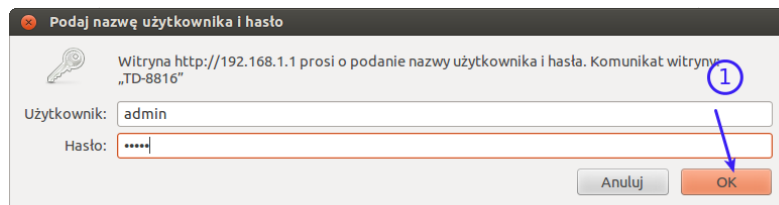


Konfiguracja ROUTERA TP-LINK TD-8816

- ✓ 2. Aby rozpocząć konfigurację routera należy uruchomić dowolną przeglądarkę internetową np. Mozilla Firefox i w pasku adresu wpisać następującą wartość: 192.168.1.1 zatwierdzając wybór klawiszem ENTER z klawiatury komputera.



- ✓ 2.1 Po zatwierdzeniu adresu w przeglądarce, przed nami powinna pojawić się strona logowania. W polu „User Name” wpisujemy „admin”, w pole „Password” wpisujemy „admin”. Aby przejść do panelu konfiguracji wciskamy przycisk OK.



- ✓ 3.1 Wybierz menu Interface Setup.
- ✓ 3.2 Ustaw Virtual Circuit : PVC2.
- ✓ 3.3 Zaznacz Encapsulation PPPoA/PPPoE.
- ✓ 3.4 PPP Username, PPP Password wpisz użytkownika i hasło, dane które otrzymałeś od swojego operatora.
- ✓ 3.5 Zapisz zmiany Save.

Interface Quick Start **Interface Setup** Advanced Setup Access Management Maintenance Status Help

Internet LAN

1

ATM VC

Virtual Circuit : PVC2 PVCs Summary

Status : Activated Deactivated

VPI : 0 (range: 0~255)

VCI : 35 (range: 1~65535)

2

QoS

ATM QoS : UBR

PCR : 0 cells/second

SCR : 0 cells/second

MBS : 0 cells

Encapsulation

ISP : Dynamic IP Address
 Static IP Address
 PPPoA/PPPoE 3
 Bridge Mode

PPPoE/PPPoA

Servicename :

Username : 4

Password :

Encapsulation : PPPoE LLC

Bridge Interface : Activated Deactivated

Connection Setting

Connection : Always On (Recommended)
 Connect On-Demand (Close if idle for 15 minutes)
 Connect Manually

TCP MSS Option : TCP MSS(default:1400) 1400 bytes

IP Address

Get IP Address : Static Dynamic

Static IP Address : 0.0.0.0

IP Subnet Mask : 0.0.0.0

Gateway : 0.0.0.0

NAT : Enable

Default Route : Yes No

TCP MTU Option : TCP MTU(default:1480) 1480 bytes

Dynamic Route : RIP2-B Direction : Both

Multicast : Disabled

MAC Spoofing : Enabled Disabled 5

00:00:00:00:00:00

SAVE DELETE

Zabezpieczenie Routera przed złośliwym oprogramowaniem i atakiem z zewnątrz.

Tworzenie ACL.

W celu ochrony routera przed dostępem z zewnątrz należy ustawić ACL.

- ✓ 4.1 Wybierz w menu Access Management.
- ✓ 4.2 Zaznacz ACL Activated, ACL Rule Index 1 Active :YES.
- ✓ 4.3 Source IP Address: Wpisz 0.0.0.0, wybierz Application All ,interface LAN.
- ✓ 4.4 Zapisz zmiany Save.

The screenshot shows the 'Access Management' configuration page. The top navigation bar includes 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Access Management', there are sub-menus: 'ACL', 'Filter', 'SNMP', 'UPnP', 'DDNS', and 'CWMP'. The 'ACL' sub-menu is selected. The page is divided into three sections: 'Access Control Setup', 'Access Control Editing', and 'Access Control Listing'. In the 'Access Control Setup' section, 'ACL' is set to 'Activated'. In the 'Access Control Editing' section, 'ACL Rule Index' is 1, 'Active' is 'Yes', 'Secure IP Address' is '0.0.0.0', 'Application' is 'ALL', and 'Interface' is 'LAN'. The 'Access Control Listing' section contains a table with one row: Index 1, Active Yes, Secure IP Address 0.0.0.0-0.0.0.0, Application ALL, Interface LAN. At the bottom, there are 'SAVE', 'DELETE', and 'CANCEL' buttons.

Access Management

Quick Start | Interface Setup | Advanced Setup | **Access Management** | Maintenance | Status | Help

ACL | Filter | SNMP | **UPnP** | DDNS | CWMP

Access Control Setup

2 → ACL : Activated Deactivated

1 →

Access Control Editing

3 → ACL Rule Index : 1

Active : Yes No

Secure IP Address : 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application : ALL

Interface : LAN

Access Control Listing

4 →

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN

SAVE DELETE CANCEL