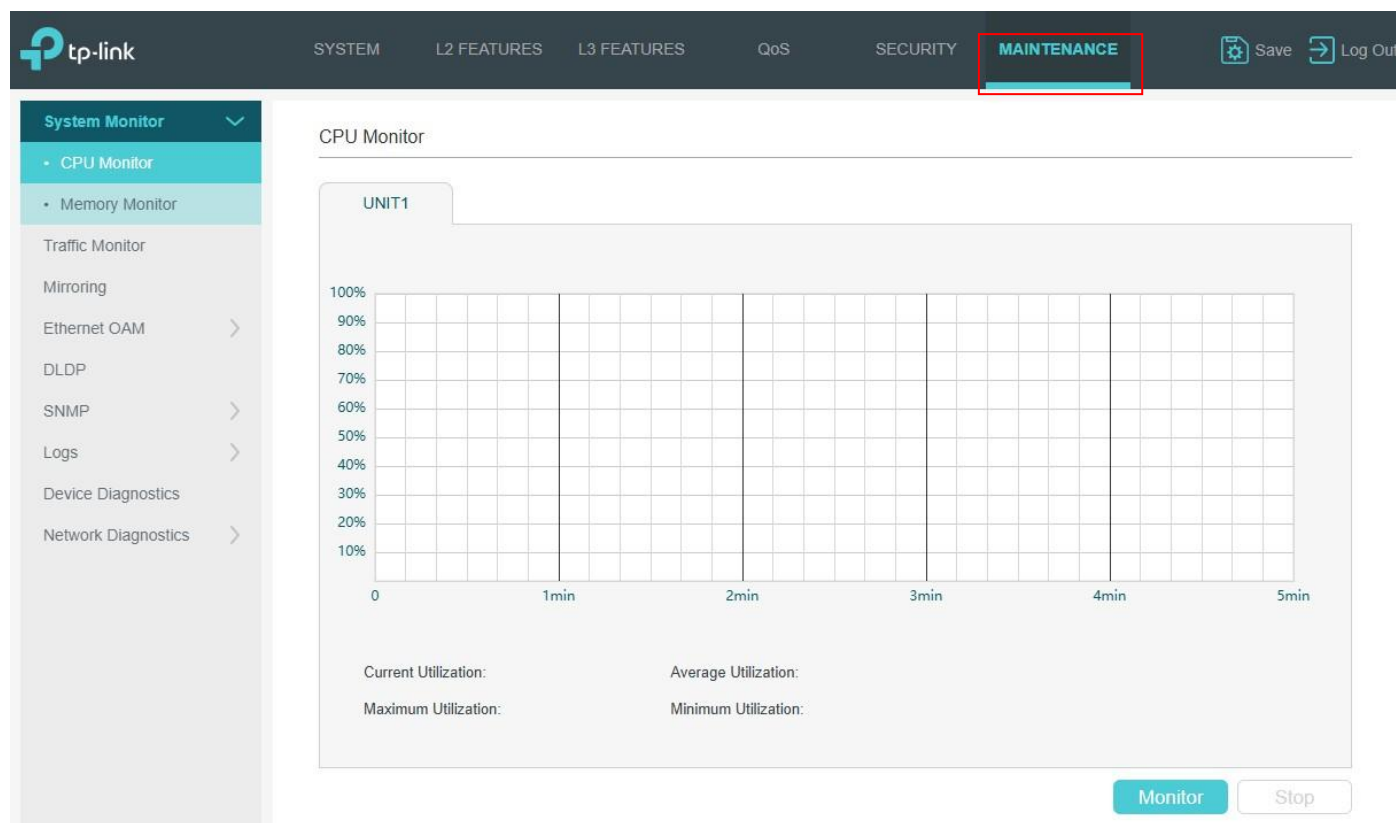


Port mirroring na switchu TP-Link TL-SG3210 – przekierowanie portów

Mirroring to funkcja switcha do analizy ruchu sieciowego i rozwiązywania problemów występujących w sieci. Funkcja ta umożliwia switchowi przesyłanie kopii ruchu przechodzącego przez określone źródła z określonego portu źródłowego do określonego portu docelowego

Kliknij **Maintenance** z górnego menu switcha



Przejdźmy do konfiguracji przekierowań pakietów. Wybierz **Mirroring** z lewego menu oraz **Edit**

The screenshot shows the TP-Link web interface with the 'MAINTENANCE' menu selected. The left sidebar shows 'Mirroring' highlighted with a red box. The main area displays the 'Port Mirroring Session List' table. The table has columns: 'Session', 'Destination Port', 'Mode', 'Source Interfaces', and 'Operation'. There is one session listed with 'Session' 1, 'Destination Port' empty, 'Mode' set to 'Ingress Only', 'Egress Only', and 'Both', and 'Source Interfaces' empty. The 'Operation' column shows 'Edit' and 'Clear' buttons, with 'Edit' highlighted by a red box. Below the table, it says 'Total: 1'.

Session	Destination Port	Mode	Source Interfaces	Operation
1		Ingress Only Egress Only Both		Edit Clear

Total: 1

Ingress Jeżeli włączysz tę opcję, pakiety odebrane przez odpowiedni interfejs zostaną skopiowane do portu docelowego. Domyślnie ta opcja jest włączona. **Egress** Jeżeli włączysz tę opcję, pakiety przesłane przez odpowiedni interfejs zostaną skopiowane do portu docelowego. Domyślnie ta opcja jest wyłączona.

Przekierowanie portów otwarte do edycji

tp-link SYSTEM L2 FEATURES L3 FEATURES QoS SECURITY MAINTENANCE Save Log Out

System Monitor
Traffic Monitor
Mirroring
Ethernet OAM
DLDP
SNMP
Logs
Device Diagnostics
Network Diagnostics

Back

Destination Port Config

UNIT1

1 2 3 4 5 6 7 8 9 10

Apply

Source Interfaces Config

UNIT1	LAGS	CPU		
☐	Port	Ingress	Egress	LAG
☐	1/0/1	Disabled	Disabled	--
☐	1/0/2	Disabled	Disabled	--
☐	1/0/3	Disabled	Disabled	--
☐	1/0/4	Disabled	Disabled	--
☐	1/0/5	Disabled	Disabled	--
☐	1/0/6	Disabled	Disabled	--
☐	1/0/7	Disabled	Disabled	--
☐	1/0/8	Disabled	Disabled	--
☐	1/0/9	Disabled	Disabled	--
☐	1/0/10	Disabled	Disabled	--
Total: 10				

Wybieramy port **docelowy** – ten **na który zostaną przekierowane pakiety**. W naszym przypadku jest to **port 6 switcha**. Wybór akceptujemy przyciskiem **Apply**

tp-link SYSTEM L2 FEATURES L3 FEATURES QoS SECURITY MAINTENANCE Save Log Out

System Monitor
Traffic Monitor
Mirroring
Ethernet OAM
DLDP
SNMP
Logs
Device Diagnostics
Network Diagnostics

Back

Destination Port Config

UNIT1

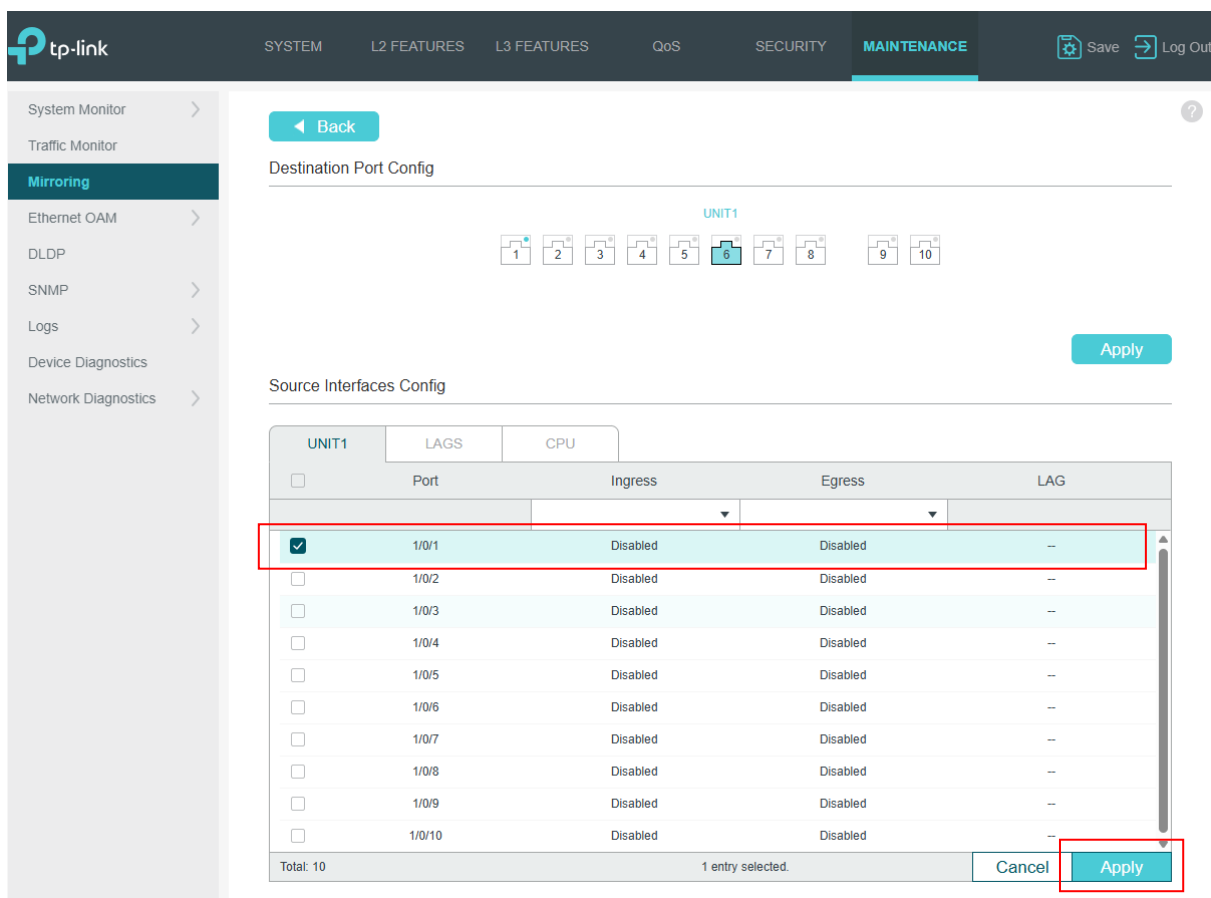
1 2 3 4 5 6 7 8 9 10

Apply

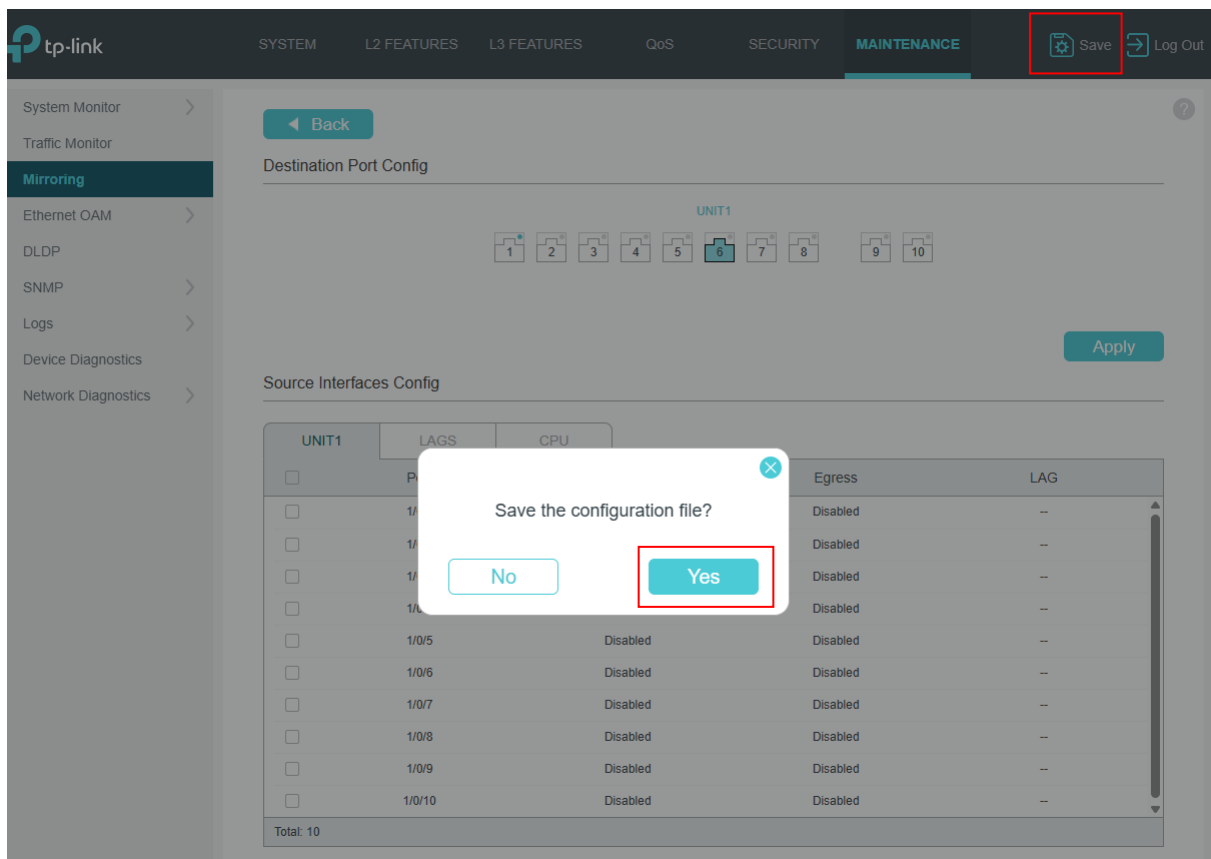
Source Interfaces Config

UNIT1	LAGS	CPU		
☐	Port	Ingress	Egress	LAG
☐	1/0/1	Disabled	Disabled	--
☐	1/0/2	Disabled	Disabled	--
☐	1/0/3	Disabled	Disabled	--
☐	1/0/4	Disabled	Disabled	--
☐	1/0/5	Disabled	Disabled	--
☐	1/0/6	Disabled	Disabled	--
☐	1/0/7	Disabled	Disabled	--
☐	1/0/8	Disabled	Disabled	--
☐	1/0/9	Disabled	Disabled	--
☐	1/0/10	Disabled	Disabled	--
Total: 10				

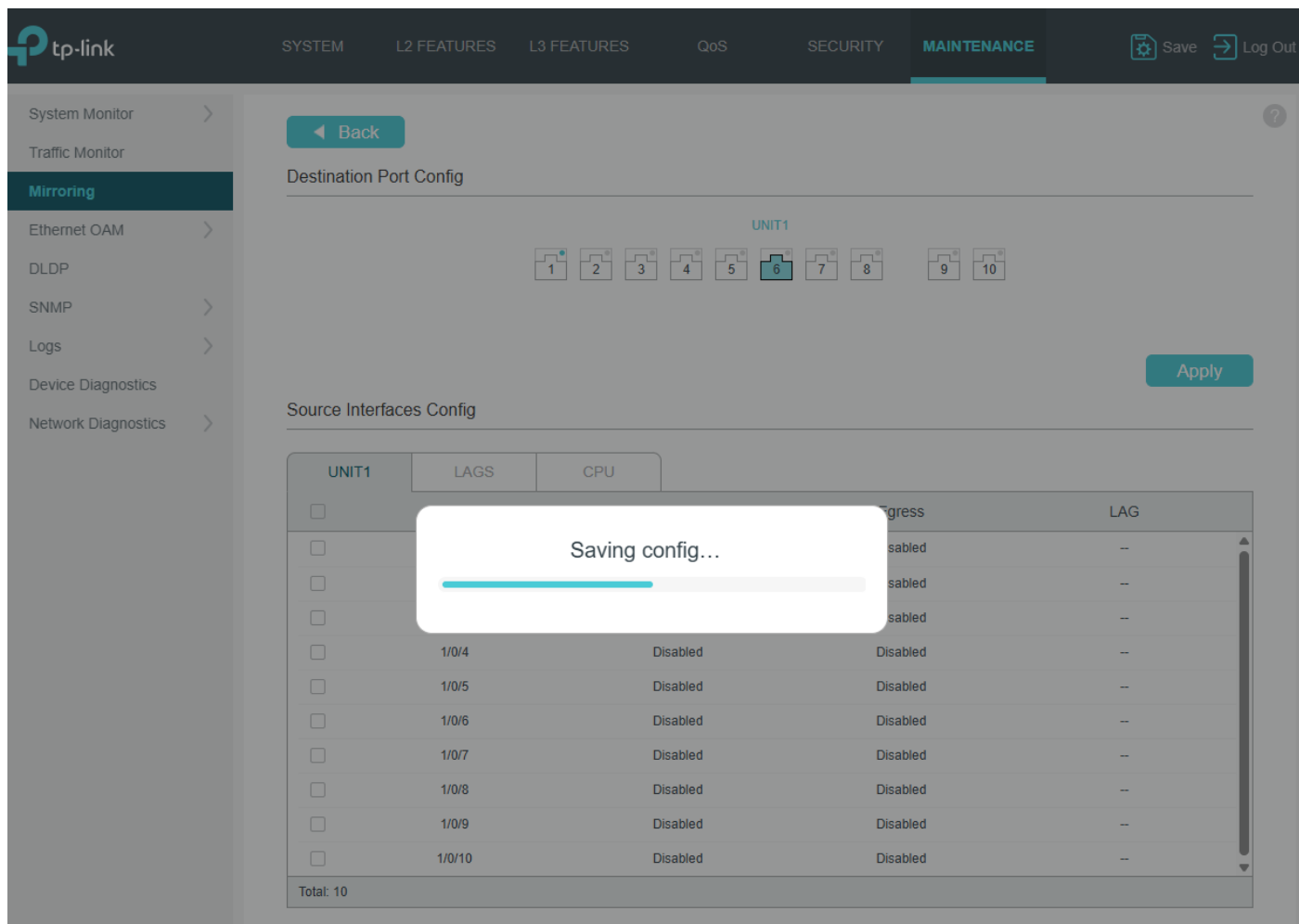
Po kliknięciu przycisku **Apply** w poprzednim oknie, otwiera się możliwość wybrania portu **źródłowego** z którego zostaną przechwycone pakiety danych. Wybrany port źródłowy to **port 1**. Wybór akceptujemy przyciskiem **Apply**



Zapisujemy konfigurację switcha wybierając **Save** z górnego menu oraz potwierdzamy ją przyciskiem **Yes**



Switch zachowuje konfigurację



Połączenia switcha: **port 1** – dostęp do Internetu (połączenie switcha do routera lub gniazda w ścianie), **port 6** – podłączony komputer 2 z zainstalowanym programem Wireshark przechwytyjący pakiety z portu 1, **port 7** komputer 1 korzystający z Internetu poprzez switch. **Cały ruch sieciowy przechodzący przez port 1 jest przechwytywany przez port 6**



Program **Wireshark** zainstalowany na komputerze 2 przechwytyjący ruch sieciowy z **portu 6** switcha. Wybierz **Przechwytywanie** z górnego menu programu, by wyświetlić dane. Dane można filtrować, wybierając do monitorowania np. odpowiedni protokół sieciowy (TCP, UDP, ICMP, ARP...) oraz zapisywać do pliku do późniejszej analizy

Capturing from Wi-Fi

Plik Edycja Widok Przejdź **Przechwytywanie** Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

Zastosuj filtr wyświetlania ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
158	15.871726300	192.168.10.44	255.255.255.255	UDP	762	39100 → 29810 Len=720
159	16.070428800	HuaweiTechno_44:68:...	Broadcast	0x9998	60	Ethernet II
160	16.377614500	FroniusSchwe_1b:4b:...	Broadcast	ARP	60	Who has 192.168.100.1? Tell 192.168.100.101
161	16.788821300	192.168.10.50	192.168.10.255	UDP	182	1027 → 1283 Len=140
162	16.895870900	192.168.10.96	255.255.255.255	UDP	781	48835 → 29810 Len=739
163	17.196819900	LiteonTechno_84:df:...	Broadcast	ARP	60	Who has 192.168.10.199? Tell 192.168.10.12
164	17.708966300	192.168.10.50	224.0.0.251	MDNS	78	Standard query 0x0000 PTR _nc-cmf._tcp.local, "QM" questi
165	18.119139000	LiteonTechno_84:df:...	Broadcast	ARP	60	Who has 192.168.10.199? Tell 192.168.10.12
166	18.227086300	192.168.10.95	255.255.255.255	UDP	781	58115 → 29810 Len=739
167	18.229048000	HuaweiTechno_bd:b0:...	Broadcast	0x9998	60	Ethernet II
168	18.236505600	192.168.10.42	255.255.255.255	UDP	780	34453 → 29810 Len=738
169	18.630569400	192.168.10.50	224.0.0.251	MDNS	78	Standard query 0x0000 PTR _nc-cmf._tcp.local, "QM" questi
170	19.142389200	LiteonTechno_84:df:...	Broadcast	ARP	60	Who has 192.168.10.199? Tell 192.168.10.12

> Frame 1: Packet, 781 bytes on wire (6248 bits), 781 bytes captured
> Ethernet II, Src: TplinkTechno_49:7b:97 (50:d4:f7:49:7b:97), Dst:
> Internet Protocol Version 4, Src: 192.168.10.163, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 47383, Dst Port: 29810
> Data (739 bytes)

0000 ff ff ff ff ff ff 50 d4 f7 49 7b 97 08 00 45 a0P
0010 02 ff 54 51 00 00 40 11 57 b2 c0 a8 0a a3 ff ff ..TQ..@.
0020 ff ff b9 17 74 72 02 eb 3e 9b 00 00 02 df 7b 0atr..
0030 09 22 68 65 61 64 65 72 22 3a 09 7b 0a 09 09 22 .."header
0040 76 65 72 73 69 6f 6e 22 3a 09 22 54 50 2d 4c 49 version"
0050 4e 4b 20 45 43 53 20 76 65 72 20 31 2e 31 2e 30 NK ECS v
0060 22 2c 0a 09 09 22 6d 61 63 22 3a 09 22 35 30 3a ",...ma
0070 64 34 3a 66 37 3a 34 39 3a 37 62 3a 39 37 22 2c d4:f7:49
0080 0a 09 09 22 74 79 70 65 22 3a 09 31 2c 0a 09 09 ..."type
0090 22 65 72 72 6f 72 22 3a 09 30 0a 09 7d 2c 0a 09 "error":
00a0 22 62 6f 64 79 22 3a 09 7b 0a 09 09 22 64 65 76 "body":
00b0 69 63 65 49 6e 66 6f 22 3a 09 7b 0a 09 09 22 iceInfo"
00c0 6d 6f 64 65 6c 22 3a 09 22 45 41 50 31 31 30 22 model":
00d0 2c 0a 09 09 09 22 6e 61 6d 65 22 3a 09 22 45 41 ,...na
00e0 50 31 31 30 2d 35 30 2d 44 34 2d 46 37 2d 34 39 P110-50-
00f0 2d 37 42 2d 39 37 22 2c 0a 09 09 09 22 66 69 72 -7B-97",
0100 61 77 64 73 65 66 6f 72 73 66 6f 6f 6f 6f 6f ..

Wi-Fi: <live capture in progress> Pakiety: 170 Profil: Default