

Security Filter

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**Security Filter**".

Die Security Filter Einstellungen erscheinen.

Port Id	Filter Mode
Port_1	BlackList
Port_2	BlackList
Port_3	BlackList
Port_4	BlackList

Port Id	Drection	EthType	SrcMac	DstMac	SrcIp	DstIp	IpProtocol	SrcStartPort	SrcEndPort	DstStartPort	DstEr
1	Ingress		00:00:00:11:11:11				0	0	0	0	0

Auf dieser Seite können Sie folgende Einstellungen vornehmen:

- Port ID
- Filter mode
- Filterkonfiguration

Sie können mit diesen Einstellungen den Datenverkehr einzelner LAN-Ports einschränken und steuern. Wir bitten diese Einstellungen nur dann vorzunehmen, wenn Sie einzelne LAN-Segmente voneinander trennen wollen!

Nach dem Auswählen des White/Black-List Modus, können Sie die einzelnen Regeln konfigurieren. Folgende Filterkriterien stehen zur Auswahl: Ethernet-Type, Source-MAC, Destination-MAC, Source-IP, Destination-IP, Protokoll sowie Source- und Destination-Port!

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

UPnP

Auf dem Web-Interface klicken Sie auf "**Application**" und dann auf den "**UPNP**" Reiter.

Die Einstellmöglichkeit für UPNP erscheint.

Status	Network	Security	Application	Management	Diagnose
NAT	UPNP	VoIP	IGMP	CATV	MAC Limited
				MLD	

UPnP Setting

Enable UPnP

Save/Apply

Der UPNP-Dienst kann entweder ein-/ oder ausgeschaltet werden.

UPnP (Universal Plug and Play) ist eine Zusammenarbeit von Protokollen, durch welche die Verbindung von Geräten möglich wird. Damit können Sie konfigurationsfrei über ihr Netzwerk miteinander kommunizieren. Media-Streaming ist der am häufigsten genutzte Dienst, da dadurch Mediendateien (Filme, Musik, usw.) direkt zu Ihrem TV-Gerät, Tablet oder Smartphone gestreamt werden können. Voraussetzung dafür sind die entsprechenden Apps auf Ihren Geräten!

Nach der Aktivierung klicken Sie auf "**Save/Apply**", um die Einstellung dauerhaft zu speichern.

NAT ALG Settings

Im Webinterface Ihres Routers, klicken Sie auf "**Application**" in der obersten Reihe, dann auf "**NAT**" und schließlich auf "**ALG**" auf der linken Seite.

Die NAT Application-Level Gateway Einstellungen erscheinen.

Application	Status	Network	Security	Application	Management	Diagnose
	NAT	UPNP	VoIP	IGMP	CATV	MAC Limited
ALG						
DMZ						
Virtual Server						

Application-level Gateway Settings

Select ALG :

- Enable H.323
- Enable SIP
- Enable RTSP
- Enable IPSEC
- Enable FTP
- Enable L2TP

[Save/Apply](#)

Hier können Sie folgende Einstellungen vornehmen:

- aktivieren/deaktivieren H.323 Access
- aktivieren/deaktivieren SIP
- aktivieren/deaktivieren RTSP
- aktivieren/deaktivieren IPSEC
- aktivieren/deaktivieren FTP
- aktivieren/deaktivieren L2TP
- aktivieren/deaktivieren

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

NAT DMZ Settings

Im Webinterface Ihres Routers, klicken Sie auf "**Application**" in der obersten Reihe, dann auf "**NAT**" und schließlich "**DMZ**" auf der linken Seite.

Die NAT DMZ Einstellungen erscheinen.

The screenshot shows the PBN PM520 Web Management interface. At the top left is the PBN logo and the text "PBN PM520 Web Management". At the top right is a "[Logout]" link. Below the header is a navigation menu with tabs for "Application", "Status", "Network", "Security", "Application", "Management", and "Diagnose". Under the "Application" tab, there are sub-tabs for "NAT", "UPNP", "VoIP", "IGMP", "CATV", "MAC Limited", "MLD", and "Other". The "NAT" sub-tab is selected, and the "DMZ" option is highlighted in the left sidebar. The main content area is titled "NAT -- DMZ Host" and contains the following text: "The CPE Router will send all WAN packets which are not included on the allowed list of the virtual server to the Demilitarised Zone. Input the DMZ Host IP address and click Save/Apply to activate the DMZ host. Clear the IP address and click Save/Apply to deactivate the DMZ host." Below this text is a text input field labeled "DMZ Host IP Address:" and a "Save/Apply" button.

Hier können Sie einen lokalen Computer oder eine IP-Adresse (Host) als DMZ (Demilitarized Zone) konfigurieren.



Ein DMZ Host wird nicht durch die Firewall geschützt und ist somit leicht angreifbar. Wenn Sie einen DMZ Host konfigurieren, müssen Sie das Sicherheitsrisiko berücksichtigen und sich gegebenenfalls selbst vor Attacken schützen.

Wollen Sie nur einzelne Ports für das Internet öffnen, so verwenden Sie bitte die Funktion **Virtual Server (Port Forwarding)**

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

NAT Virtual Server Settings

Im Webinterface Ihres Routers, klicken Sie auf "**Application**" in der obersten Reihe, dann auf "**NAT**" und schließlich "**Virtual Server**" auf der linken Seite.

Die NAT Virtual Server Einstellungen erscheinen.

Application	Status	Network	Security	Application	Management	Diagnose
NAT	UPNP	VoIP	IGMP	CATV	MAC Limited	MLD

ALG																			
DMZ																			
Virtual Server	<p>NAT -- Virtual Servers Setup</p> <p>Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.</p> <p style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </p> <table border="1"> <thead> <tr> <th>Server Name</th> <th>External Port Start</th> <th>External Port End</th> <th>Protocol</th> <th>Internal Port Start</th> <th>Internal Port End</th> <th>Server IP Address</th> <th>WAN Interface</th> <th>Remove</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove									
Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove											

Klicken Sie auf "**Add**" um zum Konfigurationsschirm zu gelangen. Hier können Sie vorkonfigurierte Einstellungen wählen oder eigene Port-Forwards einrichten. Verwenden Sie dazu immer das Interface „43_INTERNET_R_VID_401/epon0.3“.

Wenn Sie eine Regel hinzugefügt haben, klicken Sie auf „**Apply/Save**“ um diese zu speichern. Um eine Regel wieder zu entfernen, wählen Sie diese über die Checkbox aus und klicken Sie auf "**Remove**".