



instrukcja obsługi

Comtrend VI-3225u

Wersja E2.0,
15 czerwiec 2016



Wstęp

Instrukcja ta zawiera informacje o instalacji i działaniu urządzenia. Aby w pełni skorzystać z instrukcji wymagana jest podstawowa znajomość terminologii telekomunikacyjnej.

Informacje o produktach, nowe wersje urządzeń oraz poprawki instrukcji znajdziesz na naszej stronie: <http://www.orange.pl/>

Ważne instrukcje bezpieczeństwa

Następujące reguły postępowania są wskazane podczas rozpakowywania, instalacji oraz użytkowania twojego urządzenia elektronicznego.

- Aby uniknąć porażenia prądem, nie używaj, oraz nie instaluj tego urządzenia w pobliżu wody, na przykład blisko wanny, zlewu kuchennego, w pralni, blisko basenu. Nie umieszczaj urządzenia w miejscu narażonym na działanie deszczu lub wilgoci (np. wilgotna piwnica).
- Nie podłączaj przewodu zasilającego tak aby wisiął, lecz umieść go tak aby leżał swobodnie. Na jego drodze nie powinno być żadnych przeszkód, jak również nie powinny na nim leżeć żadne ciężkie przedmioty. Nie chodź po nim, nie deptaj i nie gnij przewodu.
- Używaj tylko przewodu zasilającego i zasilacza dostarczonego z urządzeniem.
- Aby zabezpieczyć urządzenie przed przegrzaniem upewnij się, że żaden otwór w obudowie nie jest zablokowany.
- Unikaj używania telefonu (z wyłączeniem bezprzewodowych) podczas burzy. Istnieje ryzyko porażenia podczas uderzenia błyskawicy. Nie używaj telefonu, do powiadomienia o wycieku gazu, będąc w pobliżu wycieku.
- Nigdy nie instaluj okablowania telefonicznego podczas pogody burzowej.

UWAGA:

- Aby zniwelować ryzyko pożaru, używaj jedynie kabla telekomunikacyjnego nr 26 AWG lub grubszego.
- Zawsze odłączaj wszystkie linie telefoniczne z gniazdka przed naprawą lub rozbiórką urządzenia



OSTRZEŻENIE

- Odłącz zasilanie od urządzenia, zanim zaczniesz naprawę.
- Parametry zasilacza są podane w Załącznik B - Specyfikacje

Chroń nasze środowisko naturalne.



Ten symbol informuje, że dane urządzenie powinno być przekazane do specjalnej jednostki zajmującej się segregacją i przetwarzaniem odpadów komunalnych.

Pudełko kartonowe, plastik znajdujący się w opakowaniu, oraz części które są elementami routera mogą być segregowane w zgodzie z miejscowymi regulacjami prawnymi. Nigdy nie wyrzucaj tego urządzenia elektronicznego razem z odpadkami z Twojego gospodarstwa domowego. Możesz w związku z tym zostać pociągnięty do odpowiedzialności karnej lub innej przez lokalne organy ścigania. Proszę postępuj odpowiedzialnie i zdobądź informacje o wyrzuceniu urządzenia od lokalnej jednostki samorządowej.

Spis treści

Spis treści	4
Rozdział 1 Wstęp	7
1.1 Właściwości urządzenia	7
1.2 Zastosowanie	7
Rozdział 2 Instalacja	8
2.1 Konfiguracja sprzętu	8
2.2 Panel przedni - diody informacyjne LED	9
Rozdział 3 Interfejs użytkownika WWW	12
3.1 Ustawienia domyślne	12
3.2 Konfiguracja IP	12
3.3 Logowanie	14
Rozdział 4 Informacje o urządzeniu	17
4.1 Statystyki	17
4.1.1 Statystyki LAN	18
4.1.2 Statystyki WAN	18
4.1.3 Statystyki xTM	19
4.1.4 Statystyki xDSL	20
4.2 Routing	24
4.3 ARP	25
4.4 DHCP	25
4.5 Sesje NAT	26
4.6 IPv6	27
4.6.1 IPv6 info	27
4.6.2 IPv6 Route	27
Rozdział 5 Zaawansowana konfiguracja	28
5.1 WAN	28
5.2 LAN	30
5.2.1 Autokonfiguracja IPv6	32
5.3 NAT	33
5.3.1 Serwery wirtualne	33
5.3.2 Wyzwalanie portów	35
5.3.3 Host DMZ	36
5.4 Bezpieczeństwo	36
5.4.1 Filtrowanie adresów IPv4	36

5.4.2	Filtrowanie adresów IPv6	38
5.5	Kontrola rodzicielska	41
5.5.1	Ograniczenia czasu dostępu	41
5.5.2	Filtr URL	42
5.6	DNS	42
5.6.1	Serwer DNS	43
5.6.2	Dynamiczny DNS	43
5.7	UPnP	44
5.8	DNS Proxy/Relay	44
5.9	Serwer wydruku	45
5.10	DLNA	45
5.11	Przechowywanie plików	46
5.12	Zarządzanie energią	46
Rozdział 6	Sieć bezprzewodowa	48
6.1	Podstawowa konfiguracja	48
6.2	Bezpieczeństwo	49
6.2.1	WPS	52
6.3	Filtrowanie MAC	56
6.4	Zaawansowana konfiguracja	56
6.5	Informacje o urządzeniach	59
Rozdział 7	Połączenia głosowe	60
7.1	Ustawienia Podstawowe SIP	60
7.1.1	Parametry globalne	60
7.1.2	Usługodawca	61
7.2	Zaawansowane ustawienia SIP	62
7.2.1	Parametry globalne	62
7.2.2	Usługodawca	63
7.3	Ustawienia Debugowania SIP	65
7.3.1	Parametry globalne	65
7.3.2	Usługodawca	66
7.4	Połączenia telefoniczne	66
Rozdział 8	Diagnostyka	69
Rozdział 9	Zarządzanie	70
9.1	Ustawienia	70
9.1.1	Przywróć ustawienia domyślne	70
9.2	Logi systemowe	71
9.3	Zarządzanie kontem	73
9.3.1	Hasła	73

9.4 Ponowne uruchomienie	74
Załącznik A – Zapora sieciowa	75
Załącznik B - Specyfikacje	77
Załącznik C – Zewnętrzny Rejestrator WPS.....	79
Załącznik D – Serwer Wydruku.....	82
Windows XP	82
Windows 7.....	87
Windows VISTA.....	93
Windows 10.....	98

Rozdział 1 Wstęp

Router **Comtrend VI-3225u** Multi-DSL WLAN IAD pozwala na przewodowy i bezprzewodowy dostęp wysokiej przepustowości w domu lub biurze. Wyposażony jest w cztery porty Sieci lokalnej RJ-45, oraz wspiera ADSL2+ i VDSL2 przez port RJ-11. ADSL2+ wspiera wiele jednoczesnych połączeń internetowych, podczas gdy VDSL2 jest połączeniem odpowiednim dla usług triple-play (Wideo + Dźwięk + Dane).

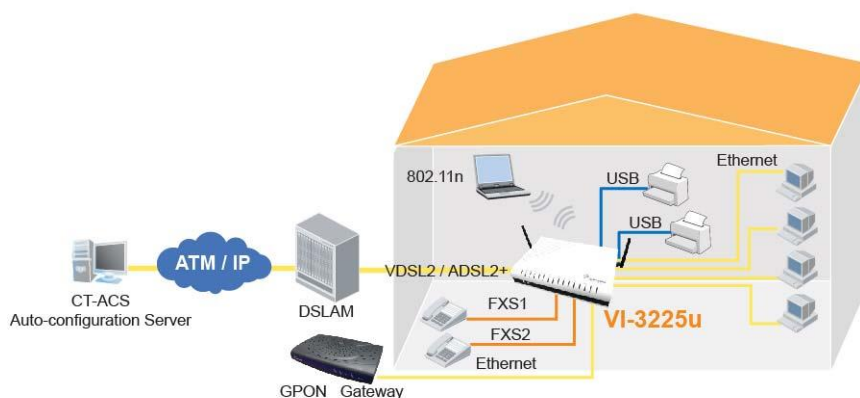
Zintegrowany punkt dostępowego WLAN ACCESS Point (AP) zgodny ze standardem 802.11n pozwala na szybszy dostęp bezprzewodowy ze zwiększonym zasięgiem, w porównaniu do 802.11b i 802.11g, oraz pozwala na wsteczną kompatybilność z tymi starszymi standardami. Przyciski WPS (Wi-Fi Protected Setup) oraz Wi-Fi On/Off znajdują się z przodu obudowy w celu łatwiejszego dostępu do funkcji obsługi sieci Wi-Fi.

1.1 Właściwości urządzenia

- Zintegrowany punkt dostępu 802.11n (kompatybilny z 802.11b/g)
- Comtrend VI-3225u - Annex A
- Wsparcie dla profilu VDSL2 17a
- QoS na poziomie pakietów IP oraz per VC
- WAP and 802.1x
- Statyczny routing & RIP/RIP v2
- NAT/PAT
- IGMP Proxy
- Zarządzanie przez stronę WWW
- Automatyczne przełączanie pomiędzy ADSL2+ / VDSL2 zgodnie z ustawieniami DSLAM
- Wsparcie dla VPN Pass-Through
- Wsparcie dla T.38
- Automatyczna konfiguracja PVC
- IP/MAC filtrowanie
- Dynamiczne przypisywanie IP
- Kontrola rodzicielska
- DHCP Server/Relay/Client
- Wsparcie dla połączeń alarmowych
- Wsparcie dla wyświetlania i blokowania numeru dzwoniącego
- Wsparcie dla bezpośredniego wybierania numeru
- Wspiera zdalne zarządzanie

1.2 Zastosowanie

Następujący rysunek pokazuje typowe zastosowanie routera **Comtrend VI-3225u**.



Rozdział 2 Instalacja

2.1 Konfiguracja sprzętu

Postępuj zgodnie z instrukcją poniżej.



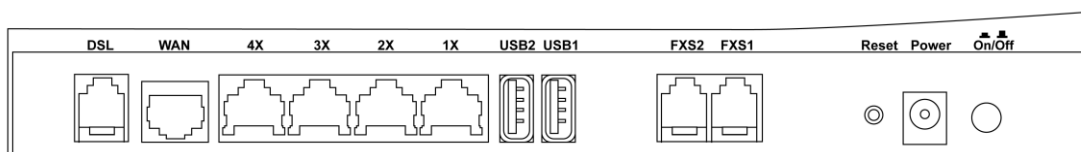
DO NOT STACK

Nie stawiaj urządzeń na sobie!

Te urządzenia nie mogą pracować ustawione jedno na drugim. Może to powodować pogorszenie osiągnięć, przegrzewanie się routera, a w efekcie jego uszkodzenie.

PANEL TYLNY

Poniższy rysunek pokazuje tylny panel urządzenia



PORT DSL

Podłącz linię ADSL2+/VDSL do tego portu używając kabla telefonicznego (RJ-11).

PORT WAN

Podłącz do źródła Internetu używając kabla RJ-45

PORTY LAN

Użyj kabli RJ-45 klasy 1000-BASE-T aby podłączyć do czterech urządzeń do sieci Gigabit LAN lub 10/100BASE-T RJ-45 dla wolniejszych sieci. Porty automatycznie rozpoznają kable MDI/X typu prostego lub skrosowane.

PORTY USB

Dwa porty USB 2.0 wspierają kompatybilne drukarki. Sprawdź Załącznik D w celu uzyskania instrukcji. Wsparcie dla innych urządzeń może być dodane w następnych aktualizacjach oprogramowania.

Porty FXS

Podłącz telefony kablem RJ-11, aby skorzystać z sieci VoIP.

Przycisk Reset

Przywróć ustawienia domyślne urządzenia wciskając przycisk Reset przez 5 do 10 sekund.

UWAGA: Jeśli przycisk zostanie wciśnięty przez powyżej 20 sekund router Comtrend VI-3225u zostanie zablokowany (dioda Power świeci się na kolor czerwony). Przed resetem modemu należy skontaktować się z obsługą techniczną.

Power ON

Wciśnij przycisk, aby znalazł się w pozycji OFF (wyciśnięty). Podłącz zasilacz do gniazda zasilania w urządzeniu. Podłącz zasilacz do gniazdka w ścianie lub do listwy zasilającej. Wciśnij przycisk Power, aby znalazł się w pozycji ON (wciśnięty). Jeśli wskazania LED są poprawne, urządzenie jest gotowe do konfiguracji (sprawdź rozdział 2.2 *Panel przedni - diody informacyjne LED*).

UWAGA 1: Jeśli urządzenie nie włącza się lub nie działa, sprawdź czy wszystkie kable zasilające są podłączone prawidłowo i uruchom ponownie urządzenie. Jeśli problem nadal występuje skontaktuj się ze wsparciem technicznym.

UWAGA 2: Przed naprawą lub rozebraniem urządzenia, odłącz wszystkie przewody zasilające oraz telefoniczne od urządzenia.

PANEL PRZEDNI

Przyciski W-Fi & WPS znajdują się z lewej strony panelu, zgodnie z rysunkiem.



Przycisk Wi-Fi

Wciśnij ten przycisk, aby włączyć sieć Wi-Fi

Przycisk WPS

Wciśnij ten przycisk aby rozpocząć wyszukiwanie klientów WPS. Klienci ci muszą również wspierać tryb WPS. Jeśli WPS jest aktywny, Dioda LED WPS będzie się świeciła.

2.2 Panel przedni - diody informacyjne LED

Diody informacyjne LED panelu przedniego są pokazane i wyjaśnione poniżej. Informacje te może być wykorzystana do sprawdzenia stanu urządzenia i jego połączeń.



LED	Kolor	Tryb	Funkcja
POWER	Zielony	 Wł.	Urządzenie jest włączone.
		 Wył.	Urządzenie jest wyłączone.
		 Miga	Urządzenie pobiera nową wersję oprogramowania
	Czerwony	 Wł.	Błąd POST (Power On Self Test); może być to dowolny błąd wewnętrznej sekwencji uruchamiania urządzenia lub stan w którym niemożliwe jest podłączenie do sieci i przesyłania danych użytkownika.
	Pomarańczowy	 Wł.	Jeśli przycisk Reset był wciśnięty przez więcej niż 5 sekund, w celu przywrócenia ustawień fabrycznych, dioda zasilania powinna zmienić kolor na pomarańczowy (mrużyć przez 1 sekundę) powiadamiając o gotowości do restartu fabrycznego.
LAN 1X-4X	Zielony	 Wł.	Ustanowiono połączenie sieci lokalnej.
		 Wył.	Brak połączenia sieci lokalnej.
		 Miga	Transmisja danych w sieci lokalnej.
WAN	Czerwony	 Wł.	Ustanowiono połączenie sieci lokalnej WAN z prędkością 1000 Mb/s.
		 Wył.	Brak połączenia sieci lokalnej WAN.
		 Miga	Transmisja danych po interfejsie WAN
	Zielony	 Wł.	Ustanowiono połączenie sieci lokalnej WAN z prędkością 10/100 Mb/s.
		 Wył.	Brak połączenia sieci lokalnej WAN.
		 Miga	Transmisja danych w sieci lokalnej WAN.
WLAN	Zielony	 Wł.	Moduł bezprzewodowy jest gotowy (zainstalowany i uruchomiony).
		 Wył.	Moduł bezprzewodowy jest nieaktywny (nie jest zainstalowany lub uruchomiony).
		 Miga	Transmisja danych w sieci WLAN.
WPS	Zielony	 Wł.	WPS jest aktywny i urządzenie PC jest połączone do sieci WLAN.
		 Wył.	WPS wyłączony (wyłącza się po 5 minutach).
		 Miga	Router szuka klientów WPS lub WPS nie jest skonfigurowany.
FXS	Zielony	 Wł.	Telefon podłączony do portu FSX ma podniesioną słuchawkę.
		 Wył.	Telefon podłączony do portu FSX ma odłożoną słuchawkę.
DSL	Zielony	 Wł.	Ustanowiono połączenie DSL.
		 Wył.	Brak połączenia DSL.

		 Miga	Testowanie połączenia DSL.
INTERNET	Zielony	 Wł.	Sieć IP połączona, brak transmisji danych, Jeśli sesja IP lub PPPoE została odłączona, powiadomienie nadal pozostanie zielone, jeśli sesja ADSL jest aktywna.
		 Wył.	Modem wyłączony, w trybie mostka lub brak połączenia ADSL, dodatkowo, jeśli sesja IP lub PPPoE jest zerwana z innego powodu niż nieaktywność powiadomienie jest wyłączone.
		 Miga	Połączenie IP aktywne, oraz ruch IP przesyłany przez urządzenie.
	Czerwony	 Wł.	Urządzenie nie uzyskało połączenia IP (brak odpowiedzi DHCP, brak PPPoE lub brak uwierzytelnienia PPPoE, brak odpowiedzi adresu IP z IPCP, itd.).

Rozdział 3 Interfejs użytkownika WWW

Ten rozdział opisuje jak uzyskać dostęp do urządzenia przez interfejs WWW używając przeglądarki internetowej, takiej jak Internet Explorer (wersja 5.0 lub późniejsza).

3.1 Ustawienia domyślne

Ustawienia fabryczne urządzenia są wymienione poniżej:

- Adres IP LAN: 10.0.0.1
- Maska podsieci LAN: 255.255.255.0
- Dostęp dla użytkownika:
 - Dla usługi Internet DSL: (użytkownik: **user**, hasło: **user**)
 - Dla usługi Biznes pakiet: (użytkownik: **bpack**, hasło: **bpack**)

UWAGA: W trakcie pierwszej konfiguracji zalecane jest zmiana domyślnego hasła dostępu do routera. Należy to wykonać w zakładce Zarządzanie, następnie przejść do Zarządzanie kontem, i wybrać Hasła. (sprawdź rozdział 9.3.1 Hasła)

Informacja techniczna

Podczas uruchamiania urządzenia, wszystkie ustawienia są przywracane do wartości domyślnych. Następnie odczytany zostanie profil konfiguracji z pamięci lub pamięci flash. Wartości domyślne są nadpisane nowymi wartościami, jeśli zostały odpowiednio wcześniej skonfigurowane. Konfiguracja w pamięci może zostać utworzona przez interfejs WWW. Konfiguracja fabryczna może zostać przywrócona przez wciśnięcie przycisku reset przez 5 sekund, aż dioda LED zasilania będzie migać.

UWAGA: Jeśli przycisk zostanie wciśnięty przez powyżej 20 sekund router Comtrend VI-3225u zostanie zablokowany (dioda Power świeci się na kolor czerwony). Przed resetem modemu należy skontaktować się z obsługą techniczną.

3.2 Konfiguracja IP

TRYB DHCP

Podczas uruchamiania routera Comtrend VI-3225u aktywowany jest na nim serwer DHCP. Jego rola to przydzielanie adresów IP urządzeniom sieci LAN, czyli twoim komputerom.

Aby uzyskać adres IP z serwera DHCP, postępuj wg kroków wymienionych poniżej.

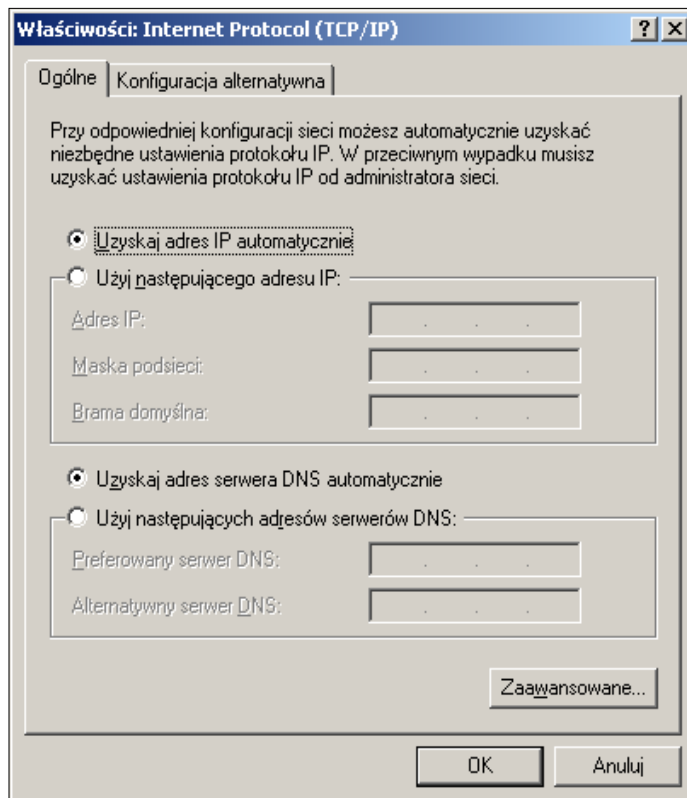
UWAGA: Ta procedura zakłada, że używasz systemu Windows XP, aczkolwiek, główne kroki wymienione poniżej są zbliżone dla wszystkich systemów operacyjnych. Skorzystaj ze wsparcia dla twojego systemu, aby uzyskać dalsze informacje.

KROK 1: Z okna Połączeń sieciowych wybierz **Połączenie sieci lokalnej** (Local Area Connection). Możesz również uzyskać dostęp do tego okna przez dwukrotne kliknięcie ikony Połączenie sieci lokalnej na

twoim pasku zadań. Kliknij przycisk **Właściwości**.

KROK 2: Wybierz **Internet Protocol (TCP/IP)** oraz kliknij przycisk właściwości.

KROK 3: Wybierz opcję "Uzyskaj adres IP automatycznie".



KROK 4: Wybierz **OK**, aby zapisać ustawienia.

Jeśli masz problem z połączeniem DHCP, spróbuj trybu IP statycznego.

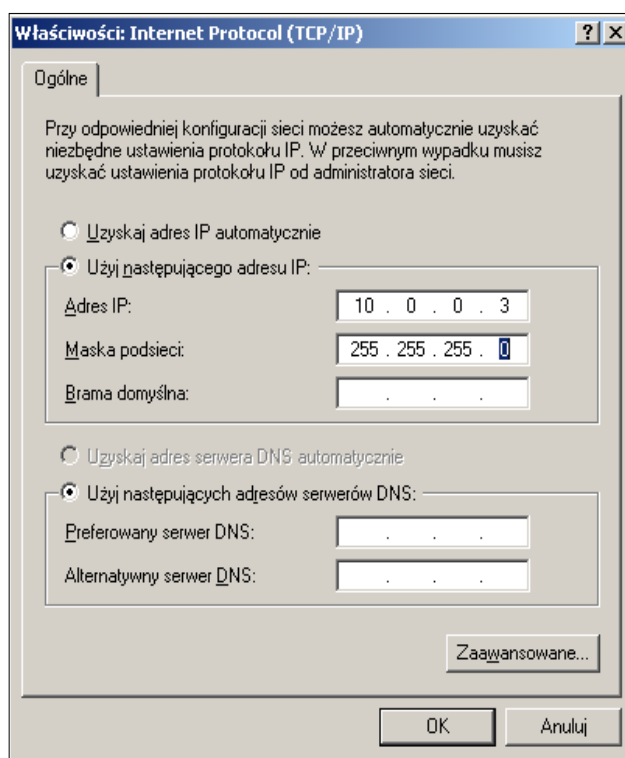
TRYB IP STATYCZNEGO

W trybie statycznego adresu IP, podajesz adresy komputerów samodzielnie.

Postępuj według poniższych kroków, aby skonfigurować adres z podsieci 10.0.0.x, ustawionej domyślnie na modemie lub by skorzystać z adresacji publicznej.

UWAGA: Ta procedura zakłada, że używasz systemu Windows XP, aczkolwiek, główne kroki wymienione poniżej są zbliżone dla wszystkich systemów operacyjnych. Skorzystaj ze wsparcia dla twojego systemu, aby uzyskać dalsze informacje.

- KROK 1:** Z okna Połączeń sieciowych wybierz **Połączenie sieci lokalnej** (Local Area Connection). Możesz również uzyskać dostęp do tego okna przez dwukrotne kliknięcie ikony Połączenie sieci lokalnej na twoim pasku zadań. Kliknij przycisk **Właściwości**.
- KROK 2:** Wybierz **Internet Protocol (TCP/IP)** oraz kliknij przycisk właściwości.
- KROK 3:** Wybierz opcję *Użyj następującego adresu IP*. Zmień adres IP na jeden z podsieci 10.0.0.x (1<x<255) z maską podsieci 255.255.255.0. Ekran powinien wyglądać jak poniżej:



- KROK 4:** Wybierz **OK** aby zapisać ustawienia.

3.3 Logowanie

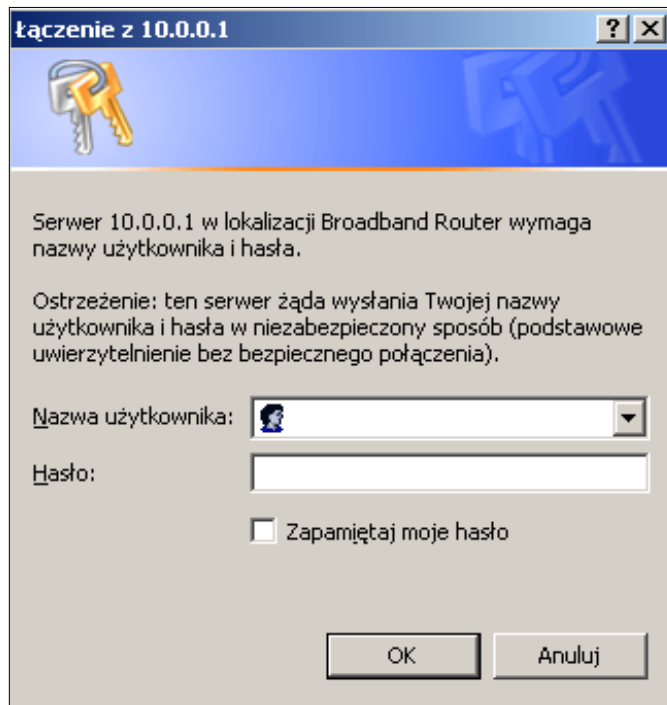
Postępuj wg poniższych instrukcji, aby uzyskać dostęp do konfiguracji routera za pomocą strony WWW

UWAGA: Ustawienia domyślne znajdują się w rozdziale 3.1 Ustawienia domyślne

KROK 1: Uruchom przeglądarkę internetową i wpisz adres IP routera. Jeśli jest niezmieniony, to domyślny adres to 10.0.0.1. W polu adresu wpisz zatem adres: <http://10.0.0.1>

UWAGA: W celu zarządzania siecią lokalną komputer z przeglądarką musi być podłączony do sieci lokalnej, niekoniecznie do samego urządzenia.

KROK 2: Pokaże się okno dialogowe, jak na rysunku poniżej, wpisz nazwę użytkownika i hasło (domyślne wartości znajdują się w rozdziale *3.1 Ustawienia domyślne*).



KROK 3: Wybierz **OK** aby kontynuować.

UWAGA: Hasło może zostać zmienione (sprawdź rozdział 9.3.1 Hasła).

KROK 4: Po prawidłowym zalogowaniu, zobaczysz ten ekran:

Ze względów bezpieczeństwa zalecana jest zmiana domyślnego hasła Wi-Fi.
Domyślne hasło może różnić się od zapisanego na obudowie modemu.

SSID:	COMTREND-VI-3223u-5555
Aktualne hasło Wi-Fi:	74F3D03A6C15AAD
Proszę podać nowe hasło Wi-Fi:	74F3D03A6C15AAD

☐ Wygeneruj nowe hasło Wi-Fi automatycznie

Zastosuj / Zapisz

Język (Language):

Polski (Polish)	▼
Angielski (English)	
Polski (Polish)	

Wybierz żądany język z rozwijanej listy i kliknij przycisk Zastosuj.

UWAGA: Jeśli zostanie wybrane pole  „Wygeneruj nowe hasło Wi-Fi automatycznie” router automatycznie wygeneruje nowe hasło do sieci Wi-Fi, inne niż to podane na naklejce.

Rozdział 4 Informacje o urządzeniu

Interfejs WWW użytkownika jest podzielony na dwie ramki. Główne menu (po lewej) i ekran wyświetlający informacje (po prawej). Główne menu zawiera wiele opcji, a wybranie dowolnej z nich otwiera menu niższego poziomu z większą ilością opcji.

UWAGA: Pozycje menu pokazane poniżej zależą od skonfigurowanych połączeń, ustawień użytkownika, oraz jego uprawnień. Na przykład jeśli ustawienia NAT oraz Firewall są aktywne, główne menu wyświetli ustawienia NAT i bezpieczeństwa. Jeśli jedno z nich jest nieaktywne, dane menu również będzie nieaktywne.

Informacje o urządzeniu to pierwsza sekcja głównego menu, dlatego będzie opisana jako pierwsza. Kolejne rozdziały będą opisywać następne opcje menu w kolejności ich występowania.

Ekran Informacji o urządzeniu uruchamia się po zalogowaniu.

najlepszy biznesowy internet

Informacje o urządzeniu

Zaawansowana konfiguracja

Sieć bezprzewodowa

Połączenie głosowe

Diagnostyka

Zarządzanie

Język

użytkownik: user

Informacje o urządzeniu

Wersja hardware (HW)	96368IT-1441N1
Wersja oprogramowania (SW)	W631-S410TPS-C04_R04.A2pv6C037h.d24d
Wersja bootloadera (CFE)	1.0.37-110.4-2
DSL PHY i wersja sterownika	A2pv6C037h.d24d
Wersja sterownika WLAN	5.100.123.0.cpe4.10L02.6
Numer seryjny	VI3223uv2-2013000007
Adres MAC	00:1d:20:ff:cc:43

Ta informacja odzwierciedla aktualny status połączenia WAN.

Przepustowość łącza - Upstream (Kbps)	0
Przepustowość łącza - Downstream (Kbps)	0
Adres IPv4 LAN	10.0.0.1
Brama domyślna	
Preferowany serwer DNS	0.0.0.0
Alternatywny serwer DNS	0.0.0.0
Brama domyślna IPv6	AutoWan
Data/Godzina	Thu Jan 1 00:19:31 1970

Informacja ta odzwierciedla stan rejestracji połączenia VoIP.

telefon 0_0 Stan Rejestracja:	Disabled
telefon 0_1 Stan Rejestracja:	Disabled

Odśwież

Ten ekran pokazuje informacje o ustawieniach urządzenia, oprogramowaniu, sieci IP oraz inne przydatne informacje.

4.1 Statystyki

Ten ekran pokazuje statystyki LAN, WAN, ATM/PTM i xDSL.

UWAGA: Informacje są odświeżane automatycznie co 15 sekund. Wciśnij przycisk Zresetuj statystyki, aby odświeżyć manualnie.

4.1.1 Statystyki LAN

Ten ekran pokazuje statystyki ruchu IP dla interfejsów LAN

Informacje o urządzeniu

Podsumowanie

WAN

Statystyki

LAN

WAN

xTM

xDSL

Routing

ARP

Statystyki -- LAN

Interfejs	Odebrane				Wysłane			
	Bajty	Pakiety	Błędy	Odrzucone	Bajty	Pakiety	Błędy	Odrzucone
ETH1x	52100	472	0	0	597816	641	0	0
ETH2x	0	0	0	0	0	0	0	0
ETH3x	0	0	0	0	0	0	0	0
ETH4x	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0

Resetuj statystyki

Odśwież

Pole	Opis
Interfejs	Numer interfejsu LAN
Odebrane/Wysłane:	- Bajty - Pakiety - Błędy - Zgubione Liczba Bajtów Liczba pakietów Liczba pakietów z błędami Liczba zgubionych pakietów

4.1.2 Statystyki WAN

Ten ekran pokazuje statystyki każdego interfejsu WAN.

Informacje o urządzeniu

Podsumowanie

WAN

Statystyki

LAN

WAN

xTM

xDSL

Statystyki -- WAN

Interfejs	Opis	Odebrane				Wysłane			
		Bajty	Pakiety	Błędy	Odrzucone	Bajty	Pakiety	Błędy	Odrzucone
ppp0a0	ppp0a_0_0_35	0	0	0	0	0	0	0	0
ppp1.1	pppoe_0_0_1.35	0	0	0	0	0	0	0	0
ppp2.1	pppoe_eth0.35	0	0	0	0	0	0	0	0

Resetuj statystyki

Odśwież

Pole	Opis
Interfejs	Interfejsy WAN
Opis	Nazwa usługi WAN
Odebrane/Wysłane:	- Bajty - Pakiety - Błędy - Zgubione Liczba Bajtów Liczba pakietów Liczba pakietów z błędami Liczba zgubionych pakietów

4.1.3 Statystyki xTM

Następujący rysunek pokazuje statystyki Asynchronous Transfer Mode (xTM).

Informacje o urządzeniu Podsumowanie WAN Statystyki LAN WAN xTM xDSL	Statystyki -- xTM										
	Numer portu	Oktety wejściowe	Oktety wyjściowe	Pakiety wejściowe	Pakiety wyjściowe	Wejściowe komórki OAM	Wyjściowe komórki OAM	Wejściowe komórki ASM	Wyjściowe komórki ASM	Błędne pakiety wejściowe	Błędne komórki wejściowe
	Resetuj statystyki										
	Odśwież										

Statystyki interfejsu ATM

Pole	Opis
Numer portu	PORT ATM (0-3)
Oktety wejściowe	Liczba oktetów odebranych przez interfejs
Oktety wyjściowe	Liczba oktetów wysłanych przez interfejs
Pakiety wejściowe	Liczba pakietów odebranych przez interfejs
Pakiety wyjściowe	Liczba pakietów wysłanych przez interfejs
Wejściowe komórki OAM	Liczba komórek OAM odebranych przez interfejs
Wyjściowe komórki OAM	Liczba komórek OAM wysłanych przez interfejs
Wejściowe komórki ASM	Liczba komórek ASM odebranych przez interfejs
Wyjściowe komórki ASM	Liczba komórek ASM wysłanych przez interfejs
Błędy pakietów wyjściowych	Liczba błędów wyjściowych
Błędy pakietów wejściowych	Liczba błędów wejściowych

4.1.4 Statystyki xDSL

Ten ekran pokazuje statystyki na interfejsie xDSL.

Informacje o urządzeniu

Podsumowanie

WAN

Statystyki

LAN

WAN

xTM

xDSL

Routing

ARP

DHCP

sesje NAT

IPv6

Zaawansowana konfiguracja

Sieć bezprzewodowa

Połączenie głosowe

Diagnostyka

Zarządzanie

Język

Statystyki -- xDSL

Tryb:		
Typ ruchu:		
Status:	Wyłączona	
Stan zasilania łącza:		
	Downstream	Upstream
Kodowanie liniowe (Trellis):		
SNR stosunek sygnału do szumu (0.1 dB):		
Tłumienie (0.1 dB):		
Moc wyjściowa (0.1 dBm):		
Osiągalna szybkość (Kbps):		
Szybkość (Kbps):		
Super ramki:		
Błędne super ramki:		
Słowa RS:		
Możliwe do skorygowania błędy RS:		
Niemożliwe do skorygowania błędy RS:		
Błędy HEC:		
Błędy OCD:		
Błędy LCD:		
Wszystkie komórki:		
Komórki danych:		
Błędne bity:		
Komórki danych:		
Wszystkie SES:		
Wszystkie UAS:		

TEST xDSL BER

Resetuj statystyki

Przykład ADSL jest pokazany poniżej

Informacje o urządzeniu
Podsumowanie
WAN
Statystyki
LAN
WAN
xTM
xDSL
Routing
ARP
DHCP
sesje NAT
3G
IPv6
Zaawansowana konfiguracja
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: root

Statystyki -- xDSL

Tryb:	ADSL_G.dmt			
Typ ruchu:	ATM			
Status:	Up			
Stan zasilania łącza:	L0			
	Downstream (Odbieranie)	Upstream (Wysyłanie)		
Kodowanie liniowe (Trellis):	Off	Off		
SNR stosunek sygnału do szumu (0.1 dB):	126	110		
Tłumienie (0.1 dB):	0	25		
Moc wyjściowa (0.1 dBm):	77	46		
Osiągalna szybkość (Kbps):	10380	900		
	Path 0		Path 1	
	Downstream (Odbieranie)	Upstream (Wysyłanie)	Downstream (Odbieranie)	Upstream (Wysyłanie)
Szybkość (Kbps):	8032	640	0	0
K (number of bytes in DMT frame):	252	21	0	0
R (number of check bytes in RS code word):	0	16	0	0
S (RS code word size in DMT frame):	0.50	8.00	0.0	0.0
D (interleaver depth):	64	8	0	0
Delay (msec):	8.00	16.00	0.0	0.0
INP (DMT symbol):	0.00	0.22	0.0	0.0
Super ramki:	1297	1297	0	0
Błędne super ramki:	703	0	0	0
Słowa RS:	0	10514	0	0
Możliwe do skorygowania błędy RS:	0	0	0	0
Niemożliwe do skorygowania błędy RS:	0	0	0	0
Błędy HEC:	12211	0	0	0
Błędy OCD:	0	0	0	0
Błędy LCD:	0	0	0	0
Wszystkie komórki:	412951	0	0	0
Komórki danych:	412951	0	0	0
Błędne bity:	0	0	0	0
Wszystkie ES:	12	0		
Wszystkie SES:	12	0		
Wszystkie UAS:	405	405		

TEST xDSL BER

Resetuj statystyki

Odśwież Statystyki

Wciśnij przycisk **Resetuj statystyki** aby odświeżyć dane.

Pole	Opis
Tryb	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+,VDSL, VDSL2
Typ ruchu	Typ kanału Interleave lub Fast
Status	Pokazuje stan połączenia DSL

Pole	Opis
Stan zasilania łącza	Pokazuje stan zasilania łącza
Kodowanie liniowe (Trellis)	Trellis On/Off
SNR stosunek sygnału do szumu (0.1 dB)	Stosunek sygnału od szumu
Oslabienie (0.1 dB)	Wyliczenie średniego tłumienie linii w kierunku do urządzenia
Moc wyjściowa (0.1 dBm)	Całkowita moc w kierunku od urządzenia
Osiągalna szybkość (Kbps)	Maksymalna szybkość
Szybkość (Kbps)	Obecna szybkość

W trybie VDSL, aktywna jest następująca sekcja.

Pole	Opis
B	Liczba bajtów w ramce danych MUX
M	Liczba ramek danych MUX w słowie kodowym RS.
T	Liczba ramek danych MUX w pod-ramce OH
R	Liczba bajtów redundantnych w słowie kodowym RS
S	Liczba symboli kodowych objętych słowem kodowym RS
L	Liczba bitów przesyłanych w każdym symbolu danych
D	Głębokość przeplotu
I	Rozmiar bloku przeplotu w bajtach
N	Rozmiar słowa kodowego RS
Opóźnienie	Opóźnienie w milisekundach (ms)
INP	Symbol DMT

W trybie ADSL2+, aktywna jest następująca sekcja.

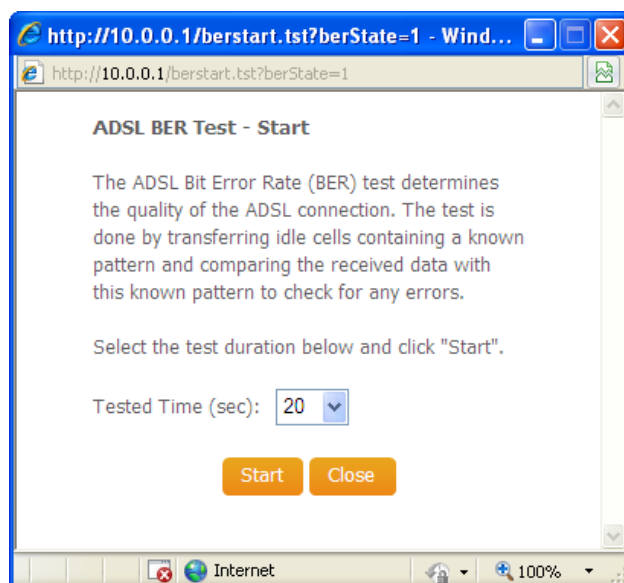
Pole	Opis
MSGc	Liczba bajtów w wiadomości nadmiarowej kanału
B	Liczba bajtów w ramce danych MUX
M	Liczba ramek danych MUX w ramce danych FEC
T	Ramki danych MUX nad bajtami synchronizacji
R	Liczba bajtów kontrolnych w ramce danych FEC
S	Stosunek długości ramek danych FEC do PMD
L	Liczba bitów ramki danych PMD
D	Głębokość przeplotu
Opóźnienie	Opóźnienie w milisekundach (ms)
INP	Symbol DMT

W trybie G.DMT, aktywna jest następująca sekcja

Pole	Opis
K	Liczba bajtów w ramce DMT
R	Liczba bajtów kontrolnych w słowie kodowym RS
S	Rozmiar słowa kodowego RS w ramce DMT
D	Głębokość przeplotu
Opóźnienie	Opóźnienie w milisekundach (ms)
Ramki OH	Całkowita liczba ramek OH
Błędy ramek OH	Liczba ramek OH odebranych z błędami
Słowa RS	Liczba błędów kodowych Reeda-Solomona
Możliwe do skorygowania błędy RS	Liczba możliwych do skorygowania błędów RS
Nieemożliwe do skorygowania błędy RS	Liczba niemożliwych do skorygowania błędów RS
Błędy HEC	Liczba błędów sumy kontrolnej błędu nagłówka
Błędy OCD	Liczba błędów liniowości poza komórkami
Błędy LCD	Liczba błędów straty liniowości komórek
Wszystkie komórki	Liczba komórek ATM (komórki bezczynności oraz danych)
Komórki danych	Liczba komórek danych ATM
Błędne bity	Liczba błędnych bitów
Wszystkie ES	Liczba błędnych sekund (Errored Seconds)
Wszystkie SES	Liczba poważnie błędnych sekund (Severely Errored Seconds)
Wszystkie UAS	Liczba niedostępnych sekund (Unavailable Seconds)

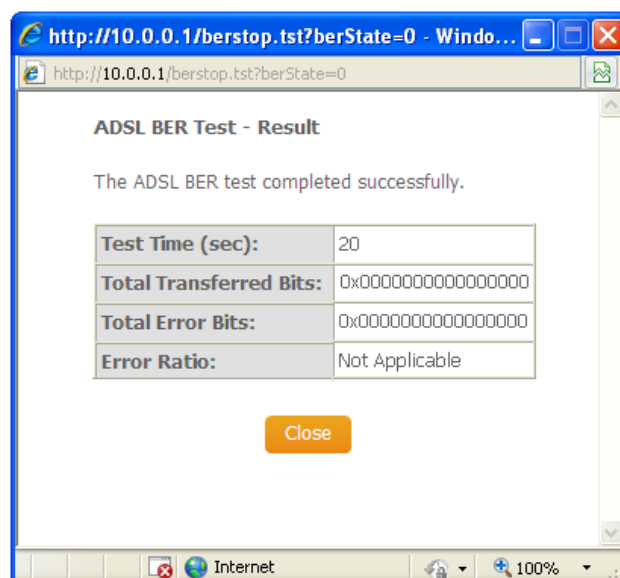
TEST xDSL BER

Kliknij na **Test xDSL BER** w oknie statystyk xDSL, aby sprawdzić stopę błędów (Bit Error Rate). Okno typu pop-up pokaże się na ekranie o wyglądzie jak poniżej.



Kliknij **Start** aby zacząć lub kliknij **Close**, aby anulować test.

Po zakończeniu testu, okno wyglądać będzie przykładowo tak:



4.2 Routing

Wybierz menu **Routing** aby wyświetlić ścieżki IP znalezione przez router.

Informacje o urządzeniu

Podsumowanie

WAN

Statystyki

Routing

ARP

Informacje o urządzeniu - Routing

Flagi: U-podniesiona, I-odrzucona, G-brama, H-host, R-przywrócona
D-dynamiczna (przekierowana), M-zmodyfikowana (przekierowana)

Adres docelowy	Brama	Maska podsieci	Flaga	Metryka	Usługa	Interfejs
10.0.0.0	0.0.0.0	255.255.255.0	U	0		br0

Pole	Opis
Adres docelowy	Docelowa podsieć lub host
Brama	Adres IP następnego punktu sieci
Maska podsieci	Maska podsieci docelowej
Flaga	U: Trasa aktywna !: Trasa odrzucona G: Użyj bramy H: Cel jest hostem R: Odtwórz trasę na potrzeby routingu dynamicznego D: Zainstalowana automatycznie przez demona M: Zmodyfikowana od trasy demona routingu
Metryka	Odległość do celu zazwyczaj mierzona w 'skokach'. Nie jest używana przez nowsze jądra, ale może być używana przez demony routingu.
Usługa	Pokazuje nazwę połączenia WAN
Interfejs	Pokazuje interfejs połączenia

4.3 ARP

Wybierz **ARP**, aby pokazać ustawienia ARP.

Informacje o urządzeniu
Podsumowanie
WAN
Statystyki
Routing
ARP

Informacje o urządzeniu - ARP

Adres IP	Flagi	MAC adres	Urządzenie
10.0.0.3	Kompletny	00:25:11:af:fd:f8	br0

Pole	Opis
Adres IP	Adres IP komputera
Flagi	Kompletny, niekompletny, stały, publikowany
Adres HW	Adres MAC komputera
Urządzenie	Interfejs połączenia

4.4 DHCP

Wybierz **DHCP**, aby wyświetlić adresy przyznane przez serwer DHCP

Informacje o urządzeniu
Podsumowanie
Statystyki
Routing
ARP
DHCP
sesje NAT

Informacje o urządzeniu - dzierżawa DHCP

Nazwa hosta	Adres MAC	Adres IP	Wygasa za
TP0000PC00360W	28:d2:44:c5:9f:e9	10.0.0.64	30 seconds

Odśwież

Nazwa hosta	Adres MAC	Adres IP	Wygasa za
TP0000PC00360W	28:d2:44:c5:9f:e9	10.0.0.64	30 seconds

Odśwież

Pole	Opis
Nazwa hosta	Pokazuje nazwę sieciową urządzenia
Adres MAC	Pokazuje adres MAC urządzenia
Adres IP	Pokazuje adres IP urządzenia
Wygasa za	Pokazuje ile czasu pozostało do zakończenia okresu, na jaki został przydzielony adres IP

Sesje NAT są powiązaniem pomiędzy sesjami TCP w domenie lokalnej a sesjami TCP w domenie publicznej, poprzez mechanizm translacji NAT. Sesje NAT pozwala połączyć dwie reprezentacje sesji.

sesje NAT (IPv4)

Po naciśnięciu przycisku "Pokaż wszystko" zostaną pokazane wszystkie sesje NAT...

Po naciśnięciu przycisku IPv6 zostaną pokazane sesje IPv6.

IP Źródłowy	Port Źródłowy	IP docelowy	Port docelowy	Protokół	Limit czasu
-------------	---------------	-------------	---------------	----------	-------------

4.6 IPv6

4.6.1 IPv6 info

Informacje o urządzeniu

- Podsumowanie
- WAN
- Statystyki
- Routing
- ARP
- DHCP
- sesje NAT
- IPv6
- IPv6 Info**
- IPv6 Route

Informacje o urządzeniu - IPv6 informacje WAN

Interfejs	Status	Adres IPv6	Prefix
pppoe_0_0_35	Unconfigured		
pppoe_0_0_1.35	Unconfigured		
pppoe_eth0.35	Unconfigured		

Podstawowe informacje

Adres Link-local	fe80::200:ff:fe55:5555/64
Brama domyślna IPv6	AutoWan
Serwer DNS IPv6	

Pole	Opis
Interfejs	Interfejs WAN, na którym adresacja IPv6 jest aktywna
Status	Status połączenia interfejsu WAN
Adres IPv6	Adres IPv6 przypisany do interfejsu WAN
Prefix	Prefix przypisany/skonfigurowany na interfejsie WAN
Adres Link-Local	Adres Link-Local IPv6 na interfejsie LAN
Brama domyślna IPv6	Brama domyślna IPv6
Serwer DNS IPv6	Adres IPv6 DNS serwera przypisany/skonfigurowany na interfejsie WAN

4.6.2 IPv6 Route

Informacje o urządzeniu

- Podsumowanie
- WAN
- Statystyki
- Routing
- ARP
- DHCP
- sesje NAT
- IPv6
- IPv6 Info
- IPv6 Route**

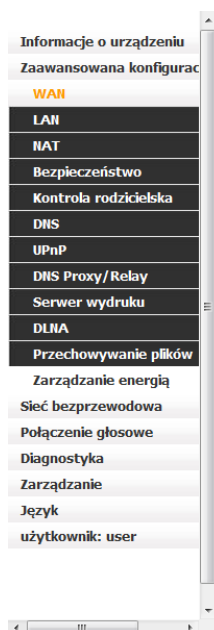
Informacje o urządzeniu - Routing IPv6

Adres docelowy	Brama	Metryka	Interfejs
----------------	-------	---------	-----------

Pole	Opis
Adres docelowy	Docelowy adres IPv6
Brama	Domyślna brama dla adresów docelowych IPv6
Metryka	Metryka trasy
Interfejs	Interfejs dla ruchu wychodzącego IPv6

Rozdział 5 Zaawansowana konfiguracja

5.1 WAN



Ustawienia usług WAN

Wybierz Dodaj, Usuń lub Edytuj, aby skonfigurować usługę WAN na wybranym interfejsie.
UWAGA: po wyłączeniu lub włączeniu zapory sieciowej wszystkie aktywne połączenia zostaną zerwane i zestawione ponownie.

Interfejs	Opis	Typ	Vlan8021p	VlanMuxId	Igmp	NAT	Nienumerowane IP	IPv6	Mld	Edytuj
ppp0a0	ppp0a_0_0_35	PPPoA	N/A	N/A	Wyłączona	Włączona	Włączona	Włączona	Wyłączona	Edytuj
ppp0a3	ppp0a_0_0_36	PPPoA	N/A	N/A	Wyłączona	Wyłączona	Wyłączona	Włączona	Wyłączona	Edytuj
ppp1.1	pppoe_0_0_1.35	PPPoE	2	35	Wyłączona	Włączona	Włączona	Włączona	Wyłączona	Edytuj
ppp2.1	pppoe_eth0.35	PPPoE	2	35	Wyłączona	Włączona	Włączona	Włączona	Wyłączona	Edytuj

Stan zapory sieciowej(IPv4): Wyłączona

[Włącz zapórę sieciową](#) [Wyłącz zapórę sieciową](#)

Interfejs	Opis	Zapora sieciowa	Syn Flooding	Ping of Death
ppp0a0	ppp0a_0_0_35	Wyłączona	Włączona	Włączona
ppp0a3	ppp0a_0_0_36	Wyłączona	Wyłączona	Wyłączona
ppp1.1	pppoe_0_0_1.35	Wyłączona	Włączona	Włączona
ppp2.1	pppoe_eth0.35	Wyłączona	Włączona	Włączona

Stan zapory sieciowej(IPv6): Wyłączona

[Włącz zapórę sieciową](#) [Wyłącz zapórę sieciową](#)

Ten ekran pozwala na konfigurację interfejsów WAN jak również włączenie i wyłączenie firewalla.

Pole	Opis
Interfejs	Nazwa interfejsu WAN
Opis	Nazwa połączenia WAN
Typ	Typ połączenia
Vlan8021p	VLAN ID użyte do tagowania VLAN (IEEE 802.1Q)
VlanMuxId	Pokazuje VLAN ID 802.1Q
IGMP	Pokazuje stan (Internet Group Management Protocol)
NAT	Pokazuje stan NAT (Network Address Translation)
Nienumerowane IP	Funkcja umożliwiająca obsługę publicznej adresacji LAN.
IPv6	Pokazuje, czy adresacja IPv6 jest aktywowana na interfejsie
MLD	Pokazuje stan MLD (Multicast Listener Discovery)
Edytuj	Wybierz interfejs do edycji

Opis pul dla firewall IPv4 i IPv6

Pole	Opis
Interfejs	Nazwa interfejsu WAN
Opis	Nazwa połączenia WAN
Zapora sieciowa	Pokazuje stan bezpieczeństwa, firewall włączony/wyłączony

Pole	Opis
Syn Flooding	Atak Syn flood, polega na wysyłaniu połączeń TCP szybciej, niż urządzenie jest w stanie przetworzyć. • Atakujący tworzy losowy adres dla każdego pakietu. • Flaga SYN w każdym pakiecie jest żądaniem otwarcia nowego połączenia do serwera z nieistniejącego adresu IP. • Ofiara odpowiada na nieistniejący adres IP i czeka na potwierdzenie, które nigdy nie przychodzi (około 3 minuty). • Tabela połączeń ofiary wypełnia się podczas oczekiwania. • Po wypełnieniu tablicy, wszystkie nowe połączenia są ignorowane. • Uprawnieni użytkownicy są również ignorowani i nie mogą uzyskać dostępu. • Zazwyczaj serwer wraca do normalnego stanu w momencie przerwania ataku. • Nowsze systemy operacyjne oferują lepsze zarządzanie zasobami, jest trudniej przepełnić w nich tablice, jednak wciąż mogą paść ofiarą ataku. Atak Syn flood może być użyty jako część innych ataków, takich jak dezaktywacja jednej strony podczas przechwytywania połączenia TCP lub powstrzymanie uwierzytelnienia lub logowania pomiędzy serwerami.
Ping of Death	Atak Ping of Death polega na wysyłaniu pakietów IP o rozmiarze większym niż 65,535 bajtów. Pakiety o tym rozmiarze są nieprawidłowe, ale możliwe jest stworzenie ich w specjalnej aplikacji. Prawidłowo napisane i zabezpieczone systemy operacyjne są w stanie wykryć takie pakiety, ale niektóre mogą paść ofiarą. Narzędzia typu ping ICMP zazwyczaj zawierają funkcjonalność wysyłania dużych pakietów, stąd nadały nazwę tej metodzie, choć UDP lub inne protokoły również mogą przekazywać Ping of Death.

WŁĄCZ ZAPORĘ SIECIOWĄ

Kliknij przycisk Włącz zaporę sieciową by uruchomić firewall odpowiednio dla adresacji IPv4 bądź IPv6.

WYŁĄCZ ZAPORĘ SIECIOWĄ

Kliknij przycisk Wyłącz zaporę sieciową by wyłączyć firewall odpowiednio dla adresacji IPv4 bądź IPv6, jeśli funkcja Zapory sieciowej nie jest potrzebna.

Kliknij przycisk **Edytuj**, aby rekonfigurować połączenie.

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

NAT

Bezpieczeństwo

Kontrola rodzicielska

UPnP

DNS Proxy/Relay

Serwer wydruku

Zarządzanie energią

Sieć bezprzewodowa

PPP Ustawienie NAT (konto użytkownika)

NAT pozwala na podzielenie adresu IP WAN dla wielu komputerów w sieci lokalnej (LAN).

Nazwa usługi PPPoE:

☐ Włącz Fullcone NAT

☒ Włącz NAT

Stan zapory sieciowej: **Włączona**

☒ Włącz Ochrona SYN Flood

☒ Włącz Ochrona Ping of Death

Powrót **Następny**

WŁĄCZ FULLCONE NAT

Opcja jest dostępna jeśli włączana jest usługa NAT. Znana jako one-to-one NAT, wszystkie żądania z tego samego wewnętrznego adresu IP i portu są mapowane na taki sam zewnętrzny adres IP i port. Zewnętrzny host może wysyłać pakiety do wewnętrznego hosta przez wysyłanie pakietów na zmapowany zewnętrzny adres.

WŁĄCZ NAT

Jeśli LAN został skonfigurowany z wykorzystaniem prywatnego adresu IP, użytkownik powinien zaznaczyć to pole wyboru. Po ponownym uruchomieniu w menu Zaawansowana konfiguracja pojawi się podmenu NAT. Jeśli prywatny adres IP nie został wykorzystany po stronie LAN (tzn. strona LAN wykorzystuje publiczny adres IP) to pole wyboru powinno pozostać niezaznaczone aby zwolnić zasoby systemowe i poprawić wydajność urządzenia.

WŁĄCZ OCHRONA SYN flood – zaznacz to pole, aby włączyć ochronę przed atakami typu SYN flood.

WŁĄCZ OCHRONA Ping of Death – zaznacz to pole, aby włączyć ochronę przed atakami typu Ping of Death.

Aby kontynuować kliknij przycisk **Następny** lub przycisk **Powrót** aby powrócić do poprzedniego ekranu.

Konfiguracja WAN - Podsumowanie	
Upewnij się, że poniższe ustawienia są zgodne z ustawieniami podanymi przez usługodawcę internetowego.	
Typ połączenia:	PPPoA
NAT:	Włączona
Full Cone NAT:	Wyłączona
Zapora sieciowa:	Wyłączona
Włącz Ochrona SYN Flood:	Włączona
Włącz Ochrona Ping of Death:	Włączona

Kliknij przycisk "Zastosuj / Zapisz" aby aktywować ustawienia tego interfejsu. Kliknij przycisk "Powrót" aby dokonać poprawek.

[Powrót](#) [Zastosuj / Zapisz](#)

Ekran Konfiguracji WAN – Podsumowanie pokazuje szczegóły usługi WAN, którą właśnie skonfigurowano.

Sprawdź wszystkie ustawienia a następnie kliknij przycisk **Zapisz/Zastosuj** jeśli są poprawne albo **Powrót** jeśli chcesz je poprawić.

Po kliknięciu przycisku **Zapisz/Zastosuj** na głównym ekranie powinna się pojawić nowa usługa. Aby ją aktywować musisz uruchomić ponownie router. Przejdź do Zarządzanie → Ponowne uruchomienie i kliknij przycisk **Uruchom ponownie**.

5.2 LAN

Skonfiguruj interfejs LAN, a następnie wciśnij **Zastosuj/Zapisz**.

najlepszy biznesowy internet

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

Autokonfiguracja IPv6

NAT

Bezpieczeństwo

Kontrola rodzicielska

DNS

UPnP

DNS Proxy/Relay

Serwer wydruku

DLNA

Przechowywanie plików

Zarządzanie energią

Sieć bezprzewodowa

Połączenie głosowe

Diagnostyka

Zarządzanie

Język

użytkownik: user

Ustawienia sieci lokalnej (LAN)

Skonfiguruj adres IP routera szerokopasmowego i maskę podsieci dla interfejsu LAN.

Adres IP:

10.0.0.1

Maska podsieci:

255.255.255.0

Stan zapory sieciowej: Włączona

☐ Wyłącz serwer DHCP
 ☒ Włącz serwer DHCP

Początkowy adres IP:

10.0.0.64

Końcowy adres IP:

10.0.0.253

Czas dzierżawy (godzina):

24

☐ Włącz serwer DHCP Relay

DHCP Server IP Address:

Lista dzierżawy statycznego IP (maksymalnie 32 pozycje mogą zostać skonfigurowane)

Adres MAC	Adres IP	Usuń
Dodaj wpis Usuń wpis		

Zastosuj / Zapisz

Sprawdź opis poszczególnych pól poniżej.

Adres IP: Wpisz adres IP portu LAN.

Maska podsieci: Wpisz maskę podsieci portu LAN.

Włącz serwer DHCP: Aby włączyć serwer DHCP, zaznacz przełącznik ☒. Wpisz początkowy, końcowy adres IP i czas dzierżawy. Te ustawienia konfiguruje router do automatycznego przydzielania adresów IP, domyślnej bramy, serwera DNS komputerom Twojej sieci LAN.

Włącz serwer DHCP Relay: Uruchom przełącznikiem ☐ oraz wpisz adres IP serwera DHCP. To pozwala routerowi na przekazywanie pakietów DHCP zdalnemu serwerowi DHCP. Zdalny serwer DHCP przypisze adres IP. *Ta opcja jest ukryta, jeśli NAT jest aktywny lub gdy router jest skonfigurowany tylko w z jednym mostkowym PVC.*

Lista dzierżawy statycznego IP: Maksymalnie 32 pozycje mogą być skonfigurowane.

Adres MAC	Adres IP	Usuń
Dodaj pozycję Usuń pozycję		

Aby dodać wpis, wpisz adres MAC i statyczne IP, następnie kliknij **Zastosuj/Zapisz**.

Statyczne IP w DHCP
 Podaj adres MAC oraz statyczny adres IP, następnie wybierz "Zastosuj/Zapisz".

Adres MAC:

12:34:56:78:90:12

Adres IP:

10.0.0.33

Zastosuj/Zapisz

Aby usunąć pozycję, wybierz odpowiednie pole w kolumnie Usun i kliknij **Usuń wpisy**.

Adres MAC:	Adres IP:	Usun
12:34:56:78:90:12	10.0.0.33	☐

Dodaj pozycję

Usuń pozycję

5.2.1 Autokonfiguracja IPv6

Skonfiguruj adresację IPv6 na interfejsie LAN, a następnie wciśnij **Zastosuj/Zapisz**.

Informacje o urządzeniu
 Zaawansowana konfiguracja
 WAN
 LAN
Autokonfiguracja IPv6
 NAT
 Bezpieczeństwo
 Kontrola rodzicielska
 DNS
 UPnP
 DNS Proxy/Relay
 Serwer wydruku
 DLNA
 Przechowywanie plików
 Zarządzanie energią
 Sieć bezprzewodowa
 Połączenie głosowe
 Diagnostyka
 Zarządzanie
 Język
 użytkownik: user

Autokonfiguracja sieci LAN IPv6
 Uwaga: Stateless DHCPv6 jest obsługiwany w oparciu o założenie, że długość prefixu jest mniejsza niż 64. ID interfejsu nie obsługuje KOMPRESJI ZER "::". Proszę podać pełne informacje. Np.: Proszę wprowadzić "0:0:0:2" zamiast "::2".

Konfiguracja statycznego adresu IPv6 sieci LAN
 Adres interfejsu (długość prefixu jest wymagana):

Aplikacje LAN IPv6
☒ Włącz DHCPv6
☒ Stateless
☐ Stateful
 Początkowy adresu IP: 0:0:0:2
 Końcowy adresu IP: 0:0:0:FE
 Czas dzierżawy (godzina):

☒ Włącz RADVD
☐ Włącz przekazywanie długości prefixu
☐ Wysłać RDNSS
☐ Włącz rozgłaszanie prefixu ULA
 Prefix: fd00::/64
 Preferowany okres ważności (godzina): -1
 Obowiązujący okres ważności (godzina): -1

☐ Włącz MLD Snooping

Zastosuj / Zapisz

Poniżej szerszy opis pól z zakładki „Autokonfiguracja IPv6”.

Konfiguracja statycznego adresu LAN IPv6:

Pole	Opis
Adres interfejsu (długość prefix jest wymagana)	Skonfiguruj statyczny adres IPv6 LAN i długość prefixu podsieci

Aplikacje LAN IPv6

Pole	Opis
Stateless	Użyj konfiguracji <i>stateless</i>

Pole	Opis
Statefull	Użyj konfiguracji <i>stateful</i>
Początkowy adres IPv6:	Początkowy adres IPv6 jaki zostanie wyznaczony dla klienta IPv6
Końcowy adres IPv6:	Ostatni adres IPv6 jaki zostanie wyznaczony dla klienta IPv6
Czas dzierżawy (godzina):	Czas dzierżawy adresu IPv6 jaki zostanie wyznaczony dla klienta IPv6
Włącz RADVD	Włącz użycie RADVD
Włącz przekazywanie długości prefixu	Użyj długość prefixu odbieranego z interfejsu WAN
Wysłać DNSS	Wyślij do LAN wiadomość DHCPv6 z opcją Recursive DNS Server
Włącz rozgłaszanie prefixu ULA	Zezwala RADVD na rozgłaszanie prefix ULA
Prefix	Prefix adresu IPv6
Preferowany czas życia (godzina)	Preferowany czas życia dla wyznaczonego prefixu
Obowiązujący czas życia (godzina)	Obowiązujący czas życia dla wyznaczonego prefixu
Włącz MLD Snooping	Włączenie/wyłączenie przekazywania multicastu IPv6 do portów LAN.

5.3 NAT

UWAGA: Aby wyświetlić tę opcję, NAT musi być aktywny dla co najmniej jednego PVC. NAT nie jest dostępny w trybie mostkowym.

5.3.1 Serwery wirtualne

Serwery wirtualne pozwalają ci na kierowanie całego ruchu przychodzącego ze strony WAN (identyfikowane przez protokół lub port zewnętrzny) do portu wewnętrznego po stronie LAN. Port wewnętrzny jest wymagany jedynie wtedy, gdy port zewnętrzny musi być przekonwertowany na inny port po stronie LAN. Maksymalnie 32 pozycje mogą być skonfigurowane

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

NAT

Serwery wirtualne

Wyzwalanie portów

Host DMZ

Bezpieczeństwo

Kontrola rodzicielska

DNS

UPnP

DNS Proxy/Relay

Serwer wydruku

DLNA

Przechowywanie plików

Zarządzanie energią

Sieć bezprzewodowa

Połączenie głosowe

Diagnostyka

Zarządzanie

Język

użytkownik: user

NAT - ustawienia wirtualnych serwerów

Serwer wirtualny pozwala skierować ruch przychodzący od strony WAN (rozpoznany przez protokół i port zewnętrzny) do wewnętrznego serwera z prywatnym adresem IP po stronie sieci LAN. Wewnętrzny port jest wymagany tylko wtedy, gdy zewnętrzny port musi zostać zmieniony na inny numer portu używanego przez serwer po stronie sieci LAN. Maksymalnie mogą zostać skonfigurowane 32 pozycje.

Dodaj Usun

Nazwa serwera	Początkowy port zewnętrzny	Końcowy port zewnętrzny	Protokół	Początkowy port wewnętrzny	Końcowy port wewnętrzny	Adres IP serwera	Interfejs WAN	Usun
---------------	----------------------------	-------------------------	----------	----------------------------	-------------------------	------------------	---------------	------

Aby dodać Serwer Wirtualny, wybierz **Dodaj**. Wyświetli się następujące okno.

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

NAT

Serwery wirtualne

Wyzwalanie portów

Host DMZ

Bezpieczeństwo

Kontrola rodzicielska

DNS

UPnP

DNS Proxy/Relay

Serwer wydruku

DLNA

Przechowywanie plików

Zarządzanie energią

Sieć bezprzewodowa

Połączenie głosowe

Diagnostyka

Zarządzanie

Język

użytkownik: user

NAT - wirtualne serwery

Wybierz nazwę usługi, wpisz adres IP serwera i kliknij przycisk "Zastosuj / Zapisz" aby przekazać pakiety IP dla tej usługi określoneму serwerowi.
UWAGA: "Końcowy port wewnętrzny" nie może zostać zmodyfikowany bezpośrednio. Zwykle jego wartość jest taka sama jak wartość "Końcowego portu zewnętrznego". Jeśli jednak zmodyfikujesz "Początkowy port wewnętrzny", wówczas "Końcowy port wewnętrzny" będzie miał taką samą wartość jak "Początkowy port wewnętrzny".
Pozostała liczba pozycji, które mogą zostać skonfigurowane:32

Użyj interfejsu: pppoe_0_0_35/pppoe0

Wybierz usługę:

Select One

Usługa niestandardowa:

Adres IP serwera:

10.0.0.

Zastosuj/Zapisz

Początkowy port zewnętrzny	Końcowy port zewnętrzny	Protokół	Początkowy port wewnętrzny	Końcowy port wewnętrzny
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

W tabelce poniżej znajdziesz opisy poszczególnych pól.

Pole	Opis
Użyj interfejsu	Wybierz interfejs WAN z listy.
Wybierz usługę lub Usługa niestandardowa	Wybierz usługę z listy lub Wpisz własną nazwę
Adres IP serwera	Wpisz adres IP serwera.
Początkowy port zewnętrzny	Wpisz początkowy port zewnętrzny (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie).
Końcowy port zewnętrzny	Wpisz końcowy port zewnętrzny (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie).

Strona 34 z 103
instrukcja obsługi **Comtrend VI-3225u**

Pole	Opis
Protokół	TCP, TCP/UDP lub UDP.
Początkowy port wewnętrzny	Wpisz początkowy port wewnętrzny (gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie.
Końcowy port wewnętrzny	Wpisz końcowy port wewnętrzny (gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie.

5.3.2 Wyzwalanie portów

Niektóre aplikacje wymagają otwarcia określonych portów w zaporze sieciowej routera dla uzyskania zdalnego dostępu. Wyzwalanie portów dynamicznie otwiera porty w zaporze, gdy aplikacja w sieci LAN zainicjuje połączenie TCP / UDP przy użyciu Wyzwalania portów router umożliwia zdalnej usłudze z sieci WAN ustanowienie nowych połączeń z powrotem do aplikacji po stronie sieci LAN za pomocą otwartych portów. Maksymalnie 32 wpisy mogą zostać skonfigurowane.

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Serwery wirtualne
Wyzwalanie portów
Host DMZ
Bezpieczeństwo
Kontrola rodzicielska

NAT - ustawienia wyzwalania portów

Niektóre aplikacje wymagają otwarcia określonych portów w zaporze sieciowej routera dla uzyskania zdalnego dostępu. Trigger Port dynamicznie otwiera porty w zaporze, gdy aplikacja w sieci LAN zainicjuje połączenie TCP / UDP przy użyciu "Triggering ports". Router umożliwia zdalnej usłudze z sieci WAN ustanowienie nowych połączeń z powrotem do aplikacji po stronie sieci LAN za pomocą "Otwartych portów". Maksymalnie 32 wpisy mogą zostać skonfigurowane.

Dodaj
Usun

Nazwa aplikacji	Trigger		Otwarte		Interfejs WAN	Usun
	Protokół	Zakres portów Początek Koniec	Protokół	Zakres portów Początek Koniec		

Aby dodać nową pozycję wybierz **Dodaj**. Pojawi się następujące okno.

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Serwery wirtualne
Wyzwalanie portów
Host DMZ
Bezpieczeństwo
Kontrola rodzicielska
DNS
UPnP
DNS Proxy/Relay
Serwer wydruku
DLNA
Przechowywanie plików
Zarządzanie energią
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

NAT - ustawienia wyzwalania portów

Niektóre aplikacje wymagają otwarcia określonych portów w zaporze sieciowej routera dla uzyskania zdalnego dostępu. Trigger Port dynamicznie otwiera porty w zaporze, gdy aplikacja w sieci LAN zainicjuje połączenie TCP / UDP przy użyciu "Triggering ports". Router umożliwia zdalnej usłudze z sieci WAN ustanowienie nowych połączeń z powrotem do aplikacji po stronie sieci LAN za pomocą "Otwartych portów". Maksymalnie 32 wpisy mogą zostać skonfigurowane.
Porty (20, 21, 22, 23, 69, 80, 161, 443, 30005) są wykorzystywane przez ISP.
Pozostała liczba wpisów, które mogą zostać skonfigurowane: 32

Użyj interfejsu:

☒ Wybierz usługę:
☐ Usługa niestandardowa:

Zastosuj / Zapisz

Początkowy Trigger port	Końcowy Trigger port	Trigger Protokół	Początkowy otwarty port	Końcowy otwarty port	Otwarty protokół
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Zastosuj / Zapisz

W tabeli poniżej znajdziesz opisy poszczególnych pól.

Pole	Opis
Ubiór interfejsu	Wybierz interfejs WAN z listy

Pole	Opis
Wybierz usługę Lub Usługa niestandardowa	Wybierz usługę z listy Lub Wpisz swoją nazwę usługi
Początkowy Trigger port	Wpisz początkowy otwarty port (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie).
Końcowy Trigger port	Wpisz końcowy otwarty port zakresu (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie).
Trigger Protokół	TCP, TCP/UDP lub UDP.
Początkowy otwarty port	Wpisz początkowy port wyzwalania(gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie.
Końcowy otwarty port	Wpisz końcowy port wyzwalania(gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie.
Otwarty protokół	TCP, TCP/UDP lub UDP.

5.3.3 Host DMZ

Router prześle pakiety IP z sieci WAN, które nie należą do żadnej z aplikacji skonfigurowanej w tabeli serwerów wirtualnych do komputera hosta DMZ.

Aby aktywować Host DMZ wpisz adres IP hosta i wciśnij **Zastosuj/Zapisz**.

Aby dezaktywować Host DMZ, wyczyść adres IP i wciśnij **Zastosuj/Zapisz**.

5.4 Bezpieczeństwo

UWAGA: Aby wyświetlić tę funkcję, musisz mieć aktywną zaporę sieciową w menu WAN w Zaawansowanej konfiguracji. Dokładny opis z przykładami znajdziesz w Załącznik A – Zapora sieciowa.

5.4.1 Filtrowanie adresów IPv4

Ten ekran definiuje reguły, które limitują ruch IPv4 (wychodzący/przychodzący). Może być stworzone wiele reguł, które dotyczą co najmniej jednego warunku. Aby dany pakiet przeszedł filtrowanie, nie może zostać odrzucony przez żaden z filtrów.

PRZYCHODZĄCY I WYCHODZĄCY FILTR IP

Domyślnie, cały ruch IPv4 jest dozwolony, ale może być blokowany filtrami. Kliknij na karcie **Filtrowanie adresów IP**.

Do wyboru jest 6 predefiniowanych profili filtrów wychodzących i przychodzących:

By móc edytować reguły dla filtrów wychodzących i przychodzących należy w polu **Nazwa Profilu** wybrać z rozwijanej listy *Custom_Profile*, a następnie kliknąć w **Edytuj filtr dla ruchu przychodzącego** lub **Edytuj filtr dla ruchu wychodzącego**.

Ustawienia filtrowania IP dla ruchu przychodzącego

Gdy zapora sieciowa jest włączona na interfejsie WAN lub LAN, wybierz opcję Dodaj lub Usuń aby skonfigurować filtr IP dla ruchu przychodzącego, aby ZEZWALAĆ / BLOKOWAĆ ruch.

Uwaga: Reguła z najniższym priorytetem powinna zostać utworzona jako pierwsza

Nazwa filtru	Interfejs	Protokół	Wersja IP	Akcja	Adres Źródłowy / Maska	Port Źródłowy	Adres docelowy / Maska	Port docelowy	Reject Type	ICMP Type	Usuń
ICMP(Incoming) permit	pppoa0	ICMP	4	Permit						echo-request	☐
ICMP(Incoming) permit	ppp1.1	ICMP	4	Permit						echo-request	☐
ICMP(Incoming) permit	ppp2.1	ICMP	4	Permit						echo-request	☐
ICMP(Incoming) permit	br0	ICMP	4	Permit						echo-request	☐
ICMP(Incoming) permit	pppoa3	ICMP	4	Permit						echo-request	☐

Dodaj **Usuń**

Aby dodać filtr (blokujący część ruchu wychodzącego lub przychodzącego), wciśnij **Dodaj**.

Na następnym ekranie wpisz kryteria filtru i wciśnij **Zastosuj/Zapisz**.

Dodaj filtr IPv4 - Przychodzące

Ekran ten pozwala na utworzenie reguły filtrowania w celu identyfikacji przychodzącego ruchu IP, poprzez określenie nowej nazwy filtra i co najmniej jednego z warunków poniżej. Wszystkie z wymienionych warunków w tej regule filtrowania muszą być spełnione, aby zasada zadziałała. Kliknij "Zastosuj/Zapisz", aby zapisać i uaktywnić filtr.

Uwaga: Przy konfiguracji określonego adresu IP (w dozwolonej podsięci) aby nie omijać zapory sieciowej, proszę wprowadzić podsieć jako pierwszą w regule zezwalającej na przejście zapory sieciowej. Następnie należy skonfigurować blokowany adres IP w celu pomyślnej implementacji w późniejszy czasie. Jeżeli Użytkownik utworzy inną nazwę filtra, a nazwa ta jest taka sama jak istniejąca nazwa reguły o tym samym kierunku i interfejsie, to zmieni nazwę istniejącej reguły.

Nazwa filtra:

Wersja IP:

Protokół:

Strategia:

Źródłowy adres IP [/ długość prefiksu]:

Port źródłowy (port lub port: port):

Docelowy adres IP [/ długość prefiksu]:

Port docelowy (port lub port: port):

Interfejsy WAN (skonfigurowane w trybie routingu i przy włączonej zaporze sieciowej) i interfejsy LAN
Wybierz jeden lub więcej interfejsów WAN / LAN wyświetlonych poniżej aby zastosować tę zasadę.

- ☐ Zastosuj regułę do wszystkich interfejsów
- ☐ pppoa_0_0_35/pppoa0
- ☐ pppoa_0_0_36/pppoa3
- ☐ pppoe_0_0_1.35/ppp1.1
- ☐ pppoe_eth0.35/ppp2.1
- ☐ br0/br0
- ☐ br0:1/br0:1

W tabeli poniżej znajdziesz opisy poszczególnych pól.

Opis	Opis
Nazwa filtra	Wpisz nazwę filtra.
Wersja IP	IPv4 wybrane domyślnie.
Protokół	TCP, TCP/UDP, UDP lub ICMP.
Strategia	Wybierz Allow lub Deny z listy.
Źródłowy adres IP	Wpisz źródłowy adres IP
Port źródłowy (port lub port: port)	Wpisz port lub zakres portów źródłowych
Docelowy adres IP	Wpisz docelowy adres IP
Port docelowy (port lub port: port)	Wpisz port lub zakres portów docelowych

5.4.2 Filtrowanie adresów IPv6

Ten ekran definiuje reguły, które limitują ruch IPv6 (wychodzący/przychodzący). Może być stworzone wiele reguł, które dotyczą co najmniej jednego warunku. Aby dany pakiet przeszedł filtrowanie, nie może zostać odrzucony przez żaden z filtrów.

PRZYCHODZĄCY I WYCHODZĄCY FILTR IP

Domyślnie, cały ruch IPv6 jest dozwolony, ale może być blokowany filtrami. Kliknij na karcie **Filtrowanie adresów IP**.

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

IAT

Bezpieczeństwo

Filtrowanie adresów IP

Filtrować IPv4

Filtrować IPv6

Kontrola rodzicielska

DHIS

UPnP

DHIS Proxy/Relay

Serwer wydruku

DLNA

Przechowywanie plików

Zarządzanie energią

Sieć bezprzewodowa

Połączenie głosowe

Diagnostyka

Ustawienia profilu filtrowania adresów IPv6 (Stan zapory sieciowej: **Włączona**)

Wybierz profil filtrowania adresów IPv6.
Uwaga: Jedynie w profilu "Custom Profile" można DODAĆ / USUNĄĆ filtr. Pozostałych profili nie można edytować.

Nazwa profilu

Custom Profile

Zmiana profilu

Edytuj filtr dla ruchu przychodzącego

Edytuj filtr dla ruchu wychodzącego

Filtry przychodzące:

Nazwa filtru	Interfejs	Protokół	Kierunek	Wersja IP	Akcja	Adres Źródłowy / Maska	Port Źródłowy	Adres docelowy / Maska	Port docelowy	ICMP Type	Reject Type
DropAll(Incoming)	pppoe0	ALL	INCOMING	6	Drop						
DropAll(Incoming)	ppp1.1	ALL	INCOMING	6	Drop						
DropAll(Incoming)	ppp2.1	ALL	INCOMING	6	Drop						
DropAll(Incoming)	pppoe3	ALL	INCOMING	6	Drop						

Filtry wychodzące:

Nazwa filtru	Interfejs	Protokół	Kierunek	Wersja IP	Akcja	Adres Źródłowy / Maska	Port Źródłowy	Adres docelowy / Maska	Port docelowy	ICMP Type	Reject Type
HTTP	pppoe0	TCP	OUTGOING	6	Permit				80		
HTTPS	pppoe0	TCP	OUTGOING	6	Permit				443		
FTP(1)	pppoe0	TCP	OUTGOING	6	Permit				20		
FTP(2)	pppoe0	TCP	OUTGOING	6	Permit				21		
POP3	pppoe0	TCP	OUTGOING	6	Permit				110		

Do wyboru jest jeden z 4 predefiniowanych profili filtrów wychodzących i przychodzących:

Nazwa profilu

Medium Profile

High Profile

Medium Profile

Low Profile

Custom Profile

Zmiana

By móc edytować reguły dla filtrów wychodzących i przychodzących należy w polu **Nazwa Profilu** wybrać z rozwijanej listy *Custom_Profile* , a następnie kliknąć w **Edytuj filtr dla ruchu przychodzącego** lub **Edytuj filtr dla ruchu wychodzącego**.

Ustawienia filtrowania IP dla ruchu przychodzącego

Gdy zapora sieciowa jest włączona na interfejsie WAN lub LAN, wybierz opcję Dodaj lub Usuń aby skonfigurować filtr IP dla ruchu przychodzącego, aby ZEZWALAĆ / BLOKOWAĆ ruch.

Uwaga: Reguła z najniższym priorytetem powinna zostać utworzona jako pierwsza

Nazwa filtru	Interfejs	Protokół	Wersja IP	Akcja	Adres Źródłowy / Maska	Port Źródłowy	Adres docelowy / Maska	Port docelowy	Reject Type	ICMP Type	Usuń
DropAll (Incoming)	pppoe0	ALL	6	Drop							☐
DropAll (Incoming)	ppp1.1	ALL	6	Drop							☐
DropAll (Incoming)	ppp2.1	ALL	6	Drop							☐
DropAll (Incoming)	pppoe3	ALL	6	Drop							☐

Dodaj

Usuń

Aby dodać filtr (blokujący część ruchu wychodzącego lub przychodzącego), wciśnij **Dodaj**.

Na następnym ekranie wpisz kryteria filtru i wciśnij **Zastosuj/Zapisz**.

Dodaj filtr IPv6 - Przychodzące

Ekran ten pozwala na utworzenie reguły filtrowania w celu identyfikacji przychodzącego ruchu IP, poprzez określenie nowej nazwy filtra i co najmniej jednego z warunków poniżej. Wszystkie z wymienionych warunków w tej regule filtrowania muszą być spełnione, aby zasada zadziałała. Kliknij "Zastosuj/Zapisz", aby zapisać i uaktywnić filtr.

Uwaga: Przy konfiguracji określonego adresu IP (w dozwolonej podsieci) aby nie omijać zapory sieciowej, proszę wprowadzić podsieć jako pierwszą w regule zezwalającej na przejście zapory sieciowej. Następnie należy skonfigurować blokowany adres IP w celu pomyślnej implementacji w późniejszy czasie. Jeżeli Użytkownik utworzy inną nazwę filtra, a nazwa ta jest taka sama jak istniejąca nazwa reguły o tym samym kierunku i interfejsie, to zmieni nazwę istniejącej reguły.

Nazwa filtra:

Wersja IP:

Protokół:

Strategia:

Źródłowy adres IP [/ długość prefiksu]:

Port źródłowy (port lub port: port):

Docelowy adres IP [/ długość prefiksu]:

Port docelowy (port lub port: port):

Interfejsy WAN (skonfigurowane w trybie routingu i przy włączonej zaporze sieciowej) i interfejsy LAN

Wybierz jeden lub więcej interfejsów WAN / LAN wyświetlonych poniżej aby zastosować tę zasadę.

- ☐ Zastosuj regułę do wszystkich interfejsów
- ☐ pppoa_0_0_35/ppp0a0
- ☐ pppoa_0_0_36/ppp0a3
- ☐ pppoe_0_0_1.35/ppp1.1
- ☐ pppoe_eth0.35/ppp2.1
- ☐ br0/br0
- ☐ br0:1/br0:1

Zastosuj / Zapisz

W tabeli poniżej znajdziesz opisy poszczególnych pól.

Opis	Opis
Nazwa filtra	Wpisz nazwę filtra.
Wersja IP	IPv6 wybrane domyślnie.
Protokół	TCP, TCP/UDP, UDP lub ICMP.
Strategia	Wybierz Allow lub Deny z listy.
Źródłowy adres IP	Wpisz źródłowy adres IP
Port źródłowy (port lub port: port)	Wpisz port lub zakres portów źródłowych
Docelowy adres IP	Wpisz docelowy adres IP
Port docelowy (port lub port: port)	Wpisz port lub zakres portów docelowych

5.5 Kontrola rodzicielska

Ten rozdział opisuje możliwości ograniczenia dostępu do Internetu.

5.5.1 Ograniczenia czasu dostępu

Ten ekran definiuje reguły blokowania dostępu do sieci zewnętrznej dla urządzenia sieci lokalnej w wyznaczonych terminach

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

NAT

Bezpieczeństwo

Kontrola rodzicielska

Ograniczenie czasu

Filtr URL

DNS

Ograniczenie czasu dostępu - można skonfigurować maksymalnie 16 pozycji

Nazwa użytkownika	MAC	pon.	wt.	śr.	czw.	pt.	sob.	Początek	Koniec	Usuń
-------------------	-----	------	-----	-----	------	-----	------	----------	--------	------

Dodaj **Usuń**

Wybierz **Dodaj** aby utworzyć nową regułę a następnie kliknij **Zastosuj/Zapisz**.

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

NAT

Bezpieczeństwo

Kontrola rodzicielska

Ograniczenie czasu

Filtr URL

DNS

UPnP

DNS Proxy/Relay

Serwer wydruku

DLNA

Ograniczenie czasu dostępu

Ta strona dodaje czas dziennego ograniczenia dla konkretnego urządzenia z sieci LAN podłączonego do routera. Adres MAC hosta sieci LAN jest automatycznie wyświetlany w uruchomionej przeglądarce. Aby ograniczyć dostęp od innych urządzeń LAN, kliknij przycisk "Inny adres MAC" i wprowadź adres MAC innego urządzenia LAN. Aby dowiedzieć się jaki jest adres MAC komputera z systemem Windows, przejdź do okna poleceń i wpisz "ipconfig /all".

Nazwa użytkownika

☐ Adres MAC hosta 28:d2:44:c5:9f:e9

☐ Inny adres MAC (xx:xx:xx:xx:xx:xx)

Dni tygodnia	pon.	wt.	śr.	czw.	pt.	sob.	nd.
Kliknij aby wybrać	☐	☐	☐	☐	☐	☐	☐

Początek czasu blokowania (gg:mm)

Koniec czasu blokowania (gg:mm)

Zastosuj/Zapisz

Pole	Opis
Nazwa użytkownika	Twoja nazwa dla tej reguły.
Adres MAC przeglądarki	Adres MAC komputera.
Inny adres MAC	Adres MAC innego urządzenia
Dni tygodnia	Dni działania blokady.
Początek czasu blokowania	Początek czasu blokowania
Koniec czasu blokowania	Koniec czasu blokowania

5.5.2 Filtr URL

Ten ekran pozwala stworzyć regułę dostępu do stron na podstawie ich adresu URL i numeru portu.

 Zabraniaj ☐ Zezwalaaj'. At the bottom right are two buttons: 'Dodaj' and 'Usuń'."/>

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Bezpieczeństwo
Kontrola rodzicielska
Ograniczenie czasu
Filtr URL
DNS

Filtr URL - Najpierw wybierz typ listy, a następnie skonfiguruj pozycje listy. Maksymalnie 100 wpisów może zostać skonfigurowanych.

Typ listy URL: ☐ Zabraniaj ☐ Zezwalaaj

Adres Port Usun

Dodaj Usun

W pierwszej kolejności wybierz rodzaj listy Zabraniaj lub Zezwalaaj, potem kliknij **Dodaj** aby wyświetlić ten ekran.

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Bezpieczeństwo
Kontrola rodzicielska
Ograniczenie czasu
Filtr URL
DNS

Kontrola rodzicielska - dodaj filtr URL

Wpisz adres URL i numer portu, a następnie kliknij przycisk "Zastosuj / Zapisz", aby dodać wpis do filtra URL.

Adres URL:

Numer portu: (Jeśli pole pozostanie puste zostanie przypisana domyślna wartość 80)

Zastosuj / Zapisz

Wpisz adres URL i numer portu, oraz wciśnij **Zastosuj/Zapisz**.

Adresy zaczynają się od WWW.

 Zabraniaj ☐ Zezwalaaj'. The table has three columns: 'Adres', 'Port', and 'Usun'. The first row contains 'www.yahoo.co.uk', '80', and a delete button. At the bottom are two buttons: 'Dodaj' and 'Usuń'."/>

Filtr URL - Najpierw wybierz typ listy, a następnie skonfiguruj pozycje listy. Maksymalnie 100 wpisów może zostać skonfigurowanych.

Typ listy URL: ☒ Zabraniaj ☐ Zezwalaaj

Adres	Port	Usun
www.yahoo.co.uk	80	X

Dodaj Usun

Może być dodane maksymalnie 100 wpisów.

Wybierz przycisk **Zabraniaj**, aby zablokować dostęp do stron poniżej.

Wybierz **Zezwalaaj**, aby przyznać dostęp do stron poniżej.

5.6 DNS

Poniżej została przedstawiona możliwość modyfikacji serwerów DNS jak i Dynamicznych DNSów.

5.6.1 Serwer DNS

W zakładce Server DNS możliwa jest konfiguracja serwera DNS.

Istnieje możliwość wybrania interfejsu WAN na którym będzie pracował serwer DNS bądź wprowadzić statyczne ustawienia

Serwer DNS może zostać przypisany do większej liczby interfejsów WAN, lecz pracować będzie tylko na jednym z najwyższym priorytetem (tzn. pierwszy interfejs posiada najwyższy priorytet). Priorytety można modyfikować poprzez usunięcie wszystkich interfejsów i ponowne ich dodanie.

Aby aktywować konfigurację wciśnij **Zastosuj/Zapisz**.

UWAGA: Aby aktywować zapisaną konfigurację należy zrestartować router

5.6.2 Dynamiczny DNS

Usługa Dynamiczny DNS pozwala na mapie dynamicznego adresu IP na stałą nazwę hosta przy wykorzystaniu jednej z wielu dostępnych domen świadczących takie usługi.

Aby dodać usługę Dynamicznego DNS należy kliknąć przycisk **Dodaj**:

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Bezpieczeństwo
Kontrola rodzicielska
DNS
Serwer DNS
Dynamiczny DNS
UPnP
DNS Proxy/Relay
Serwer wydruku
DLNA

Dodaj dynamiczny DNS

Ta strona pozwala na dodawanie dynamicznych adresów DNS z DynDNS.org lub TZO.

Dostawca D-DNS: DynDNS.org

Nazwa hosta:

Interfejs: pppoe_0_0_35/pppoe0

Ustawienia dynamicznego DNS

Nazwa użytkownika:

Hasło:

Zastosuj/Zapisz

Pole	Opis
Dostawca D-DNS	Wybierz dostawcę usługi Dynamicznego DNS z rozwijanej listy
Nazwa hosta	Podaj nazwę hosta
Interfejs	Wybierz interfejs z listy
Nazwa użytkownika	Wpisz swoją nazwę użytkownika u Twojego dostawcy usługi Dynamicznego DNS
Hasło	Wpisz swoje hasło do usługi Dynamicznego DNS

5.7 UPnP

Protokół UPnP umożliwia przesyłanie danych między dwoma urządzeniami pod kontrolą dowolnego urządzenia sterującego w sieci. UPnP jest niezależna od systemu operacyjnego, języka programowania i fizycznego medium. Usługa UPnP minimalizuje konieczność konfiguracji komputera lub oprogramowania do pracy w sieci. Komputer obsługujący UPnP automatycznie konfiguruje swoją kartę sieciową oraz wyświetla informacje o stanie bramy sieciowej, dzięki czemu kompatybilne z tą technologią aplikacje sieciowe mogą zostać natychmiast uruchomione i nie wymagają dodatkowej konfiguracji zapory sieciowej, np. otwierania portów.

Aby aktywować protokół UPnP zaznacz pole  i kliknij **Zastosuj/Zapisz**.

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Bezpieczeństwo
Kontrola rodzicielska
DNS
UPnP
DNS Proxy/Relay

Konfiguracja UPnP

UWAGA: Konfiguracja UPnP jest aktywna tylko wtedy, kiedy istnieje interfejs WAN z włączoną usługą NAT.

☒ Włącz UPnP

Zastosuj/Zapisz

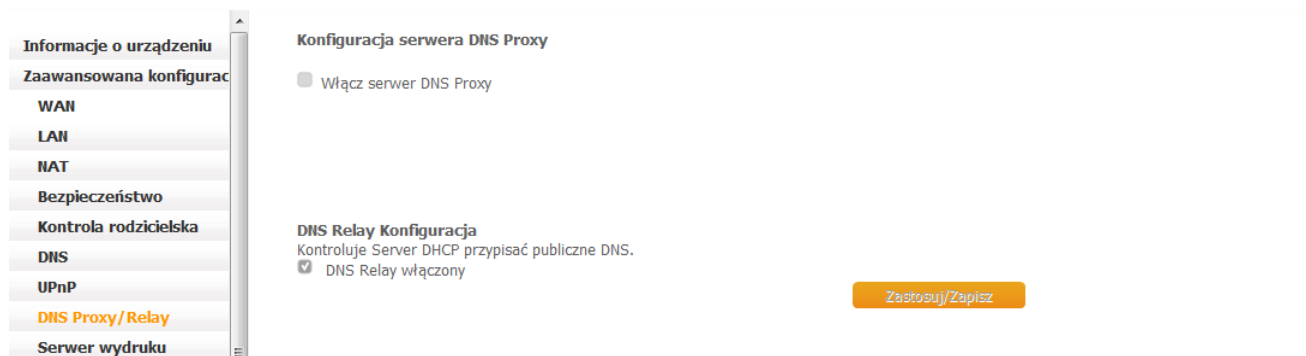
5.8 DNS Proxy/Relay

Strona wyświetla informacje na temat konfiguracji DNS Proxy i DNS Relay.

DNS proxy odbiera zapytania DNS i przekazuje je do Internetu. Po odebraniu odpowiedzi z serwera internetowego, przekazuje odpowiedzi klientom sieci lokalnej. Po skonfigurowaniu Proxy DNS z ustawieniami

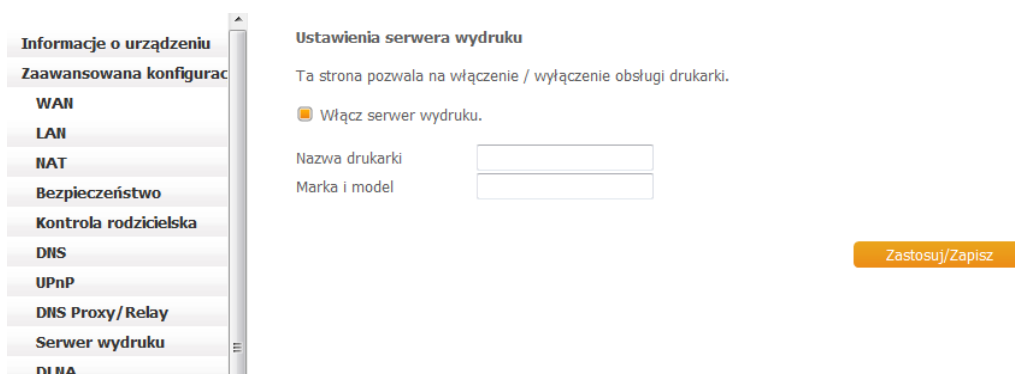
domyślnymi, komputer w sieci lokalnej otrzyma od serwera DHCP nazwę domeny „Business”, będzie ona dodana do sufiksu wyszukiwania DNS.

DNS Relay, ustawione domyślnie, powoduje przekazywania publicznego DNS przez serwer DHCP



5.9 Serwer wydruku

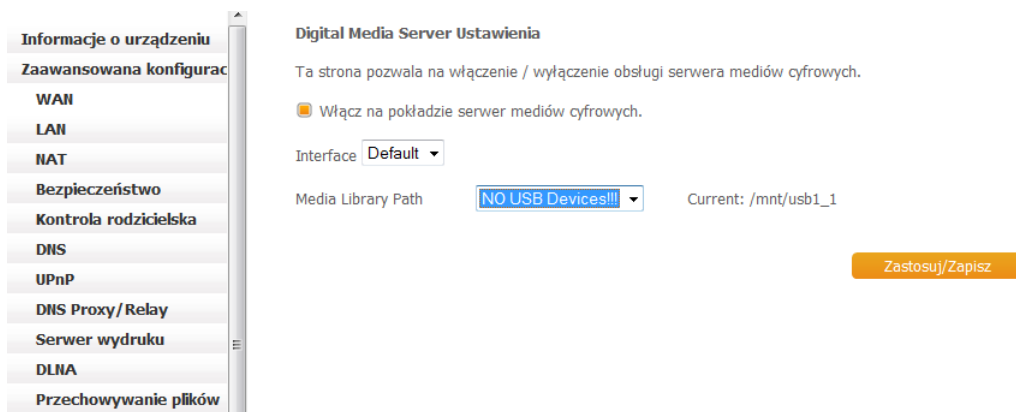
Router Comtrend VI-3225u posiada wsparcie dla drukowania sieciowego. Drukarka powinna zostać podłączona do jednego z portów USB. Dokładne instrukcje instalacji znajdują się w Załącznik D – Serwer Wydruku.



UWAGA: Upewnij się, że Twoja drukarka posiada wsparcie dla protokołu IPP (Internet Printing Protocol)

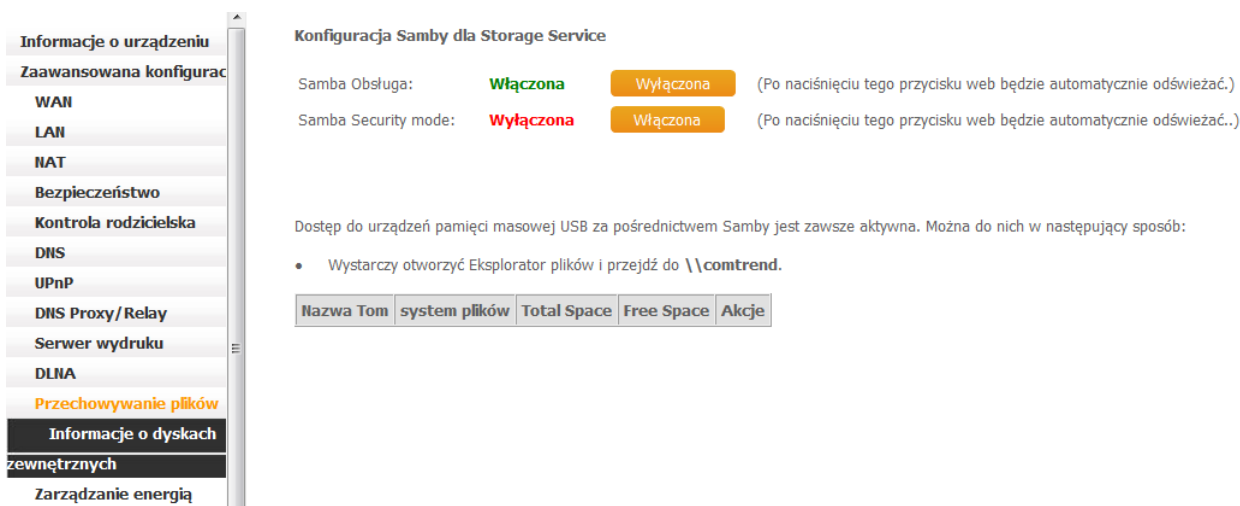
5.10 DLNA

DLNA jest standardem komunikacji wykorzystywanym przez producentów elektroniki użytkowej dla umożliwienia współdzielenia zasobów multimedialnych w ramach sieci domowej. Włączenie tego protokołu umożliwi wymianę plików multimedialnych w sieci lokalnej LAN.



5.11 Przechowywanie plików

Dzięki włączonej usłudze Samba, po podłączeniu do routera Comtrend VI-3225u zewnętrznego dysku do portu USB możliwe jest współdzielenie plików wewnątrz sieci lokalnej LAN.



5.12 Zarządzanie energią

Zarządzanie energią to ważna funkcjonalność, ze względu na:

- Zmniejszenie zużycia energii
- Przedłużenie życia baterii, w przenośnych i wbudowanych urządzeniach
- Zmniejszenie wymagań na chłodzenie
- Zmniejszenie hałasu
- Zmniejszenie kosztów energii i chłodzenia

Mniejsze zużycie energii znaczy mniej wydzielonego ciepła, co zwiększa stabilność systemu i koszty utrzymania. Oszczędza pieniądze i wpływ na środowisko naturalne.

Informacje o urządzeniu

Zaawansowana konfiguracja

WAN

LAN

NAT

Bezpieczeństwo

Kontrola rodzicielska

DIIS

UPnP

DHCP Proxy/Relay

Serwer wydruku

DLNA

Przechowywanie plików

Informacje o dyskach zewnętrżnych

Zarządzanie energią

Zarządzanie energią

Strona ta pozwala na kontrolowanie przez moduły sprzętowe oceny zużycia energii. Użyj przycisków kontrolnych, aby wybrać żadaną opcję, kliknij przycisk Zastosuj i zaznacz odpowiedni statusu.

Instrukcja WAIT w przypadku bezczynności:

Włącz

Status: **Włączona**

Wyłącz automatycznie ethernet

Liczba interfejsów ethernetowych w:

Włącz

Status: **Włączona**

pełnym trybie zasilania: 1

trybie niskiego poboru energii: 4

Zastosuj

Odśwież

Aby aktywować zaznacz odpowiednie pole i wciśnij **Zastosuj**, aby zapisać ustawienia.

Rozdział 6 Sieć bezprzewodowa

Ten rozdział opisuje jak skonfigurować i diagnozować sieci bezprzewodowe.

6.1 Podstawowa konfiguracja

Zakładka **Podstawowa konfiguracja** pozwala na konfigurację podstawowych funkcji bezprzewodowej sieci LAN. Możesz między innymi aktywować lub dezaktywować interfejs sieci bezprzewodowej, ukryć sieć, określić nazwę sieci (SSID) i określić zbiór kanałów, w zależności od twojego kraju.

The screenshot shows the 'Sieć bezprzewodowa - ustawienia podstawowe' (Wireless LAN - basic settings) page. On the left is a navigation menu with options like 'Informacje o urządzeniu', 'Zaawansowana konfiguracja', 'Sieć bezprzewodowa', 'Podstawowa konfiguracja' (highlighted), 'Bezpieczeństwo', 'Filtrowanie MAC', 'Zaawansowana konfiguracja', 'Informacja o urządzeniu', 'Połączenie głosowe', 'Diagnostyka', 'Zarządzanie', 'Język', and 'użytkownik: user'. The main content area has a title 'Sieć bezprzewodowa - ustawienia podstawowe' and a description: 'Ta strona pozwala skonfigurować podstawowe funkcje bezprzewodowego interfejsu LAN. Można włączyć lub wyłączyć interfejs bezprzewodowy LAN, ukryć sieć bezprzewodową przed skanowaniem, ustawić jej nazwę (SSID) oraz ograniczyć zestaw kanałów zgodnie z wymaganiami krajowymi. Kliknij przycisk "Zastosuj / Zapisz", aby zastosować zmiany.'

Below the description are several settings:

- ☒ Włącz sieć bezprzewodową
- ☐ Ukryj punkt dostępu
- ☐ Izolacja klientów
- ☐ Wyłącz rozgłaszanie WMM
- ☐ Wyłącz Wireless Multicast Forwarding (WMF)

Below these are input fields for:

- SSID: COMTREND-VI-3223u-CC43
- BSSID: 00:1D:20:FF:CC:44
- Kraj: POLAND (dropdown menu)
- Maksymalna liczba klientów: 16

Below this is a table titled 'Sieć bezprzewodowa - Wirtualne punkty dostępowe:'.

Włączona	SSID	Ukryta	Izoluj klientów	Wyłącz rozgłaszanie WMM	Włącz WMF	Maksymalna liczba klientów	BSSID
☐	wl0_Guest1	☐	☐	☐	☐	16	N/A
☐	wl0_Guest2	☐	☐	☐	☐	16	N/A
☐	wl0_Guest3	☐	☐	☐	☐	16	N/A

At the bottom right of the main content area is an orange button labeled 'Zastosuj/Zapisz'.

Wybierz **Zastosuj/Zapisz**, aby zapisać zaznaczone opcje sieci bezprzewodowej.

W tabeli poniżej znajdziesz opisy opcji.

Pole	Opis
Włącz sieć bezprzewodową	Pole ☒ aktywuje lub dezaktywuje interfejs bezprzewodowej sieci LAN. Po zaznaczeniu, na ekranie pojawią się podstawowe opcje.
Ukryj punkt dostępu	Wybierz Ukryj punkt dostępu, aby ukryć nazwę sieci na listach sieci Wi-Fi. Aby sprawdzić stan otwórz w Windows XP Połączenia sieciowe , z menu Start , następnie wybierz pokaż dostępne połączenia sieciowe . Jeśli twoja sieć jest ukryta, nie będzie tu widoczna. Aby móc podłączyć do niej swoje urządzenie PC należy skonfigurować ją ręcznie.
Izolacja klientów	Aktywowana blokuje dostęp między sobą komputerów będących w sieci lokalnej, w Otoczeniu sieciowym lub Moich Miejscach Sieciowych. Blokuje także inne sposoby komunikacji bezpośredniej.
Wyłącz rozgłaszanie WMM	Wyłącza funkcję rozgłaszanie funkcji multimedialnych przez router, ta funkcja pozwala na podstawowe QoS dla aplikacji typu VoIP lub Video.

Pole	Opis
Włącz Wireless Multicast Forwarding (WMF)	Zaznacz pole  aby aktywować Wireless Multicast Forwarding (WMF).
SSID [1-32 znaków]	Ustawia nazwę sieci bezprzewodowej. SSID (ang. Service Set Identifier). Wszystkie urządzenia muszą mieć skonfigurowany prawidłowy SSID, aby uzyskać dostęp do sieci. Jeśli nazwa SSID się nie zgadza, użytkownik nie zostanie połączony.
BSSID	BSSID to 48-bitowe słowo, używane do identyfikacji konkretnego BSS (Basic Service Set) w okolicy. W infrastrukturze sieci BSS, jest to adres MAC punktu dostępowego (AP – Access Point). W sieciach niezależnych lub Ad-hoc, jest ono generowane losowo.
Kraj	Menu, które udostępnia międzynarodowe i specyficzne lokalne ustawienia. Lokalne regulacje limitują zakresy kanałów: US= wszystkie, Japonia=1-14, Jordan= 10-13, Izrael= 1-13
Maksymalna ilość klientów	Maksymalna liczba klientów, którzy mogą uzyskać dostęp do routera.
Sieć bezprzewodowa - Wirtualne punkty dostępowe	Ten router wspiera wiele SSID, zwanych Gościnnymi SSID lub Wirtualnymi punktami dostępowymi. Aby aktywować jeden lub więcej punktów, zaznacz pole  w kolumnie Włączona. Aby ukryć sieć, zaznacz pole  w kolumnie Ukryta. Postępuj analogicznie dla ustawień Izolacji klientów, oraz reklamy WMM. Aby uzyskać informację o tych dwóch funkcjach, powróć do poprzedniego punktu. Podobnie, sprawdź informacje o Włącz WMF, Maksymalna ilość klientów, BSSID w tej tabeli UWAGA: Zdalne urządzenia bezprzewodowe nie mogą skanować Gościnnych SSID.

6.2 Bezpieczeństwo

Następujący ekran pokazuje się w momencie wybrania zakładki **Bezpieczeństwo**. Opcje opisane poniżej pozwalają na konfigurację ustawień bezpieczeństwa interfejsu bezprzewodowego sieci lokalnej.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Podstawowa konfiguracja
Bezpieczeństwo
Filtrowanie MAC
Zaawansowana konfiguracja
Informacja o urządzeniu
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

Sieć bezprzewodowa - bezpieczeństwo

Ta strona umożliwia skonfigurowanie zabezpieczeń bezprzewodowej sieci LAN.
Można ustawić konfigurację ręcznie
LUB
poprzez WiFi Protected Setup (WPS)

Konfiguracja WPS

Włącz WPS Disabled

Ręczna konfiguracja AP

Ustaw metodę uwierzytelnienia, wybierając sposób szyfrowania danych, określając czy klucz szyfrujący jest potrzebny do uwierzytelnienia w tej sieci bezprzewodowej, oraz określając siłę szyfrowania.
Kliknij przycisk "Zastosuj / Zapisz", aby zachować zmiany.

Wybierz SSID: COMTREND-VI-3223u-CC43

Uwierzytelnianie sieci: WPA-PSK

Hasło WPA / WAPI: •••••••••• [Kliknij tutaj, aby wyświetlić](#)

Okres odnawiania klucza grupowego WPA: 0

Szyfrowanie WPA / WAPI: TKIP+AES

Szyfrowanie WEP: Disabled

Zastosuj / Zapisz

Wybierz **Zastosuj/Zapisz**, aby zapisać nowe ustawienia.

KONFIGURACJA ZABEZPIECZEŃ SIECI BEZPRZEWODOWEJ

Ustawienia bezpieczeństwa sieci bezprzewodowej mogą być skonfigurowane zgodnie ze standardem WPS (Wi-Fi protected setup) lub ręcznie. Metoda WPS pozwala skonfigurować ustawienia bezprzewodowe automatycznie (sprawdź rozdział 6.2.1 WPS), podczas gdy metoda ręczna wymaga ustawienia wszystkich opcji z użyciem interfejsu WWW (informacje w tabeli poniżej).

Wybierz SSID
Wybierz nazwę sieci z listy. SSID to Identyfikator sieci. Wszystkie urządzenia muszą mieć skonfigurowany prawidłowy SSID, aby uzyskać dostęp do sieci. Jeśli nazwa SSID się nie zgadza, użytkownik nie zostanie połączony.

Uwierzytelnianie sieci
Ta opcja definiuje, czy klucz sieciowy jest używany do uwierzytelniania do sieci bezprzewodowej. Jeśli uwierzytelnianie jest ustawione na Open, nie używa się klucza. Pomimo tego identyfikacja klienta jest wciąż sprawdzana.
Każdy typ uwierzytelniania ma swoje ustawienia. Na przykład wybranie uwierzytelniania 802.1X wyświetli ustawienia adresu IP, portu i klucza serwera RADIUS. Szyfrowanie WEP będzie również aktywowane, jak pokazano poniżej.

Uwierzytelnianie sieci:	802.1X
Adres IP serwera RADIUS:	0.0.0.0
Port RADIUS:	1812
Klucz RADIUS:	
Szyfrowanie WEP:	Enabled
Siła szyfrowania:	128-bit
Bieżący klucz sieciowy:	2
Klucz sieciowy 1:	1234567890123
Klucz sieciowy 2:	1234567890123
Klucz sieciowy 3:	1234567890123
Klucz sieciowy 4:	1234567890123

Wprowadź 13 znaków ASCII lub 26 cyfr szesnastkowych dla 128-bitowych kluczy szyfrowania
Wprowadź 5 znaków ASCII lub 10 cyfr szesnastkowych dla 64-bitowych kluczy szyfrowania

Zastosuj / Zapisz

Ustawienia dla WPA są pokazane na następnym ekranie.

Uwierzytelnianie sieci:	WPA
Okres odnawiania klucza grupowego WPA:	0
Adres IP serwera RADIUS:	0.0.0.0
Port RADIUS:	1812
Klucz RADIUS:	
Szyfrowanie WPA / WAPI:	TKIP+AES
Szyfrowanie WEP:	Disabled

Zastosuj / Zapisz

Następnie, ustawienia WPA-PSK

Uwierzytelnianie sieci:	WPA-PSK
Hasło WPA / WAPI:	•••••••••••••••• Kliknij tutaj, aby wyświetlić
Okres odnawiania klucza grupowego WPA:	0
Szyfrowanie WPA / WAPI:	TKIP+AES
Szyfrowanie WEP:	Disabled

Zastosuj / Zapisz

Hasło WPA/WAPI

Sekwencja znaków, pozwalająca uzyskać bezpieczny dostęp.

Okres odświeżania grupy klucza

Domyślne to "0"

Szyfrowanie WPA/WAPI

AES lub TKIP+AES, domyślny to AES

Szyfrowanie WEP

Ta opcja ustala czy dane są przesyłane po sieci w postaci zaszyfrowanej. Ten sam klucz jest używany do uwierzytelniania i szyfrowania. Cztery klucze mogą być zdefiniowane, ale tylko jeden może być używany jednocześnie. Użyj listy Obecny Klucz sieciowy, aby wybrać odpowiedni klucz.

Opcje bezpieczeństwa to między innymi usługi uwierzytelniania i szyfrowania oparte na algorytmie WEP. WEP to

zbiór usług bezpieczeństwa używanych do zabezpieczania sieci 802.11 przed nieautoryzowanym dostępem, podsłuchiowaniem. W tym przypadku dokładnie chodzi o przechwytywanie ruchu sieciowego. Podczas gdy aktywowane jest szyfrowanie danych, tajne klucze szyfrowania są tworzone i używane przez stacje źródłowe i docelowe do ukrywania ramek bitowych, czyli ukrywania danych przed podsłuchującymi.

W trybie współdzielonego klucza, każde urządzenie musi otrzymać tajny współdzielony klucz bezpiecznym kanałem, czyli na przykład innym niż kanał komunikacyjny sieci 802.11.

Siła szyfrowania

Ta lista wyświetli się, gdy szyfrowanie WEP jest aktywowane. Siła klucza jest proporcjonalna do liczby bitów z których się składa. To znaczy, że dłuższe klucze odznaczają się większym poziomem bezpieczeństwa i są znacznie trudniejsze do złamania. Siła szyfrowania może być ustawiona na 64 lub 128 bitów. Klucz 5-bitowy to 5 znaków ASCII lub 10 liczb szesnastkowych. Klucz 128 bitowy, składa się z 13 znaków ASCII lub 26 liczb szesnastkowych. Każdy klucz zawiera 24-bitowy nagłówek (tak zwany wektor inicjujący) który pozwala na równoległe dekodowanie wielu strumieni zaszyfrowanych danych.

6.2.1 WPS

Wi-Fi Protected Setup (WPS), czyli Bezpieczna konfiguracja Wi-Fi, to standard który ułatwia konfigurację ustawień bezpieczeństwa wspierającym go urządzeniom sieciowym. Każde certyfikowane urządzenie WPS posiada numer PIN i przycisk zlokalizowany na urządzeniu lub dostępny przez oprogramowanie. Router posiada przycisk na obudowie i wirtualny przycisk osiągalny przez interfejs WWW.

Urządzenia z logo WPS (po prawej) wspierają WPS. Jeśli logo nie jest obecne na urządzeniu, może mimo wszystko wspierać WPS, w takim przypadku sprawdź dokumentację pod kątem hasła „Wi-Fi protected Setup”



UWAGA: WPS jest dostępny jedynie w trybie Open, WPA-PSK, WPA2-PSK oraz mieszanym WPA2/WPA-PSK. Inne tryby uwierzytelniania nie używają WPS, czyli muszą być konfigurowane ręcznie.

Aby skonfigurować ustawienia z użyciem WPS, postępuj według procedury poniżej. Musisz wybrać metodę wciśnięcia przycisku lub konfigurację kodem PIN dla kroków 6 i 7.

I. Konfiguracja

KROK 1: Aktywuj WPS, przez wybranie **Enabled** z listy Włącz WPS.

Sieć bezprzewodowa - bezpieczeństwo

Ta strona umożliwia skonfigurowanie zabezpieczeń bezprzewodowej sieci LAN. Można ustawić konfigurację ręcznie LUB poprzez WiFi Protected Setup (WPS)

Konfiguracja WPS

Włącz WPS: **Enabled**

Dodaj klienta (Ta funkcja jest dostępna tylko wtedy, gdy jest skonfigurowany tryb WPA-PSK, WPA2-PSK lub tryb otwarty)

☐ Przycisk ☐ Wprowadź PIN STA ☐ Użyj PIN AP **Dodaj Enrollee**

Ustaw tryb WPS AP: **Configured**

Konfiguruj AP (skonfiguruj wszystkie ustawienia zabezpieczeń z zewnętrznym rejestrem)

PIN urządzenia: **20554606** [Help](#)

Konfiguracja AP

Ręczna konfiguracja AP

Ustaw metodę uwierzytelnienia, wybierając sposób szyfrowania danych, określając czy klucz szyfrujący jest potrzebny do uwierzytelnienia w tej sieci bezprzewodowej, oraz określając siłę szyfrowania. Kliknij przycisk "Zastosuj / Zapisz", aby zachować zmiany.

Wybierz SSID: **COMTREND-VI-3223u-CC43**

KROK 2: Ustaw tryb WPS AP:

- **Configured** jest używany, gdy router przyzna ustawienia bezpieczeństwa klientom.
- **Unconfigured** odpowiada sytuacji odwrotnej, gdy klient zewnętrzny przydziela ustawienia routerowi.

UWAGA: Twój klient niekoniecznie musi mieć możliwość przydzielenia ustawień bezpieczeństwa routerowi. Jeśli nie posiada takiej funkcjonalności, musisz ustawić tryb WPS AP w Configured. Sprawdź dokumentację urządzenia aby sprawdzić jego możliwości. Dodatkowo, używając Windows Vista, możesz dodać zewnętrzny rejestrator używając przycisku StartAddER (Załącznik C – Zewnętrzny Rejestrator WPS).

II. UWIERZYTELNIANIE SIECIOWE

KROK 3: Wybierz Open, WPA-PSK, WPA2-PSK lub mieszany WPA2/WPA-PSK z listy trybów uwierzytelniania sekcji ręcznej konfiguracji AP, ekranu bezpieczeństwa bezprzewodowego. Przykład poniżej pokazuje przypadek WPA-PSK.

Ręczna konfiguracja AP

Ustaw metodę uwierzytelnienia, wybierając sposób szyfrowania danych, określając czy klucz szyfrujący jest potrzebny do uwierzytelnienia w tej sieci bezprzewodowej, oraz określając siłę szyfrowania. Kliknij przycisk "Zastosuj / Zapisz", aby zachować zmiany.

Wybierz SSID: **COMTREND-VI-3223u-5555**

Uwierzytelnianie sieci: **WPA-PSK**

Hasło WPA / WAPI: **.....** [Kliknij tutaj, aby wyświetlić](#)

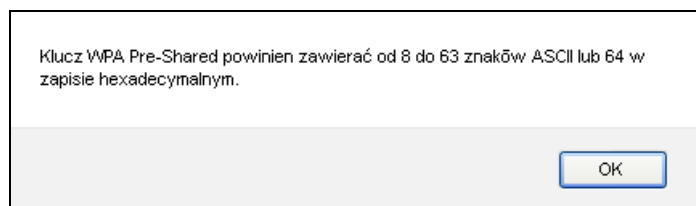
Okres odnawiania klucza grupowego WPA: **0**

Szyfrowanie WPA / WAPI: **TKIP+AES**

Szyfrowanie WEP: **Disabled**

Zastosuj / Zapisz

KROK 4: Dla trybu PSK (klucz współdzielony) wpisz klucz WPA. Zobaczysz następujące okno dialogowe, jeśli klucz jest zbyt krótki lub zbyt długi.



KROK 5: Kliknij **Zastosuj/Zapisz** na dole ekranu.

IIIa. KONFIGURACJA Z UŻYCIEM PRZYCISKU

Przycisk WPS, pozwala na półautomatyczną konfigurację. Przycisk z tyłu urządzenia lub konfiguracja za pomocą strony WWW mogą być używane zamiennie.

Procedura konfiguracji przycisku WPS jest opisana poniżej. Zostało przyjęte założenie, że funkcja sieci bezprzewodowej jest aktywowana, oraz że router jest skonfigurowany jako AP (Access Point) sieci WLAN. Dodatkowo, klient musi być również skonfigurowany poprawnie i mieć aktywowaną funkcję WPS.

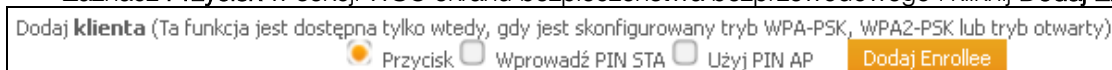
UWAGA: Router wyszukuje klientów przez 2 minuty, jeśli router zaprzestanie poszukiwań zanim ukończysz krok 7, powrót do kroku 6.

KROK 6: Pierwsza metoda: przycisk WPS

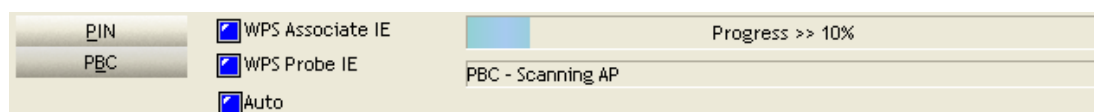
Wciśnij przycisk WPS na tylnej części obudowy. Lampka LED WPS zacznie migać, sygnalizując, że router rozpoczął poszukiwanie klientów.

Druga metoda: wirtualny przycisk interfejsu WWW

Zaznacz **Przycisk** w sekcji WSC ekranu bezpieczeństwa bezprzewodowego i kliknij **Dodaj Enrollee**.



KROK 7: W twoim kliencie WPS aktywuj funkcję przycisku. Standardowy, przykładowy klient WPS jest pokazany poniżej.



Teraz udaj się do kroku 8 (część IV sprawdź konfigurację), aby sprawdzić połączenie WPS.

IIIb. WPS – USTAWIENIA PIN

Używając tej metody, ustawienia bezpieczeństwa są konfigurowane z użyciem osobistego numeru PIN. Ten numer może być umieszczony na urządzeniu lub w oprogramowaniu. W drugim przypadku może on być wygenerowany losowo. Aby uzyskać numer PIN twojego klienta, sprawdź dokumentację urządzenia.

Konfiguracja kodu PIN dla WPS jest opisana poniżej. Zostało przyjęte założenie, że funkcja sieci

bezprzewodowej jest aktywowana, oraz że router jest skonfigurowany jako AP (Access Point) sieci WLAN. Dodatkowo, klient musi być również skonfigurowany poprawnie i włączony z aktywowaną funkcją WPS.

UWAGA: W przeciwieństwie do metody przycisku WPS, metoda PIN nie ma ustanowionego limitu czasowego. Znaczy to tyle, że router będzie poszukiwał klienta do skutku.

KROK 6: Wybierz **Wprowadź PIN STA** w sekcji ustawień WSC ekranu bezpieczeństwa bezprzewodowego, jak w opcji **A** lub **B** poniżej, następnie kliknij odpowiedni przycisk, wybrany w kroku 2.

A – W trybie **Configured** wybierz **Wprowadź PIN STA** i wpisz kod PIN dla klienta (czyli urządzenia które podłączy się do sieci). Następnie wciśnij przycisk **Dodaj Enrollee**.

Dodaj klienta (Ta funkcja jest dostępna tylko wtedy, gdy jest skonfigurowany tryb WPA-PSK, WPA2-PSK lub tryb otwarty)

☐ Przycisk ☒ Wprowadź PIN STA ☐ Użyj PIN AP [Help](#) **Dodaj Enrollee**

B – w trybie **Unconfigured**, po wybraniu trybu z listy wybierz **Zastosuj/Zapisz**. Skopiuj kod PIN urządzenia i wklej je do aplikacji klienta. Klient musi być skonfigurowany jako Zewnętrzny Rejestrator WPS. Kliknij przycisk Konfiguracja AP.

PIN urządzenia [Help](#)

Konfiguracja AP

UWAGA: Aktywowanie kodu PIN na kliencie bezprzewodowym
W trybie **Configured**, klient musi być skonfigurowany jako Enrollee.
W trybie **Unconfigured**, klient musi być skonfigurowany jako Zewnętrzny Rejestrator WPS. Jest to inna funkcja niż funkcjonalność External Registrar w Windows Vista.

Ekran poniżej przedstawia przykładowego klienta WPS w trakcie trwania funkcji PIN WPS.

PIN	☒ WPS Associate IE	Progress >> 30%
PBC	☒ WPS Probe IE	PIN - Sending EAP-Rsp(ID)
	☒ Auto	

Następnie przejdź do kroku 8 (część IV. Sprawdź połączenie) aby sprawdzić połączenie WPS.

IV. Sprawdź połączenie

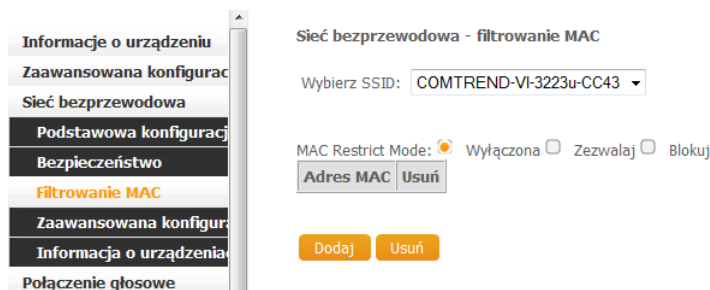
KROK 8: Jeśli metoda konfiguracji WPS zakończyła się sukcesem, będziesz w stanie uzyskać dostęp do sieci bezprzewodowej. Aplikacja klienta zakomunikuje ten stan. Przykład poniżej pokazuje ekran klienta WPS po zakończeniu ustawiania połączenia.

PIN	☒ WPS Associate IE	Progress >> 100%
PBC	☒ WPS Probe IE	PBC - Get WPS profile successfully.
	☒ Auto	

Możesz również kliknąć dwukrotnie ikonę Połączenia Bezprzewodowego w oknie Połączeń Sieciowych (lub zasobniku systemowym) aby sprawdzić stan nowego połączenia.

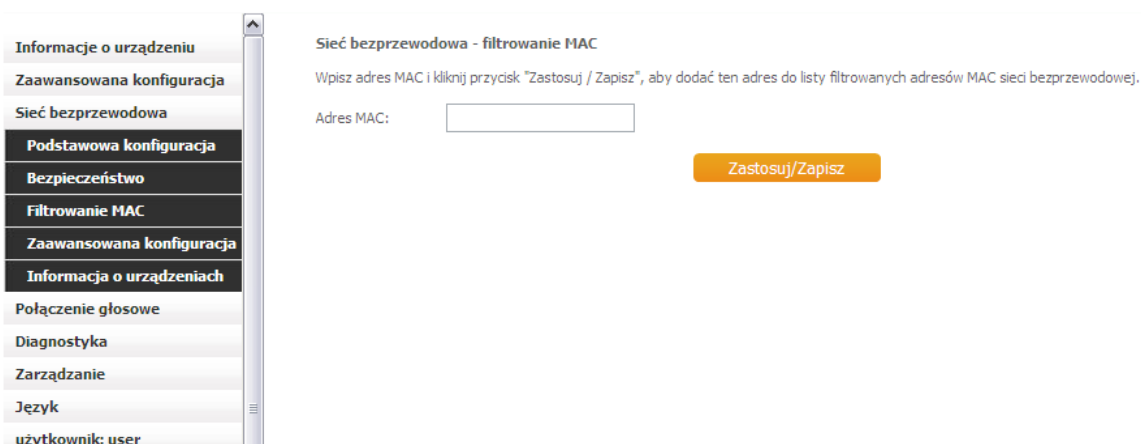
6.3 Filtrowanie MAC

Opcja ta pozwala zastrzec dostęp do routera na podstawie adresów MAC urządzeń bezprzewodowych. Aby dodać filtr MAC adresu, kliknij przycisk **Dodaj**, pokazany na poniższym ekranie. Aby usunąć filtr MAC adresu, wybierz go z tabeli filtrów MAC adresów i kliknij przycisk **usuń** pokazany na poniższym ekranie.



Pole	Opis
Wybierz SSID	Wybierz nazwę sieci bezprzewodowej z rozwijanej listy. SSID (Service Set Identifier) jest nazwą współdzieloną przez wszystkie urządzenia w sieci bezprzewodowej. Wszystkie urządzenia w Twojej sieci bezprzewodowej muszą mieć ustawione odpowiednie SSID. Jeśli nazwy SSID nie będą takie same, urządzenie nie uzyska dostępu do sieci WLAN.
Filtrowanie MAC	Wyłączony: Filtrowanie adresów MAC jest wyłączone. Zezwalaj: Zezwalaj na dostęp urządzeniom o wybranych adresach MAC. Odmawiaj: Odmawiaj dostępu urządzeniom o wybranych adresach MAC.
Adres MAC	Lista adresów MAC w zależności od wybranej opcji. Można dodać maksymalnie 60 adresów MAC. Każde urządzenie sieciowe ma unikalny 48-bitowy adres MAC. Wyświetla się go jako xx.xx.xx.xx.xx.xx, gdzie xx są liczbami zapisanymi w kodzie szesnastkowym.

Po kliknięciu na przycisk **Dodaj** pojawi się ekran, jak poniżej.



Wprowadź adres MAC w odpowiednie pole i kliknij przycisk **Zastosuj/Zapisz**.

6.4 Zaawansowana konfiguracja

Zakładka ta umożliwia sprawdzenie konfiguracji zaawansowanych funkcji interfejsu sieci bezprzewodowej.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Podstawowa konfiguracja
Bezpieczeństwo
Filtrowanie MAC
Zaawansowana konfiguracja
Informacja o urządzeniu
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

Bezprzewodowy - Zaawansowane (zalogowany jako "user")

Ustawienia te może modyfikować jedynie użytkownik zalogowany jako "root".

Kanał:

Auto

Aktualnie:

1

Prędkość multicast:

Auto

Prędkość podstawowa:

Default

Próg RTS:

2347

Próg fragmentacji:

2346

Odstęp DTIM:

1

Okres wiadomości sygnalizatora:

100

Maksymalna liczba wszystkich klientów:

16

Technologia XPress™ :

Disabled

WMM(Wi-Fi Multimedia):

Enabled

802.11n/EWC:

Auto

Szerokość pasma:

20MHz in Both Bands

Kanał dodatkowy:
(Górny/Dolny)

Lower

802.11n Rate:

auto

Ochrona 802.11n:

auto

Obsługa wyłącznie klientów 802.11n:

off

Ogłoszenie RIFS:

Off

Koegzystencja OBSS:

Enable

Oszczędzanie energii toru RX:

Disable

Oszczędzanie energii toru TX:

Disable

Pole	Opis
Pasma	Ustawiono na 2.4 GHz aby zachować kompatybilność ze standardami IEEE 802.11x. Nowy standard IEEE 802.11n pozwala również na pracę z mniejszymi przepływnościami, tak by starsze urządzenia zgodne ze standardem IEEE 802.11b lub g mogły współistnieć w tej samej sieci. Standard IEEE 802.11a ma pewne różnice w porównaniu do standardu IEEE 802.11b lub g, np. oferując więcej kanałów. Nie jest on jednak stosowany w Europie
Kanał	Rozwijane menu pozwala wybrać konkretny kanał.
Automatyczny timer kanałów (min)	Automatyczny timer kanałów w minutach (0 oznacza wyłączony)
802.11n/EWC	Standard współdzielenia sieci oparty na IEEE 802.11n Draft 2.0 oraz Enhanced Wireless Consortium (EWC)
Przepustowość	Pasma 20GHz lub 40GHz. Pasma 40GHz wykorzystuje dwa sąsiednie pasma 20GHz dla zwiększonej przepustowości.
Kontrola wstęgi	W przypadku wyboru pasma 40 GHz wybierz wstęgę Górną lub Dolną.
Wskaźnik 802.11n	Wybierz physical transmission rate (PHY).
Zabezpieczenie 802.11n	Wyłącz dla maksymalnej przepustowości. Włącz dla lepszego bezpieczeństwa.
Wsparcie 802.11n tylko dla klienta	Wyłącz aby urządzenia standardu 802.11b/g miały dostęp do routera. Włącza aby umożliwić urządzeniom standardu 802.11b/g dostęp do routera.
Reklama RIFS	Reduced Interframe Space (RIFS) jest techniką tworzenia krótkich opóźnień pomiędzy PDU aby zwiększyć wydajność łączności bezprzewodowej.
Koegzystencja OBSS	Koegzystencja pomiędzy 20 MHz i 40 MHz Overlapping Basic Service Set (OBSS) w sieci WLAN.

Pole	Opis
Chain RX Oszczędzanie mocy	Włączenie tej opcji umożliwia oszczędzenie energii poprzez wyłączenie Chain RX (przejście z 2x2 na 2x1).
Chain RX Oszczędzanie czasu	Ilość sekund , przez które ruch musi być poniżej wartości PPS aby aktywowała się opcja Chain RX Oszczędzanie mocy .
RX Chain PPS Oszczędzanie energii	Maksymalna ilość pakietów na sekundę, które mogą być przetworzone przez interfejs WLAN podczas Oszczędzania czasu (opisanego powyżej) zanim włączy się opcja RX Chain PPS Oszczędzanie energii.
Wskaźnik 54g™	Rozwijane menu zawierające stałe szybkości: Auto: Domyślne. Jeśli możliwe używa przepustowości 11 Mb/s ale w razie potrzeby zmniejsza przepustowość. Stałe szybkości 1 Mb/s, 2 Mb/s, 5.5 Mb/s i 11Mb/s. Odpowiednie ustawienie jest zależne od siły sygnału.
Szybkość multimedialna	Ustawienie Szybkość multimedialna pakietów (1-54 Mb/s)
Szybkość podstawowa	Ustawienie szybkości podstawowej.
Próg fragmentacji	Próg fragmentacji, określony w bajtach, określa, czy pakiety podlegną fragmentacji i rozmiar tych fragmentów. W 802.11 WLAN, pakiety, które przekraczają próg fragmentacji podlegają fragmentacji tzn. podzieleniu na mniejsze fragmenty odpowiednie dla obiegu danych. Pakiety mniejsze od określonego progu fragmentacji nie podlegają fragmentacji. Należy wprowadzić wartość pomiędzy 256 i 2346. Jeśli doświadczysz dużego wskaźnika straty pakietów spróbuj nieznacznie zwiększyć próg fragmentacji. Wartość powinna pozostać na swoim domyślnym poziomie 2346. Ustawienie progu fragmentacji na za niskim poziomie może skutkować niską wydajnością.
Próg RTS	Request to Send, gdy ustawiony w bajtach, określa rozmiar pakietu poza którym karta WLAN uruchomi swój mechanizm RTS/CTS. Pakiety, które przekraczają określony próg RTS wywołują mechanizm RTS/CTS. NIC przesyła mniejsze pakiety bez użycia mechanizmu RTS/CTS. Domyślna wartość progu RTS 2347 (maksymalna długość pakietu) wyłącza próg RTS.
Interwał DTIM	Delivery Traffic Indication Message (DTIM) zwany jest także wskaźnikiem sygnału identyfikacji. Przyjmuje wartości od 1 do 65535. DTIM jest odliczaną w dół zmienną, która informuje klienta o następnym przedziale czasu, w którym należy oczekiwać kolejnych wiadomości nadawanych lub wiadomości multimedialnej. Gdy AP zbuforuje te wiadomości dla odpowiednich klientów, wysła kolejny DTIM z interwałem DTIM. Klienci AP otrzymując ten sygnał przygotowują się do odbioru wiadomości. Domyślna wartość Interwału DTIM wynosi 1.
Przedział czasowy pomiędzy transmisjami sygnału identyfikacji	Czas pomiędzy kolejnymi transmisjami sygnału identyfikacji w milisekundach. Domyślna wartość wynosi 100 ms (powinna przyjmować wartości od 1 do 65535). Wysłanie sygnału identyfikacji identyfikuje obecność punktu dostępowego AP. Wszystkie urządzenia sieciowe, domyślnie, skanują wszystkie kanały RF w poszukiwaniu sygnału identyfikacji AP. Zanim stacja przejdzie w tryb oszczędzania energii musi znać wartość przedziału czasowego pomiędzy transmisjami sygnału identyfikacji aby wiedzieć kiedy ponownie wyjść z trybu oszczędzania energii by odebrać kolejny sygnał identyfikacji, oraz dowiedzieć się czy na AP nie oczekują dla niej zbuforowane ramki danych.
Maksymalna liczba klientów globalnych	Maksymalna liczba klientów, którzy mogą być podłączeni do rutera.

Pole	Opis
Technologia XPress™	Technologia Xpress jest zgodna z projektami specyfikacji dwóch nadchodzących standardów bezprzewodowych.
Moc nadawania	Ustawia określoną moc nadawania (w procentach).
WMM (Wi-Fi Multimedia)	Technologia ta umożliwia usługom audio, video, aplikacjom głosowym i innym usługom multimedialnym uzyskanie wyższego priorytetu w sieci Wi-Fi.
Brak potwierdzenia WMM	Odnosi się do polityki potwierdzania wysyłanych i odebranych danych na poziomie MAC. Włączając Brak potwierdzenia WMM może spowodować bardziej wydajną transmisję ale wyższym wskaźnikiem błędów w środowisku od dużym ruchu radiowym.
APSD WMM	Opcja automatycznego oszczędzania energii.

6.5 Informacje o urządzeniach

Ta strona pokazuje uwierzytelnione stacje bezprzewodowe i ich status. Kliknij przycisk **Odśwież** aby odświeżyć listę stacji w sieci WLAN.

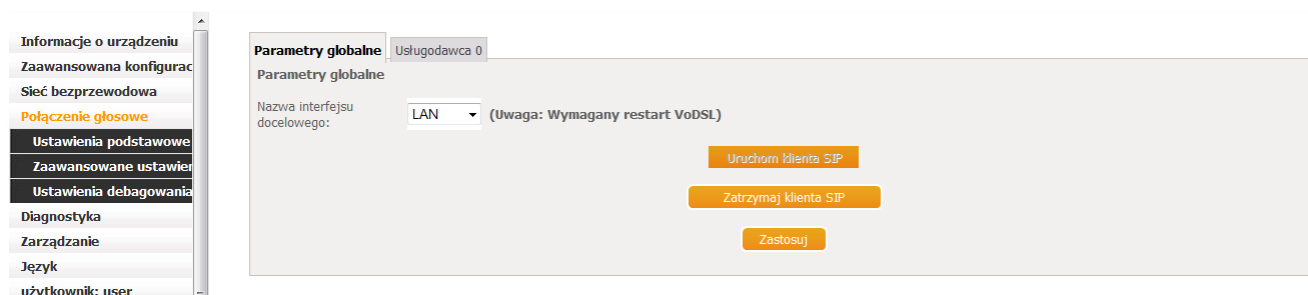
Poniższa tabela zawiera opis każdego nagłówka powyższej tabeli.

Pole	Opis
MAC	Adresy MAC wszystkich stacji.
Połączony	Wszystkie stacje powiązane z AP oraz ilość czasu, która upłynęła od ostatniej transmisji pakietów od lub do stacji. Jeśli stacja jest nieaktywna przez dłuższy okres czasu, jest usuwana z listy.
Autoryzowany	Urządzenia z autoryzowanym dostępem.
SSID	SSID modemu, do którego podłączone są stacje.
Interfejs	Interfejs modemu, do którego są podłączone stacje.

Rozdział 7 Połączenia głosowe

Na początku tego rozdziału opisane zostaną różne opcje konfiguracji usług głosowych SIP. Następnie pokazane zostaną szczegółowe instrukcje dotyczące połączeń głosowych wykorzystujących usług VoIP (Voice over IP) oraz PSTN (Public Switched Telephone Network).

Session Initiation Protocol (SIP) jest protokołem peer-to-peer wykorzystywanym w Internecie do konferencji, telefonii, powiadamianiu o zdarzeniach i wiadomościach natychmiastowych. SIP został zaprojektowany do zarządzania funkcjami sygnalizacji i zarządzania sesją w sieci pakietowej. Sygnalizacja pozwala na przeniesienie informacji o połączeniu poza granice sieci. Zarządzanie sesją zapewnia możliwość kontroli właściwości połączeń end-to-end.



Standard SIP definiuje następujących urządzenia agent/serwer:

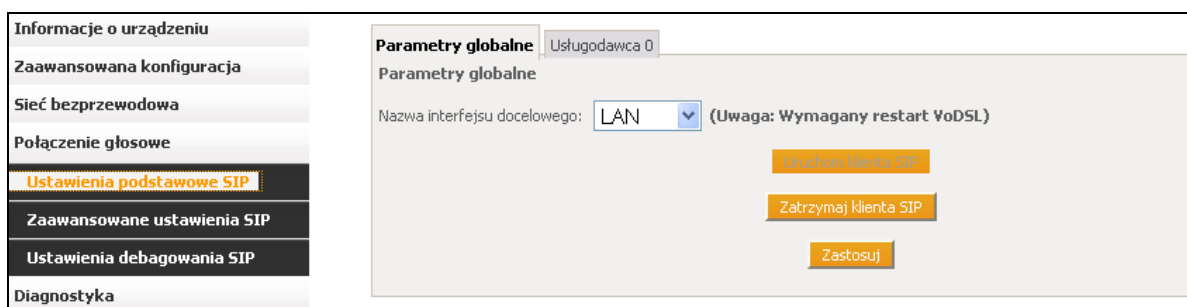
- User Agents (UA) – Klient telefoniczny SIP (fizyczny lub softwareowy)
- Proxy Server – transmituje dane pomiędzy UA i zewnętrznymi serwerami
- Registrar Server – serwer akceptujący żądania rejestracji od UA
- Redirect Server – zapewnia funkcje wyszukiwania adresów dla UA

Poniżej zostały przedstawione kolejne ekrany konfiguracji SIP (**Ustawienia Podstawowe**, **Zaawansowane** i **Ustawienia Debugowania**). Każdy ekran pokazuje zróżnicowane opcje konfiguracji SIP.

7.1 Ustawienia Podstawowe SIP

7.1.1 Parametry globalne

Ustawienia podstawowych parametrów.



7.1.2 Usługodawca

Poniższy ekran przedstawia podstawowe ustawienia konfiguracji SIP.

Parametry globalne **Usługodawca 0**

Połączenie głosowe - konfiguracja SIP

Wprowadź parametry SIP i kliknij przycisk Start / Stop, aby zapisać parametry i uruchomić / zatrzymać aplikację głosową.

Wybór ustawień*: POL - POLAND (Uwaga: Wymagany restart VoDSL)

Nazwa domeny SIP*:

Cyfry Max Ustawianie:

Option Timer:

☐ Użyj serwera proxy SIP.

☐ Użyj wychodzącego serwera proxy SIP.

Konto SIP	0	1
Konto włączone	☒	☒
Przedłużenie	1001	2001
Wyświetlana nazwa	1001	2001
Nazwa uwierzytelniania		
Hasło		
Preferowany ptime	20	20
Preferowany kodek 1	G.711ALaw	G.711ALaw
Preferowany kodek 2	G.729a	G.729a
Preferowany kodek 3	G.723.1	G.723.1
Preferowany kodek 4	G.726_24	G.726_24
Preferowany kodek 5	G.726_32	G.726_32
Preferowany kodek 6	AMR_WB_66	AMR_WB_66

Uruchom klienta SIP

Zatrzymaj klienta SIP

Zastosuj

* Zmiana tego parametru dla jednego usługodawcy wpłynie na ustawienia wszystkich innych dostawców usług.

Po skonfigurowaniu ustawień kliknij przycisk **Zastosuj**, aby rozpocząć korzystać z usługi.

Pole	Opis
Wybór ustawień	Określa ton, rodzaj dzwonka i fizyczne parametry specyficzne dla danego kraju.
Nazwa domeny SIP	Dostarczone przez Twojego dostawcę VoIP.
Cyfry Max Ustawianie	Określa maksymalną liczbę numerów, które mogą być wykręcone.

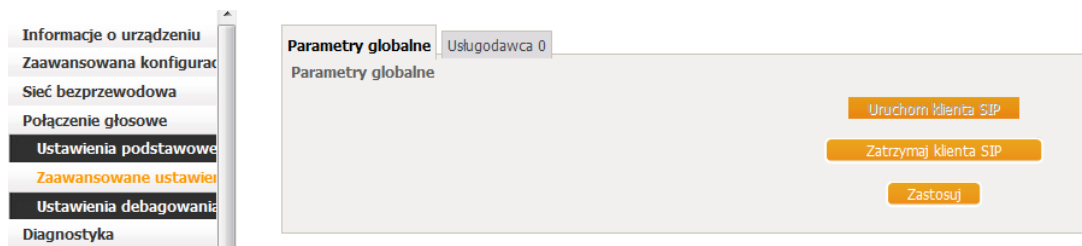
Pole	Opis
Użyj serwera proxy SIP	Włącz serwer SIP proxy zaznaczając pole wyboru  i ustawiając parametry serwera proxy.
Serwer proxy SIP	Adres IP albo nazwa domeny serwera proxy SIP, używana przez dostawcę VoIP.
Port serwera proxy SIP	Ustalony przez dostawcę VoIP.
Użyj wychodzącego serwera proxy SIP	Zaznacz jeśli wymaga tego dostawca VoIP. Włącz opcję wychodzącego serwera proxy SIP zaznaczając pole wyboru i ustawiając parametry wychodzącego serwera proxy SIP. Jeśli nie można skontaktować się bezpośrednio z serwerem proxy SIP, wiadomości są przekazywane dalej przez wychodzący serwer proxy SIP.
Wychodzący serwer proxy SIP	Adres IP wychodzącego serwera proxy SIP.
Port wychodzącego serwera proxy SIP	Port wychodzącego serwera proxy SIP.
UWAGA: Serwer proxy jest programem pośredniczącym, który zachowuje się jednocześnie jak klient i serwer aby wysłać żądania w imieniu innych klientów. Żądania są przetwarzane wewnętrznie albo wysyłane do innych serwerów. Serwer proxy interpretuje i jeśli to konieczne, przepisuje wiadomość żądania przed wysłaniem jej dalej.	
Konto SIP 1 i 2	Porty FXS1 i FXS2
Konto SIP	Mapuje konta SIP na fizyczne porty. „0” reprezentuje port FXS1 a „1” reprezentuje port FXS2.
Przedłużenie	Numer kierunkowy
Wyświetlana nazwa	Wyświetlana nazwa dzwoniącego numeru.
Nazwa uwierzytelniania	Nazwa uwierzytelniania dla serwera Registrar/Proxy, zapewniona przez dostawcę VOIP.
Hasło	Hasło dla serwera Registrar/Proxy, zapewniona przez dostawcę VOIP.
Preferowany ptime	Czas wykorzystywany do cyfrowego próbkowania analogowego sygnału głosu. Domyślna wartość to 20 ms.
Preferowany kodek 1-6	Wybierz pomiędzy kodekami G.711MuLaw/ALaw, G.729a, G.723.1, G.726_24/32, or GSM_AMR

7.2 Zaawansowane ustawienia SIP

Poniższy ekran przedstawia zaawansowane ustawienia konfiguracji SIP.

7.2.1 Parametry globalne

Ustawienia podstawowych parametrów.



7.2.2 Usługodawca

Skonfiguruj Swoje ustawienia w zależności od Twojego dostawcy usługi.

Poniższe ustawienia opisane są w tabeli. Po wprowadzeniu ustawień kliknij przycisk **Zastosuj** aby zacząć korzystać z usługi.

UWAGA: Niektóre z poniższych opcji mogą być ustawione przy pomocy poleceń z klawiatury telefonu, opisanych na liście poleceń w rozdziale 7.4 Połączenia telefoniczne.

Połączenie głosowe - Zaawansowana konfiguracja SIP

UWAGA: Dla CallCtrl 1.10.x, ta strona wyświetla status aktywacji dla każdej funkcji
 Dla CCTK 2.x, ta strona wyświetla włączony status dla każdej funkcji, nie konfigurowalnej z klawiatury

Linia	1	2
Połączenie oczekujące	☐	☐
Ilość przekazywanych połączeń		
Bezwarunkowe przekierowanie	☐	☐
Przekazuj jeśli "zajęty"	☐	☐
Przekazuj kiedy "nie odpowiada"	☐	☐
MWI	☐	☐
Gorąca linia	☐	☐
Numer gorącej linii		
Blokowanie połączeń anonimowych	☐	☐
Anonimowe połączenia	☐	☐
DND	☐	☐

☐ Włącz wsparcie T38

Rejestracja wygaśnięcia limitu czasu *

Rejestracja interwału ponawiania

DSCP dla SIP *:

DSCP dla RTP *:

Ustawienie przekaźnika DTMF *:

Ustawienie przekaźnika Hook Flash *:

Protokół transportu SIP*:

☒ Włącz dopasowywanie tagów SIP

Uruchom klienta SIP

Zatrzymaj klienta SIP

Zastosuj

* Zmiana tego parametru dla jednego usługodawcy wpłynie na ustawienia wszystkich innych dostawców usług.

Linia 1 i 2	Porty FXS1 i FXS2
Połączenie oczekujące	Zaznacz pole wyboru ☒ aby włączyć tą opcję.
Ilość przekazywanych połączeń	Numer, na który zostaną przekazane połączenia
Bezwarunkowe przekierowanie	Zaznacz pole wyboru ☒ aby włączyć tą opcję.
Przekazuj jeśli "zajęty"	Zaznacz pole wyboru ☒ aby włączyć tą opcję.
Przekazuj kiedy "nie odpowiada"	Zaznacz pole wyboru ☒ aby włączyć tą opcję.

Linia 1 i 2	Porty FXS1 i FXS2
MWI	Włącz lub wyłącz opcję Message-Waiting Indicator (MWI) dla telefonów FXS za pomocą tego pola wyboru  .
Blokowanie połączeń anonimowych	Zaznacz pole wyboru  aby włączyć tę opcję.
Anonimowe połączenia	Zaznacz pole wyboru  aby włączyć tę opcję.
DND (Do Not Disturb)	Zaznacz pole wyboru  aby włączyć tę opcję. DND (Do Not Disturb) – nie przeszkadzać

Włącz wsparcie T38	Włącz lub wyłącz wsparcie dla trybu T.38 Fax za pomocą pola wyboru  . Możesz podłączyć fax do gniazda telefonicznego aby wysłać i odbierać faksy. Funkcjonalność zależy od wsparcia twojego dostawcy VoIP dla usługi Fax.
Rejestracja wygaśnięcia limitu czasu	Okres czasu, przez który rejestracja na serwerze Registrar/ Proxy pozostanie ważna. Domyślna wartość to 3600 s.
Rejestracja interwału ponawiania	Interwał czasu pomiędzy kolejnymi próbami ponownej rejestracji.
DSCP dla SIP	Diff Serv Code Point (DSCP) dla SIP
DSCP dla RTP	Diff Serv Code Point (DSCP) dla RTP
Ustawienie przekaźnika DTMF	Ustaw specjalne wykorzystanie pakietów RTP do przesyłu kodów DTMF.
Ustawienie przekaźnika Hook Flash	Przyporządkowanie zdarzenia hook flash odpowiedniemu sygnałowi.
Protokół transportu SIP	Ustawienie protokołu transportu wiadomości SIP
Włącz dopasowywanie tagów SIP (odznaczone - Vonage Interop).	Ponieważ CPE wykorzystuje tagi SIP do parowania, implementacja musi wspierać specyfikację SIP, która wymaga używania tagów.

7.3 Ustawienia Debugowania SIP

Poniższy ekran przedstawia ustawienia konfiguracji SIP wykorzystywanej do debugowania.

7.3.1 Parametry globalne

Ustawienia podstawowych parametrów.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Połączenie głosowe
Ustawienia podstawowe SIP
Zaawansowane ustawienia SIP
Ustawienia debugowania SIP
Diagnostyka

Parametry globalne

Usługodawca 0

Parametry globalne

Poziom logowania z konsoli VoDSL
:

Error

Unieśmiałenie SIP

Zatrzymaj klienta SIP

Zastosuj

7.3.2 Usługodawca

Skonfiguruj Swoje ustawienia w zależności od Twojego dostawcy usługi.

Powyższe ustawienia opisane są w poniższej tabeli. Po wprowadzeniu ustawień kliknij przycisk **Zastosuj** aby zacząć korzystać z usługi.

Pole	Opis
Adres IP i Port serwera SIP log	Wprowadź adres IP i port serwera SIP log.
Wsparcie VAD	Zaznacz pole wyboru ☐ aby włączyć wsparcie VAD. Dostosowuje poziom wejściowy (Zysk wejściowy) i wyjściowy (Zysk wyjściowy) przy pomocy rozwijanych list.
Zysk wejściowy	Zwiększa poziom głośności mikrofonu (głośność z jaką jesteśmy słyszani po drugiej stronie).
Zysk wyjściowy	Zwiększa poziom głośności głośnika.

7.4 Połączenia telefoniczne

Aby wykonać połączenie telefoniczne, po prostu wprowadź numer. Schemat wybierania (np. wybierane numery) jest zróżnicowany w zależności od każdej instalacji. Domyślny schemat wybierania zezwala na wybieranie 4-cyfrowych rozszerzeń numerów lub bezpośrednio adresów IP. Aby wprowadzić krótszy numer (np. 3-cyfrowy) dodaj na końcu znak „#”.

Gdy serwer połączeń (SIP Proxy Server) jest skonfigurowany w systemie, wybierane numery są tłumaczone i przekazywane przez serwer połączeń do odpowiedniego, zarejestrowanego w serwerze połączeń, odbiorcy.

Jeśli serwer połączeń nie jest skonfigurowany, połączenia nadal mogą być wykonywane przy użyciu 4-cyfrowych rozszerzeń zamiast pełnych adresów IP. Inicjator połączenia sam tłumaczy wprowadzony numer na docelowe urządzenie, jak pokazano w poniższej tabeli:

Pierwsza cyfra:	Identyfikator linii (dla wieloliniowych bramek)
Pozostałe cyfry:	Numer Hosta w adresie IP. Numer sieci jest uznawany za taki sam jak adres IP dzwoniącego.

Na przykład jeśli dzwoniący z adresu 10.136.64.33/24 wybierze numer "2023", połączenie będzie miało miejsce na drugiej linii na adresie 10.136.64.23. Wszystkie urządzenia muszą posiadać taką samą klasę C podsieci (24-bitową maskę podsieci).

Aby zadzwonić bezpośrednio na adres IP, wpisz adres IP z klawiatury, używając symbolu „*” zamiast „.” (kropki). Zakończ wpisywanie symbolem „*” lub „#”. Przy dzwonieniu za pomocą adresów IP nie ma możliwości wyboru linii na bramce, więc bramka zawsze przekieruje połączenia na pierwszą linię.

Dźwięk zajętej sieci (fast busy) będzie odegrany w przypadku nieznanych lub nieosiągalnych celów połączeń. Aby odebrać połączenie podnieś słuchawkę lub skorzystaj z przycisku odbierającego połączenie.

Identyfikator dzwoniącego (Caller ID)

Menadżer Połączeń wykazuje wydzwaniany numer podczas wykonywania połączeń. Wydzwaniany numer jest przesyłany na linie analogową w celu przeprowadzenia rozpoznania klas.

Zawieszanie połączenia

W celu zawieszenia połączenia, naciśnij przycisk „flash”, a następnie rozłącz się (opcjonalnie). Aby powrócić do połączenia naciśnij przycisk „flash” albo podnieś słuchawkę. Telefon przypomni Ci o zawieszonym połączeniu krótkim sygnałem dzwonka co 30 sekund.

Przekazywanie połączenia

- Aby przekazać połączenie, naciśnij przycisk „flash” a następnie wybierz numer, na który ma być przekazane połączenie.
- Aby przekazać połączenie natychmiast, rozłącz się (przekazywanie domyślne).
- Aby przekazać połączenie z konsultacją, poczekaj aż połączenie zostanie odebrane, skonsultuj i się rozłącz.
- Aby anulować przekazywanie połączenia (jeśli numer na który zostało przekazane połączenie nie odbiera); naciśnij przycisk „flash” aby powrócić do początkowego połączenia.

Połączenia konferencyjne

Aby zmienić zwykłe połączenie w połączenie konferencyjne naciśnij przycisk „flash” i wprowadź numer użytkownika, który ma dołączyć do połączenia. Poczekaj aż użytkownik odbierze połączenie i naciśnij przycisk „flash”. Aby rozłączyć dodatkowego użytkownika i powrócić do początkowego połączenia ponownie naciśnij przycisk „flash”. Aby samemu opuścić połączenie konferencyjne, rozłącz się. Połączenie zostanie przekazane (Pozostałe dwie osoby nadal będą ze sobą połączone). W trybie połączenia konferencyjnego, inicjator połączenia spełnia rolę mostka/miksera audio – ustanawiane są tylko dwa strumienie głosowe.

Połączenia oczekujące

Jeśli na linii są włączone połączenia oczekujące, i usłyszysz sygnał połączenia oczekującego podczas połączenia, naciśnij przycisk „flash” aby odebrać oczekujące połączenia. Pierwsze połączenie jest automatycznie zawieszane. Aby przełączać się między połączeniami naciśnij przycisk „flash”.

- Aby wyłączyć opcję połączeń oczekujących, wykręć na klawiaturze *60.
- Aby włączyć opcję połączeń oczekujących, wykręć na klawiaturze *61.

Opcja funkcji przekazywania połączeń (Zajęte lub Wszystkie) jest nadrzędna nad funkcją połączeń oczekujących. Funkcja połączeń oczekujących jest ignorowana jeśli przyjdzie kolejne połączenia, a jedno jest już oczekujące lub w trybie połączeń konferencyjnych.

Przekazywanie połączeń - Numer

- Aby ustawić numer, na który mają być przekazywane połączenia, wybierz na klawiaturze *74 a następnie wprowadź numer. Pamiętaj, że ustawienie tego numeru nie włącza funkcji przekazywania połączeń. Aby tego dokonać uruchom opcje przekazywania połączeń tak, jak opisano poniżej.

- Aby wyłączyć wszystkie opcje przekazywania połączeń, wybierz na klawiaturze *70.

Przekazywanie połączeń - Nie odebrane

- Aby włączyć opcję przekazywania połączeń gdy połączenie nie zostało odebrane, wybierz na klawiaturze *71. Połączenia przychodzące będą przekazywane jeśli nie zostaną odebrane w ciągu 18 sekund.

Przekazywanie połączeń - Zajęte

- Aby włączyć opcję przekazywania połączeń gdy linia jest zajęta wybierz na klawiaturze *72. Jeśli słuchawka telefonu jest podniesiona przychodzące połączenia będą natychmiast przekazywane.

Przekazywanie połączeń - Wszystkie

- Aby włączyć opcję przekazywania wszystkich połączeń wybierz na klawiaturze *73.
- Aby wyłączyć opcję przekazywania wszystkich połączeń wybierz na klawiaturze *75.

Poprzednie ustawienia „Przekazywanie połączeń – Zajęte” i „Przekazywanie połączeń - Nie odebrane” nie zostaną zmienione.

Odpowiedz na połączenie

- Aby oddzwonić na numer ostatniego, znanego przychodzącego połączenia (odebranego lub nie) wybierz na klawiaturze *69.

Wybierz ponownie

- Aby połączyć się z ostatnim wybieranym numerem wybierz na klawiaturze *68.

VoIP to PSTN

- Aby wykonać połączenie na tradycyjne telefony w sieci PSTN, wybierz najpierw na klawiaturze ##.

Rozdział 8 Diagnostyka

Pierwszy ekran Diagnostyki jest tablicą rozdzielczą, pokazującą status testów. Jeżeli test przebiegnie niepomyślnie, kliknij przycisk **Test** na dole tej strony, aby upewnić się, czy wynik będzie taki sam. Jeśli test ponownie przebiegnie niepomyślnie, kliknij przycisk **Help** i postępuj zgodnie z procedurami rozwiązywania problemów.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

pppoa_0_0_35 Diagnostyka

Modem jest w stanie przetestować Twoje połączenie DSL. Poniżej znajdują się poszczególne testy. Jeżeli test przebiegnie niepomyślnie, kliknij przycisk "Help". Otworzy się nowa strona. Kliknij przycisk "Uruchom ponownie testy diagnostyczne" na dole tej strony, aby upewnić się, czy wynik będzie taki sam. Jeśli test ponownie przebiegnie niepomyślnie postępuj zgodnie z procedurami rozwiązywania problemów opisanymi pod linkiem "Help".

Przetestuj połączenie z siecią lokalną

Przetestuj połączenie: ETH1x	Pomyślny	Help
Przetestuj połączenie: ETH2x	Niepomyślny	Help
Przetestuj połączenie: ETH3x	Niepomyślny	Help
Przetestuj połączenie: ETH4x	Niepomyślny	Help
Przetestuj połączenie: ETHWAN	Niepomyślny	Help
Przetestuj połączenie sieci bezprzewodowej:	Pomyślny	Help

Przetestuj połączenie z dostawcą usługi DSL

Test ADSL Synchronization:	Niepomyślny	Help
Przetestuj ATM OAM F5 segment ping:	Niemożliwy	Help
Przetestuj ATM OAM F5 end-to-end ping:	Niemożliwy	Help

Przetestuj połączenie z dostawcą usług internetowych

Przetestuj połączenie z serwerem PPP:	Niemożliwy	Help
Przetestuj uwierzytelnianie u dostawcy usług internetowych:	Niemożliwy	Help
Przetestuj przypisanie adresu IP:	Niemożliwy	Help
Ping bramy domyślnej:	Niepomyślny	Help
Ping podstawowego serwera DNS:	Niepomyślny	Help
Przetestuj IP Loopback:	Pomyślny	Help

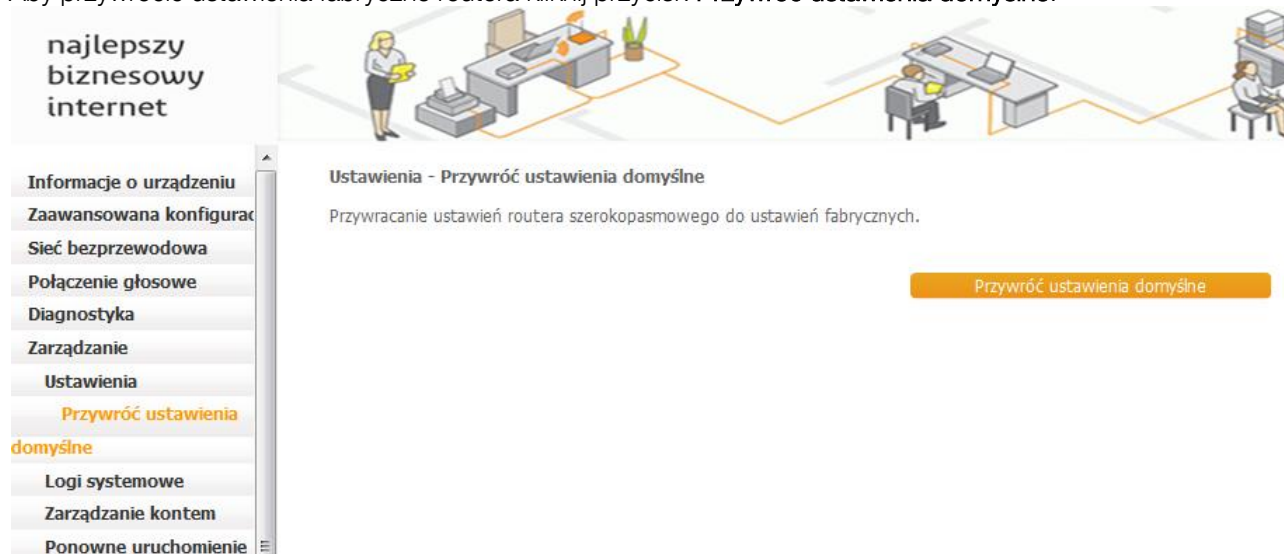
Następne połączenie
Test
Przetestuj za pomocą OAM F4

Rozdział 9 Zarządzanie

9.1 Ustawienia

9.1.1 Przywróć ustawienia domyślne

Aby przywrócić ustawienia fabryczne routera kliknij przycisk **Przywróć ustawienia domyślne**.



Po kliknięciu przycisku **Przywróć ustawienia domyślne** pojawi się poniższy ekran.

Przywracanie ustawień routera szerokopasmowego

Konfiguracja routera szerokopasmowego została przywrócona do ustawień domyślnych i router uruchamia się ponownie.

Zamknij okno konfiguracji routera szerokopasmowego i odczekaj 2 minuty przed ponownym otwarciem przeglądarki internetowej. Jeśli to konieczne, przekonfiguruj adres IP swojego komputera, aby pasował do nowej konfiguracji.

Zamknij przeglądarkę i odczekaj 2 minuty zanim powtórnie ją otworzysz. Możliwe, że będziesz musiał zmienić konfigurację IP swojego komputera aby znowu skomunikować się z routerem.

UWAGA 1: Powyższy proces ma takie samo działanie jak przycisk Reset na obudowie routera. Należy przytrzymać go przez 5 do 10 sekund, aż dioda LED zasilania będzie migać.

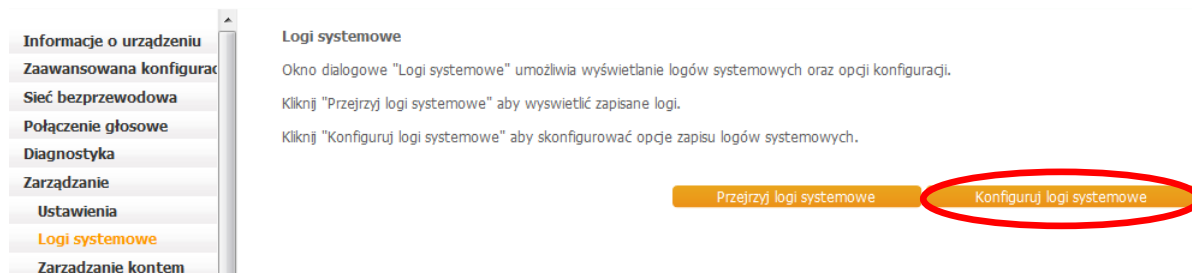
UWAGA 2: Jeśli przycisk zostanie wciśnięty przez powyżej 20 sekund router Comtrend VI-3225u zostanie zablokowany (dioda Power świeci się na kolor czerwony). Przed resetem modemu należy skontaktować się z obsługą techniczną.

9.2 Logi systemowe

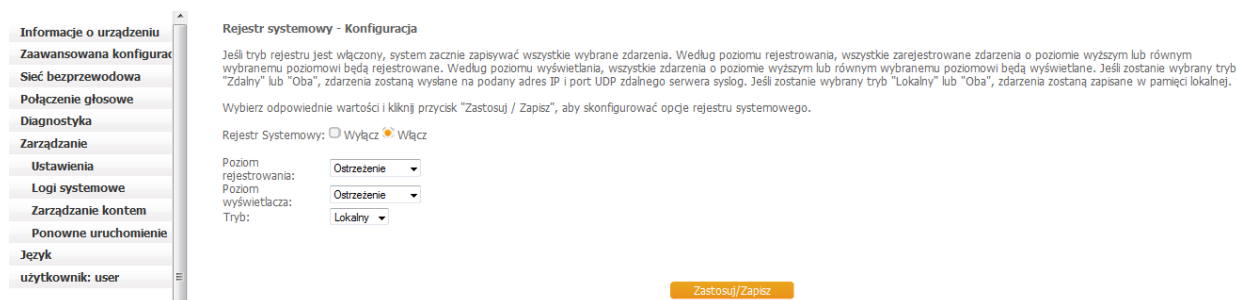
Funkcja ta pozwala zachowywać logi systemowe i przeglądać je w wybranym momencie.

Wykonaj poniższe kroki aby skonfigurować, włączyć i przeglądać logi systemowe.

KROK 1: Kliknij przycisk **Konfiguruj rejestr systemowy** pokazany poniżej (zakreślony na **Czerwono**).



KROK 2: Wybierz żadaną opcję i kliknij przycisk **Zastosuj/Zapisz**.



W poniższej tabeli przedstawiono opcje logów systemu wraz z opisami.

Pole	Opis
Rejestr Systemowy	Określa czy system zapisuje obecnie zdarzenia. Użytkownik może włączyć lub wyłączyć logowanie zdarzeń. Domyślnie logowanie jest wyłączone. Aby włączyć logowanie zaznacz pole wyboru Włącz i kliknij przycisk Zastosuj/Zapisz .

Pole	Opis
Poziom rejestrowania	Pozwala na określenie poziomu zdarzeń zapisywanych i filtrowanie niechcianych zdarzeń poniżej tego poziomu. Zdarzenia od najwyższego poziomu „Awaryjny” aż do wybranego przez użytkownika będą zapisywane w buforze logu SDRAM. Kiedy bufor się wypełni, nowsze logi nadpiszą najstarsze. Domyślnie poziom rejestru ustawiony jest na „Ostrzeżenie”, który jest najniższym poziomem krytycznym. Poziomy rejestru zdefiniowane są następująco: • Awaryjny = system nie nadaje się do użytku • Alert = należy podjąć natychmiastowe kroki • Krytyczny = warunki krytyczne • Błąd = warunki błędu • Ostrzeżenie = normalne ale niepokojące warunki • Powiadomienie= normalne i nieistotne warunki • Informacyjne= zapewnia informacje odniesienia • Usuwanie błędów = wiadomości usuwania błędów „Awaryjny” jest najpoważniejszym poziomem, podczas gdy „Usuwanie błędów” jest najmniej ważny. Na przykład jeśli poziom rejestru zostanie ustawiony na poziomie „Usuwanie błędów”, wszystkie zdarzenia od najniższego poziomu do najwyższego „Awaryjny” zostaną zapisane. Jeśli poziom rejestru zostanie ustawiony na „Błąd”, tylko zdarzenia z tego i wyższych poziomów zostaną zapisane.
Poziom wyświetlania	Pozwala wybrać zdarzenia, które mają zostać wyświetlone po naciśnięciu przycisku Przejrzyj rejestr systemowy. Pokazane zostaną tylko zdarzenia z ustawionego i wyższych poziomów aż do poziomu „Awaryjny”.
Tryb	Pozwala wybrać czy zdarzenia mają zostać zapisane lokalnie, czy wysłane do zdalnego serwera logowania, czy wykonać obydwie akcje jednocześnie. W przypadku wybrania opcji „Zdalny” przeglądanie rejestru systemowego nie będzie możliwe. W przypadku wyboru trybu „Zdalny” lub „Oba” WEB UI poprosi o wprowadzenie adresu IP i portu UDP serwera logowania.

Krok 3: Kliknij przycisk **Przejrzyj rejestr systemowy**. Wynik powinien być podobny do tego przedstawionego poniżej.

http://10.0.0.1/logview.cmd - Windows Internet Explorer provided by e-buro

http://10.0.0.1/logview.cmd

System Log

Data/Godzina	Lokalizacja	Poziom	Komunikat
Jan 1 00:00:16	user	warn	kernel: ^[[0;35mCMF:HAL pktDbgLvl[0xc00d569c]=0^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;32mCMF:HAL pktCmfHalConstruct:^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;35mCMF:HAL pktDbgLvl[0xc00d569c]=0^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;33mCMF:DRV pktCmfDrvConstruct:^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;35mCMF:DRV pktDbgLvl[0xc00dd9f4]=0^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;36;44mBroadcom Packet CMF (Experimental) Char Driver v0.1 Oct 6 2014 18:13:42 Registered<232>^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;34mCMF:PROTO pktCmfProtoConstruct:^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;35mCMF:PROTO pktDbgLvl[0xc00dd9c0]=0^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;36;44mBroadcom Packet CMF (Experimental) [6368-B2] v0.1 Oct 6 2014 18:13:42 Loaded^[[0m
Jan 1 00:00:16	user	warn	kernel: bcmxtmcf: bcmxtmcf_init entry
Jan 1 00:00:16	user	warn	kernel: adsl: adsl_init entry
Jan 1 00:00:16	user	warn	kernel: Broadcom BCM6368B2 Ethernet Network Device v0.1 Oct 6 2014 18:14:48
Jan 1 00:00:16	user	warn	kernel: ETH Init: Ch:0 - 180 tx BDs at 0xa3950000
Jan 1 00:00:16	user	warn	kernel: ETH Init: Ch:0 - 960 rx BDs at 0xa3008000
Jan 1 00:00:16	user	warn	kernel: ##### ethsw_init_table:105 ##### switch_port_phyid[0]=1
Jan 1 00:00:16	user	warn	kernel: ##### ethsw_init_table:105 ##### switch_port_phyid[1]=2
Jan 1 00:00:16	user	warn	kernel: ##### ethsw_init_table:105 ##### switch_port_phyid[2]=3
Jan 1 00:00:16	user	warn	kernel: ##### ethsw_init_table:105 ##### switch_port_phyid[3]=4
Jan 1 00:00:16	user	warn	kernel: 17
Jan 1 00:00:16	user	warn	kernel: dgaspr: kerSysRegisterDyingGaspHandler: bcmssw registered
Jan 1 00:00:16	user	warn	kernel: ^[[0;35mCMF:HW pktDbgLvl[0xc00ce640]=0^[[0m
Jan 1 00:00:16	user	warn	kernel: ^[[0;34mCMF:HW pktCmfHwReset: Reset HW layer.^[[0m

Internet | Tryb chroniony: włączony

9.3 Zarządzanie kontem

9.3.1 Hasła

Poniższy ekran pozwala skonfigurować hasła dostępu do urządzenia:

- **user** – konto dla użytkowników usługi Internet DSL. Dzięki niemu może uzyskać dostęp do routera, wyświetlić ustawienia konfiguracji i statystyki, jak również wykonać konfigurację funkcjonalności dotyczących sieci LAN.
- **bpack** – konto dla użytkowników usługi Biznes pakiet. Dzięki niemu może uzyskać dostęp do routera, wyświetlić ustawienia konfiguracji i statystyki, jak również wykonać konfigurację funkcjonalności dotyczących sieci LAN.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Ustawienia
Logi systemowe
Zarządzanie kontem
Hasła
Ponowne uruchomienie

Kontrola dostępu - Hasła

Dostęp do routera szerokopasmowego jest kontrolowany przez konto użytkownika: user.

Nazwa użytkownika "user" może uzyskać dostęp do routera szerokopasmowego, wyświetlić ustawienia konfiguracji i statystyki, jak również zaktualizować oprogramowanie routera od strony LAN.

Użyj pola poniżej aby wprowadzić maksymalnie 16 znaków i kliknij przycisk "Zastosuj / Zapisz", aby zmienić lub stworzyć hasła. Uwaga: Hasło nie może zawierać spacji.

Nazwa użytkownika:

Stare hasło:

Nowe hasło:

Potwierdź hasło:

Kliknij przycisk **Zastosuj/Zapisz** aby kontynuować.

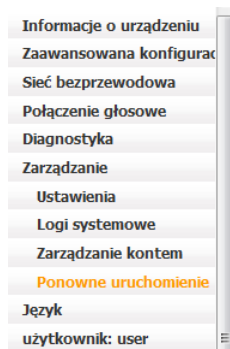
UWAGA 1: Hasło może się składać z maksymalnie 16 znaków.

UWAGA 2: Nie zaleca się stosowania polskich znaków oraz znaków specjalnych.

9.4 Ponowne uruchomienie

Kliknij przycisk **Uruchom ponownie** aby zapisać obecną konfigurację i ponownie uruchomić router.

UWAGA: Zamknij przeglądarkę i odczekaj 2 minuty zanim powtórnie ją otworzysz. Możliwe, że będziesz musiał zmienić konfigurację IP swojego komputera aby znowu skomunikować się z routerem.



Kliknij na przycisk poniżej aby ponownie uruchomić router.

Uruchom ponownie

Załącznik A – Zapora sieciowa

STATEFUL PACKET INSPECTION (SPI)

Po nawiązaniu sesji przez aplikację firewall nadzoruje stan wszystkich połączeń przechodzących przez niego i analizuje nagłówki pakietów pod kątem, czy pakiety te są przesyłane przez aplikacje dopuszczone do ruchu sieciowego. W odróżnieniu od Static Packet Filtering, który analizuje pakiety tylko na podstawie informacji zawartych w ich nagłówkach.

DENIAL OF SERVICE ATTACK (DoS)

Atak polega na przeciążeniu aplikacji serwującej określone dane czy obsługującej danych klientów (np. wyczerpanie limitu wolnych gniazd dla serwerów FTP czy WWW) lub zapełnienie całego systemu plików tak, by dogrywanie kolejnych informacji nie było możliwe. Urządzenie może wytrzymać następujące ataki DoS: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack i Tear Drop.

FILTR TCP/IP/PORT/INTERFEJSEÓW

Te reguły pomagają filtrować ruch w warstwie Sieci (warstwie 3).

Podczas tworzenia interfejsu Routowania pole **Włącz zaporę sieciową** musi być zaznaczone.

Przejdź do Zaawansowana konfiguracja → Bezpieczeństwo → Filtrowanie adresów IP.

FILTR WYCHODZĄCYCH ADRESÓW IP

Filtr ten, pomaga podczas ustanawiania reguł odrzucania pakietów interfejsu LAN. Domyślnie, jeśli Zapora sieciowa jest włączona, cały ruch adresów IP z LAN jest dozwolony. Ustanawiając jeden lub wiele filtrów, określone pakiety z LAN mogą zostać odrzucone.

Przykład 1:

Nazwa filtra	: Out_Filter1
Protokół	: TCP
Źródłowy adres IP	: 192.168.1.45
Źródłowa maska podsieci	: 255.255.255.0
Port źródłowy	: 80
Docelowy adres IP	: NA
Docelowy maska podsieci	: NA
Port docelowy	: NA

Powyższy filtr odrzuci wszystkie pakiety TCP pochodzące z LAN z adresu IP /maski podsieci 192.168.1.45/24 i posiadające port źródłowy 80. Wszystkie inne pakiety będą akceptowane.

Przykład 2:

Nazwa filtra	: Out_Filter2
Protokół	: UDP
Źródłowy adres IP	: 192.168.1.45
Źródłowa maska podsieci	: 255.255.255.0
Port źródłowy	: 5060:6060
Docelowy adres IP	: 172.16.13.4
Docelowy maska podsieci	: 255.255.255.0
Port docelowy	: 6060:7070

Powyższy filtr odrzuci wszystkie pakiety UDP pochodzące z LAN z adresu IP /maski podsieci 192.168.1.45/24 i posiadające port źródłowy z zakresu od 5060 do 6060, wysyłane na adres 172.16.13.4/24 na porty z zakresu od 6060 do 7070. Wszystkie inne pakiety będą akceptowane.

FILTR PRZYCHODZĄCYCH ADRESÓW IP

Filtr ten, pomaga podczas ustanawiania reguł odrzucania i akceptowania pakietów interfejsu WAN. Domyślnie, jeśli Zapora sieciowa jest włączona, cały ruch adresów IP z WAN jest blokowany. Ustanawiając jeden lub wiele

filtrów, określone pakiety z WAN mogą zostać zaakceptowane.

Przykład 1: Nazwa filtra : In_Filter1
Protokół : TCP
Strategia : Allow
Źródłowy adres IP : 210.168.219.45
Źródłowa maska podsieci : 255.255.0.0
Port źródłowy : 80
Docelowy adres IP : NA
Docelowy maska podsieci : NA
Port docelowy : NA
Interfejs WAN : br0

Powyższy filtr zaakceptuje wszystkie pakiety TCP pochodzące z interfejsu WAN „br0” z adresu IP /maski podsieci 10.168.219.45/16 i posiadające port źródłowy 80. Wszystkie inne pakiety będą odrzucone.

Przykład 2: Nazwa filtra : In_Filter2
Protokół : UDP
Strategia : Allow
Źródłowy adres IP : 210.168.219.45
Źródłowa maska podsieci : 255.255.0.0
Port źródłowy : 5060:6060
Docelowy adres IP : 192.168.1.45
Docelowy maska podsieci : 255.255.255.0
Port docelowy : 6060:7070
Interfejs WAN : br0

Powyższy filtr zaakceptuje wszystkie pakiety UDP pochodzące z interfejsu WAN „br0” z adresu IP /maski podsieci 10.168.219.45/16 i posiadające port źródłowy z zakresu od 5060 do 6060, wysyłane na adres 192.168.1.45/24 na porty z zakresu od 6060 do 7070. Wszystkie inne pakiety będą odrzucone.

KONTROLA RODZICIELSKA

Ta opcja pozwala ograniczyć dostęp do sieci zewnętrznej wybranemu urządzeniu LAN w wybrane dni i w wybranym czasie .

Przykład: Nazwa użytkownika : FilterJohn
Adres MAC przeglądarki : 00:25:46:78:63:21
Dni tygodnia : pon, wt, pt
Początek blokowania czasu : 14:00
Koniec blokowania czasu : 18:00

Powyższa reguła zablokuje dostęp do sieci zewnętrznej urządzeniu LAN o adresie MAC 00:25:46:78:63:21 w poniedziałki, wtorki i piątki od 14:00 do 18:00. W pozostałym przedziale czasu urządzenie będzie miało dostęp do sieci zewnętrznej.

Załącznik B - Specyfikacje

Porty zewnętrzne

- 1 x port RJ-11 dla ADSL2+/VDSL2,
- 4 x port RJ-45 dla LAN,
- 1 x port RJ-45 dla GigaWAN,
- x port FXS,
- x port USB
- przycisk Reset,
- przycisk WPS,
- przycisk Wi-Fi On/Off,
- 2 anteny Wi-Fi,
- Włącznik,

WAN

Standard ADSL

- ITU-T G.992.5,
- ITU-T G.992.3,
- ITU-T G.992.1,
- ANSI T1.413 Issue 2,
- AnnexM

ADSL2+

- Downstream : 24 Mb/s Upstream : 1.3 Mb/s

Standard VDSL2

- ITU-Y G.993.2 (wspierane profile 8a, 8b, 8c, 8d, 12a, 12b, 17a)

VDSL2

- Downstream : 100 Mbps Upstream : 60 Mbps

Interfejs LAN

- Standard IEEE 802.3, IEEE 802.3u
- 10/100 BaseT Auto-sense
- MDI/MDX support Tak

Interfejs WLAN

- Standard IEEE802.11n (kompatybilne z IEEE802.11b/g)
- Kodowanie 64/128-bit Wired Equivalent Privacy (WEP)
- Kanały 11 (USA, Canada)/ 13 (Europa)/ 14 (Japonia)
- Przesyłanie danych Do 300 Mb/s
- WPA Tak
- IEEE 802.1x Tak
- WMM Tak
- WPS Tak
- Filtrowanie MAC Tak

Funkcje Bezpieczeństwa

- Protokół uwierzytelniania: PAP, CHAP
- Wyzwalanie/Przekierowanie Portów,
- Filtrowanie pakietów IP i adresów MAC

QoS

- L3 policy-based QoS,
- IP QoS,
- ToS

Usługi Głosowe

- SIP RFC 3261
- MGCP RFC 3435
- Kodeki G.711, G.723.1, G.726, G.729ab
- RTP RFC 1889
- SDP RFC 2327
- Caller ID zgodnie z ETSI
- Echo cancellation G.168
- Wycinanie ciszy: Tak
- Połączenie alarmowe Tak

Zasilanie

- 12 Vdc / 2 A

Warunki zewnętrzne

- Temperatura pracy 0 ~ 50 stopni Celsjusza
- Względna wilgotność 5 ~ 95% (nie skondensowana)

Wymiary

- 256.2 x 166 x 47.9

Waga zestawu

- 1 x Comtrend VI-3225u,
- 1 x kabel RJ-11,
- 1 x kabel RJ-45,
- 1 x zasilacz,
- 1 x CD-ROM

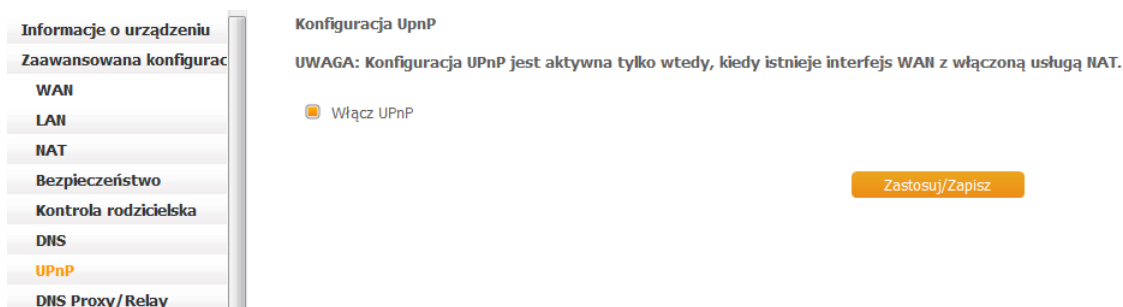
Certyfikat

- CE

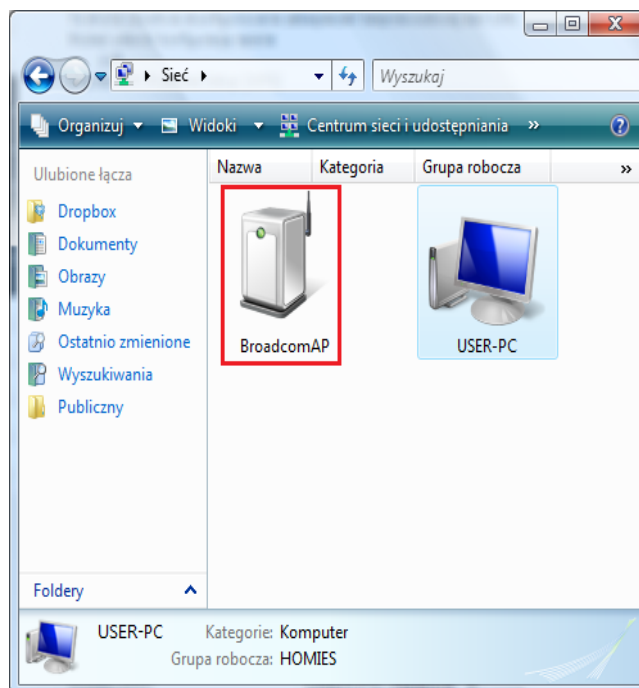
Załącznik C – Zewnętrzny Rejestrator WPS

Poniższe kroki przeprowadzą Cię przez proces dodawania external registrar za pomocą interfejsu sieciowego (Web User Interface - WUI) na Twoim Komputerze z systemem Windows Vista:

KROK 1: Włącz opcję UPnP w zakładce Zaawansowana konfiguracja.



KROK 2: Na swoim komputerze otwórz folder Sieć i znajdź ikonę BroadcomAP.



KROK 3: W konfiguracji modemu, w grupie **Sieć bezprzewodowa** → zakładce **Bezpieczeństwo** włącz WPS wybierając **Enable** z rozwijanej listy i ustaw tryb WPS AP na **Unconfigured**. Kliknij przycisk **Zastosuj/Zapisz** na dole ekranu.

Komunikacja bezprzewodowa - Bezpieczeństwo

Ta strona umożliwia skonfigurowanie zabezpieczeń bezprzewodowej sieci LAN.

Możesz ustawić konfigurację ręcznie

LUB

poprzez WiFi Protected Setup (WPS)

Konfiguracja WPS

Włącz WPS

Enabled ▾

Dodaj **klienta** (Ta funkcja jest dostępna tylko wtedy, gdy tryb WPA-PSK, WPA2 PSK lub tryb otwarty jest skonfigurowany)



Przycisk



Wprowadź PIN STA



Użyj PIN AP

[Dodaj Enrollee](#)

Ustaw **tryb WPS AP**

Unconfigured ▾

Konfiguruj **AP** (skonfiguruj wszystkie ustawienia zabezpieczeń z zewnętrznym rejestrem)

PIN urządzenia

31957199

[Help](#)

[Konfiguracja AP](#)

Ręczna konfiguracja AP

Można ustawić metodę uwierzytelniania sieci, wybierając szyfrowanie danych.

Określ, czy klucz sieciowy jest wymagany do uwierzytelniania w sieci bezprzewodowej i określ sposób szyfrowania.

Kliknij przycisk "Zastosuj / Zapisz" po zakończeniu.

Wybierz SSID:

USER-PC_Network ▾

Uwierzytelnianie sieci:

WPA-PSK ▾

Hasło WPA / WAPI:

.....

[Kliknij tutaj, aby wyświetlić](#)

WPA okres odświeżania grupy klucza:

0

Szyfrowanie WPA / WAPI:

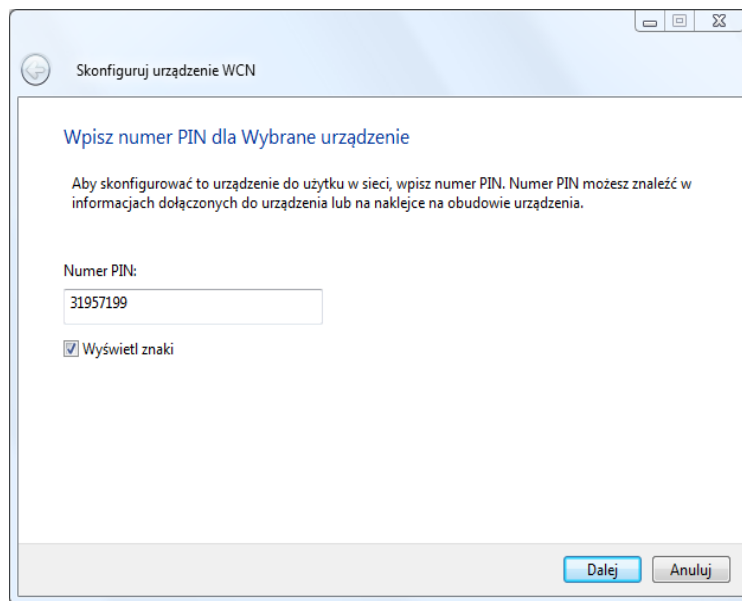
TKIP+AES ▾

Szyfrowanie WEP:

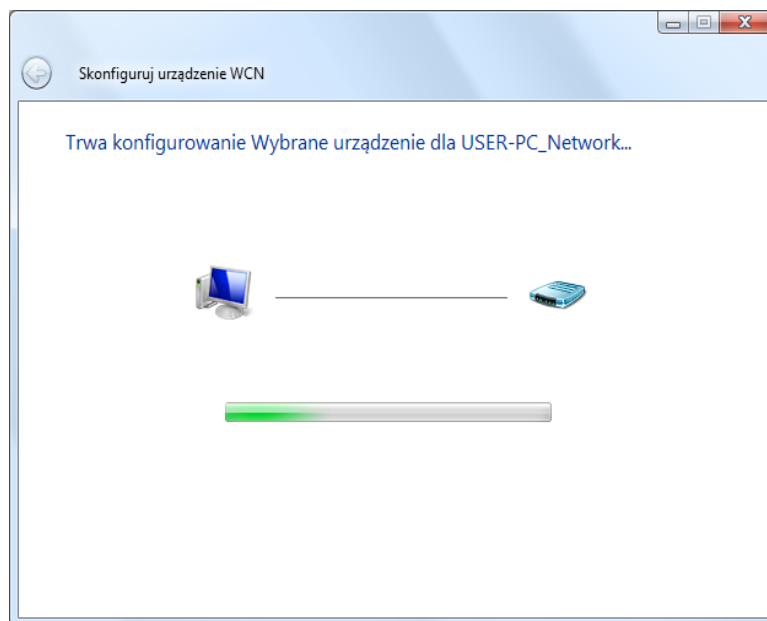
Disabled ▾

[Zastosuj / Zapisz](#)

- KROK 4:** Podczas akceptowania nowych ustawień bezprzewodowych router wyświetli przez chwilę pustą stronę. Kiedy powyższy ekran powróci kliknij przycisk **Konfiguracja AP** jak pokazano na powyższym ekranie.
- KROK 5:** Wróć do folderu Sieć na swoim komputerze i kliknij na ikonie BroadcomAP. Pojawi się okno dialogowe z pytaniem o numer PIN urządzenia. Wprowadź numer PIN taki jak pokazany na ekranie Bezprzewodowy -> Bezpieczeństwo. Kliknij przycisk **Dalej**.



KROK 6: Windows Vista podejmie próbę skonfigurowania ustawień bezpieczeństwa sieci bezprzewodowej.



KROK 7: W przypadku sukcesu, ustawienia bezpieczeństwa będą odpowiadały tym w systemie Windows Vista.

Załącznik D – Serwer Wydruku

Windows XP

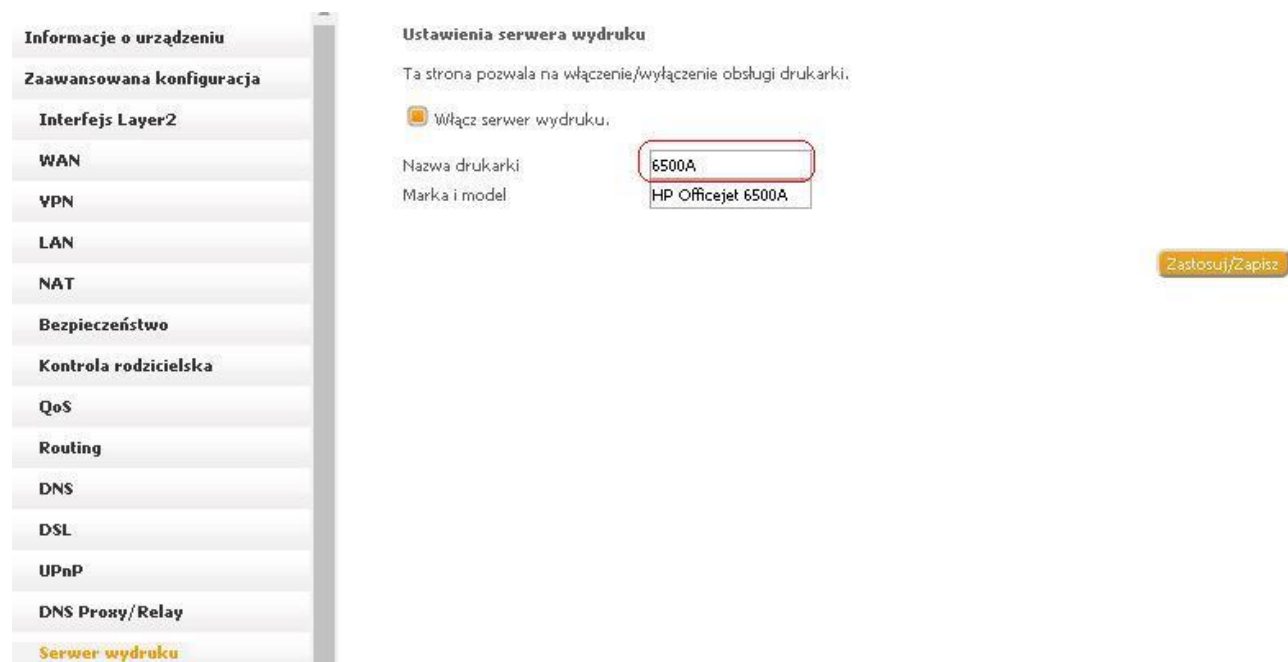
Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu **Windows XP**.

KROK 1: Zainstaluj wymagane sterowniki Twojej drukarki. Powinny się znajdować na płycie instalacyjnej producenta drukarki.

KROK 2: Włącz Serwer Wydruku za pomocą interfejsu sieciowego routera w zakładce **Serwer wydruku** w grupie **Zaawansowana konfiguracja**.

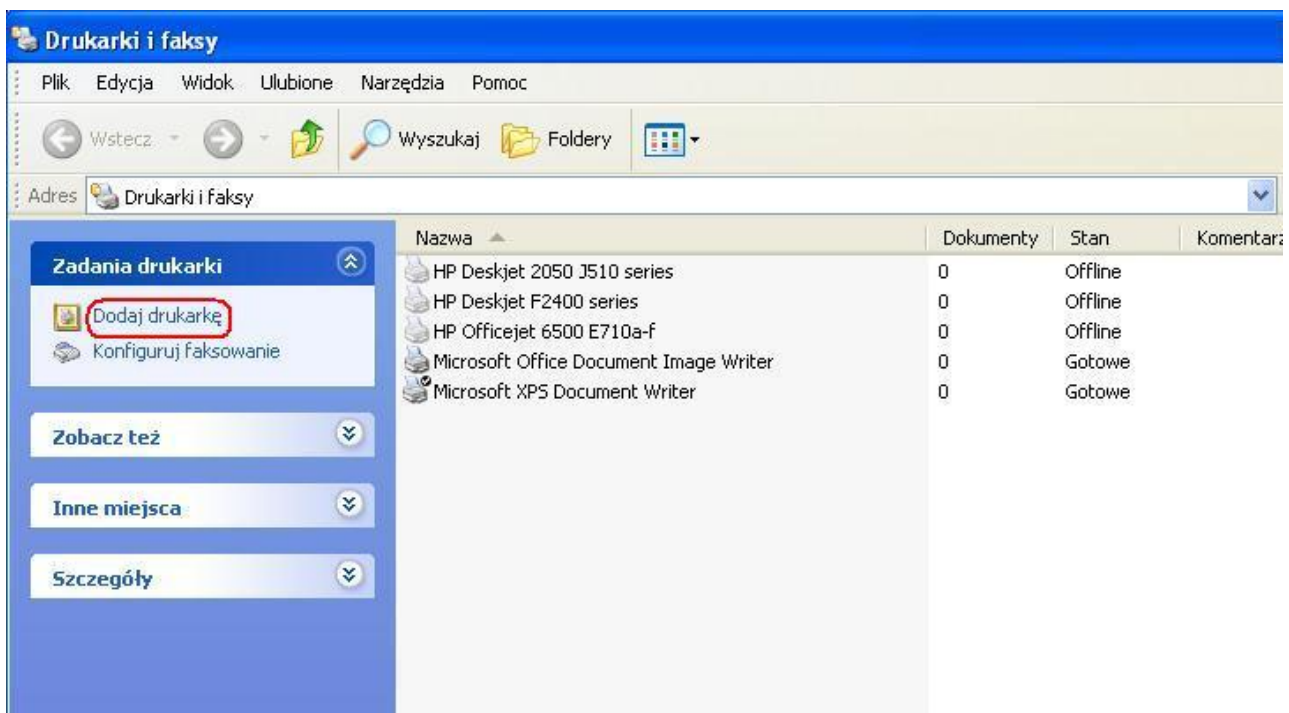
Zaznacz pole wyboru  **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.

UWAGA: Nazwa drukarki może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.
Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.

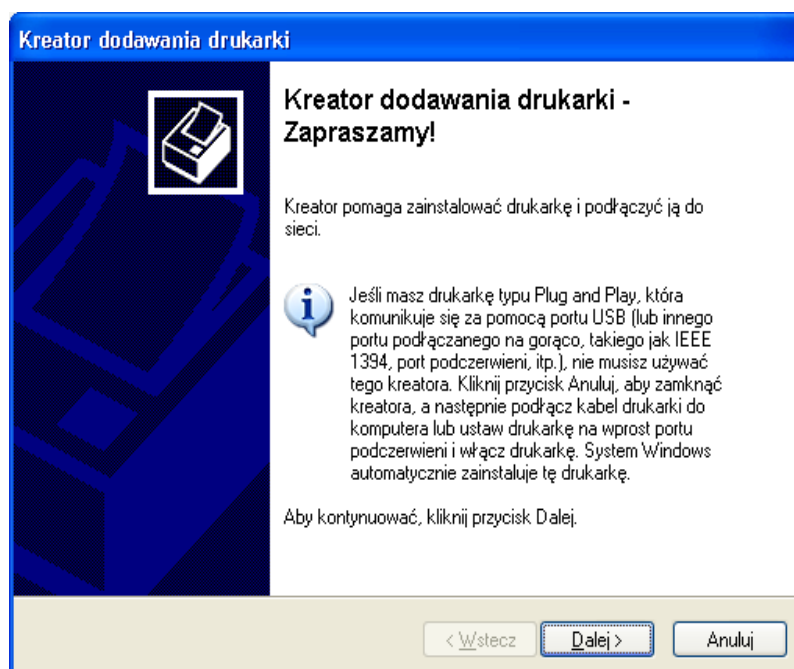


The screenshot displays the router's configuration page. On the left is a sidebar menu with the following items: 'Informacje o urządzeniu', 'Zaawansowana konfiguracja' (highlighted), 'Interfejs Layer2', 'WAN', 'VPN', 'LAN', 'NAT', 'Bezpieczeństwo', 'Kontrola rodzicielska', 'QoS', 'Routing', 'DNS', 'DSL', 'UPnP', 'DNS Proxy/Relay', and 'Serwer wydruku' (highlighted in orange). The main content area is titled 'Ustawienia serwera wydruku'. It contains the text 'Ta strona pozwala na włączenie/wyłączenie obsługi drukarki.' followed by a checked checkbox labeled 'Włącz serwer wydruku.'. Below this are two input fields: 'Nazwa drukarki' with the value '6500A' and 'Marka i model' with the value 'HP Officejet 6500A'. A red rectangle highlights the 'Nazwa drukarki' field. At the bottom right of the configuration area is an orange button labeled 'Zastosuj/Zapisz'.

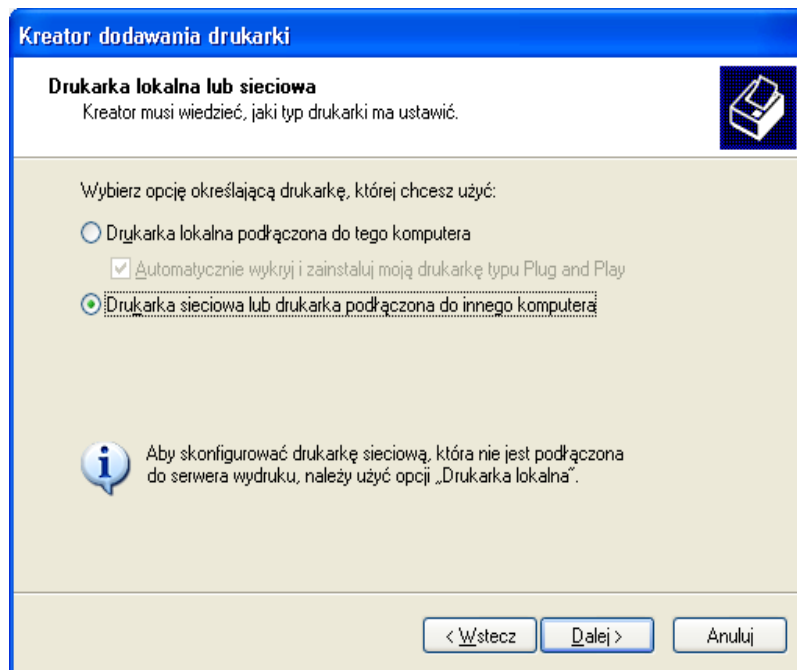
KROK 3: Przejdź do menu **Drukarki i faksy** w **Panelu sterowania** i kliknij ikonę **Dodaj drukarkę** (pokazaną na poniższym ekranie).



KROK 4: Naciśnij przycisk **Dalej** gdy pojawi się poniższe okno dialogowe.

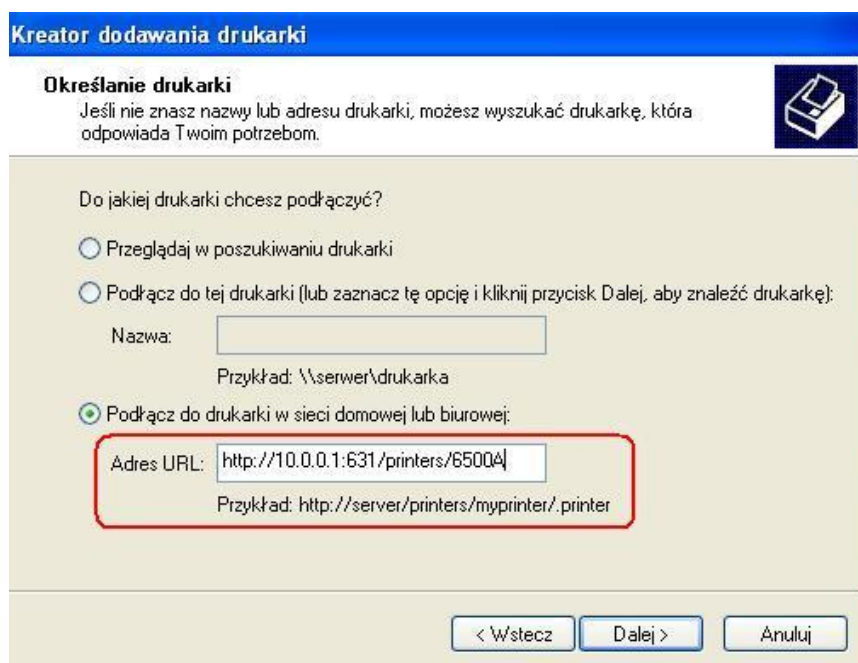


KROK 5: Wybierz pole **Drukarka sieciowa** i kliknij przycisk **Dalej**.

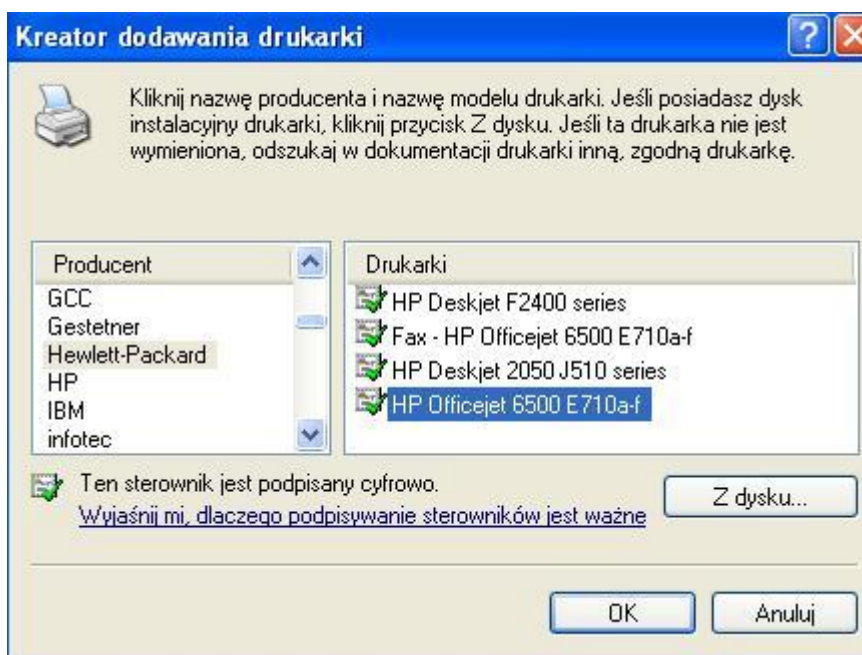


KROK 6: Wybierz pole **Podłącz do drukarki w sieci** i wprowadź link do swojej drukarki.
(np.10.0.0.1:631/printers/6500A). Następnie kliknij przycisk **Dalej**.

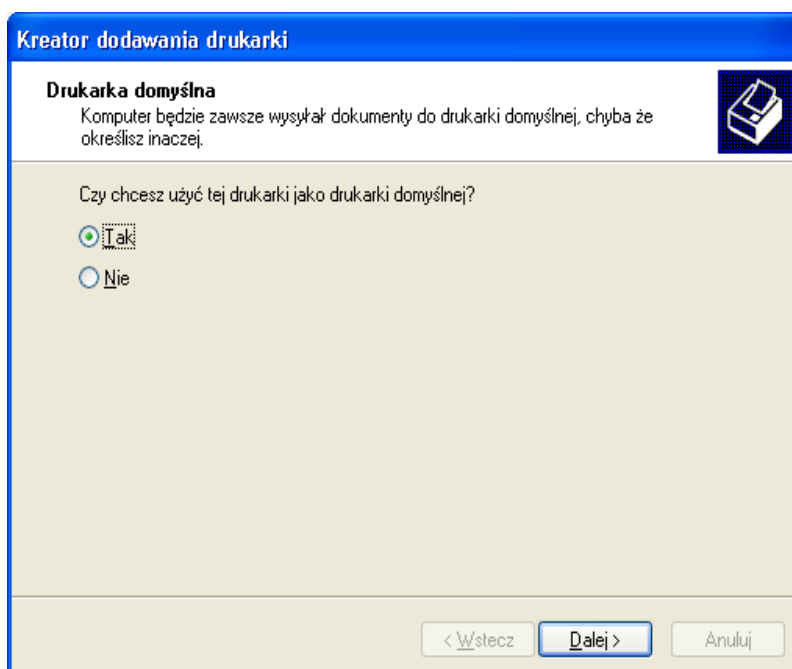
UWAGA: Nazwa drukarki musi być identyczna z tą, wprowadzoną w menu „ustawienia serwera wydruku” w kroku 2.



Krok 7: Wybierz sterownik swojej drukarki z listy dostępnych sterowników lub wybierz opcję **Z dysku...**, aby zainstalować sterownik z płyty dodanej do Twojej drukarki.



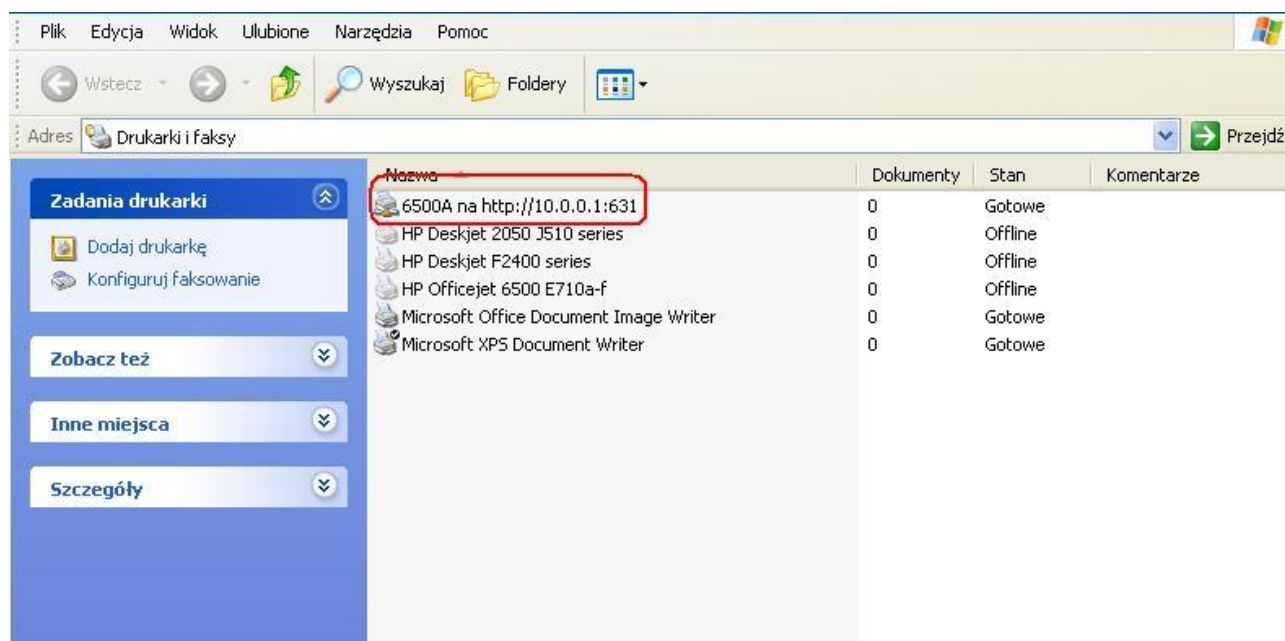
KROK 8: Wybierz **Tak** jeśli chcesz ustawić tę drukarkę jako drukarkę domyślną. W przeciwnym razie wybierz **Nie**. Kliknij przycisk **Dalej**.



KROK 9: Kliknij przycisk **Zakończ**.



KROK 9: Sprawdź stan drukarki w Panelu Sterowania w oknie Drukarki i faksy. Status powinien być widoczny jak **Gotowe**.



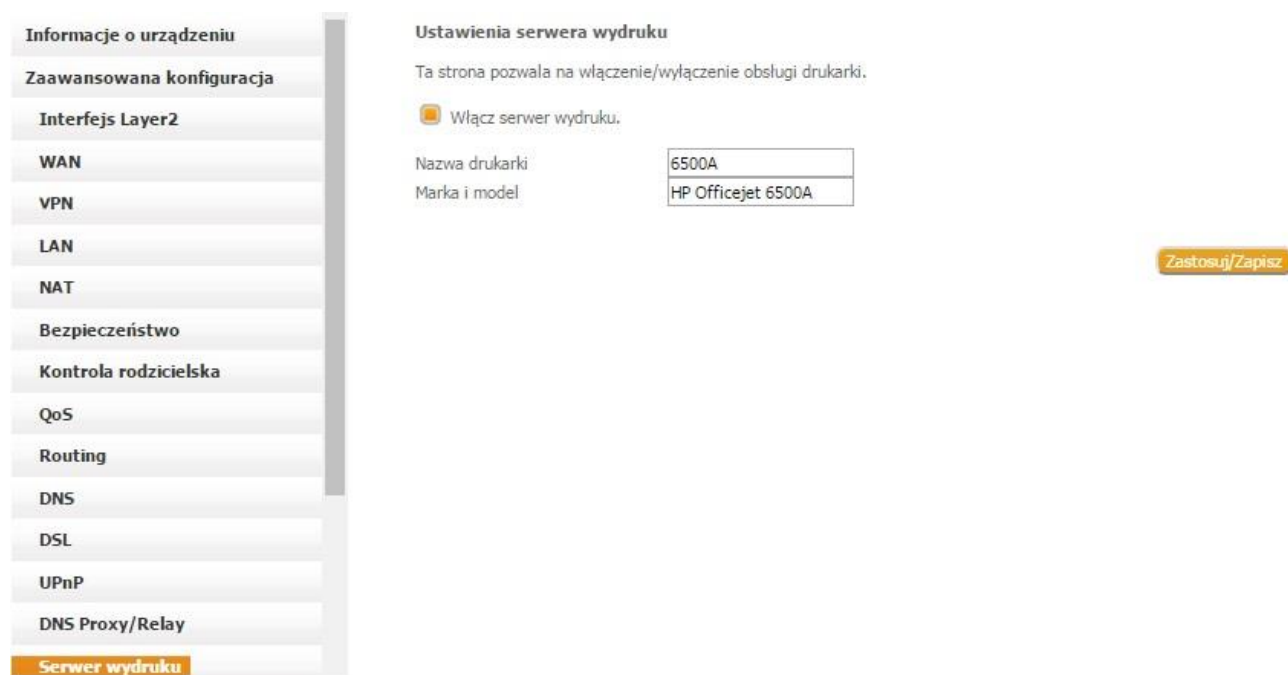
Windows 7

Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu **Windows 7**.

KROK 1: Włącz Serwer Wydruku za pomocą interfejsu sieciowego routera w zakładce **Serwer wydruku** w grupie **Zaawansowana konfiguracja**.

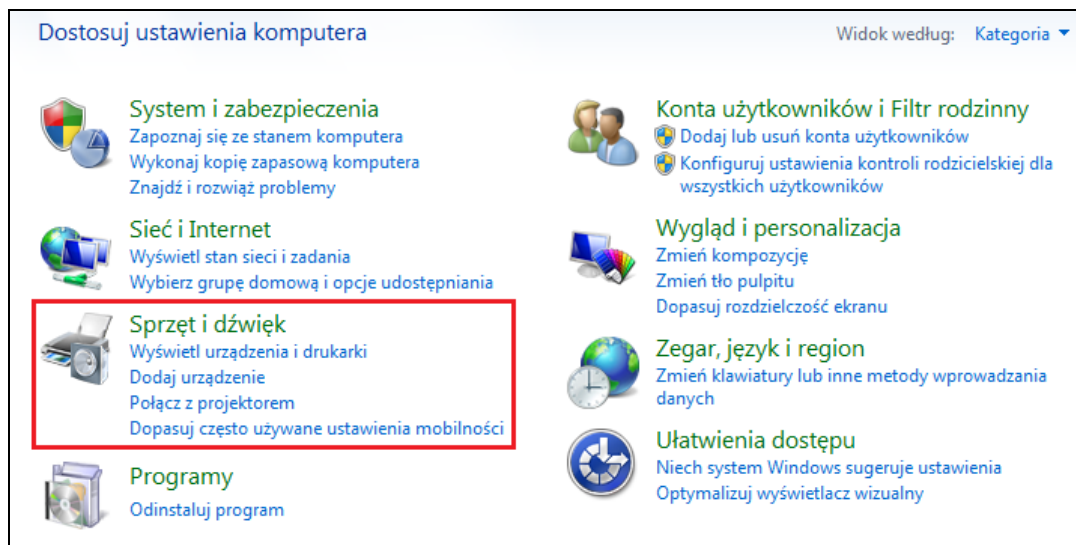
Zaznacz pole wyboru  **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.

UWAGA: **Nazwa drukarki** może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.
Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.

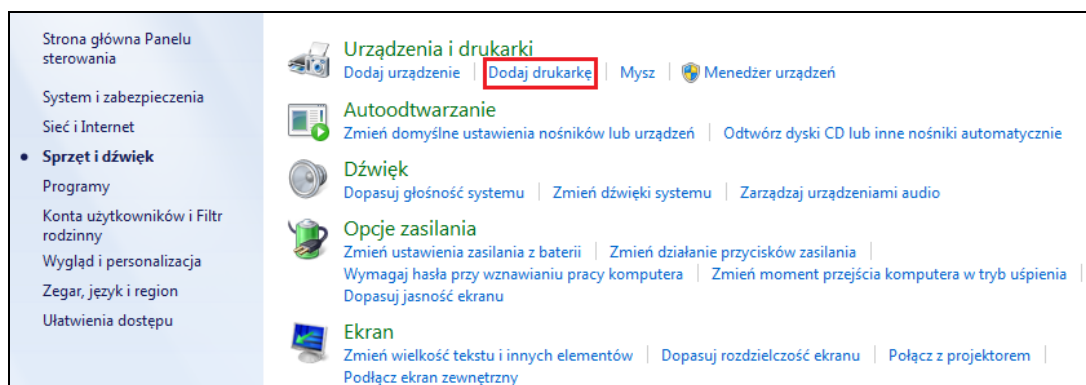


The screenshot displays the router's configuration interface. On the left is a sidebar menu with the following items: 'Informacje o urządzeniu', 'Zaawansowana konfiguracja', 'Interfejs Layer2', 'WAN', 'VPN', 'LAN', 'NAT', 'Bezpieczeństwo', 'Kontrola rodzicielska', 'QoS', 'Routing', 'DNS', 'DSL', 'UPnP', 'DNS Proxy/Relay', and 'Serwer wydruku' (which is highlighted in orange). The main area is titled 'Ustawienia serwera wydruku' (Print Server Settings) and contains the text: 'Ta strona pozwala na włączenie/wyłączenie obsługi drukarki.' (This page allows for enabling/disabling printer support). Below this is a checkbox labeled 'Włącz serwer wydruku.' (Enable print server.) which is checked. There are two input fields: 'Nazwa drukarki' (Printer name) with the value '6500A' and 'Marka i model' (Brand and model) with the value 'HP Officejet 6500A'. At the bottom right of the main area is an orange button labeled 'Zastosuj/Zapisz' (Apply/Save).

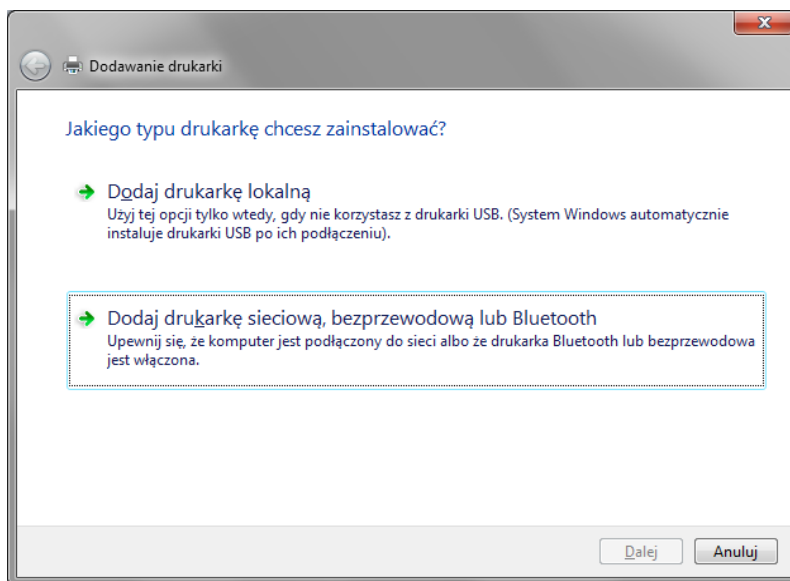
KROK 2: Przejdź do Panelu sterowania i kliknij ikonę Sprzęt i dźwięk.



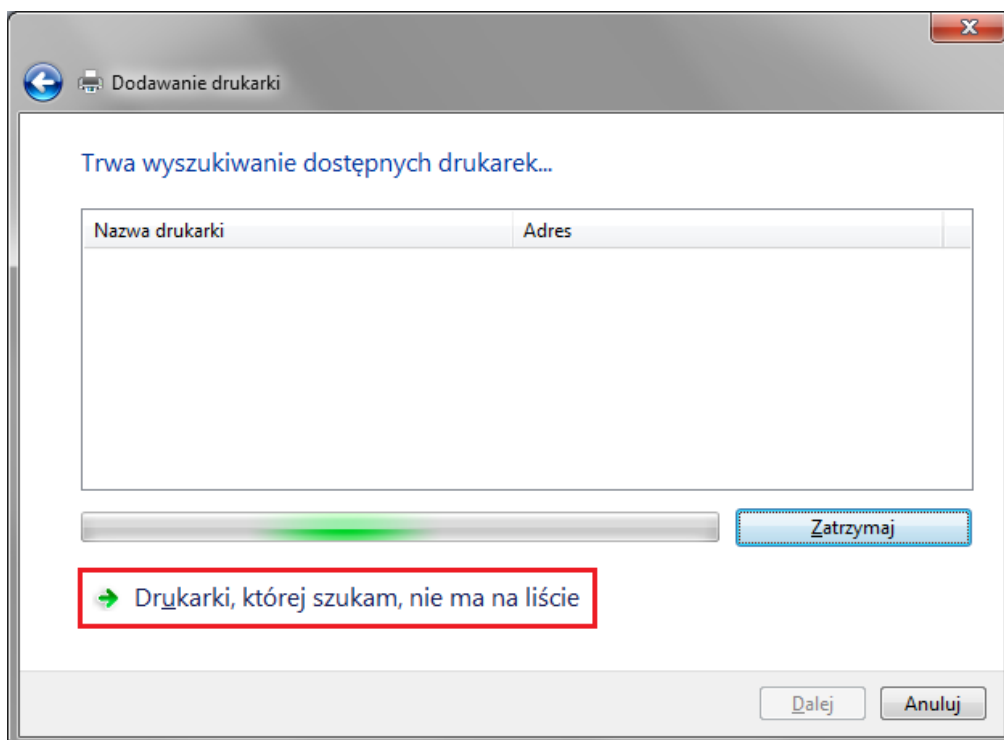
KROK 3: Kliknij pole Dodaj drukarkę.



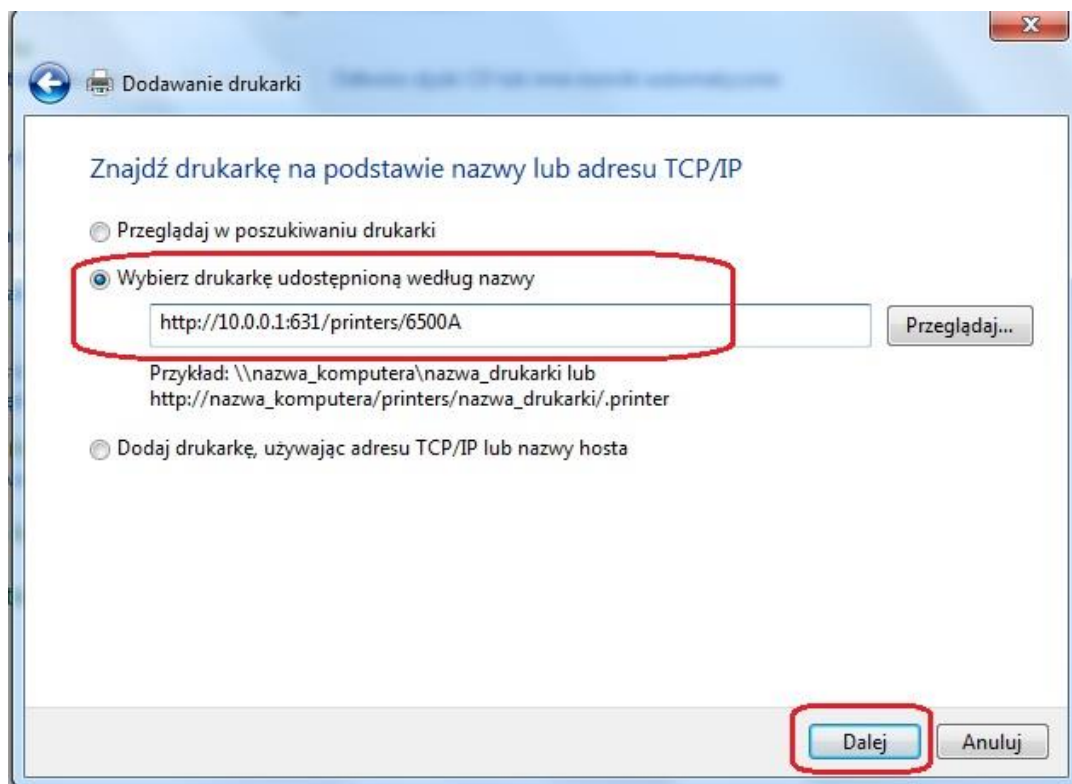
KROK 4: Wybierz pole **Dodaj drukarkę sieciową, bezprzewodową lub Bluetooth** i kliknij przycisk **Dalej**.



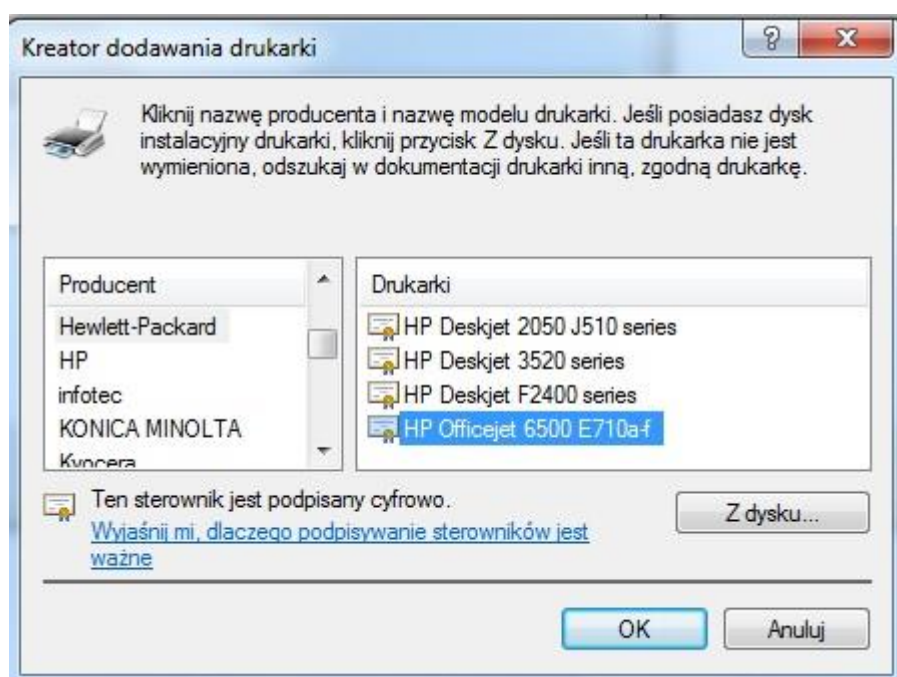
KROK 5: Kliknij pole **Drukarki, której szukam, nie ma na liście**, a następnie przycisk **Dalej**.



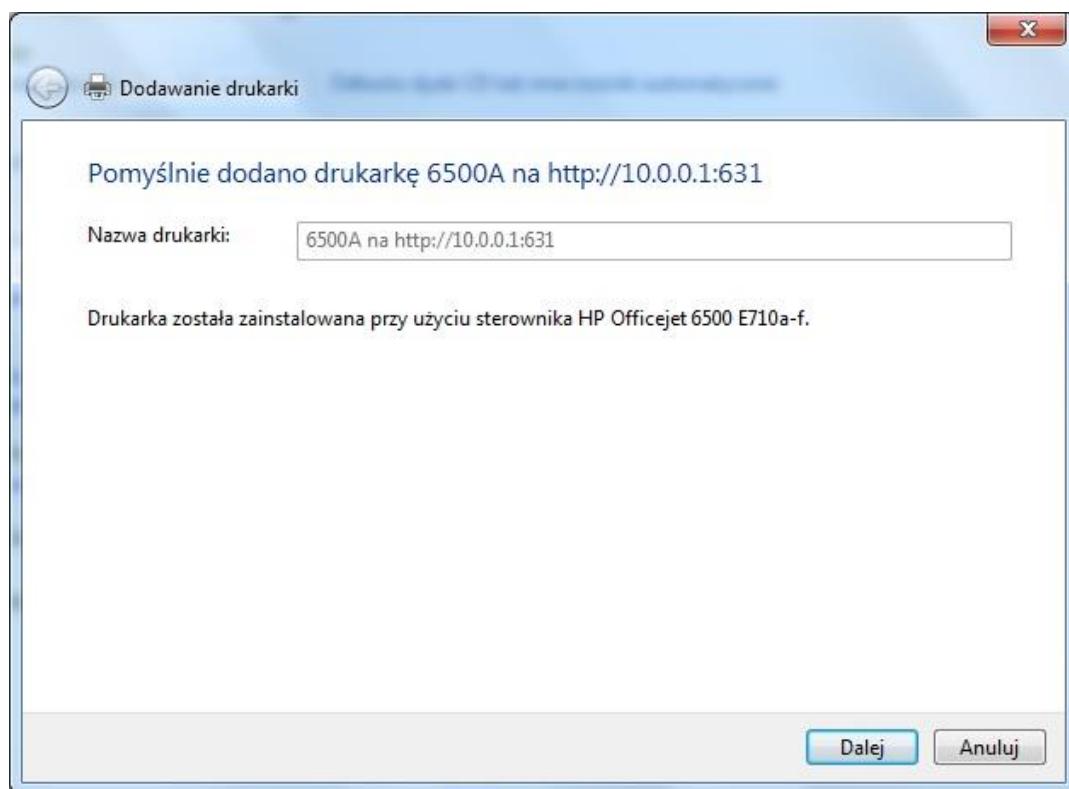
KROK 6: Zaznacz pole **Wybierz drukarkę udostępnioną wg nazwy** (<http://10.0.0.1:631/printers/6500A>), a następnie kliknij przycisk **Dalej**.



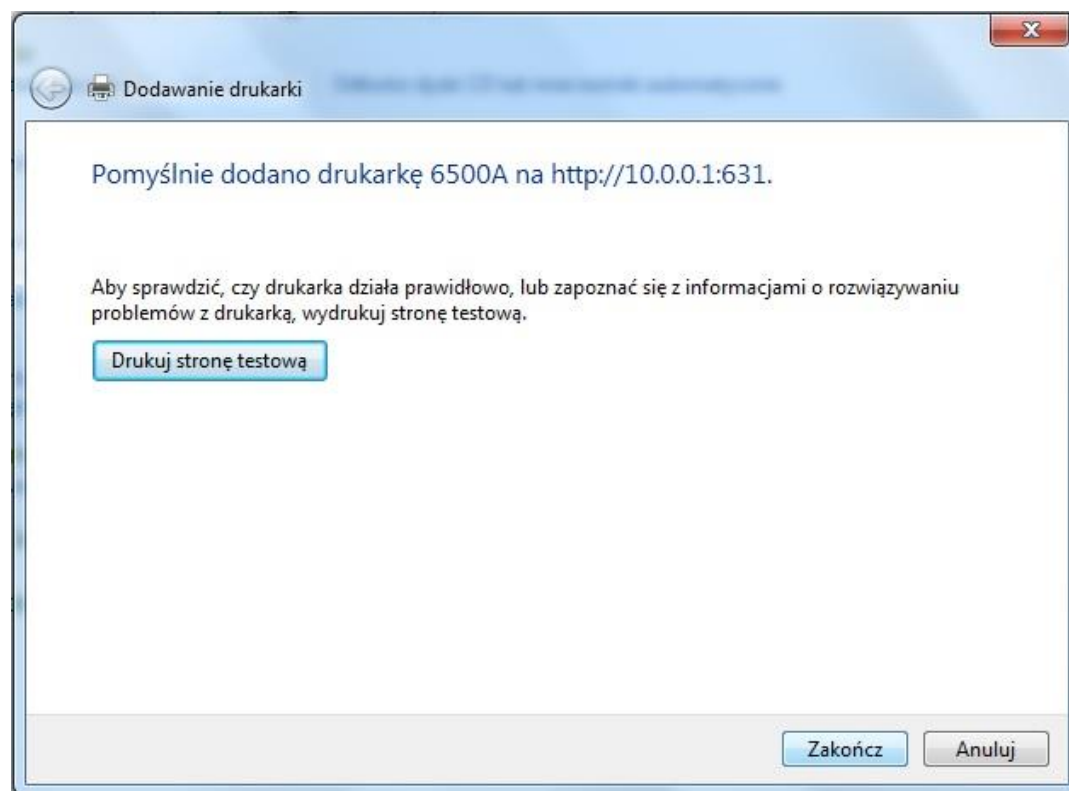
KROK 7: Wybierz sterownik swojej drukarki z listy dostępnych sterowników lub wybierz opcję **Z dysku...**, aby zainstalować sterownik z płyty dodanej do Twojej drukarki.



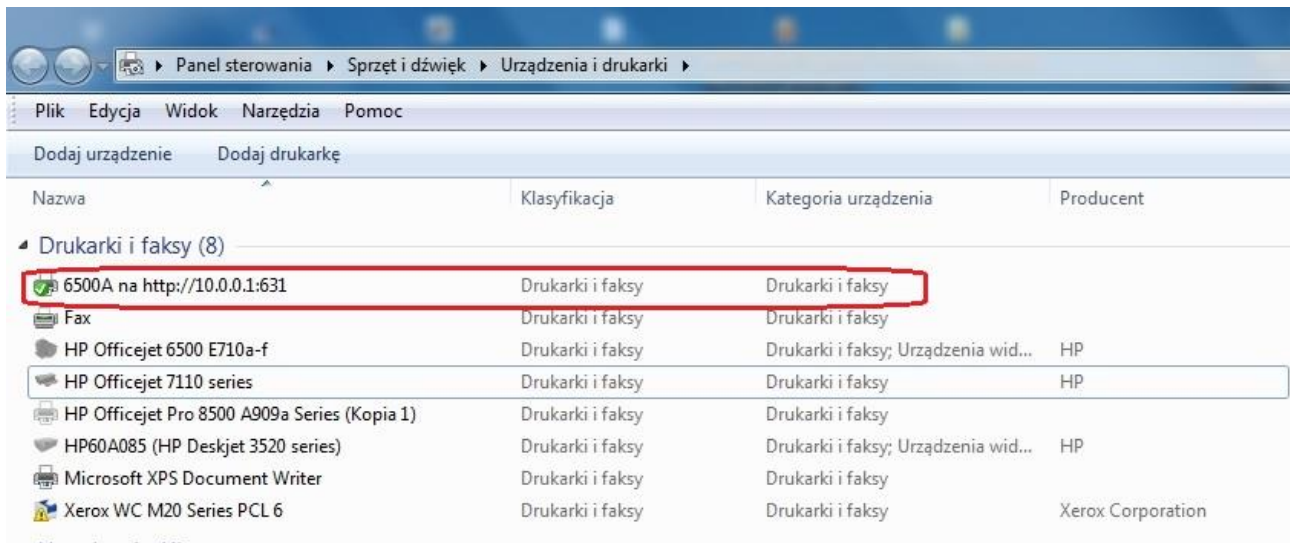
KROK 8: Aby kontynuować kliknij przycisk **Dalej**.



KROK 9: Aby kontynuować kliknij przycisk **Zakończ**.



KROK 10: Wynik instalacji drukarki sieciowej.



Panel sterowania > Sprzęt i dźwięk > Urządzenia i drukarki

Plik Edycja Widok Narzędzia Pomoc

Dodaj urządzenie Dodaj drukarkę

Nazwa	Klasyfikacja	Kategoria urządzenia	Producent
Drukarki i faksy (8)			
6500A na http://10.0.0.1:631	Drukarki i faksy	Drukarki i faksy	
Fax	Drukarki i faksy	Drukarki i faksy	
HP Officejet 6500 E710a-f	Drukarki i faksy	Drukarki i faksy; Urządzenia wid...	HP
HP Officejet 7110 series	Drukarki i faksy	Drukarki i faksy	HP
HP Officejet Pro 8500 A909a Series (Kopia 1)	Drukarki i faksy	Drukarki i faksy	
HP60A085 (HP Deskjet 3520 series)	Drukarki i faksy	Drukarki i faksy; Urządzenia wid...	HP
Microsoft XPS Document Writer	Drukarki i faksy	Drukarki i faksy	
Xerox WC M20 Series PCL 6	Drukarki i faksy	Drukarki i faksy	Xerox Corporation

Windows VISTA

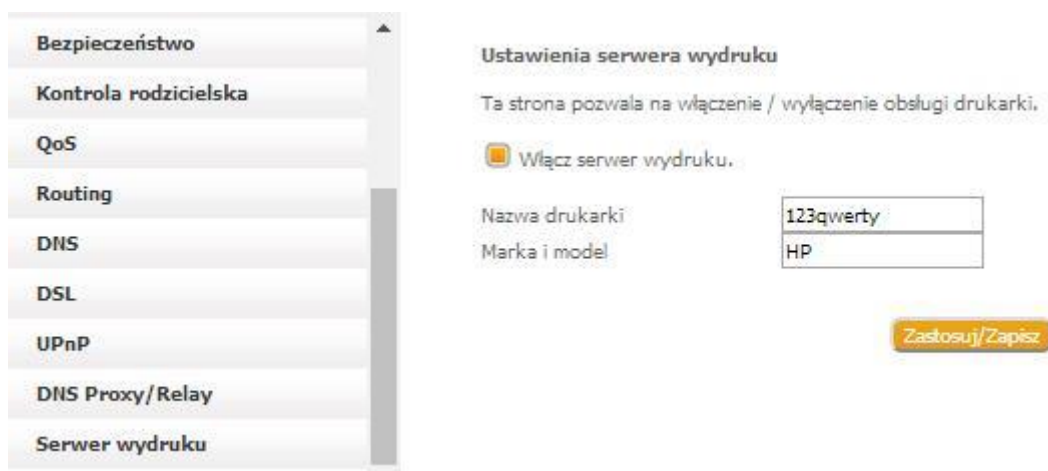
Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu Windows VISTA

UWAGA: Ta funkcja odnosi się tylko do modeli wyposażonych w port USB.

KROK 1: Włącz Serwer Wydruku za pomocą interfejsu sieciowego routera w zakładce **Serwer wydruku** w grupie **Zaawansowana konfiguracja**.

Zaznacz pole wyboru  **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.

UWAGA: Nazwa drukarki może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.
Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.



Bezpieczeństwo

Kontrola rodzicielska

QoS

Routing

DNS

DSL

UPnP

DNS Proxy/Relay

Serwer wydruku

Ustawienia serwera wydruku

Ta strona pozwala na włączenie / wyłączenie obsługi drukarki.

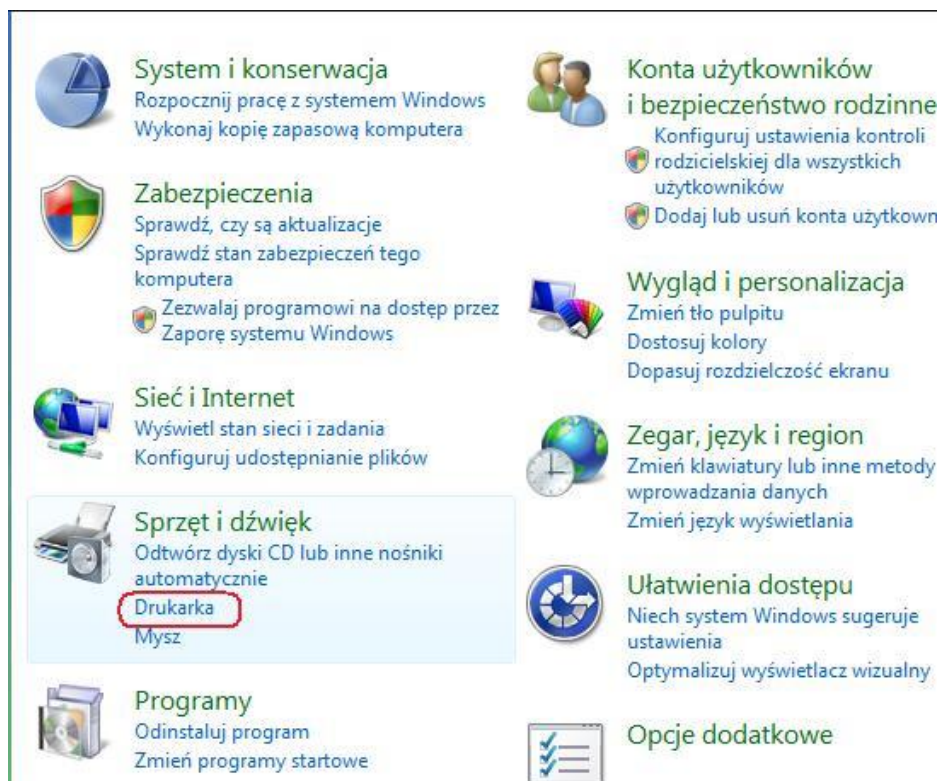
☒ Włącz serwer wydruku.

Nazwa drukarki: 123qwerty

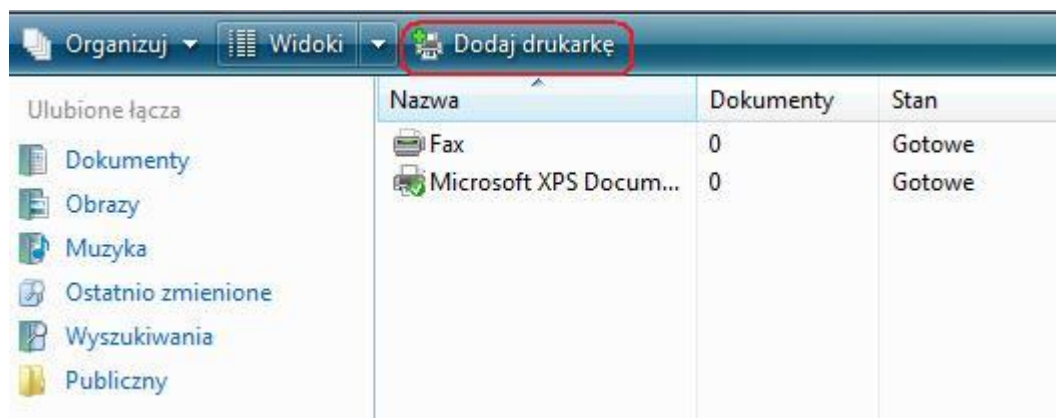
Marka i model: HP

Zastosuj/Zapisz

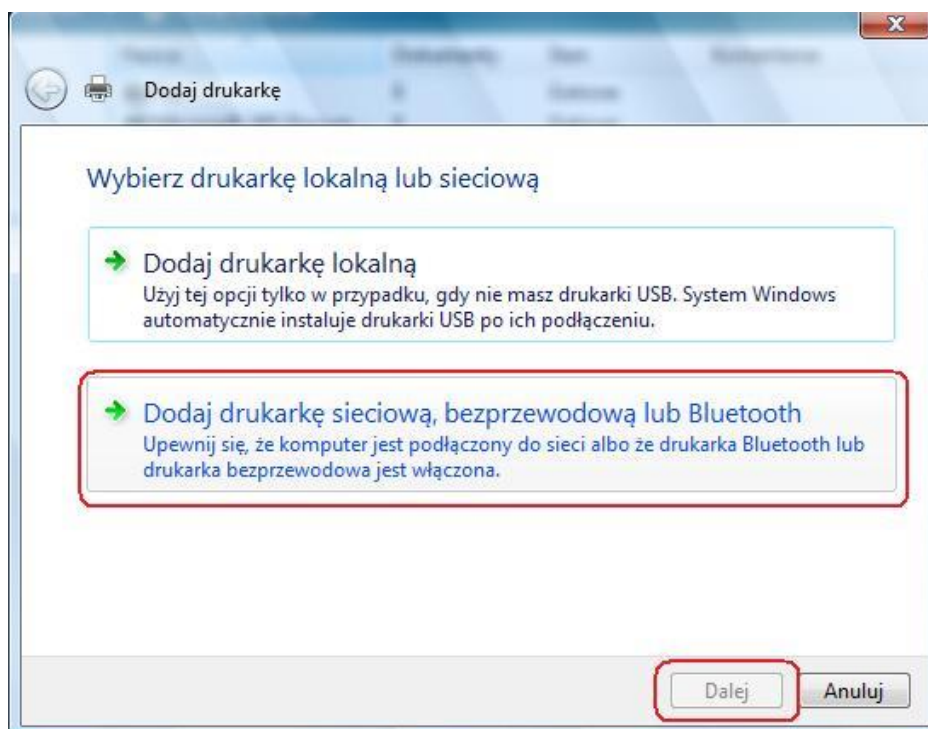
KROK 2: Przejdź do Panelu sterowania i kliknij ikonę Drukarki.



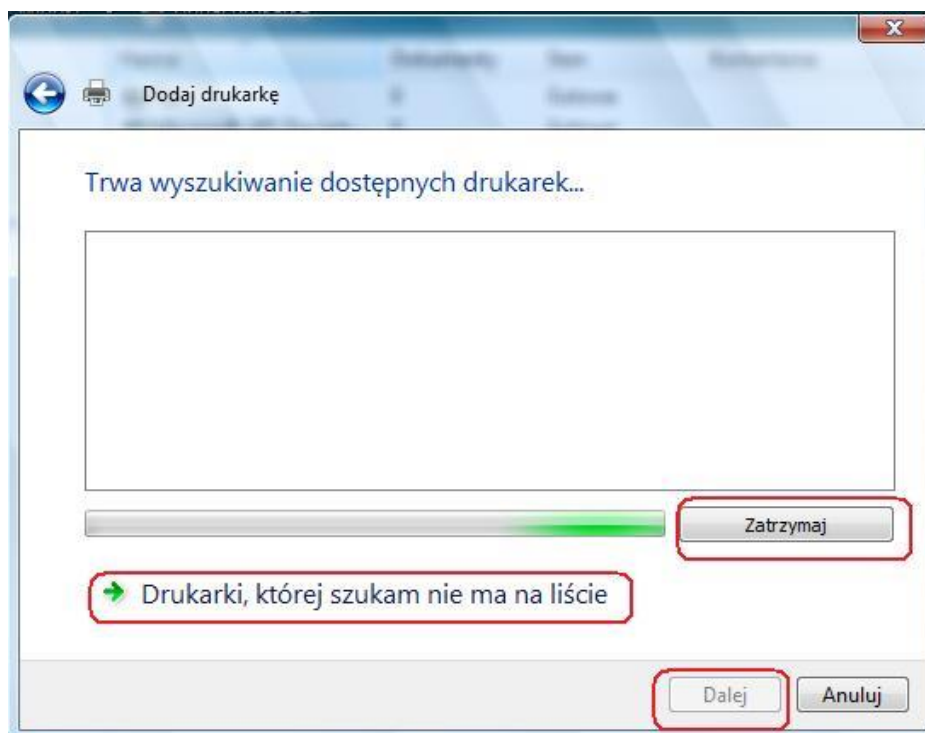
KROK 3: Kliknij pole Dodaj drukarkę.



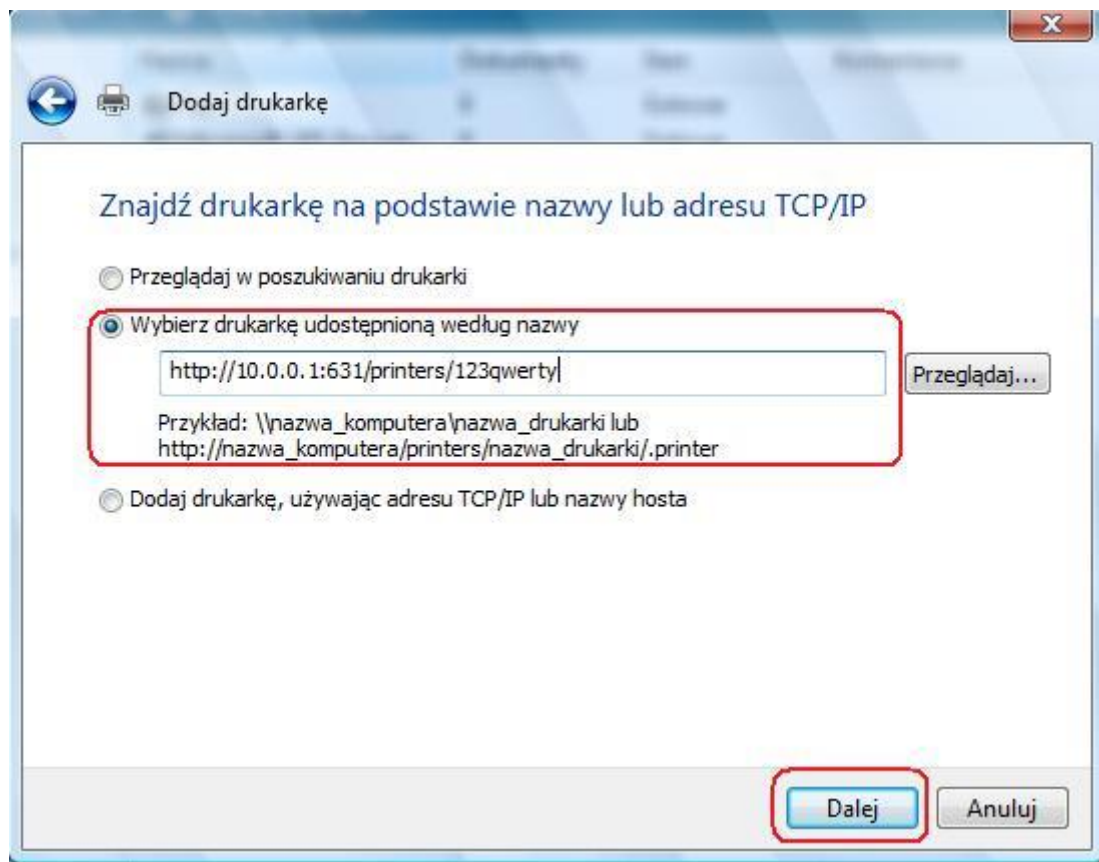
KROK 4: Wybierz pole **Dodaj drukarkę sieciową, bezprzewodową lub Bluetooth** i kliknij przycisk **Dalej**.



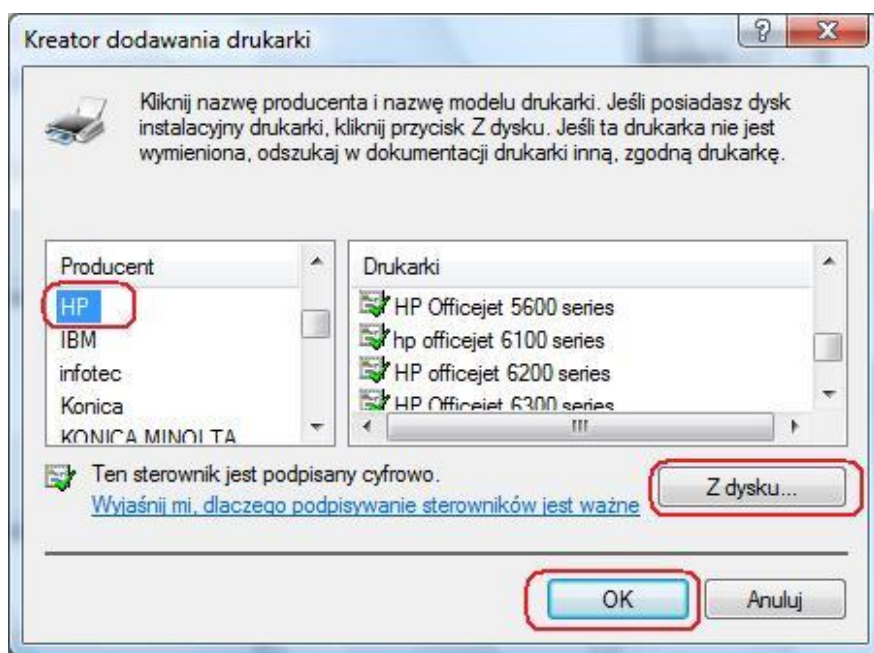
KROK 5: Kliknij pole **Drukarki, której szukam nie ma na liście**, a następnie przycisk **Dalej**.



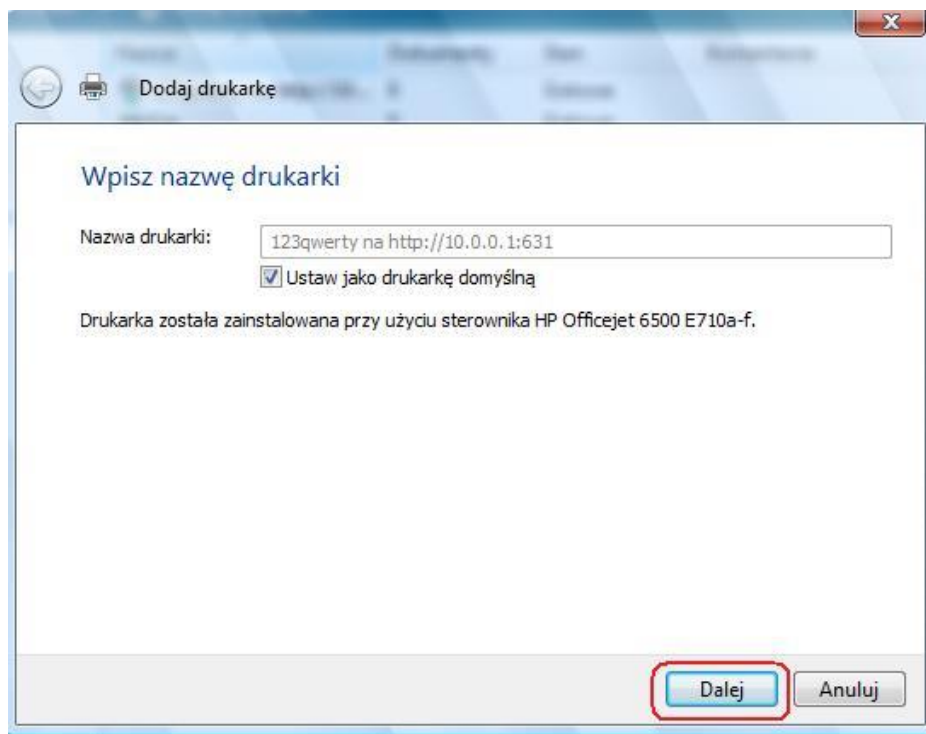
KROK 6: Zaznacz pole **Wybierz drukarkę udostępnioną według nazwy** i wpisz „http://10.0.0.1:631/printers/123qwerty”, a następnie kliknij przycisk **Dalej**.



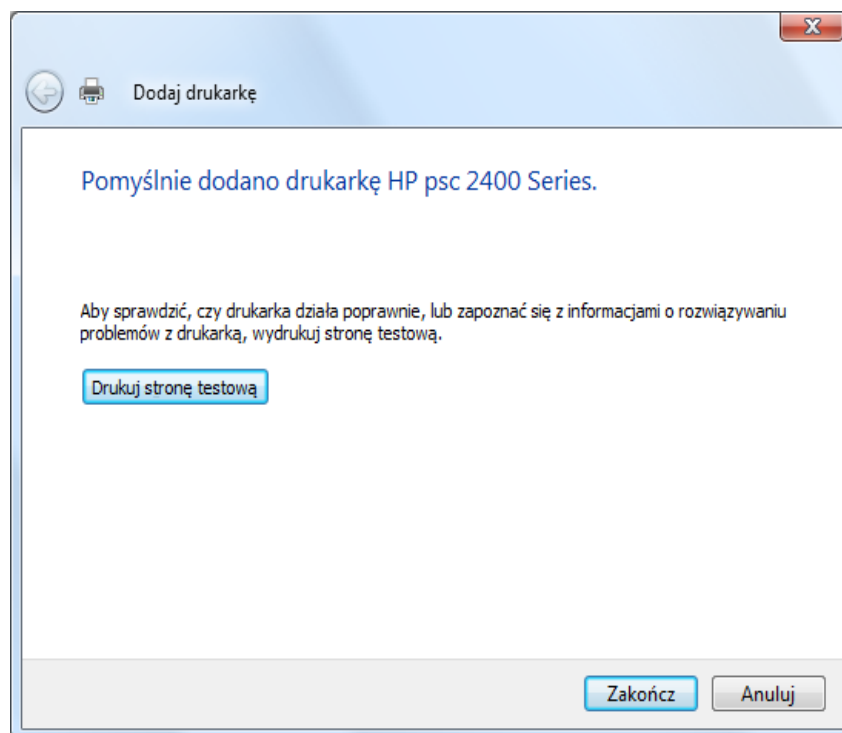
KROK 7: Wybierz sterownik swojej drukarki z listy dostępnych sterowników lub wybierz opcję **Z dysku...**, aby zainstalować sterownik z płyty dodanej do Twojej drukarki.



KROK 8: Aby kontynuować kliknij przycisk **Dalej**.



KROK 9: Kliknij przycisk **Zakończ**.



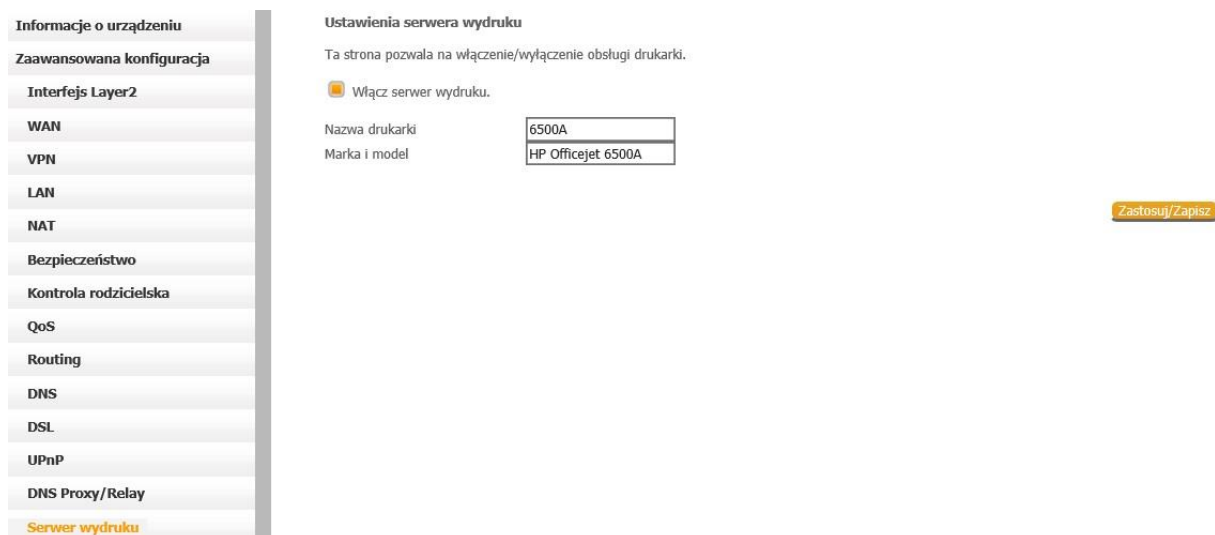
Windows 10

Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu Windows 10.

KROK 1: Włącz Serwer Wydruku za pomocą interfejsu sieciowego routera w zakładce **Serwer wydruku** w grupie **Zaawansowana konfiguracja**.

Zaznacz pole wyboru  **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.

UWAGA: **Nazwa drukarki** może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.
Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.



The screenshot displays the router's web interface. On the left is a sidebar menu with various configuration categories. The main area is titled 'Ustawienia serwera wydruku' (Print Server Settings). It includes a checkbox to enable the print server, which is currently checked. Below this are two input fields: 'Nazwa drukarki' (Printer Name) containing '6500A' and 'Marka i model' (Brand and Model) containing 'HP Officejet 6500A'. A 'Zastosuj/Zapisz' (Apply/Save) button is located at the bottom right of the form.

Informacje o urządzeniu	
Zaawansowana konfiguracja	
Interfejs Layer2	
WAN	
VPN	
LAN	
NAT	
Bezpieczeństwo	
Kontrola rodzicielska	
QoS	
Routing	
DNS	
DSL	
UPnP	
DNS Proxy/Relay	
Serwer wydruku	

Ustawienia serwera wydruku

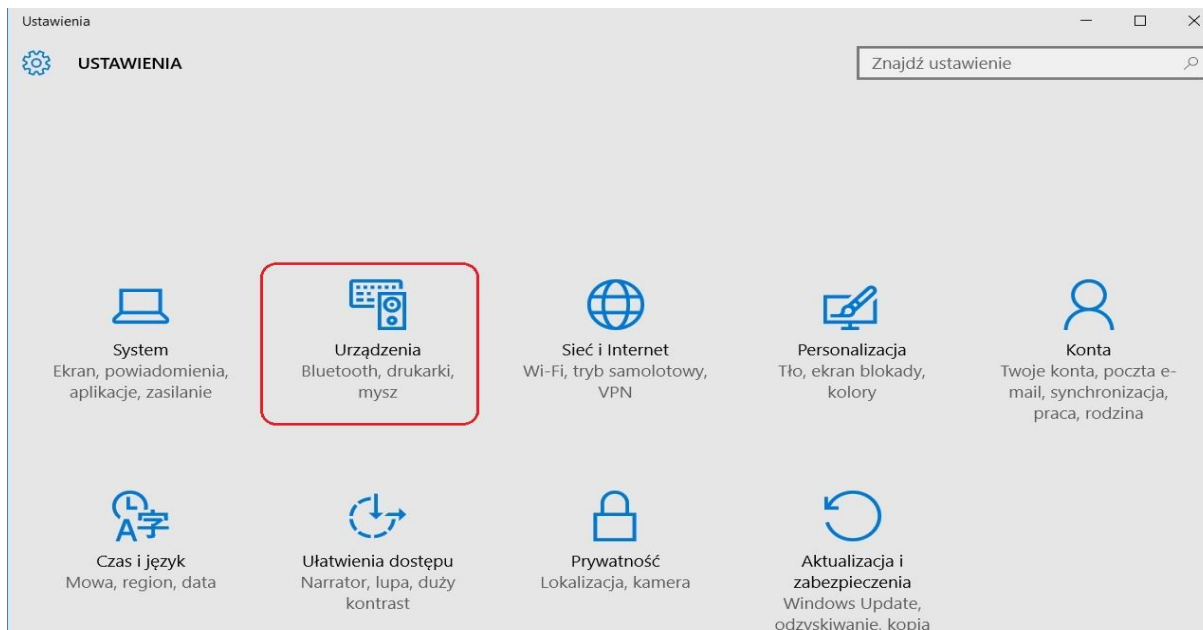
Ta strona pozwala na włączenie/wyłączenie obsługi drukarki.

☒ Włącz serwer wydruku.

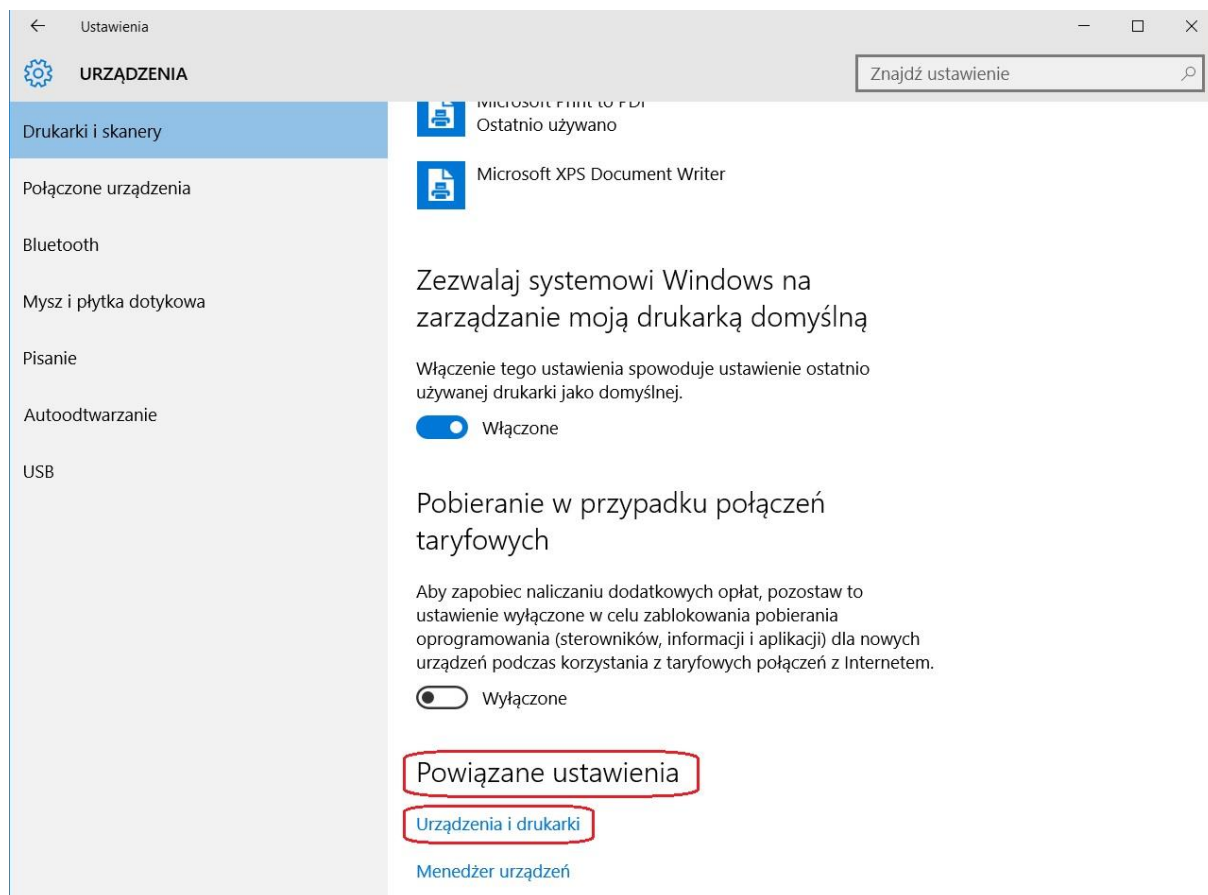
Nazwa drukarki	6500A
Marka i model	HP Officejet 6500A

Zastosuj/Zapisz

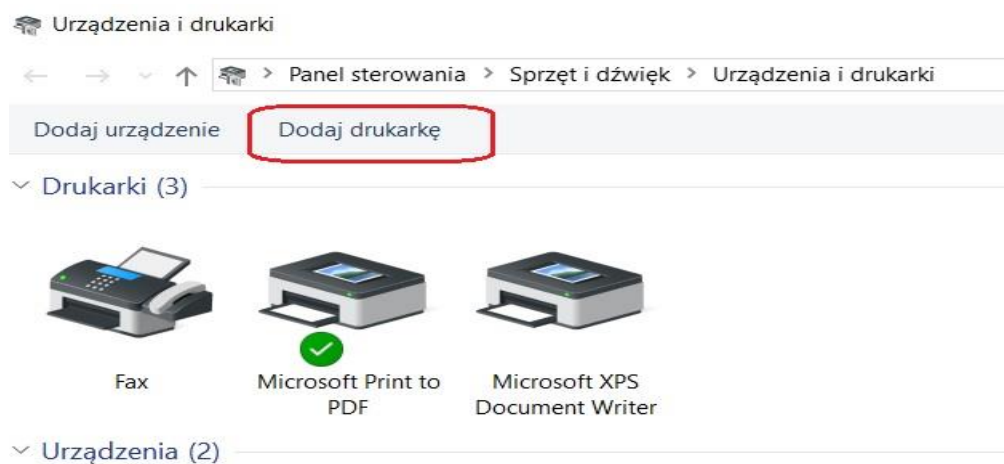
KROK 2: Przejdź do panelu „Ustawienia” i kliknij ikonę „Urządzenia”.



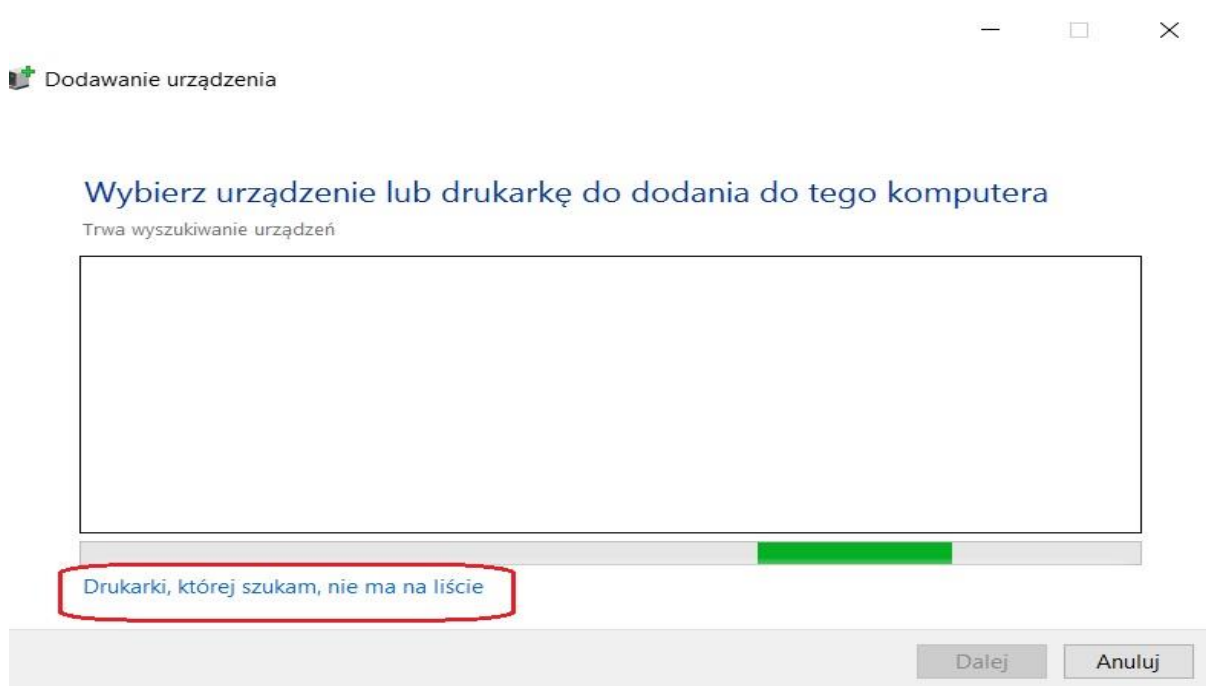
KROK 3: Przejdź do „Powiązane ustawienia” i kliknij „Urządzenia i drukarki”.



KROK 4: Kliknij „Dodaj drukarkę”.



KROK 5: Kliknij pole Drukarki, której szukam nie ma na liście, a następnie przycisk Dalej.



KROK 6: Wypełnij pole „Wybierz drukarkę udostępnioną według nazwy”.

← Dodawanie drukarki

Znajdź drukarkę na podstawie innych opcji

☐ Moja drukarka jest nieco starsza. Pomóż mi ją znaleźć.

☒ Wybierz drukarkę udostępnioną według nazwy

Przeglądaj...

Przykład: \\nazwa_komputera\nazwa_drukarki lub
http://nazwa_komputera/printers/nazwa_drukarki/.printer

☐ Dodaj drukarkę, używając adresu TCP/IP lub nazwy hosta

☐ Dodaj drukarkę Bluetooth, bezprzewodową lub wykrywalną w sieci

☐ Dodaj drukarkę lokalną lub sieciową z ustawieniami ręcznymi

Dalej Anuluj

KROK 7: Wybierz sterownik swojej drukarki z listy dostępnych sterowników lub wybierz opcję **Z dysku...**, aby zainstalować sterownik z płyty dodanej do Twojej drukarki.

Kreator dodawania drukarki

Kliknij nazwę producenta i nazwę modelu drukarki. Jeśli posiadasz dysk instalacyjny drukarki, kliknij przycisk Z dysku. Jeśli ta drukarka nie jest wymieniona, odszukaj w dokumentacji drukarki inną, zgodną drukarkę.

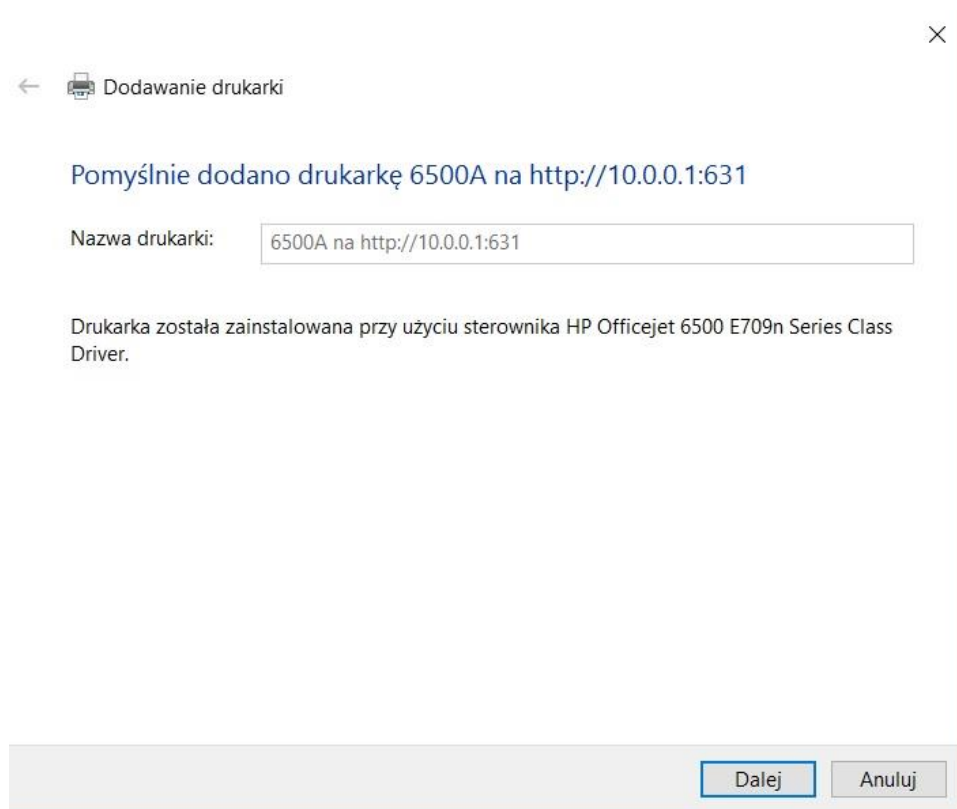
Producent: Generic, Gestetner, **HP**, InfoPrint, infotec

Drukarki: **HP Officejet 6500 E709n Series Class Driver**, HP Officejet 6500 E710a-f Class Driver, HP Officejet 6500 E710n-z Class Driver, HP Officejet 6600 Class Driver

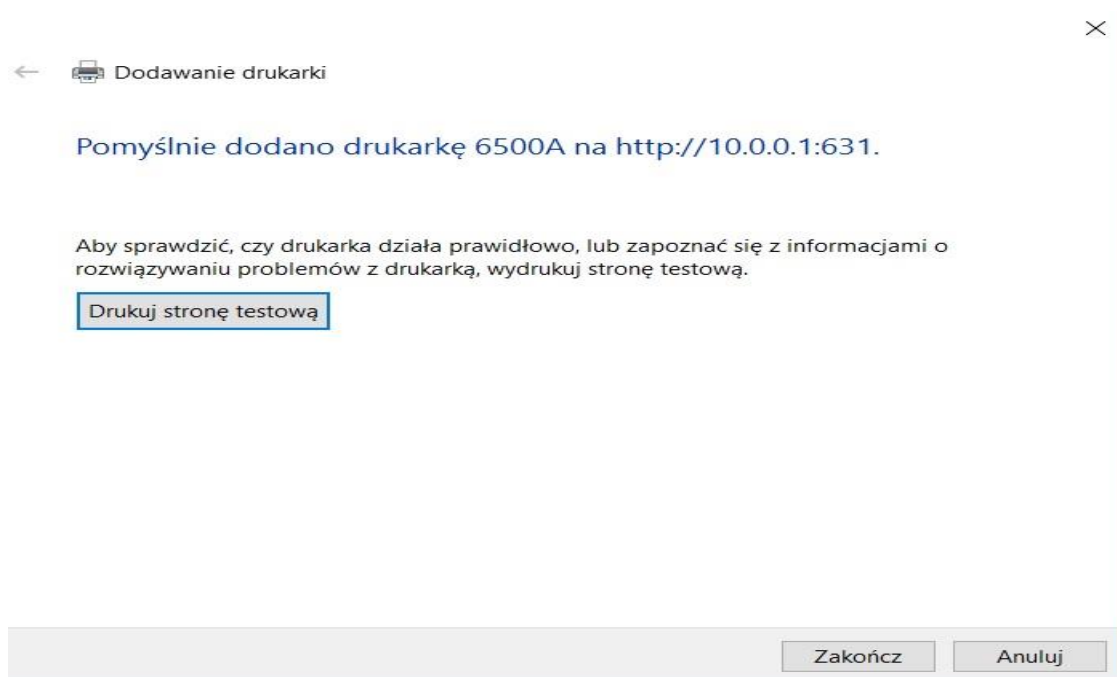
Ten sterownik jest podpisany cyfrowo. [Wyjaśnij mi, dlaczego podpisywanie sterowników jest ważne](#) Windows Update Z dysku...

OK Anuluj

KROK 8: Aby kontynuować kliknij przycisk **Dalej**.



KROK 9: Kliknij przycisk „Zakończ”.



KROK 10: Koniec instalacji.

