Bezprzewodowa brama domowa Cisco z wbudowanym cyfrowym adapterem głosu, modele DPC3925 i EPC3925 8x4 DOCSIS 3.0 — Podręcznik użytkownika

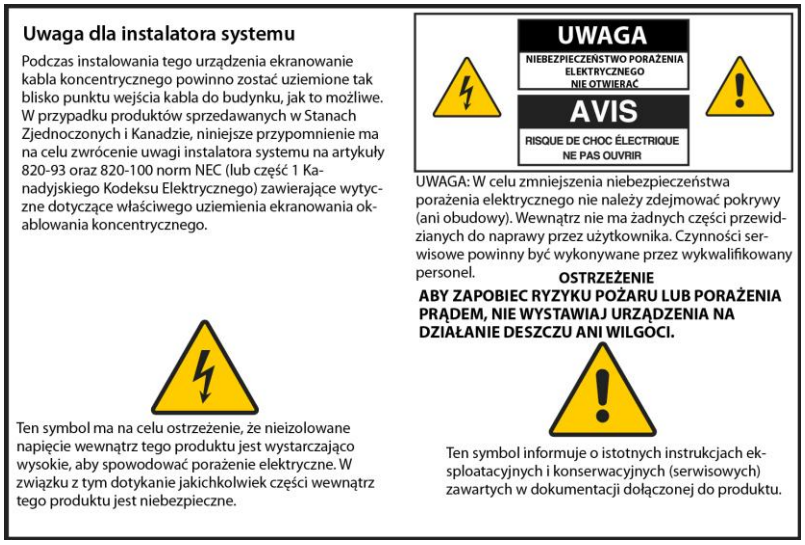
Spis treści

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA 2
Wprowadzenie 13
Zawartość opakowania 15
Opis panelu przedniego 16
Opis panelu tylnego 18
Wymagania systemowe dotyczące usług internetowych 20
Subskrypcja usług telefonicznych i szybkiego Internetu 21
Wybór najlepszej lokalizacji bramy domowej DOCSIS 23
Montaż modemu na ścianie (opcjonalnie) 24
Wymagania dotyczące usług telefonicznych 27
Podłączanie bramy do Internetu i usług telefonicznych 29
Konfigurowanie bramy domowej DOCSIS 33
Konfigurowanie ustawień łączności bezprzewodowej 43
Konfigurowanie zabezpieczeń 60
Kontrola dostępu do bramy 69
Konfigurowanie aplikacji i gier 81
Zarządzanie bramą 87
Monitorowanie stanu bramy 96
Najczęściej zadawane pytania 103
Porady dotyczące poprawy wydajności 108
Funkcje diodowego wskaźnika stanu na panelu przednim 109
Uwagi 113

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

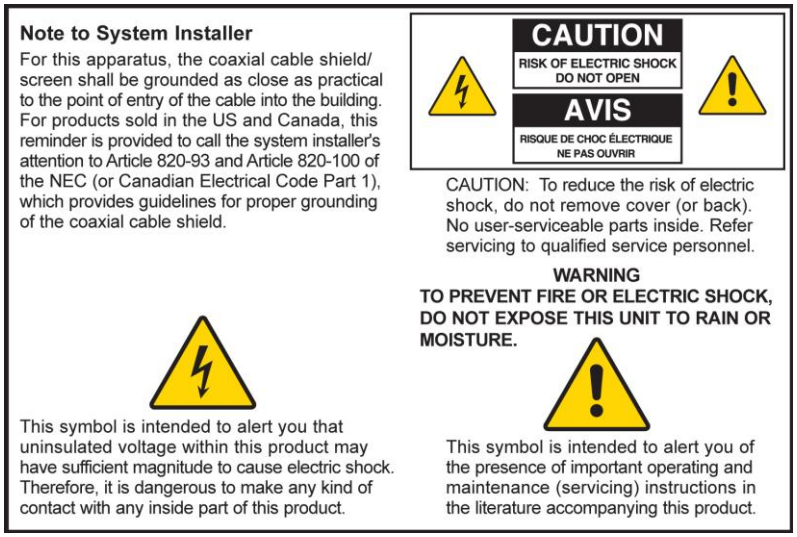
Uwagi dla instalatorów

Instrukcje serwisowania zawarte w niniejszych uwagach są przeznaczone wyłącznie dla wykwalifikowanych pracowników serwisu. Aby zmniejszyć niebezpieczeństwo porażenia napięciem elektrycznym, osoby bez odpowiednich kwalifikacji nie powinny wykonywać żadnych czynności serwisowych poza opisanymi w instrukcji użytkowania.



Notice to Installers

The servicing instructions in this notice are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions, unless you are qualified to do so.



Notice à l'attention des installateurs de réseaux câblés

Les instructions relatives aux interventions d'entretien, fournies dans la présente notice, s'adressent exclusivement au personnel technique qualifié. Pour réduire les risques de chocs électriques, n'effectuer aucune intervention autre que celles décrites dans le mode d'emploi et les instructions relatives au fonctionnement, à moins que vous ne soyez qualifié pour ce faire.

Remarque à l'attention de l'installateur du système

Avec cet appareil, le blindage/écran du câble coaxial doit être mis à la terre aussi près que possible du point d'entrée du câble dans le bâtiment. En ce qui concerne les produits vendus aux États-Unis et au Canada, ce rappel est fourni pour attirer l'attention de l'installateur sur les articles 820-93 et 820-100 du Code national de l'électricité (ou Code de l'électricité canadien, Partie 1) qui fournissent des lignes directrices concernant la mise à la terre correcte du blindage (écran) du câble coaxial.

Ce symbole a pour but de vous prévenir que des tensions électriques non isolées existent à l'intérieur de ce produit, pouvant être d'une intensité suffisante pour causer des chocs électriques. Il est donc dangereux d'établir un contact quelconque avec l'une des pièces comprises à l'intérieur de ce produit.

ATTENTION : Pour réduire les risques de chocs électriques, ne pas enlever le couvercle (ou le panneau arrière). Ne contient aucune pièce réparable par l'utilisateur. Confier les interventions aux techniciens d'entretien qualifiés.

AVERTISSEMENT

POUR ÉVITER LES INCENDIES OU LES CHOCS ÉLECTRIQUES, NE PAS EXPOSER L'APPAREIL À LA PLUIE OU À L'HUMIDITÉ.

Ce symbole a pour but de vous prévenir de la présence d'instructions importantes relatives au fonctionnement ou à l'entretien (et aux réparations) dans la documentation accompagnant ce produit.

Mitteilung für CATV-Techniker

Die in dieser Mitteilung aufgeführten Wartungsanweisungen sind ausschließlich für qualifiziertes Fachpersonal bestimmt. Um die Gefahr eines elektrischen Schlags zu reduzieren, sollten Sie keine Wartungsarbeiten durchführen, die nicht ausdrücklich in der Bedienungsanleitung aufgeführt sind, außer Sie sind zur Durchführung solcher Arbeiten qualifiziert.

Mitteilung an den Systemtechniker

Für dieses Gerät muss der Koaxialkabelschutz/ Schirm so nahe wie möglich am Eintrittspunkt des Kabels in das Gebäude geerdet werden Dieser Erinnerungshinweis liegt den in den USA oder Kanada verkauften Produkten bei. Er soll den Systemtechniker auf Paragraph 820-93 und Paragraph 820-100 der US-Elektrovorschrift NEC (oder der kanadischen Elektrovorschrift Canadian Electrical Code Teil 1) aufmerksam machen, in denen die Richtlinien für die ordnungsgemäße Erdung des Koaxial-kabelschirms festgehalten sind.

Dieses Symbol weist den Benutzer auf das Vorhandensein von nicht isolierten gefährlichen Spannungen im Gerät hin, die Stromschläge verursachen können. Ein Kontakt mit den internen Teilen dieses Produktes ist mit Gefahren verbunden.

ACHTUNG: Zur Vermeidung eines Stromschlags darf die Abdeckung (bzw. die Geräterückwand) nicht entfernt werden. Das Gerät enthält keine vom Benutzer wartbaren Teile. Wartungsarbeiten dürfen nur von qualifiziertem Fachpersonal durchgeführt werden.

WARNUNG

DAS GERÄT NICHT REGEN ODER FEUCHTIGKEIT AUSSETZEN, UM STROMSCHLAG ODER DURCH EINEN KURZSCHLUSS VERURSACHTEN BRAND ZU VERMEIDEN.

Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.

Aviso a los instaladores de sistemas CATV

Las instrucciones de reparación contenidas en el presente aviso son para uso exclusivo por parte de personal de mantenimiento cualificado. Con el fin de reducir el riesgo de descarga eléctrica, no realice ninguna otra operación de reparación distinta a las contenidas en las instrucciones de funcionamiento, a menos que posea la cualificación necesaria para hacerlo.

Nota para el instalador del sistema

En lo que se refiere a este aparato, el blindaje del cable coaxial debe conectarse a tierra lo más cerca posible al punto por el cual el cable entra en el edificio. En el caso de los productos vendidos en los EE. UU. y Canadá, el presente aviso se suministra para llamar la atención del instalador del sistema sobre los Artículos 820-93 y 820-100 del NEC (o Código Eléctrico de Canadá, Parte 1), que proporcionan directrices para una correcta conexión a tierra del blindaje del cable coaxial.

Este símbolo tiene como fin advertirle de que una tensión sin aislamiento en el interior de este producto podría ser de una magnitud suficiente como para provocar una descarga eléctrica. Por consiguiente, resulta peligroso realizar cualquier tipo de contacto con alguno de los componentes internos de este producto.

ATENCIÓN: con el fin de reducir el riesgo de descarga eléctrica, no retire la tapa (ni la parte posterior). No existen en el interior componentes que puedan ser reparados por el usuario. Encargue su revisión a personal de mantenimiento cualificado.

ADVERTENCIA

PARA EVITAR EL RIESGO DE INCENDIO O DESCARGA ELÉCTRICA, NO EXPONGA LA UNIDAD A LA LLUVIA O A LA HUMEDAD.

Este símbolo tiene como fin alertarle de la presencia de importantes instrucciones de operación y mantenimiento (revisión) contenidas en la literatura que acompaña al producto.

20080814_Installer820_Intl

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

1) Przeczytaj niniejszą instrukcję.
2) Zachowaj tę instrukcję.
3) Zwracaj szczególną uwagę na wszystkie ostrzeżenia.
4) Postępuj zgodnie ze wszystkimi instrukcjami.
5) Nie używaj urządzenia w pobliżu wody.
6) Czyść urządzenie wyłącznie przy użyciu suchej szmatki.
7) Nie zasłaniaj żadnych otworów wentylacyjnych. Podczas instalacji postępuj zgodnie z instrukcjami producenta.
8) Nie instaluj urządzenia w pobliżu źródeł ciepła, takich jak grzejniki, nawiewy ciepłego powietrza, piece lub inny sprzęt (w tym wzmacniacze) wytwarzający ciepło.
9) Nie przerabiaj zabezpieczeń wtyczki dwubiegunowej ani wtyczki z uziemieniem. Wtyczka dwubiegunowa składa się z dwóch płaskich wtyków, z których jeden jest szerszy. Wtyczka z uziemieniem składa się z dwóch płaskich wtyków oraz z trzeciego bolca uziemiającego. Szeroki płaski wtyk i trzeci bolec służą do zapewnienia bezpieczeństwa użytkownika. Jeśli dostarczona wtyczka nie pasuje do gniazda, skontaktuj się z elektrykiem w celu wymiany przestarzałego gniazda.
10) Chroń kabel zasilający przed nadepnięciem lub uszkodzeniem — zwłaszcza w pobliżu wtyczek, gniazd zasilających i miejsca, w którym kabel zasilający jest połączony z urządzeniem.
11) Używaj wyłącznie sprzętu i wyposażenia zalecanego przez producenta.

12) Używaj wyłącznie wózków, stojaków, statywów, wsporników i stołów zalecanych przez producenta lub sprzedawanych razem z urządzeniem. Jeśli korzystasz z wózka, nie dopuść do jego przewrócenia podczas przewożenia sprzętu, ponieważ może to doprowadzić do obrażeń ciała.
13) Podczas burzy lub w przypadku długiego okresu nieużywania sprzęt należy odłączyć od zasilania przez odłączenie kabla zasilającego od gniazda.
14) Wszelkie czynności serwisowe powinny być wykonywane przez wykwalifikowany personel. Czynności serwisowe są wymagane w przypadku każdego uszkodzenia sprzętu, takiego jak uszkodzenie kabla zasilającego lub wtyku, dostania się płynu lub ciał obcych do wnętrza sprzętu, wystawienia sprzętu na działanie deszczu lub wilgoci, przy objawach nieprawidłowego działania lub po upadku sprzętu na podłoże.

Ostrzeżenie dotyczące źródła zasilania

Etykieta znajdująca się na tym produkcie zawiera informacje o prawidłowym źródle zasilania. Urządzenie należy zasilać wyłącznie ze źródła zasilania o napięciu i częstotliwości podanej na etykiecie produktu. Jeśli nie wiadomo, jaki typ zasilania jest dostępny w domu lub w pracy, należy skonsultować się z dostawcą usług lub z lokalnym zakładem energetycznym.

Gniazdo napięcia zmiennego znajdujące się w urządzeniu musi pozostawać dostępne przez cały czas i musi działać prawidłowo.

Uziemienie urządzenia

OSTRZEŻENIE: Unikaj porażenia elektrycznego i niebezpieczeństwa pożaru! Jeśli urządzenie jest dołączone do okablowania koncentrycznego, należy się upewnić, że system okablowania jest uziemiony. Uziemienie stanowi ochronę przed udarami napięciowymi i gromadzeniem się ładunków elektrostatycznych.

Ochrona urządzenia przed wyładowaniami atmosferycznymi

Oprócz odłączenia kabla zasilającego od gniazda ściennego należy również odłączyć sygnały wejściowe.

Sprawdzanie źródła zasilania na podstawie stanu lampek włączenia/wyłączenia zasilania

Nawet gdy lampki włączenia/wyłączenia zasilania nie świecą się, urządzenie może nadal pozostawać podłączone do źródła zasilania. Lampki mogą zostać wyłączone po wyłączeniu urządzenia niezależnie od tego, czy jest ono nadal podłączone do źródła zasilania napięciem zmiennym.

Eliminacja przeciążeń zasilania napięciem zmiennym

OSTRZEŻENIE: Unikaj porażenia elektrycznego i niebezpieczeństwa pożaru! Nie przeciążaj źródeł zasilania napięciem zmiennym, gniazd ściennych, kabli przedłużających ani gniazd zintegrowanych w urządzeniu. W przypadku urządzeń wymagających zasilania z baterii lub innych źródeł należy zapoznać się z podręcznikami obsługi tych urządzeń.

Zapewnienie wentylacji i wybór pomieszczenia

- Przed podłączeniem zasilania usuń z produktu wszelkie opakowania.
- Nie umieszczaj urządzenia na łóżku, kanapie, dywanie ani innej podobnej powierzchni.
- Nie umieszczaj urządzenia na niestabilnym podłożu.
- Nie instaluj urządzenia w zamkniętych przestrzeniach, takich jak półka na książki lub stojak, o ile nie jest zapewniona prawidłowa wentylacja.
- Nie umieszczaj na urządzeniu innej aparatury (takiej jak magnetowidy lub odtwarzacze DVD), a także lamp, książek, wazonów z płynami ani innych przedmiotów.
- Nie zasłaniaj otworów wentylacyjnych.

Ochrona przed wilgocią i ciałami obcymi

OSTRZEŻENIE: Unikaj porażenia elektrycznego i niebezpieczeństwa pożaru! Nie wystawiaj urządzenia na działanie ściekających lub rozpryskiwanych płynów, deszczu lub wilgoci. Na urządzeniu nie można stawiać przedmiotów wypełnionych płynem, takich jak wazony.

OSTRZEŻENIE: Unikaj porażenia elektrycznego i niebezpieczeństwa pożaru! Przed rozpoczęciem czyszczenia odłącz zasilanie produktu. Nie używaj środków czyszczących w postaci płynnej ani w formie aerozolu. Do czyszczenia urządzenia nie używaj środków magnetycznych ani materiałów elektrostatycznych (np. szmatek do usuwania kurzu).

OSTRZEŻENIE: Unikaj porażenia elektrycznego i niebezpieczeństwa pożaru! Nigdy nie wkładaj żadnych przedmiotów do otworów urządzenia. Ciała obce mogą spowodować zwarcie i wywołać porażenie elektryczne lub pożar.

Ostrzeżenia dotyczące obsługi serwisowej

OSTRZEŻENIE: Unikaj porażenia elektrycznego! Nie otwieraj pokrywy urządzenia. Otwarcie lub usunięcie pokrywy może wystawić użytkownika na działanie wysokiego napięcia. Otwarcie pokrywy pociąga za sobą utratę gwarancji. To urządzenie nie zawiera żadnych części przewidzianych do naprawy przez użytkownika.

Sprawdzanie bezpieczeństwa produktu

Po zakończeniu obsługi lub naprawy tego produktu pracownik serwisu musi przeprowadzić próby bezpieczeństwa w celu określenia, czy produkt znajduje się w stanie zapewniającym prawidłowe działanie.

Ochrona produktu podczas przenoszenia

Podczas przenoszenia urządzenia oraz dołączania lub odłączania kabli zawsze należy odłączyć źródło zasilania.

Uwaga dotycząca sprzętu telefonicznego

W celu zmniejszenia ryzyka wystąpienia pożaru, porażenia elektrycznego i obrażeń osób podczas korzystania ze sprzętu telefonicznego należy zawsze przestrzegać podstawowych przepisów bezpieczeństwa, takich jak:

1. Nie używać tego produktu w pobliżu wody, na przykład obok wanny, umywalki, zlewu, pralki, w wilgotnej piwnicy lub w pobliżu basenu.

2. Unikać korzystania z telefonu (z wyjątkiem aparatów bezprzewodowych) podczas burzy. Występuje wówczas niewielkie ryzyko porażenia piorunem.

3. Nie używać telefonu do informowania o ulatnianiu się gazu podczas przebywania w pobliżu nieszczelności.

UWAGA: W celu zmniejszenia niebezpieczeństwa pożaru używać wyłącznie kabla telekomunikacyjnego nr 7/0,15 (amerykańskim odpowiednikiem jest kabel 26 AWG) lub kabla o większej średnicy.

PRZECHOWUJ TE INSTRUKCJE W BEZPIECZNYM MIEJSCU

20090915_Modem No Battery_Safety

Zgodność z przepisami FCC obowiązującymi w Stanach Zjednoczonych

Urządzenie to przetestowano **z** wynikiem pozytywnym pod względem ograniczeń, jakim powinny podlegać urządzenia cyfrowe klasy B, zgodnie z częścią 15 przepisów FCC. Ograniczenia mają na celu zapewnienie stosownej ochrony przed szkodliwymi zakłóceniami podczas eksploatacji urządzenia w środowisku domowym. Urządzenie to generuje, wykorzystuje i emituje fale o częstotliwości radiowej. Jeśli urządzenie nie będzie zainstalowane i używane zgodnie z instrukcją obsługi, może powodować szkodliwe zakłócenia w komunikacji radiowej. Nie wyklucza się jednak, że w wypadku konkretnej instalacji zakłócenia takie wystąpią. Jeśli urządzenie powoduje zakłócenia w odbiorze sygnału radiowego lub telewizyjnego, co można sprawdzić wyłączając i włączając urządzenie, należy podjąć próbę wyeliminowania tych zakłóceń, stosując następujące środki zaradcze:

- Obrócić lub przenieść antenę odbiorczą.
- Zwiększyć odległość między urządzeniem a odbiornikiem.
- Podłączyć urządzenia do gniazda lub sieci zasilającej innej niż ta, do której podłączony jest odbiornik.
- W celu uzyskania pomocy należy się skonsultować z dostawcą usług albo z doświadczonym technikiem radiowym lub telewizyjnym.

Przeróbki dokonane w tym urządzeniu bez upoważnienia firmy Cisco Systems, Inc. mogą spowodować odebranie prawa użytkownika do korzystania z tego produktu.

Informacje znajdujące się w zamieszczonej poniżej Deklaracji Zgodności FCC są wymagane przez FCC i służą do zapoznania użytkownika z informacjami dotyczącymi atestu FCC dla tego urządzenia. *Podane numery telefonów służą wyłącznie do odpowiadania na pytania związane z FCC i nie są przewidziane dla pytań dotyczących podłączania lub działania urządzenia. W przypadku pytań dotyczących działania lub instalacji tego urządzenia należy skontaktować się z dostawcą usług.*

FC Deklaracja Zgodności

To urządzenie jest zgodne z częścią 15 przepisów FCC. Użytkowanie jest dopuszczalne pod dwoma warunkami: 1) urządzenie nie powoduje szkodliwych zakłóceń; oraz 2) urządzenie musi odbierać wszelkie zakłócenia, w tym również zakłócenia powodujące niepożądane działanie.

Brama domowa DOCSIS
Model: DPC3925/EPC3925
Wyprodukowana przez:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044 USA
Telefon: +1-770-236-1077

Przepisy kanadyjskie dotyczące zakłóceń elektromagnetycznych (EMI)

To urządzenie cyfrowe klasy B jest zgodne z kanadyjską normą ICES-003.

Cet appareil numérique de la class B est conforme à la norme NMB-003 du Canada.

Częstotliwości przy pracy dwupasmowej z dynamicznym wyborem częstotliwości (DFS)

W niektórych konfiguracjach urządzenie może pracować w pasmach 5150-5250 MHz i 5470-5725 MHz. Jeśli zostanie wybrany kanał należący do jednego z powyższych zakresów częstotliwości, zgodnie z zaleceniami FCC urządzenie będzie mogło być używane wyłącznie wewnątrz budynków. Używanie urządzenia poza budynkami jest niezgodne z przepisami i zaleceniami FCC.

Oświadczenie dotyczące wystawienia na promieniowanie radiowe

Uwaga: Ten nadajnik nie może znajdować się w tym samym miejscu co inna antena lub nadajnik ani współpracować z nimi. To urządzenie powinno być zainstalowane i działać przy zachowaniu odległości co najmniej 20 cm (7,9 cala) między anteną a ciałem ludzkim.

Stany Zjednoczone

Ten system został przebadany pod kątem wystawienia osób na promieniowanie radiowe zgodnie z ograniczeniami opisanymi w normie ANSI C 95.1 (American National Standards Institute). Ocena została przeprowadzona na podstawie dokumentu FCC OET Bulletin 65C rev 01.01 w zgodności z częścią 2.1091 i częścią 15.27. W celu zachowania zgodności minimalna odległość między anteną a osobami postronnymi powinna wynosić 20 cm (7,9 cala).

Kanada

Ten system został przebadany pod kątem wystawienia osób na promieniowanie radiowe zgodnie z ograniczeniami opisanymi w normie ANSI C 95.1. Ocena została przeprowadzona na podstawie dokumentu RSS-102 Rev 2. W celu zachowania zgodności minimalna odległość między anteną a osobami postronnymi powinna wynosić 20 cm (7,9 cala).

Unia Europejska

Ten system został przebadany pod kątem wystawienia osób na promieniowanie radiowe zgodnie z ograniczeniami opisanymi w dokumencie ICNIRP (International Commission on Non-Ionizing Radiation Protection). Ocena została przeprowadzona na podstawie normy EN 50385 (Product Standard to Demonstrate Compliance of Radio Base Stations and Fixed Terminals for Wireless Telecommunications Systems) przy uwzględnieniu podstawowych ograniczeń i poziomów odniesienia dotyczących wystawiania ludzi na pola elektromagnetyczne o częstotliwości radiowej od 300 MHz do 40 GHz. Minimalna odległość między anteną a osobami postronnymi powinna wynosić 20 cm (7,9 cala).

Australia

Ten system został przebadany pod kątem wystawienia na promieniowanie radiowe zgodnie z ograniczeniami opisanymi w standardzie Australian Radiation Protection, przekształconym w dokument ICNIRP (International Commission on Non-Ionizing Radiation Protection). Minimalna odległość między anteną a osobami postronnymi powinna wynosić 20 cm (7,9 cala).

20091016 FCC DomandIntl

Zgodność z dyrektywą CE

Deklaracja zgodności z dyrektywą UE 1999/5/EC (R&TTE)

Ta deklaracja jest obowiązująca wyłącznie w przypadku konfiguracji (zestawu oprogramowania, oprogramowania sprzętowego i sprzętu) obsługiwanych lub dostarczonych przez firmę Cisco Systems do użytku na terenie Unii Europejskiej. Korzystanie z oprogramowania lub oprogramowania sprzętowego nieobsługiwanego lub niedostarczonego przez firmę Cisco Systems może spowodować niezgodność z obowiązującymi wymaganiami.

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]	Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Uwaga: Pełna deklaracja zgodności tego produktu znajduje się w sekcji Declarations of Conformity and Regulatory Information odpowiedniego podręcznika instalacji sprzętu dostępnego w witrynie Cisco.com.

Przy ocenie zgodności produktu z wymogami dyrektywy 1999/5/EC zastosowano następujące normy:

- Fale radiowe: EN 300 328
- Zgodność elektromagnetyczna (EMC): EN 301 489-1, EN 301 489-17
- Bezpieczeństwo: EN 60950 i EN 50385

Znak CE i identyfikator class-2 są umieszczone na produkcie i na jego opakowaniu. Ten produkt jest zgodny z następującymi dyrektywami Unii Europejskiej:

-1999/5/EC

Ograniczenia krajowe

Ten produkt może być używany wyłącznie w pomieszczeniach zamkniętych.

Francja

Dla częstotliwości 2,4 GHz moc wyjściowa jest ograniczona do 10 mW EIRP w przypadku, gdy produkt jest używany na zewnątrz w paśmie 2454 - 2483,5 MHz. Nie ma żadnych innych ograniczeń w przypadku korzystania z innych części pasma 2,4 GHz. Więcej informacji można znaleźć w witrynie http://www.arcep.fr/.

Pour la bande 2,4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483,5 MHz. Il n'y a pas de restrictions pour des utilisations dans d'autres parties de la bande 2,4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

Włochy

Ten produkt spełnia przepisy Krajowego Interfejsu Radiowego oraz wymagania opisane w Tabeli Krajowego Przydziału Częstotliwości dla Włoch. Z wyjątkiem przypadku wykorzystywania bezprzewodowego produktu LAN w granicach posiadłości właściciela, jego użycie wymaga tzw. „ogólnego zezwolenia”. Szczegółowe informacje można znaleźć w witrynie http://www.comunicazioni.it/it/.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una “Autorizzazione Generale”. Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Łotwa

Korzystanie z pasma 2,4 GHz na zewnątrz wymaga uzyskania zezwolenia Biura Łączności Elektronicznej. Szczegółowe informacje można znaleźć w witrynie http://www.esd.lv.

2,4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.

Uwaga: Wymagane przez przepisy ograniczenia maksymalnej mocy wyjściowej są podawane w jednostkach efektywnej mocy izotropowej wypromieniowanej (EIRP). Poziom EIRP urządzenia może być obliczony poprzez dodanie zysku energetycznego używanej anteny (podanej w dBi) do mocy wyjściowej dostępnej na złączu (podanej w dBm).

Anteny

Należy używać wyłącznie anteny dostarczonej z produktem. 20090312 CE_Gateway

Wprowadzenie

Witamy w fascynującym świecie szybkiego Internetu i cyfrowych usług telefonicznych o wysokiej jakości. Nowa brama domowa Cisco® Model DPC3925 DOCSIS® 3.0 lub EPC3925 EuroDOCSIS™ z wbudowanym cyfrowym adapterem głosu jest modemem kablowym spełniającym standardy przemysłowe dotyczące szybkich połączeń danych oraz niezawodnych cyfrowych usług telefonicznych. Urządzenia DPC3925 i EPC3925 są przewodowymi (Ethernet) lub bezprzewodowymi bramami domowymi umożliwiającymi przesyłanie danych i głosu między wieloma różnymi urządzeniami w domu lub w małej firmie. Pojedyncze urządzenie zapewnia szybki dostęp do danych oraz oferuje korzystne cenowo usługi głosowe. Dzięki bramom DPC3925 lub EPC3925 rośnie zadowolenie z Internetu oraz z łączności w domu i w firmie, jak również zwiększa się wydajność korzystających z nich osób.

Niniejszy podręcznik zawiera procedury oraz zalecenia opisujące wybór miejsca, instalowanie, konfigurowanie, obsługę i rozwiązywanie problemów z bramami domowymi DPC3925 i EPC3925 umożliwiającymi szybki dostęp do Internetu oraz udostępniającymi usługi telefonii cyfrowej w domu lub w firmie. W odpowiednich sekcjach podręcznika można znaleźć konkretne informacje dotyczące często spotykanych sytuacji. Więcej informacji o subskrypcji tych usług można otrzymać od dostawcy usług.

Zalety i funkcje

Bramy domowe DPC3925 i EPC3925 oferują następujące zalety oraz funkcje:

- Zgodność ze standardami DOCSIS 3.0, 2.0 i 1.x oraz ze specyfikacjami PacketCable™ i EuroPacketCable™ dotyczącymi wysokiej wydajności i niezawodności
- Szerokopasmowe wysokowydajne połączenie z Internetem zapewniające znakomitą jakość połączeń online
- Wbudowany cyfrowy adapter głosu dla dwóch linii umożliwiający świadczenie usług dla przewodowych połączeń telefonicznych
- Cztery porty Ethernet 1000/100/10BASE-T umożliwiające tworzenie połączeń przewodowych
- Punkt dostępu bezprzewodowego 802.11n
- Zgodność ze standardem WPS (Wi-Fi Protected Setup), w tym przełącznik włączający funkcję WPS w celu przeprowadzenia prostej i bezpiecznej konfiguracji połączenia bezprzewodowego
- Konfigurowana przez użytkownika funkcja kontroli rodzicielskiej blokująca dostęp do niepożądanych witryn internetowych

- Zaawansowana technologia zapory chroniąca sieć domową przed hakerami i przed nieautoryzowanym dostępem
- Atrakcyjna zwarta sylwetka umożliwiająca pracę w położeniu pionowym, poziomym lub zawieszenie na ścianie
- Oznaczone kolorami porty interfejsu oraz odpowiadające im kable upraszczające instalowanie i konfigurowanie
- Zgodne ze standardem DOCSIS-5 oznaczenia diod LED oraz ich zachowanie umożliwiają technikom proste sprawdzenie stanu urządzenia oraz pełnią rolę narzędzia pomocnego przy rozwiązywaniu problemów
- Możliwość automatycznego uaktualniania oprogramowania przez dostawcę usług

Zawartość opakowania

Po otrzymaniu domowej bramy bezprzewodowej należy sprawdzić, czy sprzęt oraz akcesoria znajdują się w opakowaniu i nie są uszkodzone. Opakowanie zawiera następujące elementy:

Jedna brama domowa DOCSIS (model DPC3925 lub EPC3925)

Jeden zasilacz (w przypadku modeli wymagających zewnętrznego źródła zasilania)

Jeden kabel Ethernet (CAT5/RJ-45)

Jeden dysk CD-ROM

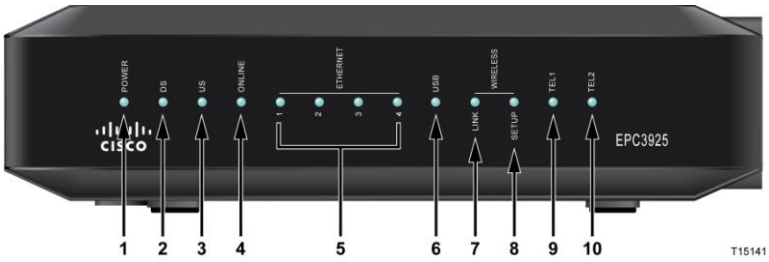
Jeśli brakuje któregoś z tych elementów lub jest on uszkodzony, należy skontaktować się z dostawcą usług w celu uzyskania pomocy.

Informacje:

- W przypadku, gdy magnetowid, terminal DHCT, dekoder telewizyjny lub telewizor korzysta z tego samego połączenia kablowego, co bezprzewodowa brama domowa, konieczne będzie zastosowanie rozgałęźnika (splittera) oraz dodatkowych standardowych kabli koncentrycznych RF.
- Kable oraz pozostały sprzęt wymagany przez usługi telefoniczne należy nabyć oddzielnie. Skontaktuj się ze swoim dostawcą usług w celu uzyskania informacji o sprzęcie i kablu wymaganym przez usługi telefoniczne.

Opis panelu przedniego

Na panelu przednim bramy znajdują się diodowe wskaźniki LED wskazujące stan urządzenia oraz funkcję aktualnie spełnianą przez bramę domową. Dodatkowe informacje o funkcjach pełnionych przez wskaźniki diodowe na panelu przednim można znaleźć w sekcji ***Funkcje diodowego wskaźnika stanu na panelu przednim*** (na stronie 109).



Na rysunku pokazano model DPC3925.

1 **POWER** — WŁĄCZONY, zasilanie jest dołączone do bezprzewodowej bramy domowej.

2 **DS** — WŁĄCZONY, bezprzewodowa brama domowa otrzymuje dane z sieci kablowej.

3 **US** — WŁĄCZONY, bezprzewodowa brama domowa wysyła dane do sieci kablowej.

4 **ONLINE** — WŁĄCZONY, bezprzewodowa brama domowa jest zarejestrowana w sieci i może pracować bez żadnych ograniczeń.

5 **ETHERNET 1 - 4** — WŁĄCZONY, do jednego z portów Ethernet podłączone jest urządzenie. MIGANIE oznacza transfer danych przez połączenie Ethernet.

6 **USB** — WŁĄCZONY, do portu USB podłączone jest urządzenie. MIGANIE oznacza transfer danych przez połączenie USB.

7 **WIRELESS LINK** — WŁĄCZONY, bezprzewodowy punkt dostępu znajduje się w stanie gotowości. MIGANIE oznacza transfer danych przez połączenie bezprzewodowe. WYŁĄCZONY oznacza wyłączenie przez użytkownika bezprzewodowego punktu dostępu.

8 **WIRELESS SETUP** — WYŁĄCZONY (stan normalny), konfiguracja połączenia bezprzewodowego jest nieaktywna. MIGANIE oznacza, że użytkownik uaktywnił konfigurację łącza bezprzewodowego w celu dodania nowych klientów bezprzewodowych do sieci bezprzewodowej.

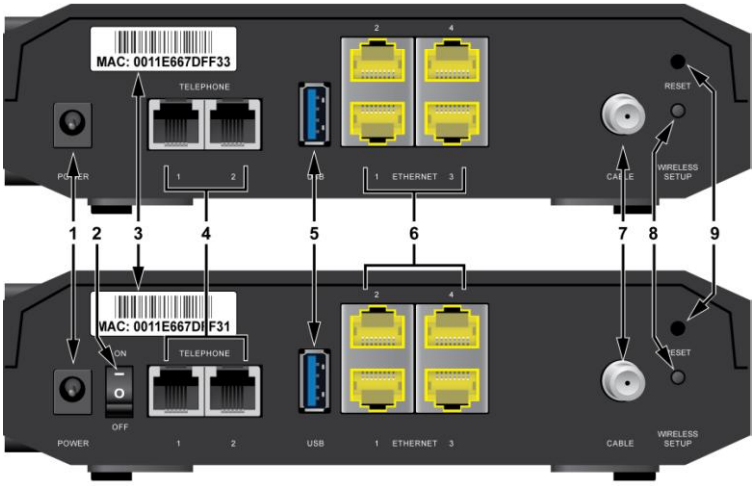
9 **TEL1 —** WŁĄCZONY oznacza włączenie usług telefonicznych. Miga, gdy używana jest linia 1. WYŁĄCZONY oznacza, że usługa telefoniczna dla interfejsu TEL 1 jest wyłączona.

10 **TEL2 —** WŁĄCZONY oznacza, że usługa telefoniczna jest włączona. Miga, gdy używana jest linia 2. WYŁĄCZONY oznacza, że usługa telefoniczna dla interfejsu TEL 2 jest wyłączona.

Opis panelu tylnego

Na poniższych ilustracjach przedstawiono opis i funkcje elementów panelu tylnego bramy domowej Cisco DPC3925.

Model DPC3925



Model EPC3925

1 **POWER** — służy do połączenia bramy domowej z zasilaczem dostarczonym wraz z urządzeniem.

> **UWAGA:**
>
> **Unikaj uszkodzenia sprzętu. Używaj wyłącznie zasilacza dostarczonego z urządzeniem.**

2 **Przełącznik ON/OFF (tylko modele dostępne w Europie)** — umożliwia wyłączenie bramy domowej bez konieczności odłączania kabla zasilającego.

3 **ETYKIETA ADRESU MAC** — zawiera adres MAC bramy.

4 **TELEPHONE 1 i 2** — porty telefoniczne RJ-11; służą do połączenia ze zwykłymi telefonami lub faksami poprzez domowe okablowanie telefoniczne.

5 **USB** — służy do połączenia z wybranymi urządzeniami klienckimi.

6 **ETHERNET** — cztery porty Ethernet RJ-45; służą do połączenia z portem Ethernet w komputerze lub w sieci domowej.

7 **CABLE** — złącze typu F; służy do połączenia z aktywnym kablem sygnałowym dostawcy usług.

8 **WIRELESS SETUP —** naciśnięcie tego przełącznika powoduje rozpoczęcie konfiguracji sieci bezprzewodowej, co umożliwia użytkownikowi dodanie do sieci domowej nowych klientów bezprzewodowych zgodnych ze standardem WPS (Wi-Fi Protected Setup).

9 **RESET —** krótkie naciśnięcie (1-2 sekundy) tego przełącznika powoduje ponowne uruchomienie urządzenia EMTA. Naciskanie tego przełącznika przez co najmniej dziesięć sekund powoduje najpierw przywrócenie domyślnych ustawień fabrycznych, a następnie ponowne uruchomienie bramy.

UWAGA:

Przycisk Reset służy wyłącznie do celów serwisowych. Nie należy go używać, o ile nie zażąda tego dostawca usług kablowych lub telefonicznych. Użycie tego przycisku może spowodować utratę wszystkich wybranych uprzednio ustawień modemu kablowego.

Wymagania systemowe dotyczące usług internetowych

Aby zapewnić efektywną obsługę szybkich usług internetowych przez bramę domową, sprawdź, czy wszystkie urządzenia internetowe w używanym systemie spełniają lub przekraczają następujące minimalne wymagania sprzętowe i programowe.

Uwaga: W tym celu potrzebna będzie linia z aktywnym wejściem kablowym i połączenie internetowe.

Minimalne wymagania dla komputerów PC

- Komputer PC z procesorem MMX 133 lub szybszym
- 32 MB pamięci RAM
- Przeglądarka sieci WWW
- Napęd CD-ROM

Minimalne wymagania dla komputerów Macintosh

- System operacyjny MAC OS 7.5 lub nowszy
- 32 MB pamięci RAM

Wymagania systemowe dla połączenia Ethernet

- Komputer PC z systemem Microsoft Windows 2000 (lub nowszym) z zainstalowanym protokołem TCP/IP lub komputer Apple Macintosh z zainstalowanym protokołem TCP/IP
- Zainstalowana i aktywna karta sieciowa Ethernet 10/100/1000BASE-T

Subskrypcja usług telefonicznych i szybkiego Internetu

Przed rozpoczęciem używania bramy domowej należy zapewnić sobie konto z dostępem do szybkiego Internetu. Jeśli nie masz konta z dostępem do szybkiego Internetu, musisz utworzyć takie konto u lokalnego dostawcy usług. W tej sekcji wybierz jedną z następujących opcji.

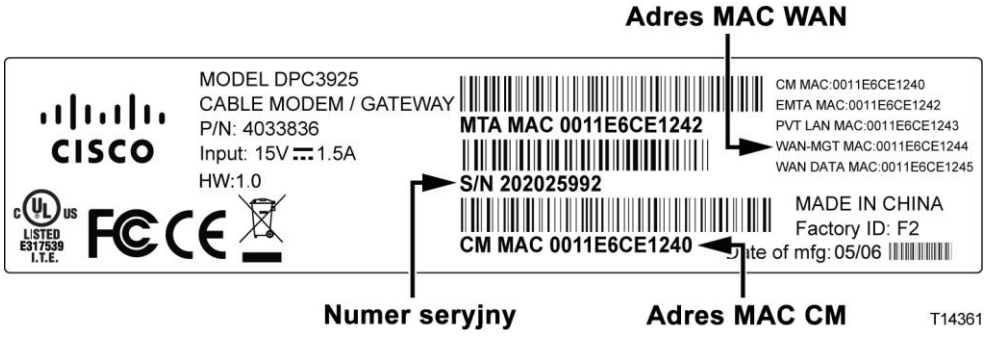
Nie mam konta z dostępem do szybkiego Internetu

Jeśli *nie* masz konta z dostępem do szybkiego Internetu, dostawca usług może je skonfigurować, stając się tym samym dostawcą usług internetowych (ISP). Dostęp do Internetu umożliwia wysyłanie i otrzymywanie wiadomości e-mail, dostęp do sieci WWW oraz dostęp do pozostałych usług internetowych.

Konieczne będzie podanie dostawcy usług następujących informacji:

- Numer seryjny modemu
- Adres MAC (Media Access Control) modemu (CM MAC)
- Inne adresy MAC, jeśli zajdzie taka potrzeba

Te dane znajdują się na etykiecie z kodem paskowym umieszczonej na bramie domowej. Numer seryjny składa się z grup znaków alfanumerycznych poprzedzonych symbolem **S/N**. Adres MAC składa się z grup znaków alfanumerycznych poprzedzonych symbolem **CM MAC**. Poniższa ilustracja przedstawia przykładową etykietę z kodem paskowym.



Zapisz poniżej te wartości odczytane z urządzenia.

Numer seryjny _____

Adres MAC _____

Mam już konto z dostępem do szybkiego Internetu

Jeśli masz już konto z dostępem do szybkiego Internetu, musisz podać swojemu dostawcy usług numer seryjny i adres MAC bramy domowej. Numer seryjny oraz adres MAC zostały opisane wcześniej w tej sekcji.

Chcę używać serwera aplikacji dla usług telefonicznych

Aby brama domowa mogła być wykorzystywana do świadczenia usług telefonicznych, należy skonfigurować konto telefoniczne u lokalnego dostawcy usług. Podczas rozmów z dostawcą usług może okazać się możliwe wykorzystanie aktualnie używanych numerów telefonów lub dostawca usług telefonii stacjonarnej może przypisać nowy numer telefonu do każdej istniejącej lub dodatkowej aktywnej linii telefonicznej. Przedyskutuj te opcje ze swoim dostawcą usług telefonicznych.

Wybór najlepszej lokalizacji bramy domowej DOCSIS

Idealną lokalizacją dla bramy domowej jest miejsce z dostępem do gniazd zasilania i innych urządzeń. Weź pod uwagę rozkład pomieszczeń w domu lub w firmie i skonsultuj się z dostawcą usług w celu wybrania najlepszej lokalizacji dla bramy domowej. Przed wybraniem miejsca dla bramy domowej zapoznaj się dokładnie z podręcznikiem użytkownika.

Weź pod uwagę następujące zalecenia:

- Jeśli brama ma być wykorzystywana do świadczenia szybkich usług internetowych, wybierz lokalizację w pobliżu komputera.
- Wybierz miejsce w pobliżu istniejącego kabla koncentrycznego RF, aby uniknąć konieczności zakładania dodatkowego gniazda koncentrycznego RF.
- Jeśli używany jest tylko jeden lub dwa aparaty telefoniczne, wybierz miejsce dla bramy domowej w pobliżu sprzętu telefonicznego.

  Uwaga: Jeśli brama domowa ma umożliwiać dostęp do kilku telefonów, doświadczony instalator może połączyć bramę z istniejącym domowym okablowaniem telefonicznym. Aby ograniczyć do minimum zmiany w domowej sieci telefonicznej, warto pomyśleć o instalacji bramy w pobliżu istniejącego gniazda telefonicznego.
- Wybierz spokojne miejsce, w którym sprzęt będzie chroniony przed przypadkowym uszkodzeniem, takie jak garderoba, piwnica lub inne bezpieczne pomieszczenie.
- Wybierz lokalizację w taki sposób, aby pozostawało w niej wystarczająco dużo miejsca na przeprowadzenie kabli dochodzących do modemu, bez konieczności ich naciągania lub skręcania.
- Nie należy blokować przepływu powietrza wokół urządzenia.
- Przed zainstalowaniem bramy domowej uważnie przeczytaj niniejszy podręcznik użytkownika.

Montaż modemu na ścianie (opcjonalnie)

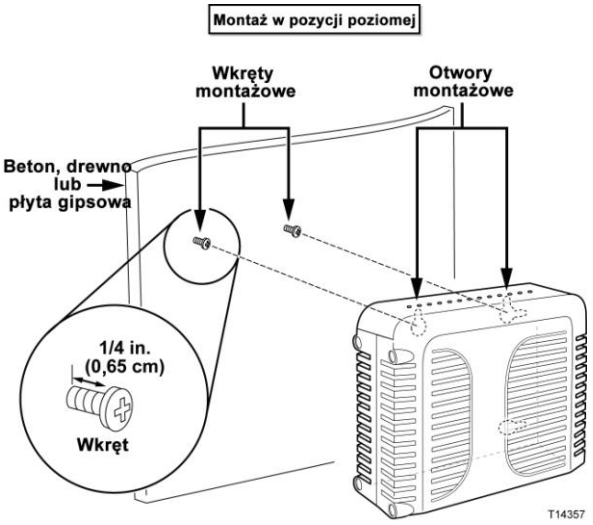
Bramę domową można zamontować na ścianie, używając dwóch kołków rozporowych, dwóch wkrętów oraz szczelin montażowych znajdujących się na urządzeniu. Modem można zamontować w położeniu pionowym lub poziomym.

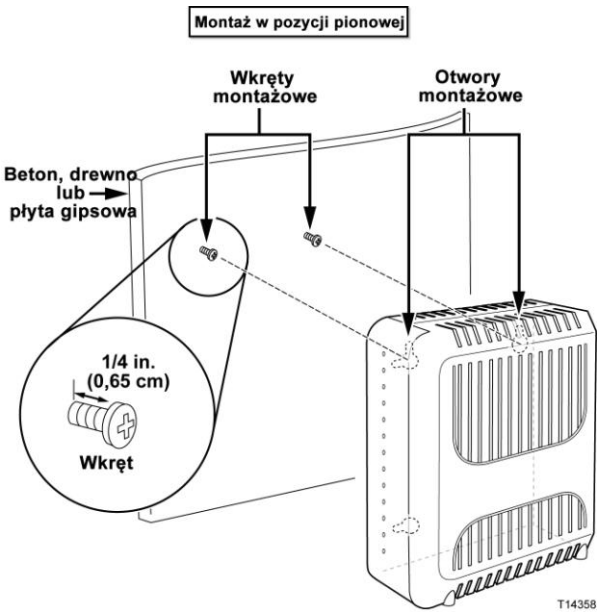
Przed rozpoczęciem

Przed rozpoczęciem należy wybrać odpowiednie miejsce montażu. Urządzenie można zamontować na ścianach betonowych, drewnianych lub wykonanych z płyt gipsowych. Dookoła miejsca montażu powinna być wolna przestrzeń, a kable dochodzące do bramy domowej nie powinny być naprężone. Należy pozostawić wystarczająco dużo wolnej przestrzeni między dolną częścią bramy a znajdującą się poniżej podłogą lub półką, tak aby umożliwić swobodne doprowadzenie kabli. Dodatkowo wszystkie kable powinny być luźne, tak aby można było wyjąć bramę w celu obsługi bez konieczności ich odłączania. Należy również sprawdzić, czy dostępne są następujące elementy:

- Dwa kołki rozporowe dla wkrętów 8 x 25,4 mm (1 cal)
- Dwa wkręty do metalu 8 x 25,4 mm (1 cal) z łbem stożkowym ściętym
- Wiertło o średnicy 4,76 mm (3/16 cala) do drewna lub betonu, w zależności od ściany
- Ilustracje obrazujące montaż na ścianie znajdują się na następnych stronach.

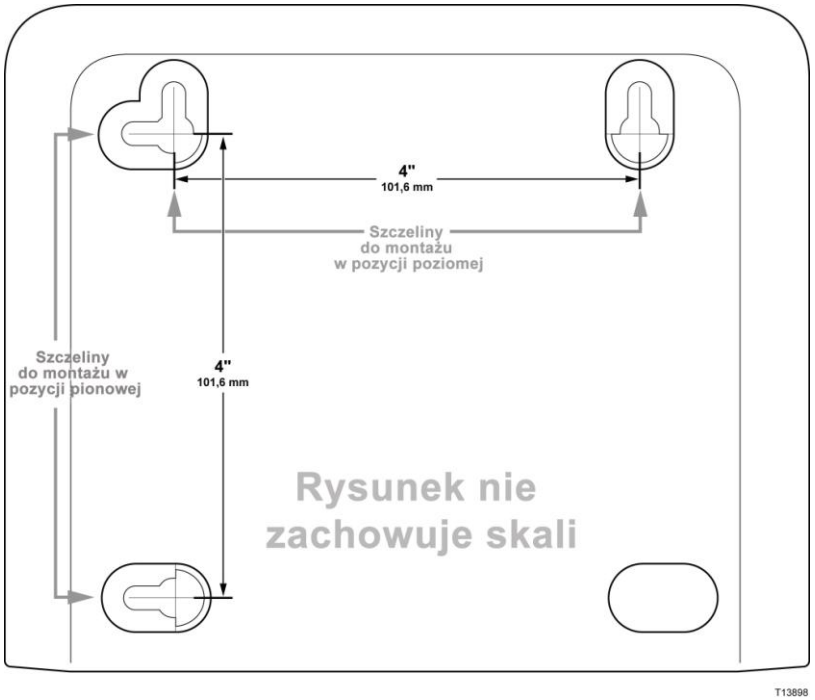
Zamontuj modem zgodnie z jedną z następujących ilustracji.





Rozmieszczenie i rozmiary szczelin montażowych

Poniższy rysunek pokazuje rozmieszczenie i rozmiary szczelin montażowych znajdujących się na spodzie modemu. Skorzystaj z informacji zawartych na tej stronie podczas montażu modemu na ścianie.



Montaż bramy domowej na ścianie

1 Używając wiertarki i wiertła 4,76 mm (3/16 cala) wywierć dwa otwory na tej samej wysokości, oddalone od siebie o 11,6 cm (4 cale).

Uwaga: Na poprzednim rysunku pokazano rozmieszczenie otworów montażowych na spodzie bramy domowej.

2 Czy brama jest montowana na płycie gipsowej lub powierzchni betonowej, na której znajduje się drewniana listwa?

- Jeśli **tak**, przejdź do kroku 3.
- Jeśli **nie**, umocuj kołki rozporowe w ścianie i wkręć w nie wkręty montażowe, pozostawiając ok. 5 mm wolnej przestrzeni między główką wkrętu a ścianą. Następnie przejdź do kroku 4.

3 Umocuj wkręty montażowe w ścianie, pozostawiając ok. 5 mm wolnej przestrzeni między główką wkrętu a ścianą. Następnie przejdź do kroku 4.

4 Upewnij się, że do bramy domowej nie są dołączone żadne kable ani przewody.

5 Umieść bramę w odpowiednim miejscu. W duże otwory szczelin montażowych (umieszczonych na spodzie bramy) wsuń wkręty montażowe, a następnie przesuwaj bramę w dół aż do momentu, gdy górna cześć szczeliny montażowej oprze się o trzon wkrętu.

Ważne: Przed zawieszeniem urządzenia sprawdź, czy wkręty montażowe wytrzymają ciężar bramy domowej.

Wymagania dotyczące usług telefonicznych

Liczba urządzeń telefonicznych

Znajdujące się w bramie domowej telefoniczne złącza RJ-11 umożliwiają świadczenie usług telefonicznych dla wielu telefonów, faksów i modemów analogowych.

Maksymalna liczba urządzeń telefonicznych dołączonych do każdego portu RJ-11 jest ograniczona przez łączne obciążenie generowane przez dołączone urządzenia telefoniczne. Wiele urządzeń telefonicznych jest oznaczonych parametrem REN (Ringer Equivalent Number). Każdy port telefoniczny znajdujący się w bramie może obsługiwać obciążenie do 5 jednostek REN.

Suma obciążeń REN dla wszystkich urządzeń telefonicznych dołączonych do każdego portu nie może przekraczać 5 REN.

Typy urządzeń telefonicznych

Użytkownik może używać urządzeń telefonicznych, które nie są opisane przez parametr REN, ale w takim przypadku nie można dokładnie określić maksymalnej, możliwej do podłączenia liczby tych urządzeń. Urządzenia telefoniczne, dla których wartość parametru REN jest nieznana, powinny być dołączane po kolei, a przed dodaniem następnego urządzenia należy przetestować sygnał dzwonka. W przypadku dołączenia zbyt dużej liczby urządzeń telefonicznych, gdy sygnał dzwonka przestanie być słyszalny, należy je odłączać po kolei aż do przywrócenia prawidłowego sygnału dzwonka.

Dla telefonów, faksów i innych urządzeń telefonicznych należy podczas łączenia z portami telefonicznymi bramy domowej używać dwóch środkowych styków złączy RJ-11. W przypadku telefonów wykorzystujących inne styki złączy RJ-11 należy stosować adaptery.

Wymagania dotyczące wybierania numerów

Wszystkie telefony powinny być skonfigurowane do wybierania numerów w trybie DTMF (tonowym). Zazwyczaj lokalny dostawca nie obsługuje wybierania impulsowego.

Wymagania dotyczące okablowania telefonicznego

Brama domowa obsługuje połączenie z domowym okablowaniem telefonicznym oraz bezpośrednie połączenie z telefonem lub faksem. Maksymalna odległość między bramą a najbardziej oddalonym urządzeniem telefonicznym nie może przekraczać 300 metrów. Należy stosować telefoniczny przewód skręcany 7/0,15 lub grubszy (oznaczenie amerykańskie: 26-gauge).

Ważne: Połączenia z istniejącą lub nową zainstalowaną na stałe domową siecią telefoniczną muszą być wykonane przez wykwalifikowanego instalatora.

Podłączanie bramy do Internetu i usług telefonicznych

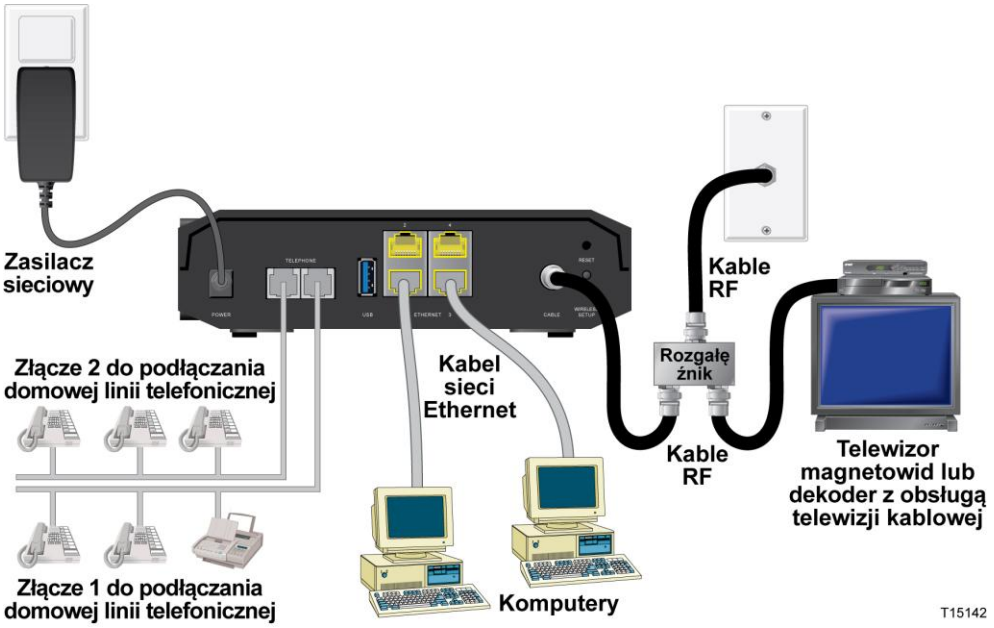
Brama domowa może służyć zarówno do świadczenia usług telefonicznych, jak i do udostępniania Internetu. Połączenie internetowe można udostępniać innym urządzeniom internetowym znajdującym się w domu lub w firmie. Korzystanie z jednego połączenia przez kilka urządzeń jest nazywane pracą w sieci.

Dołączanie i instalowanie urządzeń internetowych

Może okazać się konieczna interwencja doświadczonego instalatora. Dalszą pomoc można uzyskać u lokalnego dostawcy usług.

Dołączanie urządzeń

Poniższy rysunek przedstawia rozmaite dostępne opcje połączeń sieciowych.



Połączenie bramy domowej z usługami szybkiej transmisji danych i usługami telefonicznymi

Następująca procedura zapewnia poprawne zainstalowanie i skonfigurowanie bramy domowej.

1 Wybierz odpowiednią i bezpieczną lokalizację, w której zostanie zainstalowana brama domowa (blisko źródła zasilania, aktywnego połączenia kablowego i komputera — w przypadku korzystania z szybkiego Internetu — lub blisko linii telefonicznych w przypadku korzystania z usługi VoIP).

OSTRZEŻENIE:

- **W celu uniknięcia obrażeń ciała należy wykonywać instrukcje instalowania dokładnie w podanej kolejności.**
- **Aby zapobiec potencjalnym uszkodzeniom sprzętu, przed dołączeniem modemu kablowego do przewodów telefonicznych należy odłączyć od nich wszystkie pozostałe urządzenia telefoniczne.**
- **Niebezpieczne napięcie może pojawić się na portach telefonicznych bramy domowej oraz na innych dołączonych przewodach, takich jak okablowanie sieci Ethernet, okablowanie telefoniczne oraz kabel koncentryczny.**
- **Okablowanie telefoniczne oraz połączenia muszą być prawidłowo odizolowane w celu uniknięcia porażenia elektrycznego.**
- **Połączenia z istniejącą lub nową zainstalowaną na stałe domową siecią telefoniczną muszą być wykonane przez wykwalifikowanego instalatora. Dostawca usługi telefonii przewodowej może świadczyć usługi w zakresie instalacji i podłączania do domowej sieci okablowania telefonicznego. Taka usługa może być odpłatna.**
- **Aby uniknąć porażenia elektrycznego, okablowanie, okablowanie oraz połączenia muszą być poprawnie odizolowane.**
- **Przed próbą dołączenia dowolnego urządzenia należy odłączyć zasilanie od bramy domowej.**

2 Wyłącz zasilanie komputera i innych urządzeń sieciowych, a następnie odłącz je od źródła zasilania.

3 Dołącz aktywny kabel koncentryczny doprowadzony przez dostawcę usług do złącza koncentrycznego opisanego etykietą **CABLE** znajdującego się z tyłu bramy domowej.

Uwaga: Aby dołączyć do tego samego kabla odbiornik telewizyjny, cyfrowy terminal DHCT, dekoder telewizyjny lub magnetowid, należy zainstalować rozgałęźnik (nie jest dostarczany w zestawie). Przed użyciem rozgałęźnika należy skonsultować się z dostawcą usług, gdyż jego zastosowanie może spowodować spadek jakości sygnału.

4 Dołącz swój komputer do bramy domowej, używając jednej z następujących metod.

- **Połączenie Ethernet:** Znajdź żółty kabel Ethernet, włóż jego jedną końcówkę do portu Ethernet w komputerze, a drugą do żółtego portu **ETHERNET** znajdującego się z tyłu bramy domowej.

  Uwaga: Aby w sieci Ethernet zainstalować więcej urządzeń niż wynosi liczba portów Ethernet w bramie domowej, należy użyć zewnętrznego wieloportowego przełącznika Ethernet lub kilku takich przełączników.

- **Sieć bezprzewodowa:** Upewnij się, że zasilanie urządzenia bezprzewodowego jest włączone. Po przejściu bramy w stan aktywny należy skojarzyć urządzenie bezprzewodowe z bramą bezprzewodową. Postępuj zgodnie z instrukcjami dostarczonymi z urządzeniem bezprzewodowym, które opisują sposób kojarzenia z bezprzewodowym punktem dostępu.

  Więcej informacji o domyślnej konfiguracji fabrycznej bramy bezprzewodowej można znaleźć w niniejszym podręczniku w sekcji ***Konfigurowanie ustawień łączności bezprzewodowej*** (na stronie 43).

5 Podłącz jeden koniec telefonicznego kabla złączowego (nie jest dostarczany w zestawie) do domowego gniazda telefonicznego, do telefonu lub do faksu. Następnie podłącz drugi koniec kabla złączowego do odpowiedniego portu RJ-11 oznaczonego etykietą **TELEPHONE** znajdującego się z tyłu bramy domowej. Porty telefoniczne są w kolorze jasnoszarym i noszą oznaczenia 1/2 i 2 lub 1 i 2 w zależności od regionu, w którym jest używana brama domowa.

Informacje:

- Upewnij się, że kabel służący do świadczenia usług telefonicznych został podłączony do prawidłowego portu RJ-11. W przypadku pojedynczej usługi telefonicznej należy użyć portu 1/2 lub 1.
- W Ameryce Północnej bramy domowe mogą pracować w trybie wieloliniowym na porcie telefonicznym RJ-11 oznaczonym jako 1/2. Linia 1 jest dołączona do styków 3 i 4 portu 1/2, zaś linia 2 jest obsługiwana na stykach 2 i 5. W Europie każdy port bramy domowej obsługuje tylko jedną linię. Linia 1 znajduje się w porcie 1, zaś linia 2 w porcie 2.
- Telefony wymagające złącz elektrycznych innych niż RJ-11 mogą wymagać zastosowania zewnętrznego adaptera (do nabycia osobno).

6 Znajdź kabel zasilający dostarczony z bramą domową. Włóż wtyk kabla zasilającego do złącza zasilania znajdującego się z tyłu bramy. Następnie włóż kabel zasilający do gniazda sieciowego w celu podłączenia bramy do zasilania. Brama domowa rozpocznie automatyczne wyszukiwanie w celu zlokalizowania i zarejestrowania się w szerokopasmowej sieci danych. Może to potrwać około 2-5 minut. Modem będzie gotowy do pracy, gdy diody **POWER**, **DS**, **US** i **ONLINE** na panelu przednim bramy przestaną migać i zaczną świecić w sposób ciągły.

7 Dołącz do sieci komputer i pozostały domowy sprzęt sieciowy, po czym włącz ich zasilanie. Dioda **LINK** w bramie domowej odpowiadająca włączanym urządzeniom powinna świecić światłem ciągłym lub migać.

8 Po przejściu bramy do trybu online większość urządzeń internetowych powinna natychmiast uzyskać dostęp do Internetu.

Uwaga: Jeśli komputer nie ma dostępu do Internetu, zapoznaj się z sekcją ***Najczęściej zadawane pytania*** (na stronie 103) w celu uzyskania informacji o konfigurowaniu komputera do pracy w sieci TCP/IP. W przypadku urządzeń internetowych innych niż komputery, przeczytaj sekcję dotyczącą konfigurowania protokołu DHCP lub adresu IP w podręczniku użytkownika konkretnego urządzenia.

Konfigurowanie bramy domowej DOCSIS

Aby skonfigurować bramę domową, należy najpierw uzyskać dostęp do stron konfiguracji aplikacji WebWizard. Niniejsza sekcja zawiera dokładne instrukcje i procedury dotyczące dostępu do stron aplikacji WebWizard oraz konfigurowania bramy domowej w celu zapewnienia jej poprawnej pracy. W tej sekcji podano również przykłady i opisy wszystkich stron konfiguracyjnych aplikacji WebWizard. Strony aplikacji WebWizard służą do dostosowania ustawień domyślnych bramy domowej do potrzeb użytkownika. Strony aplikacji WebWizard są opisane w tej sekcji w kolejności przedstawionej na stronie **Konfiguracja**.

Ważne: Strony aplikacji WebWizard i przykłady przytoczone w tej sekcji mają wyłącznie charakter ilustracyjny. Strony, z którymi będzie miał do czynienia użytkownik, mogą różnić się od stron przedstawionych w niniejszym podręczniku. Strony przedstawione w tym podręczniku zawierają również wartości domyślne dla urządzenia.

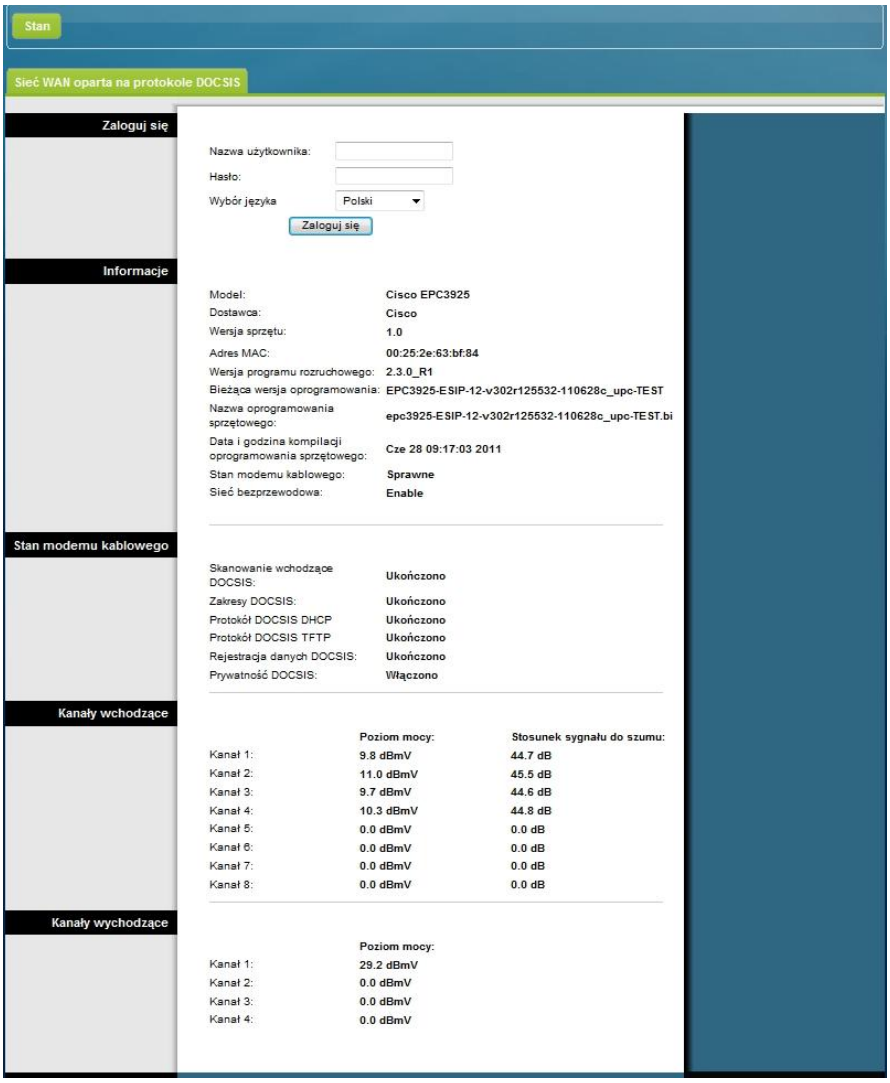
Uwaga: Jeśli po raz pierwszy używasz procedur konfigurowania sieci szczegółowo opisanych w tej sekcji, skontaktuj się z usługodawcą przed zmianą jakichkolwiek ustawień domyślnych bramy domowej.

Logowanie do bramy po raz pierwszy

W konfiguracji domyślnej bramy używany jest adres IP 192.168.0.1. Jeśli brama została prawidłowo podłączona i komputer jest prawidłowo skonfigurowany, wykonaj następujące czynności, aby zalogować się w bramie jako administrator.

1 Na komputerze otwórz używaną przeglądarkę sieci WWW.

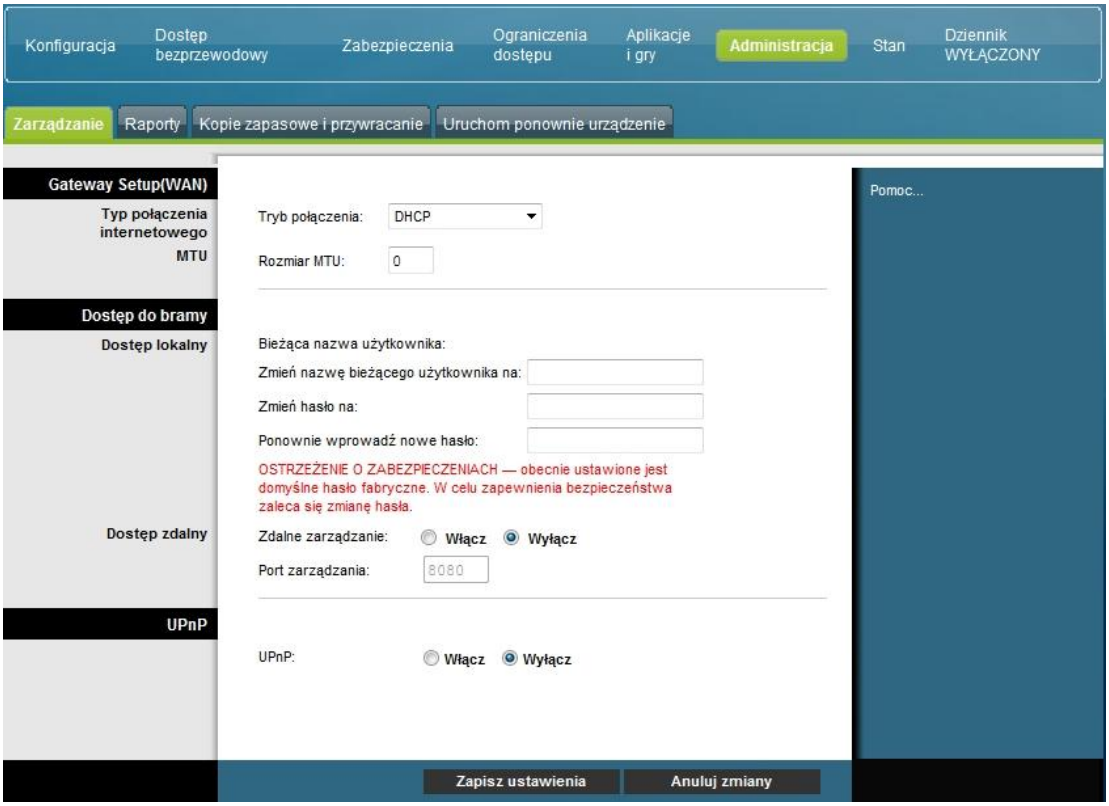
2 W polu adresu wpisz następujący adres IP: **192.168.0.1**. Zostanie otwarta strona logowania Stan > Sieć WAN oparta na protokole DOCSIS podobna do następującej.



3 Na stronie Stan > Sieć WAN oparta na protokole DOCSIS pozostaw puste pola Nazwa użytkownika i Hasło, a następnie kliknij przycisk **Zaloguj się**. Brama zostanie otwarta, a na pierwszym planie będzie wyświetlona strona Administracja > Zarządzanie. Na tej stronie można zmienić swoją nazwę użytkownika i hasło.

W tym momencie nastąpiło zalogowanie do bramy. Użytkownik może wybrać dowolną stronę sieci WWW dotyczącą instalowania i zarządzania. Nastąpi jednak przekierowanie do strony Administracja > Zarządzanie w celu przypomnienia o wybraniu nowego hasła.

Ważne: Usilnie zaleca się wybranie nowego hasła w celu ochrony przed możliwością ataków internetowych skierowanych przeciwko urządzeniom korzystającym z dobrze znanych lub domyślnych ustawień fabrycznych nazw użytkownika i haseł.



4 Na stronie Administracja > Zarządzanie utwórz swoją nazwę użytkownika i hasło, a następnie kliknij przycisk **Zapisz ustawienia**. Po zapisaniu swojej nazwy użytkownika i hasła na stronie Administracja > Zarządzanie zostanie otwarta strona Konfiguracja > Szybka konfiguracja.

   Ważne: Istnieje możliwość pozostawienia pustego pola hasła (domyślne ustawienie fabryczne). Jednak w przypadku, gdy nazwa użytkownika i hasło nie zostaną zmienione, przy każdym dostępie do bramy nastąpi przekierowanie do strony Administracja > Zarządzanie. Jest to sposób przypomnienia o konieczności utworzenia własnego hasła.

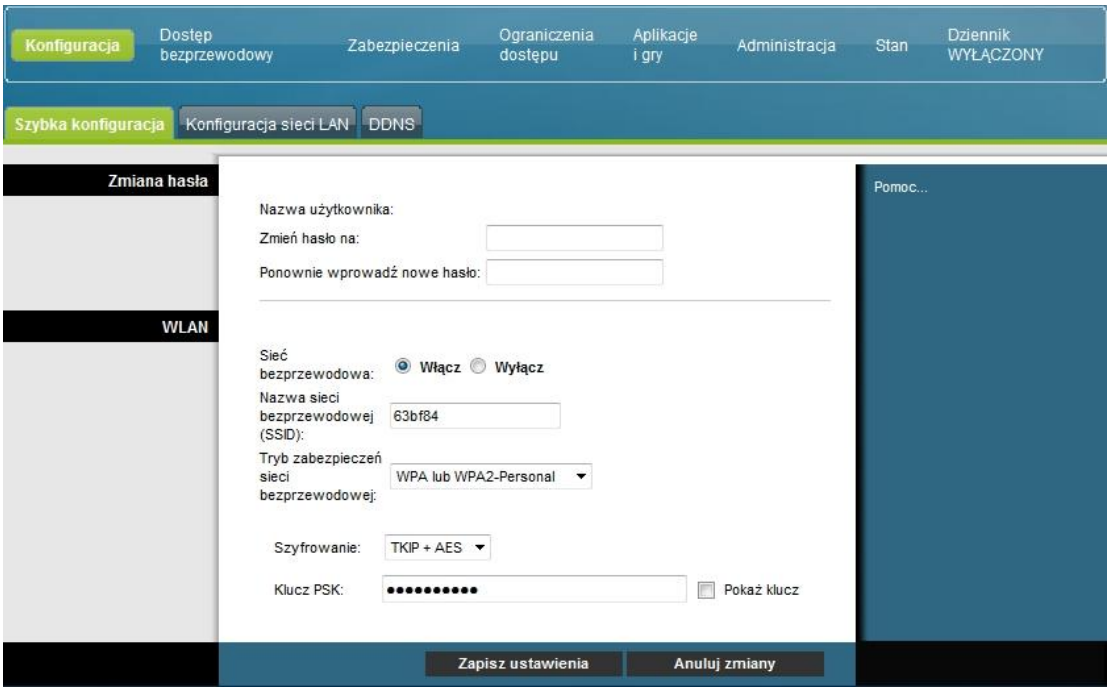
   Po wybraniu własnego hasła przy każdym następnym logowaniu nastąpi przekierowanie bezpośrednio do strony Konfiguracja > Szybka konfiguracja.

5 Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Konfiguracja > Szybka konfiguracja

Strona Konfiguracja > Szybka konfiguracja jest pierwszą stroną otwieraną po zalogowaniu do bramy. Ustawienia na tej stronie służą do zmiany hasła i do skonfigurowania sieci WLAN.

Ważne: Ustawienia na tej stronie są unikalne dla danego urządzenia. Na tej stronie nie jest konieczne wprowadzanie żadnych zmian. Ustawienia domyślne w pełni wystarczają do bezpiecznej pracy w sieci bezprzewodowej.



Konfigurowanie szybkich ustawień

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji ustawień sieciowych urządzenia. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Zmiana hasła	**Nazwa użytkownika** Wyświetla nazwę użytkownika aktualnie zalogowanego operatora. **Zmień hasło na** W tym polu możesz zmienić swoje hasło **Ponownie wprowadź nowe hasło** To pole służy do ponownego wpisania hasła. Wpisane hasło musi być takie samo, jak hasło w polu **Zmień hasło na**

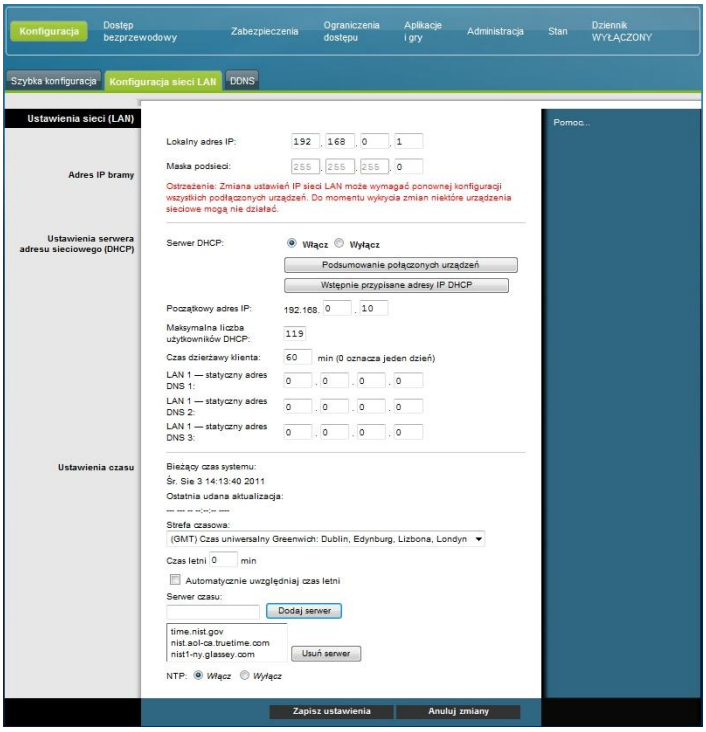
Sekcja	Opis pola
WLAN	**Sieć bezprzewodowa** Umożliwia włączenie lub wyłączenie sieci bezprzewodowej. Wybierz żądaną opcję: ■ Włącz ■ Wyłącz **Nazwa sieci bezprzewodowej (SSID)** Umożliwia wprowadzenie nazwy sieci bezprzewodowej lub używanie wartości domyślnej. Wprowadzona wartość będzie widoczna w komputerach i innych urządzeniach klienckich jako nazwa sieci bezprzewodowej. **Uwaga:** Domyślne ustawienie fabryczne identyfikatora SSID (Service Set Identifier) składa się zazwyczaj z ostatnich 6 znaków adresu CM MAC. Adres CM MAC można znaleźć na etykiecie znajdującej się na bramie bezprzewodowej. **Tryb zabezpieczeń sieci bezprzewodowej** Umożliwia wybranie trybu zabezpieczeń sieci bezprzewodowej w celu ułatwienia ochrony sieci. Po wybraniu opcji **Wyłącz** sieć bezprzewodowa nie będzie bezpieczna i będą się z nią mogły łączyć dowolne urządzenia znajdujące się w pobliżu. W sekcji ***Bezpieczeństwo sieci bezprzewodowej*** (na stronie 47) można znaleźć szczegółowy opis trybów zabezpieczeń sieci bezprzewodowej. **Uwaga:** Domyślnym ustawieniem fabrycznym trybu zabezpieczeń sieci bezprzewodowej jest WPA lub WPA2-Personal. **Szyfrowanie** Umożliwia wybranie poziomu szyfrowania w zależności od wybranego trybu zabezpieczeń sieci bezprzewodowej. W sekcji ***Zabezpieczenia sieci bezprzewodowej*** (na stronie 47) można znaleźć szczegółowy opis metod szyfrowania. **Klucz PSK** Wstępny klucz wspólny używany przez urządzenie. Klucz musi mieć od 8 do 63 znaków. Domyślne ustawienie fabryczne klucza PSK odpowiada 9-cyfrowemu numerowi seryjnemu bramy. Numer seryjny można znaleźć na etykiecie znajdującej się na bramie bezprzewodowej. **Uwaga: Dostawca usług może dostarczyć kartę konfiguracji sieci bezprzewodowej zawierającą identyfikator SSID oraz informacje o konfiguracji zabezpieczeń sieci domowej, które mogą różnić się od informacji podanych powyżej.**

Konfiguracja > Konfiguracja sieci LAN

Strona Konfiguracja > Konfiguracja sieci LAN umożliwia skonfigurowanie ustawień domowej sieci LAN. Do tych ustawień należy zakres adresów IP definiujący samą sieć LAN oraz sposób przypisywania adresów (automatycznie za pomocą protokołu DHCP lub ręcznie) w przypadku dodawania do sieci nowych urządzeń.

Ważne: Jeśli nie masz doświadczenia w administrowaniu adresami IP, zalecamy pozostawienie tych ustawień bez zmian. Nieprawidłowa zmiana tych wartości może spowodować utratę dostępu do Internetu.

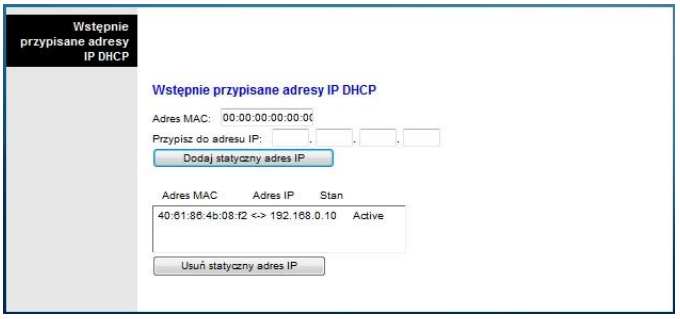
Wybierz kartę **Konfiguracja sieci LAN**, aby przejść do strony Konfiguracja > Konfiguracja sieci LAN.



Konfigurowanie ustawień sieci

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania ustawień sieci obsługiwanej przez używaną bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Ustawienia sieci (LAN) **Adres IP bramy**	**Lokalny adres IP** Podstawowy adres IP prywatnej domowej sieci LAN. Domyślnym ustawieniem fabrycznym adresu IP sieci LAN jest 192.168.0.1. **Maska podsieci** Maska podsieci sieci LAN

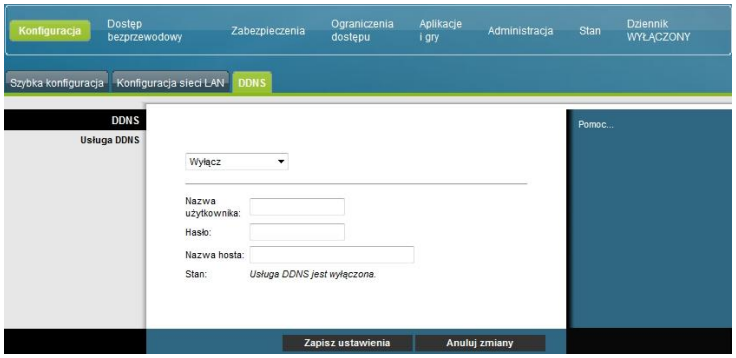
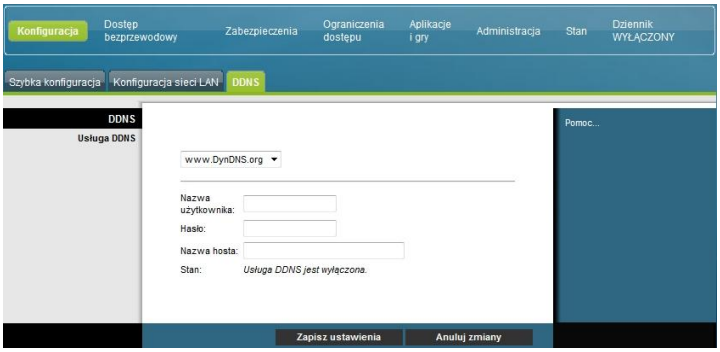
Sekcja	Opis pola
Ustawienia serwera adresu sieciowego (DHCP)	**Serwer DHCP** Umożliwia włączenie lub wyłączenie serwera DHCP wbudowanego w bramę domową. Serwer DHCP służy do automatycznego przydzielania adresów IP urządzeniom dołączonym do sieci domowej. ■ **Strona Podsumowanie połączonych urządzeń** Kliknij przycisk **Podsumowanie połączonych urządzeń** na stronie Konfiguracja sieci LAN. Zostanie otwarta strona Podsumowanie połączonych urządzeń. Ta strona jest wyskakującym oknem, w którym wyświetlane są adresy MAC i adresy IP urządzeń połączonych do bramy. ■ **Strona Wstępnie przypisane adresy IP DHCP** Kliknij przycisk **Wstępnie przypisane adresy IP DHCP** na stronie Konfiguracja sieci LAN. Zostanie otwarta strona Wstępnie przypisane adresy IP DHCP. Ta strona umożliwia przypisanie konkretnego adresu IP do komputera lub do innego urządzenia po zażądaniu przez nie adresu IP przy użyciu protokołu DHCP. Przy użyciu tej funkcji mogą być używane wyłącznie adresy z puli DHCP bramy.  **Informacje:** – Przycisk **Dodaj statyczny adres IP** powoduje dodanie statycznego adresu IP do listy wstępnie przypisanych adresów IP. – Przycisk **Usuń statyczny adres IP** powoduje usunięcie statycznego adresu IP z listy wstępnie przypisanych adresów IP **Początkowy adres IP** Wyświetla początkowy adres używany przez wbudowany serwer DHCP do dystrybucji adresów IP w prywatnej sieci LAN. Ponieważ domyślnym adresem IP bramy jest **192.168.0.1**, początkowym adresem IP musi być **192.168.0.2** lub większy, ale mniejszy niż **192.168.0.253**. Domyślny początkowy adres IP to **192.168.0.10**.

Sekcja	Opis pola
	Maksymalna liczba użytkowników DHCP Wprowadź maksymalną liczbę użytkowników, którym serwer DHCP może przypisać adresy IP używane w sieci LAN. Ta liczba nie może być większa niż 254 pomniejszone o opisany wyżej początkowy adres IP. **Czas dzierżawy klienta** Czas dzierżawy klienta to czas, przez jaki adres IP pozostaje ważny. Dzierżawione adresy IP są automatycznie odnawiane przez komputer oraz inne urządzenia korzystające z protokołu DHCP przy pobieraniu adresów IP. Jeśli dopuszczalne jest wygaśnięcie dzierżawy, adres IP zostanie zwrócony do puli dostępnych adresów IP, które mogą zostać przydzielone po dodaniu nowych urządzeń do sieci. Wartością domyślną jest 60 minut, jeśli brama jest w trybie online. **LAN - statyczny adres DNS 1-3** Serwer DNS jest używany przez komputer lub inne urządzenie klienckie do znajdowania publicznego adresu IP skojarzonego z adresem URL lub opartym na nazwie adresem witryny sieci WWW. Można ręcznie określić serwery DNS, które mają być używane przez urządzenia w sieci, podając adresy IP serwerów w odpowiednich polach. W przeciwnym razie brama będzie automatycznie rozsyłać informacje o serwerze DNS otrzymane od dostawcy usług. Domyślnie te pola pozostają puste.
Ustawienia czasu	**Strefa czasowa** Wybierz strefę czasową dla swojego miejsca pobytu. Jeśli w tym miejscu stosuje się czas letni, wybierz opcję **Automatycznie uwzględniaj czas letni**.

Konfiguracja > DDNS

Usługa DDNS (Dynamic Domain Name Service) dostarcza bramie domowej (której adres IP może się zmieniać) nazwę hosta lub adres URL rozpoznawalny przez aplikacje sieciowe za pomocą standardowych zapytań DNS. Jest to przydatne w przypadku hostingu własnej strony internetowej, serwera FTP lub innego serwera poza urządzeniem. Przed użyciem tej funkcji należy zarejestrować się w usłudze DDNS.

Wybierz kartę **DDNS**, aby przejść do strony Konfiguracja > DDNS.

Sekcja	Opis pola
Usługa DDNS	**Wyłączenie usługi DDNS** (domyślne ustawienie fabryczne) Aby wyłączyć protokół DDNS, z listy rozwijanej wybierz opcję **Wyłącz** i kliknij przycisk **Zapisz ustawienia**.  **Włączenie usługi DDNS** **Uwaga:** Aby można było korzystać z funkcji DDNS, należy najpierw założyć konto i utworzyć adres URL w witrynie www.DynDNS.org. Funkcja DDNS nie będzie działała bez prawidłowego konta. Aby skonfigurować konto DDNS, otwórz przeglądarkę i w pasku adresu wpisz www.DynDNS.org. Aby skonfigurować konto, postępuj zgodnie z instrukcjami wyświetlanymi w witrynie. Aby włączyć protokół DDNS, wykonaj następujące czynności. **1** Na stronie DDNS wybierz **www.DynDNS.org** jako swój serwer DDNS.  **2** Skonfiguruj następujące pola: ■ Nazwa użytkownika ■ Hasło ■ Nazwa hosta **3** Kliknij przycisk **Zapisz ustawienia**. Od tego momentu przy każdej zmianie adresu IP sieci WAN (internetowego) urządzenie będzie przesyłać odpowiednie informacje do usługi DDNS. **Ważne:** W obszarze Stan w oknie będzie wyświetlany stan połączenia z usługą DDNS.

Konfigurowanie ustawień łączności bezprzewodowej

W tej sekcji opisano opcje dostępne na stronach Dostęp bezprzewodowy, które służą do konfigurowania parametrów WAP w celu spełnienia konkretnych wymagań i potrzeb.

Dostęp bezprzewodowy > Ustawienia podstawowe

Skonfigurowanie bramy domowej do łączności bezprzewodowej umożliwia dostęp do Internetu z dowolnego miejsca będącego w zasięgu usługi WAP bez konieczności stosowania połączeń przewodowych. Wybierz kartę **Ustawienia podstawowe**, aby przejść do strony Dostęp bezprzewodowy > Ustawienia podstawowe.

Strona ustawień podstawowych sieci bezprzewodowej umożliwia wybranie trybu pracy sieci bezprzewodowej oraz innych podstawowych funkcji.

- Sieć bezprzewodowa: Włącz lub Wyłącz
- Konfiguracja sieci bezprzewodowej: Ręcznie lub Wi-Fi Protected Setup (WPS)
- Tryb sieciowy
- Pasmo radiowe
- Zasięg kanału
- Kanał standardowy
- Nazwa sieci bezprzewodowej (SSID)

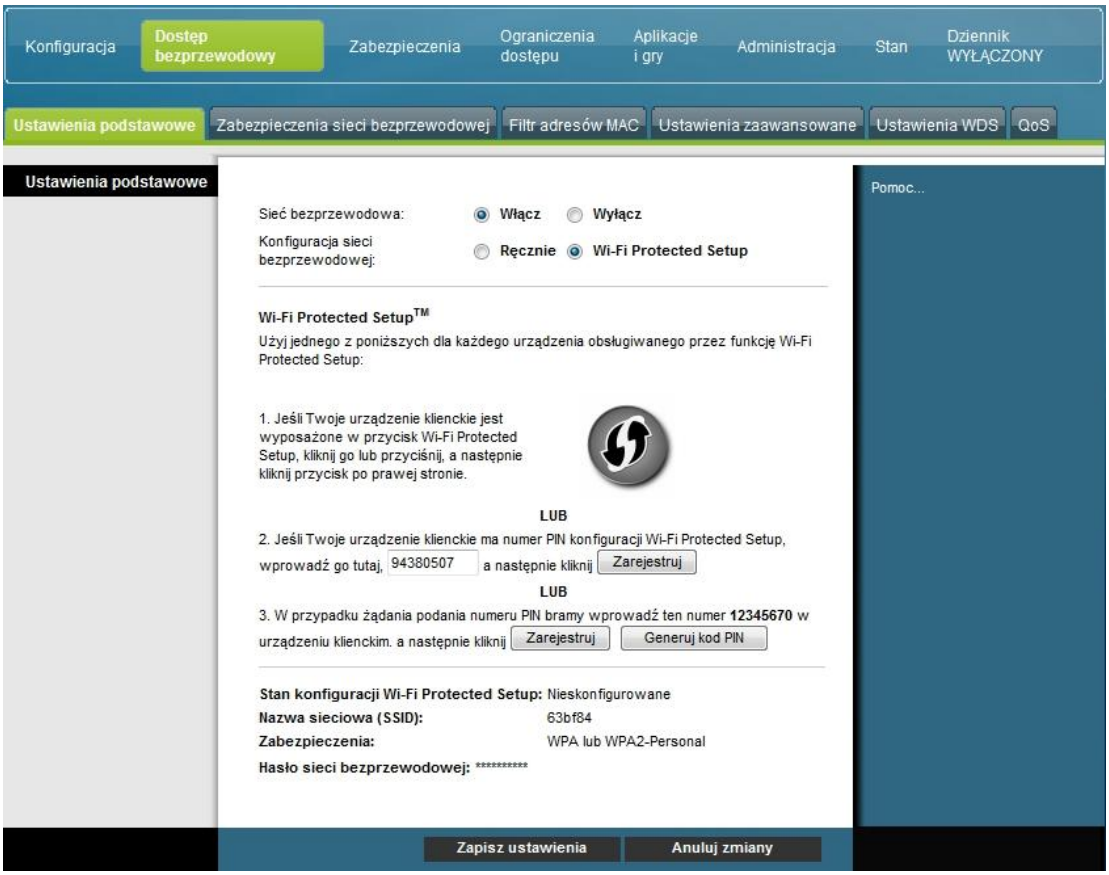
Wi-Fi Protected Setup (WPS)

Po wybraniu konfiguracji sieci bezprzewodowej Wi-Fi Protected Setup (WPS) wiele ustawień zostanie wstępnie skonfigurowanych. Protokół WPS umożliwia uproszczoną konfigurację, dzięki której łatwo dołączyć do sieci nowe urządzenia z funkcją WPA.

Ważne: Podczas pracy w trybie WPS nie jest obsługiwany algorytm szyfrowania WEP. Jeśli konieczne jest użycie algorytmu szyfrowania WEP, należy wyłączyć tryb WPS, zmieniając wartość parametru Konfiguracja sieci bezprzewodowej na **Ręcznie**.

Uwaga: Ustawieniem domyślnym jest WPS.

Przykład konfiguracji sieci bezprzewodowej w trybie Wi-Fi Protected Setup

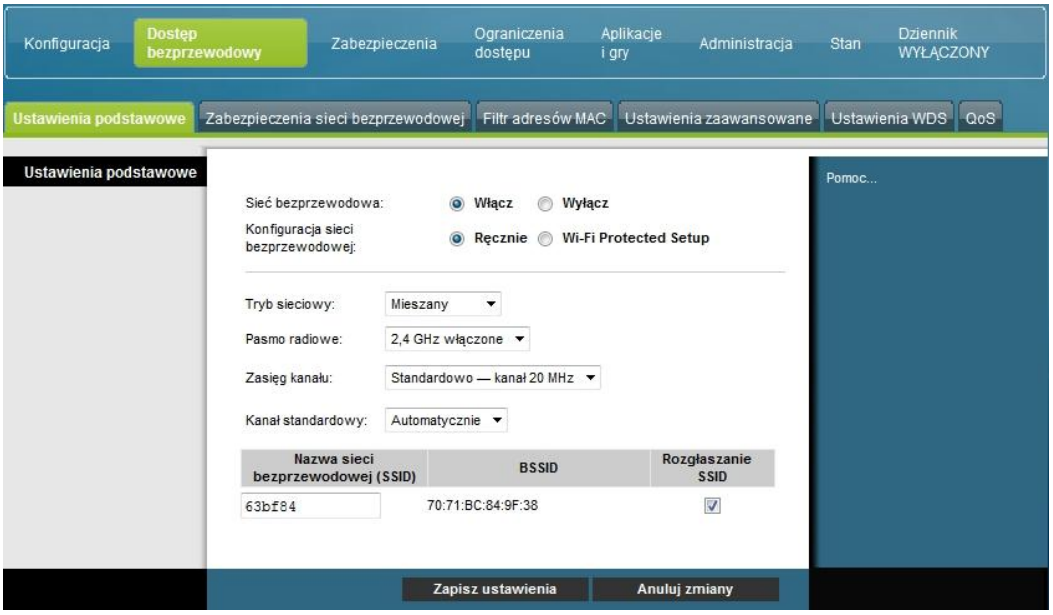


Opis konfiguracji sieci bezprzewodowej w trybie Wi-Fi Protected Setup

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji ustawień podstawowych sieci bezprzewodowej w trybie Wi-Fi Protected Setup obsługiwanej przez używaną bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Ustawienia podstawowe	**Włącz** lub **Wyłącz** sieć bezprzewodową **Konfiguracja sieci w trybie Wi-Fi Protected Setup** W trybie Wi-Fi Protected Setup sieć bezprzewodowa zabezpieczona poprzez szyfrowanie jest konfigurowana automatycznie. Aby korzystanie z tej funkcji było możliwe, w sieci musi znajdować się przynajmniej jeszcze jedno obsługujące ją urządzenie. Po skonfigurowaniu urządzeń obsługujących funkcję Wi-Fi Protected Setup można ręcznie skonfigurować pozostałe urządzenia. **Przycisk konfiguracji WPS (opcja 1)** Aby zarejestrować w bramie klienta sieci bezprzewodowej, naciśnij przycisk Wi-Fi Protected Setup na stronie podstawowych ustawień sieci bezprzewodowej lub przycisk znajdujący się na tylnym panelu bramy. Naciśnij przycisk programowy Wi-Fi Protected Setup po stronie klienta w tym samym momencie, w którym nastąpi naciśnięcie przycisku znajdującego się na panelu bramy. Połączenie zostanie skonfigurowane automatycznie. **Konfiguracja WPS przy użyciu kodu PIN adaptera Wi-Fi (opcja 2)** Jest to najbezpieczniejsza opcja rejestracji w bramie klienta sieci bezprzewodowej. Wymagana jest znajomość numeru PIN konfiguracji Wi-Fi Protected Setup, który można znaleźć w narzędziu Wi-Fi Protected Setup urządzenia klienckiego. Po wprowadzeniu numeru PIN konfiguracji Wi-Fi Protected Setup urządzenia klienckiego można ustanowić połączenie z bramą. **Konfiguracja WPS przy użyciu numeru PIN bramy (opcja 3)** Należy zauważyć, że numer PIN konfiguracji Wi-Fi Protected Setup jest wyświetlany na stronie Wi-Fi Protected Setup. W przypadku opcji 3 kliknij przycisk Zarejestruj, a następnie używając narzędzia Wi-Fi Protected Setup urządzenia klienckiego lub systemu operacyjnego Microsoft Vista wprowadź numer PIN konfiguracji Wi-Fi Protected Setup bramy do urządzenia klienckiego w celu zakończenia rejestracji.

Przykład strony ręcznej konfiguracji sieci bezprzewodowej



Opis strony Dostęp bezprzewodowy > Ustawienia podstawowe

Opisy i instrukcje przedstawione w następującej tabeli dotyczą ręcznego konfigurowania ustawień podstawowych komunikacji bezprzewodowej obsługiwanej przez bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Ustawienia podstawowe	**Sieć bezprzewodowa** **Włącz** lub **Wyłącz** sieć bezprzewodową **Konfiguracja sieci bezprzewodowej** Ustawienie domyślne to **WPS**. Więcej informacji na temat korzystania z funkcji WPS można znaleźć w sekcji ***Wi-Fi Protected Setup (WPS)*** (na stronie 38). Zaznacz pole wyboru **Ręcznie**, aby ręcznie skonfigurować sieć za pomocą tej opcji.
	Tryb sieciowy Wybierz jedną z poniższych opcji dla trybu sieciowego: **Tylko G, Mieszany B/G, Mieszany B/G/N** (domyślne ustawienie fabryczne) **Ważne:** Jeśli wybrano tylko uwierzytelnianie TKIP, nie jest dostępny tryb pracy sieci Mieszany B/G/N.

Sekcja	Opis pola
	Pasmo radiowe Wybierz opcję **2,4 GHz włączone** (domyślne ustawienie fabryczne) lub **5 GHz włączone**. **Uwaga:** Niektóre modele mogą nie obsługiwać pasma radiowego 5 GHz.
	Zasięg kanału Wybierz opcję **Standardowo — kanał 20 MHz** lub opcję **Dla całej sieci — kanał 40 MHz**. **Kanał standardowy** Z listy rozwijanej wybierz jeden z kanałów odpowiadających ustawieniom sieci. Wszystkie urządzenia w sieci bezprzewodowej muszą wykonywać rozgłaszanie na tym samym kanale, aby mogły komunikować się między sobą. W celu automatycznego wyboru kanału można wybrać opcję **Automatycznie** (domyślne ustawienie fabryczne).
	Nazwa sieci bezprzewodowej (SSID) SSID jest nazwą sieci bezprzewodowej. Nazwa SSID jest używana w technologii bezprzewodowej do odróżnienia własnej sieci od innych sieci bezprzewodowych znajdujących się w pobliżu. Nazwa SSID może zawierać do 32 znaków. Domyślne ustawienie fabryczne SSID składa się zazwyczaj z ostatnich 6 znaków adresu CM MAC, który można znaleźć na etykiecie umieszczonej na spodzie bramy. Nazwa SSID jest unikatowym identyfikatorem i nie należy jej zmieniać bez potrzeby. Dostawca usług może dostarczyć informacji o konfiguracji sieci bezprzewodowej, co może wymagać użycia innej nazwy SSID. **BSSID** Wyświetla nazwę zwaną identyfikatorem zestawu usług podstawowych (Basic Service Set Identifier, BSSID) sieci bezprzewodowej. Identyfikator BSSID jest najczęściej adresem MAC punktu dostępu sieci bezprzewodowej. **Uwaga:** Ten adres MAC może być inny niż adres CM MAC używany do określenia domyślnego fabrycznego ustawienia SSID. **Rozgłaszanie SSID** Jeśli to pole wyboru jest zaznaczone (domyślne ustawienie fabryczne), brama przeprowadza transmisję i rozgłasza swoją obecność innym urządzeniom bezprzewodowym. Urządzenia klienckie mogą automatycznie wykrywać punkt dostępu, gdy ta funkcja jest włączona. Usuń zaznaczenie tego pola, jeśli chcesz ukryć swoją sieć przed klientami bezprzewodowymi. Jeśli chcesz ukryć sieć, musisz ręcznie skonfigurować każde bezprzewodowe urządzenie klienckie oddzielnie. **Ważne:** Pole wyboru **Włącz** nie jest obecnie używane i nie wpływa na działanie bramy.

Sieć bezprzewodowa > Zabezpieczenia sieci bezprzewodowej

Wybranie trybu zabezpieczeń sieci bezprzewodowej ułatwia ochronę sieci. Po wybraniu opcji **Wyłącz** sieć bezprzewodowa nie będzie bezpieczna i będą się z nią mogły łączyć dowolne urządzenia znajdujące się w pobliżu.

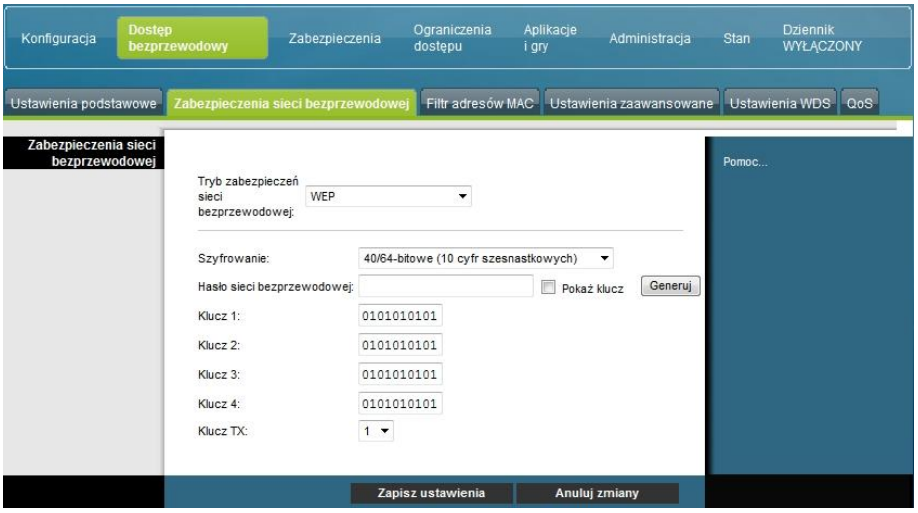
Aby uniemożliwić osobom postronnym dostęp do sieci bezprzewodowej, użyj strony Zabezpieczenia sieci bezprzewodowej do skonfigurowania parametrów zabezpieczeń, w tym trybu zabezpieczeń (poziomu szyfrowania), kluczy szyfrujących i innych ustawień zabezpieczeń.

Kliknij kartę **Zabezpieczenia sieci bezprzewodowej**, aby przejść do strony Zabezpieczenia sieci bezprzewodowej. Następująca tabela przedstawia przykładowe ustawienia strony Zabezpieczania sieci bezprzewodowej z wybranymi różnymi trybami zabezpieczeń.

Opis strony Zabezpieczenia sieci bezprzewodowej

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania zabezpieczeń sieci bezprzewodowej obsługiwanej przez używaną bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Zabezpieczenia sieci bezprzewodowej	**Tryb zabezpieczeń sieci bezprzewodowej** Ustaw tryb zabezpieczeń, wybierając jedną z poniższych opcji: **WEP** Tryb zabezpieczeń WEP (Wired Equivalent Privacy) jest zdefiniowany w oryginalnym standardzie IEEE 802.11. Zapewnia słabą ochronę, dlatego nie jest już zalecany. Użytkownicy są zachęcani do używania trybu WPA-Personal lub WPA2-Personal. **Uwaga:** W trybie WPS to urządzenie nie obsługuje algorytmu szyfrowania WEP.



Opisy pól

- **Szyfrowanie.** Wybierz poziom szyfrowania 40/64-bitowe (10 cyfr szesnastkowych) lub 104/128-bitowe (26 cyfr szesnastkowych).
- **Hasło sieci bezprzewodowej**. Aby zakończyć konfigurowanie zabezpieczeń, należy wybrać hasło sieci bezprzewodowej, które jest łatwe do zapamiętania, ale trudne do odgadnięcia przez innych użytkowników. Podczas pierwszego łączenia się z siecią przy użyciu nowego urządzenia bezprzewodowego może być konieczne wprowadzenie tego hasła do odpowiedniego pola konfiguracyjnego podłączonego urządzenia. Aby poprawić zabezpieczenia sieci, nie należy podawać tego hasła nieautoryzowanym użytkownikom. Wprowadź hasło zawierające od 4 do 24 liter i/lub cyfr. Następnie kliknij przycisk **Generuj** w celu utworzenia hasła.
- **Klucz 1-4**. Aby ręcznie wprowadzić klucze WEP, wypełnij te pola. Każdy klucz WEP składa się z liter od A do F oraz cyfr od 0 do 9. Powinien mieć długość 10 znaków dla szyfrowania 40/64-bitowego i 26 znaków dla szyfrowania 104/128-bitowego.
- **Klucz TX**. Wybierz klucz transmisyjny (TX) od 1 do 4. Klucz TX jest kluczem, który będzie używany do szyfrowania danych. Można utworzyć cztery klucze, ale do szyfrowania danych będzie używany tylko jeden z nich. Wybierz jeden z czterech kluczy, który ma być używany do szyfrowania WEP. Użyj wybranego klucza TX do skonfigurowania klientów sieci bezprzewodowej.

Sekcja	Opis pola

WPA

Zabezpieczenia sieci prywatnych – tryb WPA lub WPA2 Personal

Metoda szyfrowania Wi-Fi Protected Access (WPA) jest bezpieczniejszą technologią sieci bezprzewodowych niż WEP. Szyfrowanie WPA może być stosowane w firmowych (zastosowania korporacyjne) i osobistych (sieci domowe) sieciach bezprzewodowych. Usilnie zaleca się stosowanie metody szyfrowania WPA-Personal lub WPA2-Personal jako sposobu zabezpieczeń sieci domowej, w zależności od trybu obsługiwanego przez adapter sieci bezprzewodowej komputera lub klientów sieci bezprzewodowej.

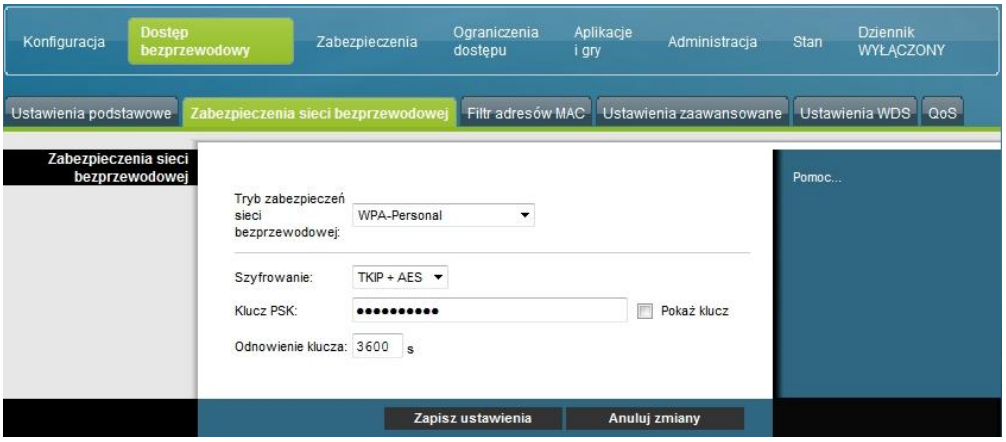
Szyfrowanie WPA-Personal (znane również jako WPA-PSK lub WPA-Pre-Shared Key) zabezpiecza sieć bezprzewodową lepiej, niż szyfrowanie WEP. W szyfrowaniu WPA-Personal stosowana jest metoda uwierzytelniania użytkowników TKIP oraz klucze szyfrowania mocniejsze niż WEP.

Szyfrowanie WPA2-Personal (znane również jako WPA2-PSK lub WPA2-Pre-Shared Key) jest najmocniejszą standardową metodą szyfrowania używaną w sieciach bezprzewodowych. W protokole WPA2-Personal do transmisji danych wykorzystywana jest metoda szyfrowania AES (Advanced Encryption Standard).

Uwaga: Nie wszystkie adaptery bezprzewodowe obsługują protokół WPA2. Protokół WPA jest obsługiwany przez większą liczbę urządzeń. Niezależnie od używanego protokołu (WPA lub WPA2) należy stosować „mocne" hasło. Mocne hasło jest ciągiem znaków losowych o długości co najmniej 21 znaków.

Wybierz jeden z następujących trzech trybów WPA lub WPA2 Personal:

- **WPA-Personal**
- **WPA2-Personal**
- **WPA lub WPA2-Personal**



Opisy pól

- **Szyfrowanie**. Ustawienie domyślne to TKIP+AES.
- **Klucz PSK**. Wprowadź klucz złożony z 8–63 znaków.
- **Odnowienie klucza**. Wprowadź okres Odnowienie klucza, który określa, jak często należy wymieniać klucz szyfrowania. Wartość domyślna to **3600** sekund.

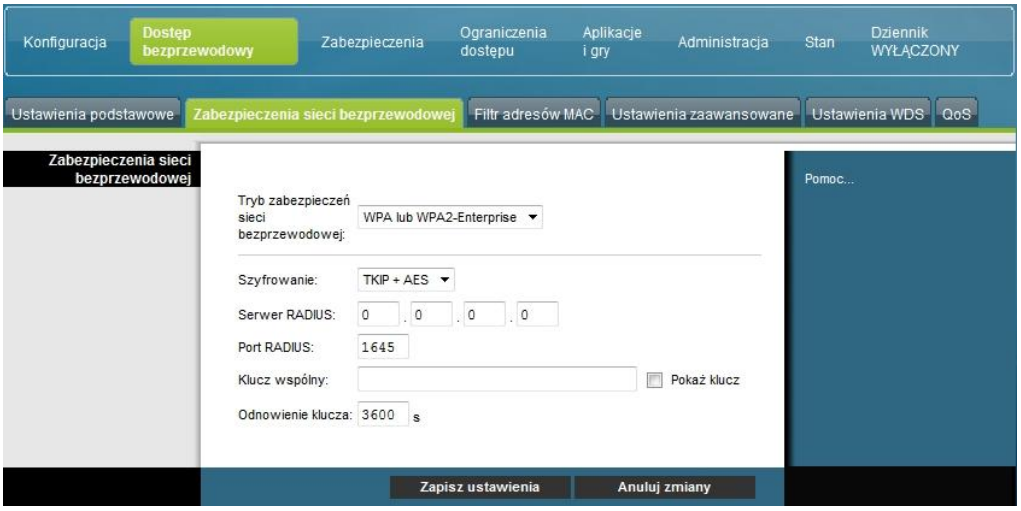
Sekcja	Opis pola

Zabezpieczenia sieci przedsiębiorstwa — tryby WPA-Enterprise

Ta opcja wykorzystuje WPA w połączeniu z serwerem RADIUS służącym do uwierzytelniania klientów (można z niej korzystać tylko wtedy, gdy do urządzenia jest podłączony serwer RADIUS).

Wybierz jeden z następujących trzech trybów WPA lub WPA2 Enterprise:

- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA lub WPA2-Enterprise**



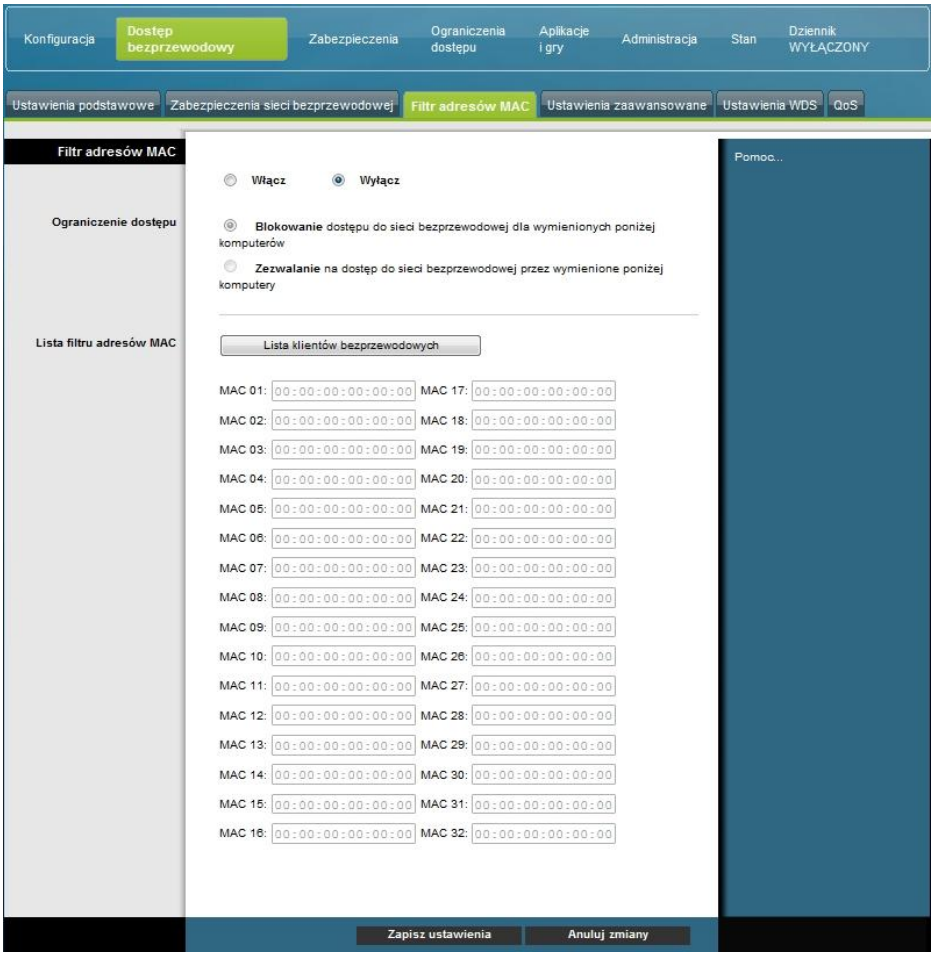
Opisy pól

- **Szyfrowanie**. Ustawienie domyślne to TKIP+AES.
- **Serwer RADIUS**. Wprowadź adres IP serwera RADIUS.
- **Port RADIUS**. Wprowadź numer portu używanego przez serwer RADIUS. Wartość domyślna to **1812**.
- **Klucz wspólny**. Wprowadź klucz używany przez urządzenie i serwer RADIUS.
- **Odnowienie klucza.** Wprowadź okres Odnowienie klucza, który określa, jak często należy wymieniać klucz szyfrowania. Wartość domyślna to **3600** sekund.

Dostęp bezprzewodowy > Filtr adresów MAC

Funkcja filtru adresów MAC służy do zezwalania na dostęp lub blokowanie dostępu do bezprzewodowej sieci LAN na podstawie adresu MAC bezprzewodowych urządzeń klienckich. Funkcja filtru adresów MAC, nazywana też listą dostępu, może służyć do ułatwienia ochrony sieci bezprzewodowej przed uzyskaniem dostępu przez nieautoryzowanych użytkowników.

Wybierz opcję **Filtr adresów MAC**, aby przejść do strony Dostęp bezprzewodowy > Filtr adresów MAC.



Opis strony Dostęp bezprzewodowy > Filtr adresów MAC

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji filtrowania adresów MAC w sieci bezprzewodowej obsługiwanej przez używaną bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Filtr adresów MAC	Umożliwia włączenie (**Włącz**) lub wyłączenie (**Wyłącz**) filtrowania adresów MAC w bramie domowej
Ograniczenie dostępu	**Ograniczenie dostępu** Umożliwia zezwalanie komputerom na dostęp do sieci bezprzewodowej lub blokowanie dostępu. Opcja wybrana tutaj ma wpływ na adresy wymienione na tej stronie. Wybierz jedną z następujących opcji: ■ Blokowanie dostępu do sieci bezprzewodowej dla wymienionych poniżej komputerów. Wybierz tę opcję, aby zablokować dostęp do Internetu tylko dla urządzeń z adresami MAC uwzględnionymi na liście w tabeli. Urządzenia z innymi adresami MAC będą mieć dostęp do Internetu. ■ Zezwalanie na dostęp do sieci bezprzewodowej przez wymienione poniżej komputery. Wybierz tę opcję, aby zezwolić na dostęp do Internetu tylko urządzeniom z adresami MAC uwzględnionymi na liście w tabeli. Wszystkie urządzenia z adresami MAC, których nie ma na liście w tabeli, będą mieć zablokowany dostęp do Internetu.
Lista filtru adresów MAC	**Lista filtru adresów MAC** Lista filtru adresów MAC obejmuje użytkowników, których dostęp do sieci bezprzewodowej chcesz kontrolować. Kliknij przycisk **Lista klientów bezprzewodowych**, aby wyświetlić listę użytkowników sieci według ich adresów MAC. Menu rozwijane Sortowanie wg umożliwia sortowanie tabeli według adresu IP, adresu MAC, statusu, interfejsu lub nazwy klienta. Kliknij przycisk Odśwież, aby wyświetlić najbardziej aktualne informacje.

Dostęp bezprzewodowy > Ustawienia zaawansowane

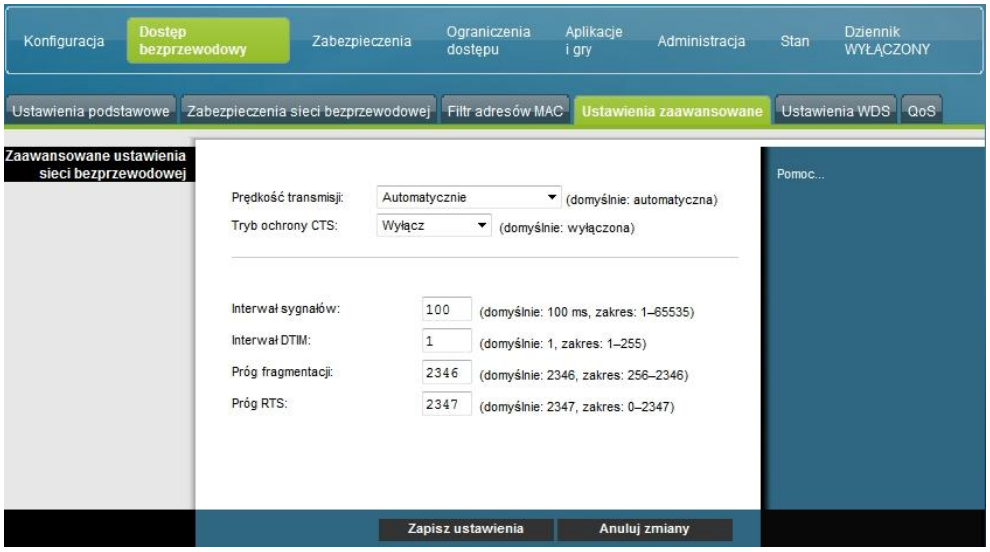
Ustawienia zaawansowane sieci bezprzewodowej zapewniają kolejną warstwę zabezpieczeń sieci bezprzewodowej obsługiwanej przez używaną bramę domową. Ta strona służy do konfigurowania zaawansowanych funkcji połączeń bezprzewodowych. Tylko doświadczony administrator powinien zmieniać te ustawienia. Wprowadzenie niepoprawnych ustawień może zmniejszyć wydajność połączeń bezprzewodowych.

Wybierz opcję **Ustawienia zaawansowane**, aby przejść do strony Dostęp bezprzewodowy > Ustawienia zaawansowane.

Ta strona umożliwia skonfigurowanie następujących opcji:

- Prędkość transmisji
- Tryb ochrony CTS
- Interwał sygnałów
- Interwał DTM

- Próg fragmentacji
- Próg RTS



Opis strony Dostęp bezprzewodowy > Ustawienia zaawansowane

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji ustawień zaawansowanych sieci bezprzewodowej obsługiwanej przez używaną bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

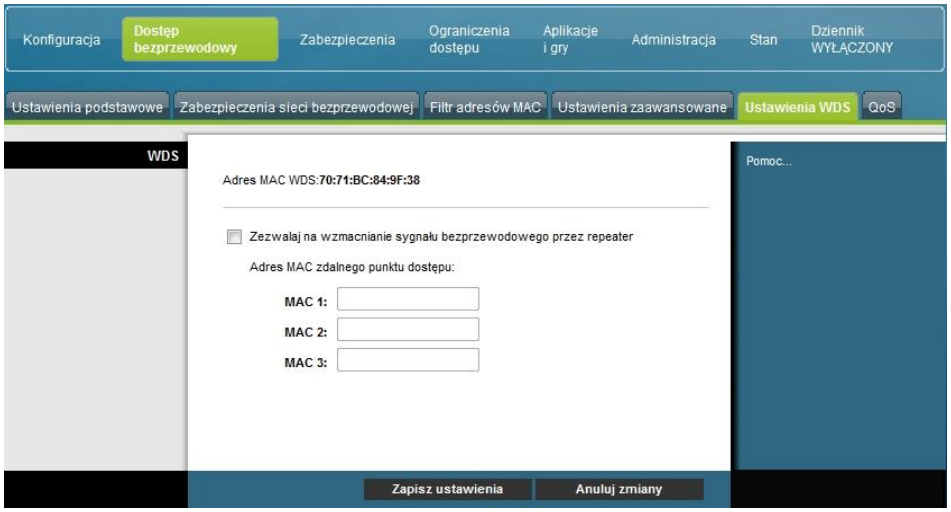
Sekcja	Opis pola
Zaawansowane ustawienia sieci bezprzewodowej	**Prędkość transmisji** Podczas ustawiania prędkości transmisji danych należy uwzględnić szybkość sieci Wireless-N. Wybierz jedną z dostępnych prędkości transmisji lub zaznacz opcję **Automatycznie**, aby urządzenie automatycznie używało najwyższej dostępnej prędkości. Zostanie włączona funkcja Auto-Fallback. Funkcja Auto-Fallback negocjuje najlepszą dostępną prędkość połączenia między urządzeniem a klientem bezprzewodowym. Domyślne ustawienie fabryczne to **Automatycznie**. Wybierz jedną z następujących opcji szybkości transmisji: ■ Automatycznie (ustawienie fabryczne) ■ Użyj starszego trybu ■ 0: 6,5 Mb/s lub 13,5 Mb/s ■ 1: 13 Mb/s lub 27 Mb/s ■ 2: 19,5 Mb/s lub 40,5 Mb/s ■ 3: 26 Mb/s lub 54 Mb/s ■ 4: 39 Mb/s lub 81 Mb/s ■ 5: 52 Mb/s lub 108 Mb/s ■ 6: 58,5 Mb/s lub 121,5 Mb/s ■ 7: 65 Mb/s lub 135 Mb/s ■ 8: 13 Mb/s lub 27 Mb/s ■ 9: 26 Mb/s lub 54 Mb/s ■ 10: 39 Mb/s lub 81 Mb/s ■ 11: 52 Mb/s lub 108 Mb/s ■ 12: 78 Mb/s lub 162 Mb/s ■ 13: 104 Mb/s lub 216 Mb/s ■ 14: 117 Mb/s lub 243 Mb/s ■ 15: 130 Mb/s lub 270 Mb/s
	Tryb ochrony CTS Tryb ochrony CTS (Clear-To-Send) znacznie zwiększa możliwości urządzenia w zakresie przechwytywania wszystkich transmisji bezprzewodowych, ale może powodować duże obniżenie wydajności. Wybierz opcję **Automatycznie**, aby używać tej funkcji, gdy jest potrzebna, tzn. gdy produkty sieciowe Wireless-N/G nie są w stanie transmitować danych do urządzenia w środowisku o dużym natężeniu ruchu 802.11b. Wybierz opcję **Wyłącz**, aby na stałe wyłączyć tę funkcję.

Sekcja	Opis pola
	Interwał sygnałów Wartość interwału sygnałów wskazuje częstotliwość wysyłania sygnałów identyfikacyjnych. Wysyłanie sygnałów identyfikacyjnych oznacza rozsyłanie przez urządzenie pakietów w celu zsynchronizowania sieci bezprzewodowej. (domyślnie: 100 ms, zakres: 20–1000)
	Interwał DTIM Opcja DTIM (Delivery Traffic Indication Message) służy do określenia interwału między transmisjami Broadcast/Multicast. Pole DTIM jest licznikiem informującym klientów z następnego okna o słuchaniu komunikatów typu broadcast i multicast. Gdy w buforze urządzenia zostaną zgromadzone komunikaty broadcast lub multicast, które są przeznaczone dla powiązanych klientów, urządzenie to wyśle następny komunikat DTIM z wartością interwału DTIM. Po odebraniu sygnałów identyfikacyjnych klienci odbierają komunikaty broadcast i multicast. (domyślnie: 1, zakres: 1–255)
	Próg fragmentacji Wartość progu fragmentacji określa maksymalny rozmiar pakietu, powyżej którego dane rozdzielane są na wiele pakietów. W razie wystąpienia dużej liczby błędów pakietów można nieznacznie podnieść wartość progu fragmentacji. Zbyt mała wartość tego parametru może spowodować słabą wydajność sieci. Zalecane jest tylko niewielkie zmniejszenie wartości domyślnej. W większości przypadków należy pozostawić wartość domyślną, równą 2346.
	Próg RTS Wartość progu RTS określa rozmiar pakietu, powyżej którego ma być stosowany mechanizm RTS/CTS (Ready-To-Send/Clear-To-Send). W przypadku wystąpienia nierównomiernego przepływu danych zalecane jest jedynie niewielkie zmniejszenie wartości domyślnej tego parametru, równej 2346. Jeśli rozmiar pakietu sieciowego jest mniejszy niż wstępnie ustawiony rozmiar progu RTS, mechanizm RTS/CTS nie zostanie włączony. Urządzenie wysyła ramki RTS (Request to Send) do określonej stacji odbiorczej i negocjuje wysłanie ramki danych. Po odebraniu ramki RTS stacja bezprzewodowa odpowiada ramką CTS (Clear to Send), aby potwierdzić prawo do rozpoczęcia transmisji. Wartość progu RTS powinna pozostać na poziomie domyślnym, równym 2347.

Dostęp bezprzewodowy > Ustawienia WDS

Strona ustawień systemu WDS (Wireless Distribution System) umożliwia poszerzenie zasięgu sieci bezprzewodowej dzięki zastosowaniu repeaterów sygnału. Upewnij się, że ustawienia kanału są takie same dla wszystkich urządzeń z funkcją WDS.

Wybierz kartę **Ustawienia WDS**, aby przejść do strony Dostęp bezprzewodowy > Ustawienia WDS. Ta strona umożliwia skonfigurowanie ustawień systemu WDS.



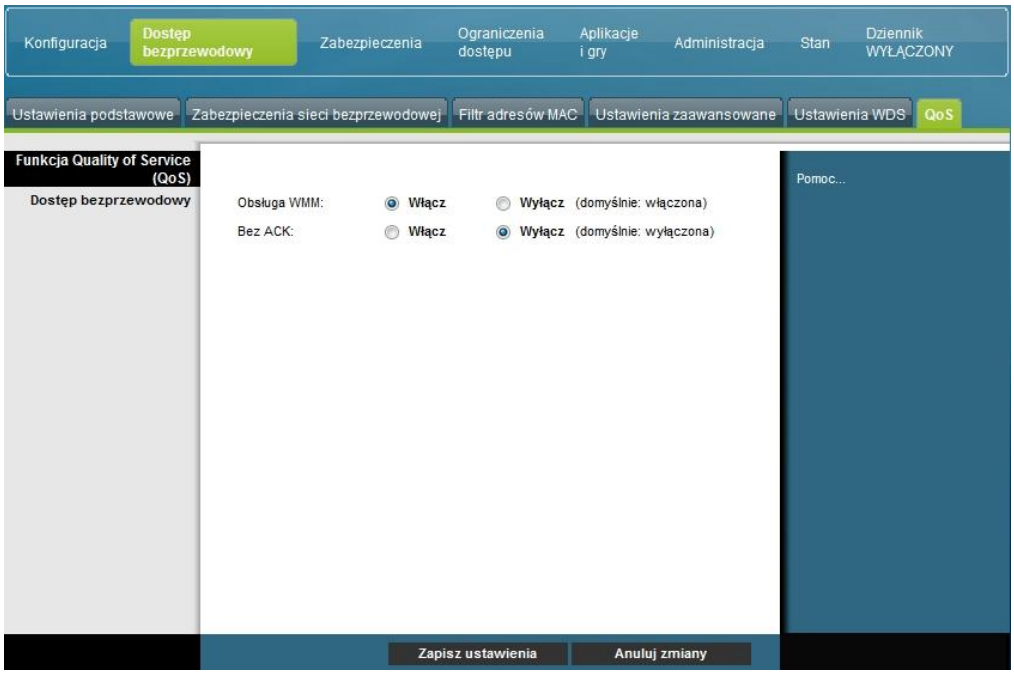
Opis strony Dostęp bezprzewodowy > Ustawienia WDS

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji ustawień systemu dystrybucji sygnału sieci bezprzewodowej obsługiwanej przez używaną bramę domową. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
WDS	**Adres MAC WDS** Wyświetla adres MAC WDS (lub identyfikator BSSID) używanego punktu dostępu bramy.
	Zezwalaj na wzmacnianie sygnału bezprzewodowego przez repeater Zaznacz to pole wyboru, aby zezwalać klientom bezprzewodowym na łączenie się z repeaterem i przekazywanie ruchu między klientem bezprzewodowym a repeaterem. Dozwolone są maksymalnie 3 repeatery.
	Adres MAC zdalnego punktu dostępu (MAC 1–3) Użyj trzech pól (MAC 1, 2 i 3), aby wprowadzić adresy MAC repeaterów.

Dostęp bezprzewodowy > QoS

Usługa Quality of Service (QoS) zapewnia wyższy poziom obsługi ruchu sieciowego o wysokim priorytecie, który może wiązać się z wymagającymi aplikacjami działającymi w czasie rzeczywistym, takimi jak wideokonferencje. Ustawienia usługi QoS umożliwiają określenie priorytetów różnych rodzajów ruchu. Ruch o niższym priorytecie zostanie spowolniony, aby umożliwić zwiększenie przepustowości ruchu o wysokim priorytecie lub zmniejszenie jego opóźnienia. Wybierz kartę **QoS**, aby przejść do strony Dostęp bezprzewodowy > QoS.



Opis strony Dostęp bezprzewodowy > QoS

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji poszczególnych ustawień usługi QoS. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Funkcja Quality of Service (QoS) Dostęp bezprzewodowy	**Obsługa WMM** Jeśli klienci bezprzewodowi obsługują standard WMM (Wi-Fi Multimedia), ruch związany z przesyłaniem głosu i multimediów otrzyma wyższy priorytet niż pozostałe rodzaje ruchu. Wybierz żądaną opcję: ■ **Włącz** (domyślne ustawienie fabryczne) ■ **Wyłącz**

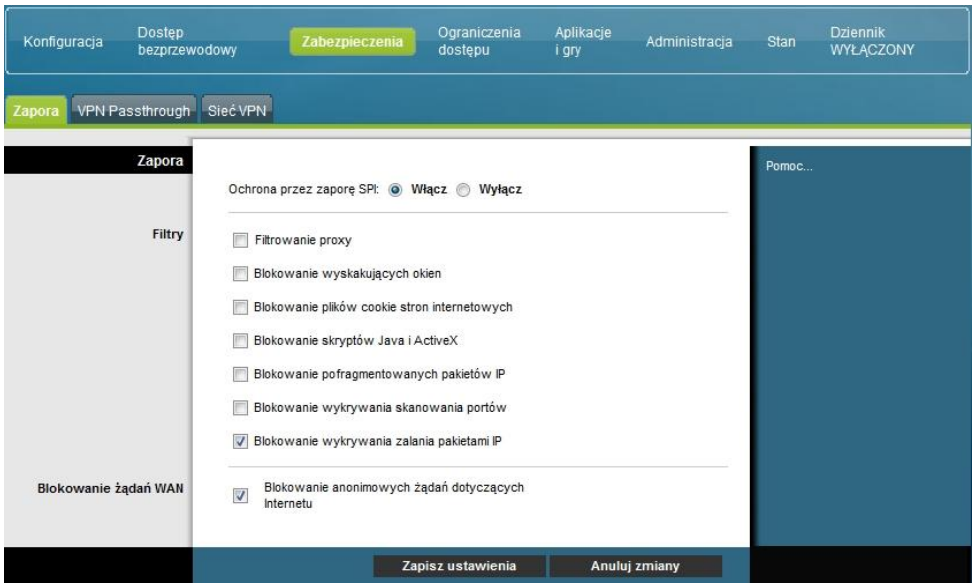
Sekcja	Opis pola
	Bez ACK Umożliwia włączenie lub wyłączenie funkcji Bez ACK. Zaleca się włączenie tej funkcji dla usług danych, dla których istotna jest transmisja, a utratę pakietów można do pewnego stopnia tolerować. Wybranie opcji **Wyłącz** spowoduje zwrócenie pakietu potwierdzenia za każdy otrzymany pakiet. Podnosi to niezawodność transmisji, ale zarazem zwiększa ruch, co powoduje obniżenie wydajności. Wybierz żądaną opcję: ■ **Włącz** ■ **Wyłącz** (domyślne ustawienie fabryczne)

Konfigurowanie zabezpieczeń

Zabezpieczenia > Zapora

Zaawansowana technologia zapory chroniąca sieć domową przed hakerami i przed nieautoryzowanym dostępem. Ta strona służy do konfigurowania zapory, która może filtrować różne rodzaje niepożądanego ruchu w sieci lokalnej obsługiwanej przez bramę.

Wybierz kartę **Zapora**, aby przejść do strony Zabezpieczenia > Zapora.



Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji zapory bramy domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

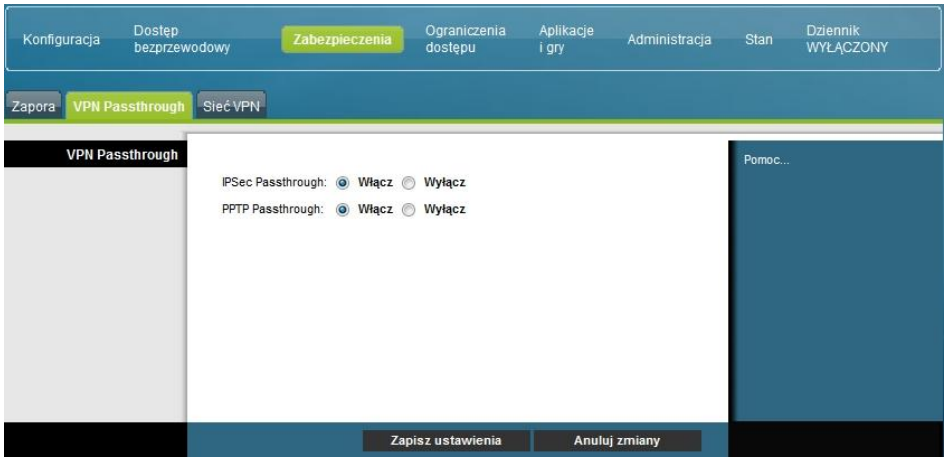
Sekcja	Opis pola
Zapora	**Ochrona przez zaporę SPI** Funkcja ochrony przez zaporę SPI blokuje ataki typu Denial of Service (DoS). Ataki DoS nie mają na celu kradzieży danych ani zniszczenia komputerów, ale powodują przeciążenie połączenia z Internetem, uniemożliwiając korzystanie z niego. Wybierz żądaną opcję: ■ **Włącz** (domyślne ustawienie fabryczne) ■ **Wyłącz**

Sekcja	Opis pola
Filtry	**Filtrowanie proxy** Włącza/wyłącza filtrowanie proxy. Jeśli użytkownicy lokalni mają dostęp do serwerów proxy sieci WAN, mogą ominąć filtry zawartości i uzyskać dostęp do witryn internetowych zablokowanych przez urządzenie. Po wybraniu funkcji Filtrowanie proxy zostanie zablokowany dostęp do wszystkich serwerów proxy w sieci WAN. **Blokowanie wyskakujących okien** Włącza/wyłącza wyskakujące okna. Podczas działania niektórych typowych aplikacji są wyświetlane wyskakujące okna. Wyłączenie wyskakujących okien może wpłynąć na działanie niektórych z nich. **Blokowanie plików cookie stron internetowych** Włącza/wyłącza blokowanie plików cookie. Ta funkcja filtruje przesyłanie niechcianych plików cookie z Internetu na urządzenia w prywatnej sieci lokalnej. Pliki cookie to pliki komputerowe zawierające dane osobowe lub informacje o przeglądanych stronach. **Blokowanie skryptów Java i ActiveX** Włącza/wyłącza aplety Java i skrypty ActiveX. Ta funkcja ułatwia ochronę urządzeń działających w prywatnej sieci przed irytującymi lub złośliwymi apletami Java wysyłanymi na urządzenia z Internetu bez zgody użytkowników. Po odebraniu przez komputer te aplety są uruchamiane automatycznie. Java to język programowania przeznaczony do tworzenia witryn internetowych. Wybranie funkcji Filtrowanie apletów Java może spowodować utratę dostępu do witryn internetowych utworzonych przy użyciu tego języka. Ta funkcja ułatwia też ochronę urządzeń działających w prywatnej sieci przed irytującymi lub złośliwymi formantami ActiveX wysyłanymi na urządzenia z Internetu bez zgody użytkowników. Po odebraniu przez komputer te formanty są uruchamiane automatycznie. **Blokowanie pofragmentowanych pakietów IP** Włącza/wyłącza filtrowanie pofragmentowanych pakietów IP. Ta funkcja ułatwia ochronę prywatnej sieci lokalnej przed atakami typu Denial of Service (DoS) przeprowadzanymi z Internetu. **Blokowanie wykrywania skanowania portów** Określa, czy brama będzie reagować na przeprowadzane z Internetu skanowania portów. Ta funkcja została opracowana w celu ochrony prywatnej sieci lokalnej przed hakerami próbującymi uzyskać nieuprawniony dostęp do sieci przez Internet, wykrywając porty IP otwarte na używanej bramie. **Blokowanie wykrywania zalania pakietami IP** (zaznaczone — domyślne ustawienie fabryczne) Blokuje złośliwe urządzenia próbujące zalać urządzenia lub sieci nieprawidłowymi pakietami typu broadcast. Taka sytuacja jest też nazywana „burzą rozgłoszeniową”.

Sekcja	Opis pola
Blokowanie żądań WAN	**Blokowanie anonimowych żądań dotyczących Internetu** (zaznaczone - domyślne ustawienie fabryczne) Włączenie tej funkcji zapobiega „pingowaniu" sieci lub jej wykrywaniu przez innych użytkowników Internetu. Funkcja Blokowanie anonimowych żądań dotyczących Internetu ukrywa także porty sieciowe. Obie funkcje utrudniają wniknięcie do sieci użytkownikom z zewnątrz.

Zabezpieczenia > VPN Passthrough

Ta strona umożliwia skonfigurowanie obsługi sieci VPN (Virtual Private Network). Włączenie ustawień na tej stronie umożliwia tworzenie tuneli VPN przy użyciu protokołów IPSec lub PPTP, służących do pokonywania zapory bramy. Wybierz kartę **VPN Passthrough**, aby przejść do strony Zabezpieczenia > VPN Passthrough.



Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania funkcji VPN Passthrough bramy domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
VPN Passthrough	**IPSec Passthrough** Włącza/wyłącza IPSec (Internet Protocol Security). IPSec to zestaw protokołów służących do implementacji bezpiecznej wymiany pakietów w warstwie IP. Po włączeniu funkcji IPSec Passthrough aplikacje korzystające z IPsec mogą pokonać zaporę. Aby wyłączyć tę funkcję, wybierz opcję **Wyłącz**. Wybierz żądaną opcję: ■ **Włącz** (domyślne ustawienie fabryczne) ■ **Wyłącz**

Sekcja	Opis pola
	PPTP Passthrough Włącza/wyłącza protokół PPTP (Point-to-Point Tunneling Protocol). Protokół PPTP umożliwia tunelowanie PPP w sieci IP. Po włączeniu funkcji PPTP Passthrough aplikacje korzystające z protokołu PPTP (Point to Point Tunneling Protocol) mogą pokonać zaporę. Aby wyłączyć tę opcję, wybierz opcję **Wyłącz**. Wybierz żądaną opcję: ■ **Włącz** (domyślne ustawienie fabryczne) ■ **Wyłącz**

Zabezpieczenia > Sieć VPN

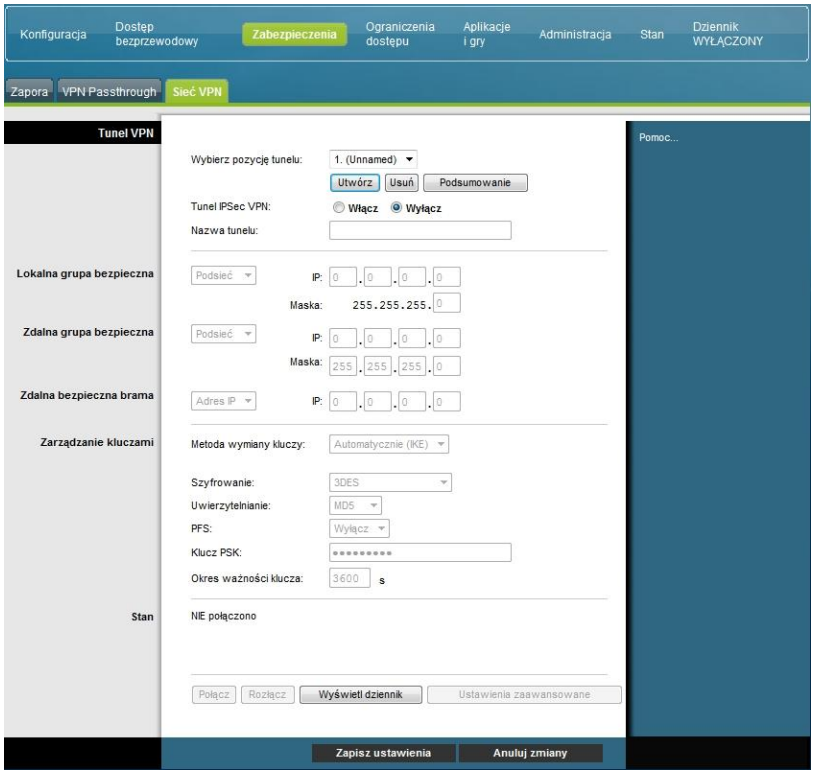
Sieć VPN (Virtual Private Network) to połączenie między dwoma punktami końcowymi znajdującymi się w różnych sieciach, umożliwiające bezpieczne wysyłanie prywatnych danych przez sieci publiczne lub inne sieci prywatne. Jest to realizowane przez utworzenie „tunelu VPN". Tunel VPN łączy dwa komputery lub dwie sieci i umożliwia przesyłanie danych przez Internet tak, jakby były przesyłane w sieci prywatnej. Tunel VPN używa zabezpieczeń IPSec do szyfrowania danych przesyłanych między dwoma punktami końcowymi, umieszczając dane w zwykłej ramce Ethernet/IP oraz umożliwiając bezpieczne i bezproblemowe przekazywanie danych między sieciami.

Sieć VPN to ekonomiczna i bezpieczniejsza opcja niż użycie prywatnego, dedykowanego łącza dzierżawionego do utworzenia sieci prywatnej. W ramach sieci VPN z zabezpieczeniami IPSec przy użyciu standardowych w branży technik szyfrowania i uwierzytelniania tworzone jest bezpieczne połączenie działające tak, jak bezpośrednie połączenie z prywatną siecią lokalną.

Na przykład, sieć VPN umożliwia użytkownikom pozostanie w domach i łączenie się z siecią przedsiębiorstwa pracodawcy oraz otrzymywanie adresów IP w ich sieciach prywatnych dokładnie tak, jak gdyby siedzieli w swoich biurach i łączyli się z siecią LAN przedsiębiorstwa.

Wybierz kartę **Sieć VPN**, aby przejść do strony Zabezpieczenia > Sieć VPN.

Ta strona umożliwia skonfigurowanie sieci VPN dla bramy domowej.



Opis strony Zabezpieczenia > Tunel VPN

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji tunelu VPN dla bramy domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Tunel VPN	**Wybierz pozycję tunelu** Umożliwia wyświetlenie listy utworzonych tuneli VPN. **Przycisk Utwórz** Kliknij ten przycisk, aby utworzyć nowy tunel. **Przycisk Usuń** Kliknij ten przycisk, aby usunąć wszystkie ustawienia zaznaczonego tunelu. **Przycisk Podsumowanie** Kliknij ten przycisk, aby wyświetlić ustawienia i stan wszystkich włączonych tuneli. **Tunel IPSec VPN** Umożliwia włączenie lub wyłączenie zabezpieczeń IPSec dla tunelu VPN. **Nazwa tunelu** Wprowadź nazwę tego tunelu.

Sekcja	Opis pola
Lokalna grupa bezpieczna	Wybierz użytkowników sieci LAN, którzy mogą korzystać z tego tunelu VPN. Może to być pojedynczy adres IP lub podsieć. Należy pamiętać, że lokalnej grupie bezpiecznej musi odpowiadać zdalna grupa bezpieczna zdalnej bramy. **IP** Wprowadź adres IP z sieci lokalnej. **Maska** Jeśli opcja Podsieć jest zaznaczona, wprowadź maskę w celu określenia adresu IP w sieci lokalnej.
Zdalna grupa bezpieczna	Wybierz użytkowników ze zdalnej sieci LAN, znajdujących się za zdalną bramą, którzy mogą używać tego tunelu VPN. Może to być pojedynczy adres IP, podsieć lub dowolne adresy. Jeśli ustawiono opcję „Dowolny", brama działa jako urządzenie odpowiadające i akceptuje żądania od wszystkich zdalnych użytkowników. Należy pamiętać, że zdalnej grupie bezpiecznej musi odpowiadać lokalna grupa bezpieczna zdalnej bramy. **IP** Wprowadź adres IP sieci zdalnej. **Maska** Jeśli opcja Podsieć jest zaznaczona, wprowadź maskę w celu określenia adresów IP w sieci zdalnej.
Zdalna bezpieczna brama	Wybierz żądaną opcję: **Adres IP**, **Dowolny** lub **FQDN**. Jeśli zdalna brama ma dynamiczny adres IP, wybierz opcję **Dowolny** lub **FQDN**. Jeśli wybrano opcję **Dowolny**, brama będzie akceptować żądania z dowolnego adresu IP. **FQDN** Jeśli wybrano opcję **FQDN**, wprowadź nazwę domeny zdalnej bramy, aby można było w bramie domowej sprawdzić bieżący adres IP przy użyciu usługi DDNS. **IP** Podany w tym polu adres IP musi być zgodny z publicznym adresem IP (adresem internetowym lub sieci WAN) zdalnej bramy znajdującej się na drugim końcu tunelu.
Zarządzanie kluczami	**Metoda wymiany kluczy** Brama domowa obsługuje zarówno automatyczne, jak i ręczne zarządzanie kluczami. Jeśli zostanie wybrane automatyczne zarządzanie kluczami, do negocjacji materiału klucza dla bezpiecznego połączenia (SA, Security Association) używane są protokoły IKE (Internet Key Exchange). Jeśli wybrane zostanie ręczne zarządzanie kluczami, negocjacja kluczy jest niepotrzebna. Ręczne zarządzanie kluczami stosuje się zasadniczo w małych, statycznych środowiskach oraz podczas rozwiązywania problemów. Należy pamiętać, że obie strony muszą używać tej samej metody zarządzania kluczami.

Sekcja	Opis pola
Zarządzanie kluczami (ciąg dalszy)	Wybierz jedną z następujących metod wymiany kluczy: ■ **Automatycznie (IKE)** – **Szyfrowanie**: Metoda szyfrowania określa długość klucza używanego do szyfrowania/odszyfrowywania pakietów ESP. Należy pamiętać, że obie strony muszą używać tej samej metody. – **Uwierzytelnianie**: Metoda uwierzytelniania określa sposób uwierzytelniania pakietów ESP (Encapsulating Security Payload). Wybierz metodę **MD5** lub **SHA**. Należy pamiętać, że obie strony (punkty końcowe sieci VPN) muszą używać tej samej metody. ▪ MD5: jednokierunkowy algorytm mieszania generujący skrót 128-bitowy ▪ SHA: jednokierunkowy algorytm mieszania generujący skrót 160-bitowy – **Funkcja PFS (Perfect Forward Secrecy)**: Włączenie funkcji PFS powoduje, że negocjacja 2 fazy IKE generuje nowy materiał klucza na potrzeby szyfrowania ruchu IP i uwierzytelniania. Należy pamiętać, że obie strony muszą włączyć funkcję PFS. – **Klucz PSK**: W ramach IKE do uwierzytelniania zdalnego punktu równorzędnego IKE używany jest klucz PSK. W tym polu dopuszczalne są znaki i wartości szesnastkowe, np. „My_@123” lub „0x4d795f40313233”. Należy pamiętać, że obie strony muszą używać tego samego klucza PSK. – **Okres ważności klucza**: W tym polu podaje się okres ważności klucza generowanego przez IKE. Po upływie wyznaczonego czasu automatycznie następuje ponowna negocjacja klucza. Okres ważności może mieć wartość od 300 do 100 000 000 sekund. Domyślna wartość okresu ważności to **3600** sekund. ■ **Ręcznie** – **Szyfrowanie**: Metoda szyfrowania określa długość klucza używanego do szyfrowania/odszyfrowywania pakietów ESP. Należy pamiętać, że obie strony muszą używać tej samej metody. – **Klucz szyfrowania**: W tym polu należy podać klucz używany do szyfrowania i odszyfrowywania ruchu IP. Dopuszczalne są w nim znaki i wartości szesnastkowe. Należy pamiętać, że obie strony muszą używać tego samego klucza szyfrowania. – **Uwierzytelnianie**: Metoda uwierzytelniania określa sposób uwierzytelniania pakietów ESP (Encapsulating Security Payload). Wybierz metodę MD5 lub SHA. Należy pamiętać, że obie strony (punkty końcowe sieci VPN) muszą używać tej samej metody. ▪ MD5: jednokierunkowy algorytm mieszania generujący skrót 128-bitowy ▪ SHA: jednokierunkowy algorytm mieszania generujący skrót 160-bitowy – **Klucz uwierzytelniania**: W tym polu podaje się klucz używany do uwierzytelniania ruchu IP. Dopuszczalne są w nim znaki i wartości szesnastkowe. Należy pamiętać, że obie strony muszą używać tego samego klucza uwierzytelniania. – **SPI wchodzące/wychodzące**: Identyfikator SPI (Security Parameter Index) jest przekazywany w nagłówku pakietów ESP. Dzięki temu odbiorca może wybrać SA, zgodnie z którym dany pakiet ma być przetwarzany. Indeks SPI jest wartością 32-bitową. Dopuszczalne są znaki i liczby szesnastkowe. np. „987654321” lub „0x3ade68b1”. Każdy tunel musi mieć unikatowy indeks SPI dla ruchu wchodzącego i wychodzącego. Nie mogą istnieć dwa tunele z takim samym indeksem SPI. Należy pamiętać, że indeks SPI dla ruchu wchodzącego musi być zgodny z indeksem SPI dla ruchu

Sekcja	Opis pola
Stan	W tym polu widoczny jest stan połączenia dla wybranego tunelu. Stan może przyjmować wartość **Połączono** lub **Rozłączono**.
Przyciski	**Połącz** Kliknij ten przycisk, aby ustanowić połączenie dla bieżącego tunelu VPN. Jeśli wprowadzono zmiany, najpierw kliknij **Zapisz ustawienia**, aby je zastosować. **Rozłącz** Kliknij ten przycisk, aby przerwać połączenie dla bieżącego tunelu VPN. **Wyświetl dziennik** Kliknij ten przycisk, aby wyświetlić dziennik VPN, który zawiera szczegółowe informacje o każdym ustanowionym tunelu. **Ustawienia zaawansowane** Jeśli wybrana metoda wymiany kluczy to Automatycznie (IKE), przycisk ten umożliwia dostęp do dodatkowych ustawień związanych z IKE. Kliknij ten przycisk, jeśli z bramy nie można ustanowić tunelu VPN do zdalnej bramy, a następnie sprawdź, czy ustawienia zaawansowane odpowiadają ustawieniom zdalnej bramy. ■ **Faza 1 — tryb działania** Wybierz metodę odpowiednią dla zdalnego punktu końcowego VPN. – **Główny**: ten tryb jest wolniejszy, ale zapewnia wyższy poziom bezpieczeństwa. – **Agresywny**: ten tryb jest szybszy, ale mniej bezpieczny. ■ **Tożsamość lokalna** Wybierz odpowiednią opcję, tak aby była zgodna z ustawieniem tożsamości zdalnej na drugim końcu tunelu. – Lokalny adres IP: adres IP sieci WAN (Internetu) – Nazwa: nazwa domeny ■ **Tożsamość zdalna** Wybierz odpowiednią opcję, tak aby była zgodna z ustawieniem tożsamości lokalnej na drugim końcu tunelu. – Lokalny adres IP: adres IP sieci WAN (Internetu) zdalnego końca VPN – Nazwa: nazwa domeny zdalnego końca VPN ■ **Szyfrowanie** Jest to algorytm szyfrowania używany dla SA IKE. Musi odpowiadać ustawieniu użytemu na drugim końcu tunelu.

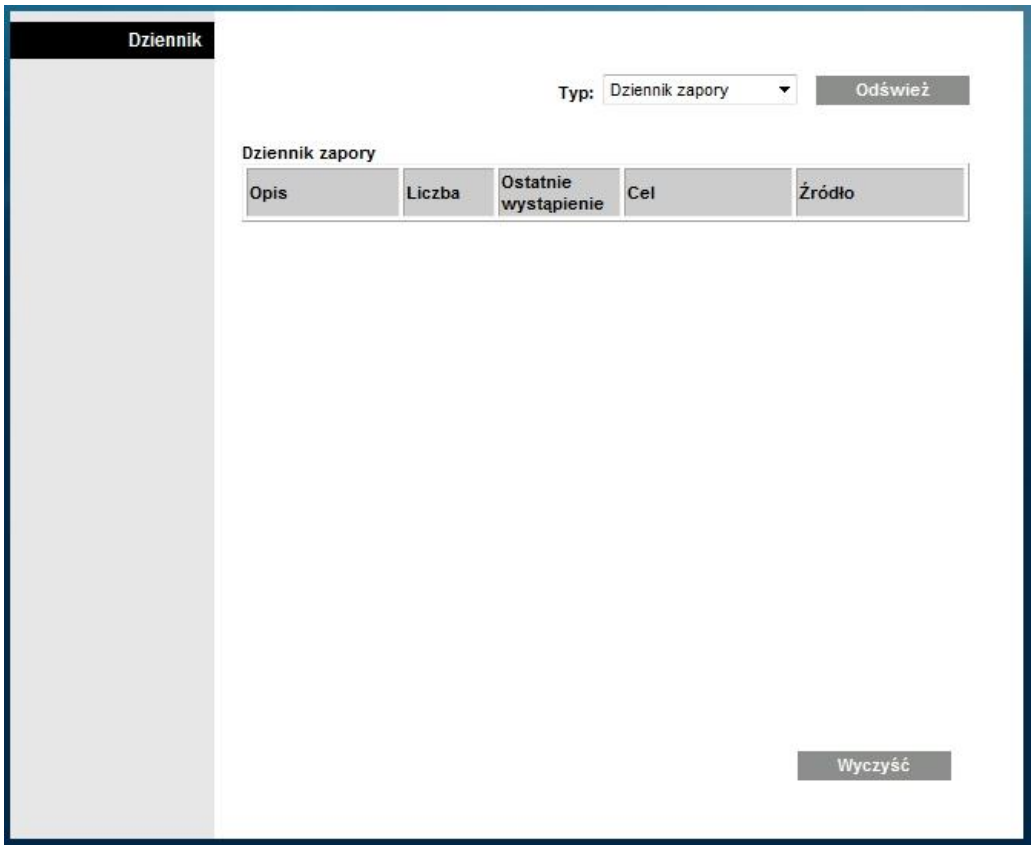
Wyświetl dziennik

Na stronie dziennika sieci VPN są wyświetlane zdarzenia przechwycone przez zaporę. Dziennik zawiera następujące informacje:

- opis zdarzenia;
- liczbę zdarzeń, które wystąpiły;
- ostatnie wystąpienie zdarzenia;
- adresy docelowe i źródłowe.

Na tej stronie można wyświetlić następujące dzienniki:

- Dziennik dostępu
- Dziennik zapory
- Dziennik VPN
- Dziennik kontroli rodzicielskiej



Kliknij przycisk **Wyczyść**, aby wyczyścić dane dziennika.

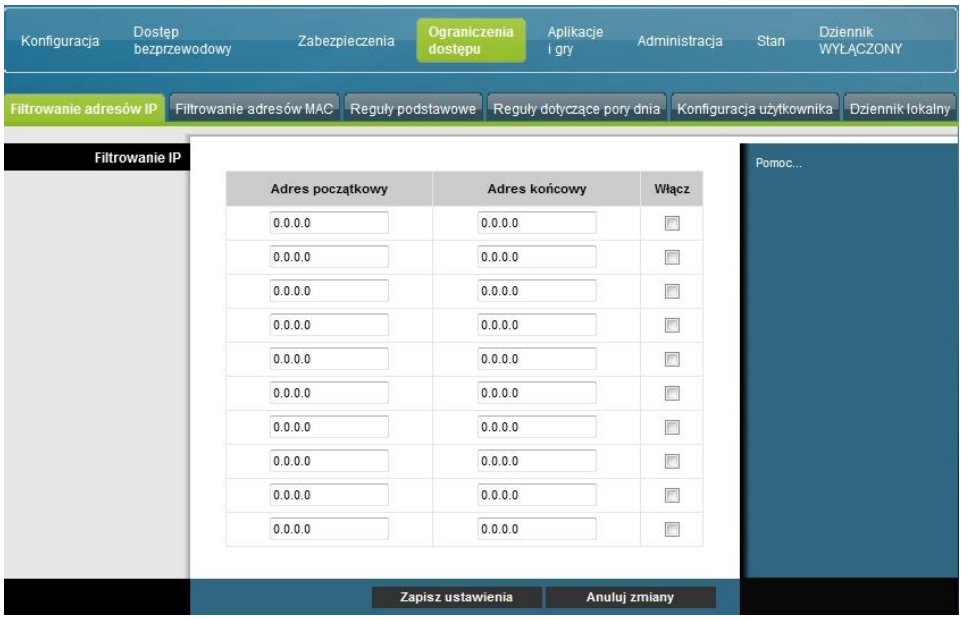
Kontrola dostępu do bramy

Ograniczenia dostępu > Filtrowanie adresów IP

Strona funkcji filtrowania adresów IP umożliwia skonfigurowanie filtrów adresów IP. Filtry te umożliwiają blokowanie dostępu do Internetu zakresowi adresów IP.

Uwaga: Jeśli po raz pierwszy używasz zaawansowanych ustawień szczegółowo opisanych w tej sekcji, skontaktuj się z usługodawcą przed zmianą jakichkolwiek zaawansowanych ustawień filtrowania adresów IP bramy sieci bezprzewodowej.

Wybierz kartę **Filtrowanie adresów IP**, aby przejść do strony Ograniczenia dostępu > Filtrowanie adresów IP. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

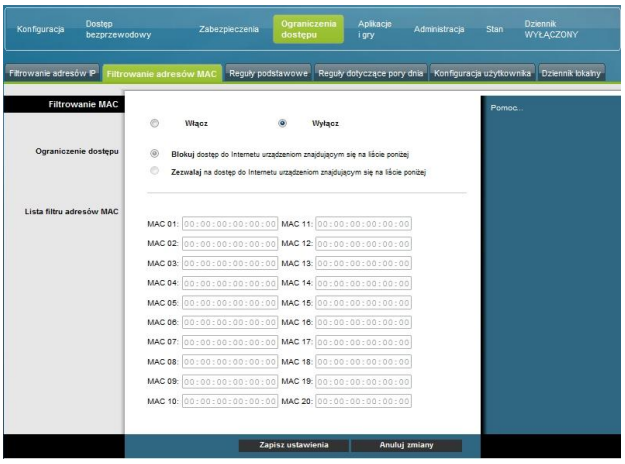


Ograniczenia dostępu > Filtrowanie adresów MAC

Strona funkcji filtrowania adresów MAC umożliwia skonfigurowanie filtrów adresów MAC. Filtry te umożliwiają blokowanie dostępu do Internetu zakresowi adresów MAC.

Uwaga: Jeśli po raz pierwszy używasz zaawansowanych ustawień szczegółowo opisanych w tej sekcji, skontaktuj się z usługodawcą przed zmianą jakichkolwiek zaawansowanych ustawień filtrowania adresów IP bramy sieci bezprzewodowej.

Wybierz kartę **Filtrowanie adresów MAC**, aby przejść do strony Ograniczenia dostępu > Filtrowanie adresów MAC.



Menu rozwijane Blokuj/Zezwalaj umożliwia blokowanie dostępu do Internetu lub zezwalanie na taki dostęp urządzeniom o adresach wymienionych w tabeli filtrów adresów MAC. W następującej tabeli opisano funkcjonowanie menu rozwijanego Blokuj/Zezwalaj. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Nazwa pola	Opis
Filtrowanie adresów MAC	**Blokuj listę (ustawienie domyślne)** Wybierz opcję **Blokuj listę**, aby zablokować dostęp do Internetu tylko urządzeniom z adresami MAC uwzględnionymi na liście w tabeli. Urządzenia z innymi adresami MAC będą mieć dostęp do Internetu.
	Zezwalaj na listę Wybierz opcję **Zezwalaj na listę**, aby zezwolić na dostęp do Internetu tylko urządzeniom z adresami MAC uwzględnionymi na liście w tabeli. Wszystkie urządzenia z adresami MAC, których *nie ma* na liście w tabeli, będą mieć zablokowany dostęp do Internetu.

Klawisze funkcyjne

Na stronie Ustawienia zaawansowane — Filtrowanie adresów MAC dostępne są następujące klawisze funkcyjne.

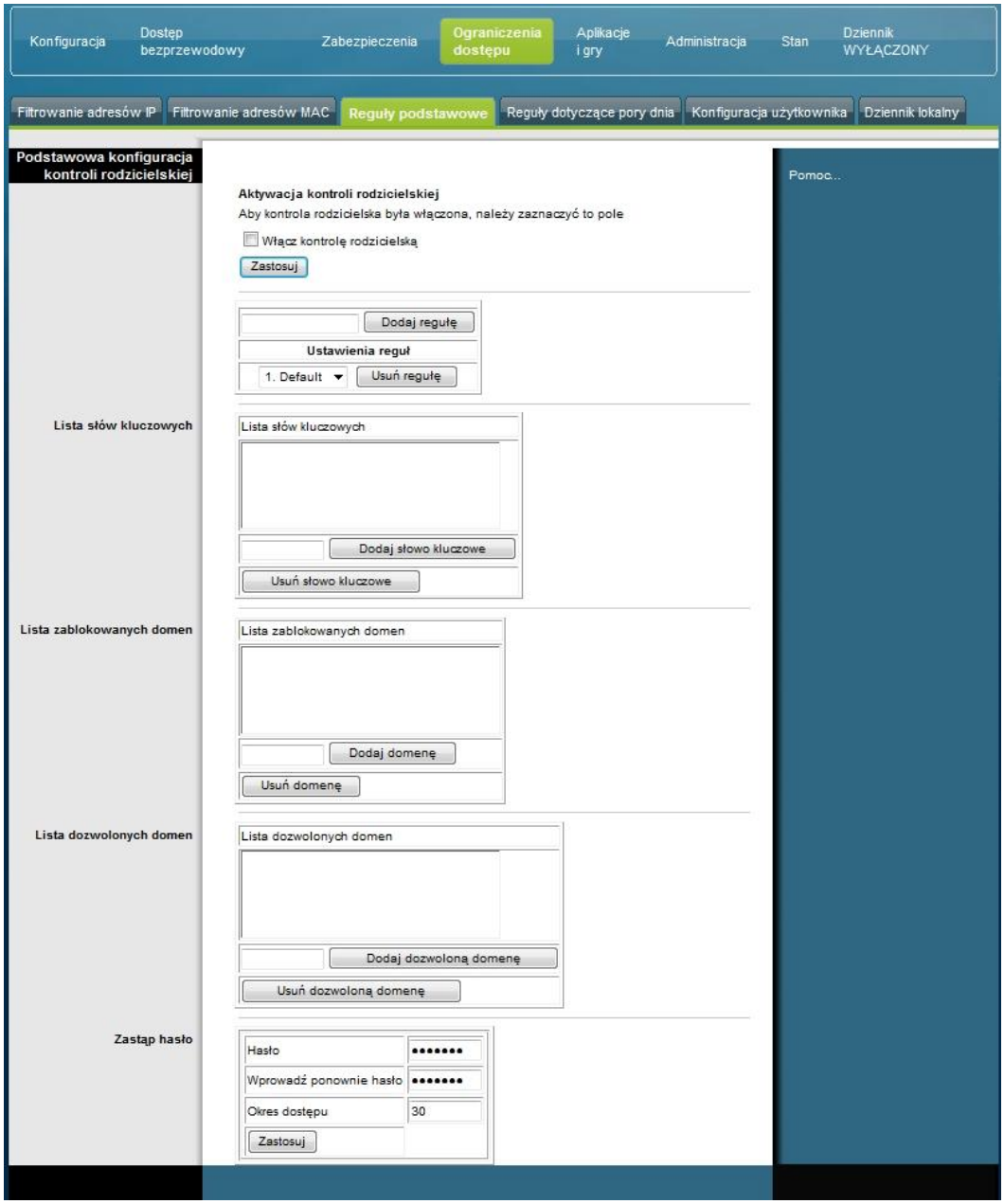
Klawisz	Opis
Zastosuj	Zapisuje wartości wprowadzone w polach bez zamykania strony.
Dodaj adres MAC	Zapisuje adres MAC wprowadzony w odpowiednim polu tekstowym.
Usuń adres MAC	Usuwa wybrany adres MAC.

Klawisz	Opis
Wyczyść wszystko	Usuwa wszystkie zdefiniowane adresy MAC.

Ograniczenia dostępu > Reguły podstawowe

Funkcja ograniczeń dostępu umożliwia zablokowanie lub dopuszczenie określonego sposobu wykorzystania Internetu oraz ruchu. Można zablokować dostęp do Internetu, określone aplikacje, witryny internetowe oraz ruch przychodzący w określonych dniach i godzinach. Strona reguł podstawowych ograniczeń dostępu służy do konfigurowania kontroli rodzicielskiej na bramie domowej oraz do monitorowania osób upoważnionych do wprowadzania ustawień kontroli rodzicielskiej.

Wybierz kartę **Reguły podstawowe**, aby przejść do strony Ograniczenia dostępu > Reguły podstawowe.



Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania reguł podstawowych ograniczeń dostępu dla bramy domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Podstawowa konfiguracja kontroli rodzicielskiej	**Aktywacja kontroli rodzicielskiej** Umożliwia włączenie lub wyłączenie kontroli rodzicielskiej. Aby włączyć kontrolę rodzicielską, zaznacz pole wyboru **Włącz kontrolę rodzicielską** i kliknij przycisk **Zastosuj**. Aby wyłączyć kontrolę rodzicielską, wyczyść pole wyboru **Włącz kontrolę rodzicielską** i kliknij przycisk **Zastosuj**. **Dodaj regułę** Dodaje nową regułę do listy reguł dotyczących zawartości i zapisuje ją. **Usuń regułę** Usuwa wybraną regułę z listy reguł dotyczących zawartości.
Lista słów kluczowych	**Lista słów kluczowych** Umożliwia utworzenie listy słów kluczowych. Każda próba uzyskania dostępu do adres URL zawierającego dowolne ze słów kluczowych z tej listy zostanie zablokowana przez bramę. **Dodaj/usuń słowo kluczowe** Umożliwia dodawanie nowych słów kluczowych do listy oraz ich usuwanie z listy.
Lista zablokowanych domen	**Lista zablokowanych domen** Umożliwia utworzenie listy domen, do których dostęp będzie blokowany przez bramę. Każda próba uzyskania dostępu do dowolnej domeny z tej listy zostanie zablokowana przez bramę. **Dodaj/usuń domenę** Umożliwia dodawanie nowych domen do listy oraz ich usuwanie z listy.
Lista dozwolonych domen	**Lista dozwolonych domen** Umożliwia utworzenie listy domen, do których dostęp przez bramę będzie możliwy. **Dodaj/usuń dozwoloną domenę** Umożliwia dodawanie nowych domen do listy oraz ich usuwanie z listy.

Sekcja	Opis pola
Zastąp hasło	**Hasło** Umożliwia utworzenie hasła w celu tymczasowego zastąpienia ograniczeń dostępu użytkowników do zablokowanej witryny internetowej. **Wprowadź ponownie hasło** Wprowadź ponownie to samo hasło w celu potwierdzenia podanego w poprzednim polu hasła zastępującego ograniczenia. **Okres dostępu** Umożliwia określenie czasu (w minutach), przez który hasło nadrzędne będzie umożliwiać tymczasowy dostęp do witryny internetowej z ograniczeniami. **Zastosuj** Powoduje zapisanie wszystkich dodanych, edytowanych i zmienionych ustawień.

Korzystanie z funkcji blokowania słów kluczowych i domen

Funkcja blokowania słów kluczowych i domen umożliwia ograniczanie dostępu do witryn internetowych przez blokowanie dostępu na podstawie słów lub ciągów znaków zawartych w adresach URL używanych do uzyskania dostępu do tych witryn.

Funkcja blokowania domen umożliwia ograniczanie dostępu do witryn na podstawie ich nazw domen. Nazwa domeny to część adresu URL poprzedzająca typowe rozszerzenie, takie jak .COM, .ORG czy .GOV.

Funkcja blokowania słów kluczowych umożliwia blokowanie dostępu do witryn internetowych na podstawie słowa kluczowego lub ciągu znaków występujących w dowolnej części adresu URL — nie tylko w nazwie domeny.

Uwaga: Funkcja blokowania domen powoduje zablokowanie dostępu do wszystkich domen z listy. Powoduje też zablokowanie domen, dla których dowolna część nazwy pasuje dokładnie do pozycji na liście.

Na przykład po wprowadzeniu ciągu **example.com** jako domeny zostanie zablokowana każda witryna, której nazwa domeny zawiera ciąg „example.com”. Zwykle nie jest pożądane uwzględnianie w nazwie domeny ciągu „www.”, ponieważ powoduje to ograniczenie blokady tylko do witryn, których nazwa domeny zawiera dokładnie taki ciąg. Na przykład po dodaniu do listy pozycji www.example.com zablokowana zostanie tylko witryna, której nazwa domeny jest dokładnie taka, jak podany ciąg. Jeśli natomiast nie zostanie podany ciąg „www.”, zablokowane zostaną wszystkie witryny w obrębie domeny „example.com”.

Blokowanie dostępu do witryn internetowych

Do blokowania dostępu do witryn internetowych służą **Lista zablokowanych domen** oraz **Lista słów kluczowych**.

Aby użyć **Listy zablokowanych domen**, należy wprowadzić adresy URL lub nazwy domen witryn, które mają zostać zablokowane.

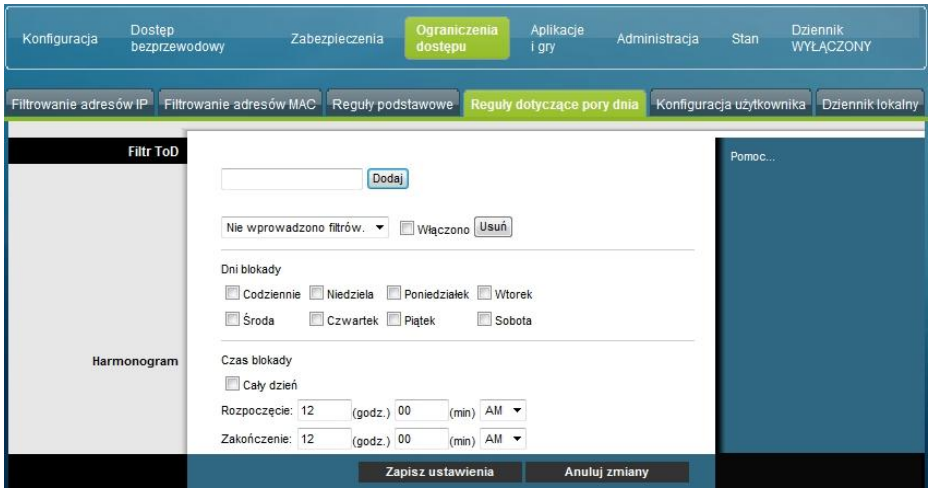
Lista słów kluczowych służy do wprowadzenia słów kluczowych, które mają zostać zablokowane. Jeśli którekolwiek z tych słów pojawi się w adresie URL witryny internetowej, dostęp do niej zostanie zablokowany. Należy pamiętać, że sprawdzany jest tylko adres URL, a nie zawartość poszczególnych stron.

Ograniczenia dostępu > Reguły dotyczące pory dnia

Strona reguł dotyczących pory dnia w ograniczeniach dostępu służy do konfigurowania filtrów dostępu do Internetu w celu zablokowania urządzeniom sieciowym całego ruchu przychodzącego i wychodzącego na podstawie wybranych ustawień dnia tygodnia oraz pory.

Wybierz kartę **Reguły dotyczące pory dnia**, aby przejść do strony Ograniczenia dostępu > Reguły dotyczące pory dnia. Ilustracja poniżej zawiera przykład tej strony.

Uwaga: Brama domowa używa zegara sieciowego zarządzanego przez dostawcę usług danych. Aby ta funkcja działała prawidłowo, zegar ten musi być dokładny i wskazywać porę dnia w strefie czasowej użytkownika. Należy sprawdzić, czy na stronie stanu i na stronie ustawień czasu jest pokazywana poprawna godzina. Jeśli pokazywana godzina nie jest poprawna, należy skontaktować się z dostawcą usług danych. Można też dostosować swoje ustawienia, aby uwzględnić różnicę.



Opis strony Ograniczenia dostępu > Reguły dotyczące pory dnia

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania reguł bramy domowej dotyczących pory dnia. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Filtr ToD	**Dodaj** Umożliwia dodanie nowej reguły lub filtru dostępu dotyczących pory dnia. Wprowadź nazwę filtru i kliknij przycisk **Dodaj**, aby dodać filtr do listy. Reguły dotyczące pory dnia służą do ograniczania dostępu do Internetu na podstawie dnia i godziny. **Usuń** Usuwa wybrany filtr z listy filtrów Pora dnia.
Harmonogram	**Dni blokady** Umożliwia kontrolę dostępu na podstawie dnia tygodnia. **Czas blokady** Umożliwia kontrolę dostępu na podstawie pory dnia.

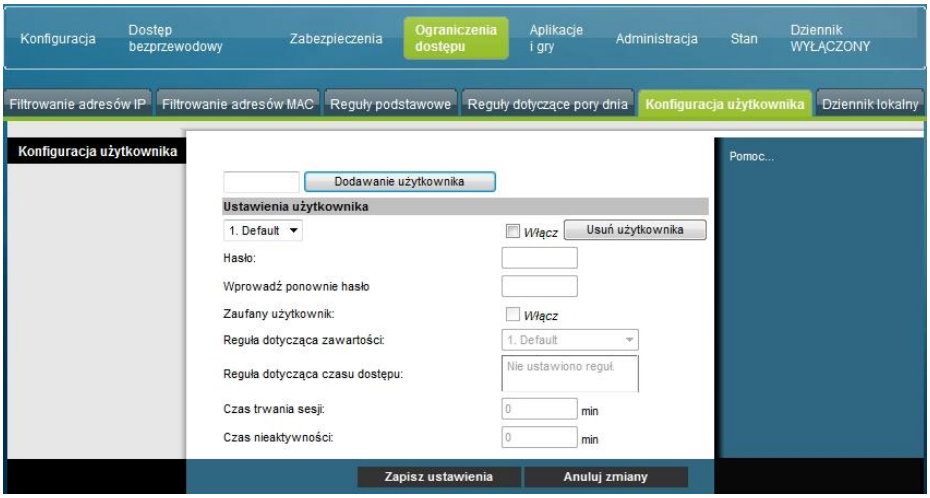
Ograniczenia dostępu > Konfiguracja użytkownika

Strona Ograniczenia dostępu > Konfiguracja użytkownika służy domownikom do konfigurowania dodatkowych kont i profili użytkowników. Każdemu profilowi można przypisać dostosowane poziomy dostępu do Internetu zdefiniowane przy użyciu reguł dostępu przypisanych do danego profilu użytkownika.

Ważne: Te dodatkowe konta nie mają dostępu administracyjnego do bramy.

Uwaga: Po zdefiniowaniu i włączeniu profili użytkowników konieczne będzie logowanie przy każdej próbie uzyskania dostępu do Internetu. Można się zalogować przy użyciu wyskakującego ekranu logowania wyświetlanego w przeglądarce internetowej. Aby uzyskać dostęp do Internetu, należy wprowadzić poprawną nazwę użytkownika i hasło.

Wybierz kartę **Konfiguracja użytkownika**, aby przejść do strony Ograniczenia dostępu > Konfiguracja użytkownika.



Opis strony Ograniczenia dostępu > Konfiguracja użytkownika

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania użytkowników bramy domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Konfiguracja użytkownika	**Dodawanie użytkownika** Umożliwia dodanie nowego profilu użytkownika. Wprowadź nazwę użytkownika i kliknij przycisk **Dodawanie użytkownika**, aby dodać użytkownika do listy. **Ustawienia użytkownika** Umożliwia edycję profilu użytkownika przy użyciu menu rozwijanego. Menu rozwijane umożliwia wybór profilu do edycji. W nazwach użytkowników i hasłach rozróżniana jest wielkość liter. Zaznacz pole **Włącz**, aby uaktywnić profil użytkownika. Jeśli profil nie będzie aktywny, dany użytkownik nie będzie mieć dostępu do Internetu. Aby usunąć profil użytkownika, wybierz użytkownika przy użyciu menu rozwijanego i kliknij przycisk **Usuń użytkownika**. **Hasło** W tym polu wprowadź hasło wybranego użytkownika. Każdy użytkownik musi wprowadzić swoją nazwę użytkownika i hasło przy każdej próbie uzyskania dostępu do Internetu. W nazwach użytkowników i hasłach rozróżniana jest wielkość liter. **Uwaga:** Brama domowa umożliwia wszystkim użytkownikom dostęp do Internetu zgodnie z regułami ustalonymi dla nich na tej stronie. **Wprowadź ponownie hasło** Wprowadź ponownie to samo hasło w celu potwierdzenia hasła podanego w poprzednim polu. **Zaufany użytkownik** Zaznacz to pole, jeśli obecnie wybrany użytkownik ma być zaufanym użytkownikiem. Zaufani użytkownicy nie podlegają regułom dostępu do Internetu. **Reguła dotycząca zawartości** Wybierz regułę dotyczącą zawartości dla bieżącego profilu użytkownika. Reguły te należy wcześniej zdefiniować na stronie konfiguracji reguł. Można uzyskać do niej dostęp, klikając kartę „Reguły podstawowe" na bieżącej stronie. **Reguła dotycząca czasu dostępu** Wybierz regułę dotyczącą czasu dostępu dla bieżącego profilu użytkownika. Reguły te należy wcześniej zdefiniować na stronie Reguły dotyczące pory dnia. Można uzyskać do niej dostęp, klikając kartę „Reguły dotyczące pory dnia" na bieżącej stronie. **Czas trwania sesji** 1440 minut [Domyślne ustawienie fabryczne dla nowo tworzonych użytkowników. W przeciwnym razie wartość ta wynosi 0 (zero)]. Wprowadź czas (w minutach), przez który użytkownik będzie mieć dostęp do Internetu, począwszy od chwili zalogowania się przy użyciu nazwy użytkownika i hasła. **Uwaga:** Aby zapobiec wygasaniu sesji, ustaw pole Czas trwania sesji na wartość 0 (zero).

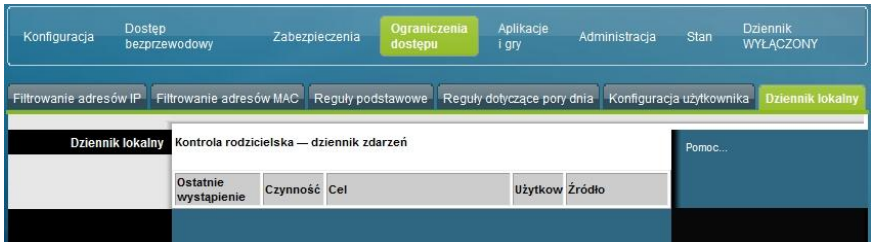
Sekcja	Opis pola
	Czas nieaktywności 60 minut [Domyślne ustawienie fabryczne dla nowo tworzonych użytkowników. W przeciwnym razie wartość ta wynosi 0 (zero)]. Wprowadź długość okresu braku aktywności w zakresie uzyskiwania dostępu do Internetu w ramach sesji użytkownika, po którym zostanie przyjęte, że ten użytkownik nie jest już w trybie online. Po uaktywnieniu licznika czasu nieaktywności sesja użytkownika zostanie automatycznie zamknięta. Aby ponownie uzyskać dostęp do Internetu, użytkownik musi znowu się zalogować, używając nazwy użytkownika i hasła. **Uwaga:** Aby zapobiec wygasaniu sesji, ustaw pole Czas nieaktywności wartość 0 (zero).

Ograniczenia dostępu > Dziennik lokalny

Ta strona umożliwia śledzenie — poszczególnym użytkownikom — wszelkich prób uzyskania dostępu do witryn internetowych z ograniczeniami. Na tej stronie można również zobaczyć zdarzenia przechwycone przez funkcje raportowania kontroli rodzicielskiej.

Wybierz kartę **Dziennik lokalny**, aby przejść do strony Ograniczenia dostępu > Dziennik lokalny.

Ilustracja poniżej przedstawia przykład tej strony.



Sekcja	Opis pola
Dziennik lokalny	**Ostatnie wystąpienie**
Kontrola rodzicielska — dziennik zdarzeń	Wyświetla czas ostatniej próby uzyskania dostępu do witryny internetowej z ograniczeniami.
	Czynność
	Wyświetla informację o działaniu podjętym przez system.
	Cel
	Wyświetla adres URL witryny z ograniczeniami.
	Użytkownik
	Wyświetla nazwę użytkownika, który próbował uzyskać dostęp do witryny z ograniczeniami.
	Źródło
	Wyświetla adres IP komputera, który został użyty podczas próby uzyskania dostępu do witryny internetowej z ograniczeniami.

Konfigurowanie aplikacji i gier

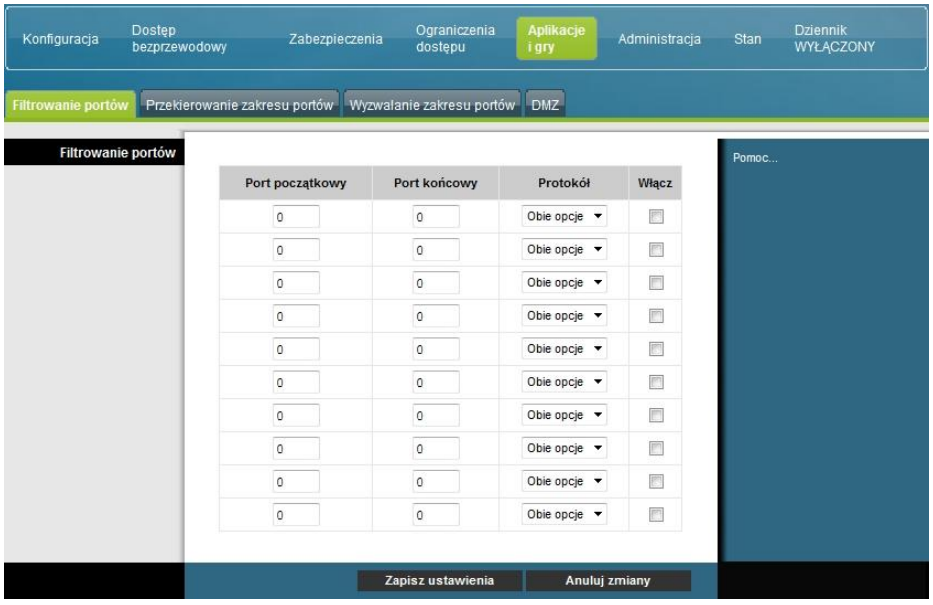
Omówienie

Większość popularnych aplikacji internetowych jest obsługiwana przez bramy ALG (Application Layer Gateway). Dostosowują one automatycznie zaporę w celu zezwolenia na przekazywanie danych bez potrzeby wprowadzania jakichkolwiek ustawień niestandardowych. Przed wprowadzeniem zmian w tej sekcji zaleca się przetestowanie aplikacji.

Aplikacje i gry > Filtrowanie portów

To okno służy do konfiguracji filtrów portów TCP (Transmission Control Protocol) oraz UDP (User Datagram Protocol). Filtry te umożliwiają blokowanie dostępu do Internetu zakresowi portów TCP/UDP. Można także zapobiegać wysyłaniu wychodzącego ruchu TCP/UDP na określone porty IP w sieci WAN. Te filtry nie zależą od adresów IP ani MAC. System blokuje określone zakresy portów wszystkich komputerów.

Wybierz kartę **Filtrowanie portów**, aby przejść do strony Aplikacje i gry > Filtrowanie portów.



Opis strony Aplikacje i gry > Filtrowanie portów

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania funkcji filtrowania portów bramy domowej na potrzeby aplikacji i gier. Kliknij pole wyboru **Włącz**, aby włączyć przekierowanie portów dla odpowiedniej aplikacji. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Filtrowanie portów	**Port początkowy:** Jest to początek zakresu portów. Wprowadź początek zakresu numerów portów (porty zewnętrzne) używanych przez serwer lub aplikację internetową. W razie potrzeby dodatkowych informacji należy szukać w dokumentacji oprogramowania aplikacji internetowej.
	Port końcowy: Jest to koniec zakresu portów. Wprowadź koniec zakresu numerów portów (porty zewnętrzne) używanych przez serwer lub aplikację internetową. W razie potrzeby dodatkowych informacji należy szukać w dokumentacji oprogramowania aplikacji internetowej.
	Protokół Wybierz jeden z następujących protokołów: ■ **TCP** ■ **UDP** ■ **Obie opcje**
	Włącz: Zaznacz to pole wyboru, aby włączyć filtrowanie określonych portów.

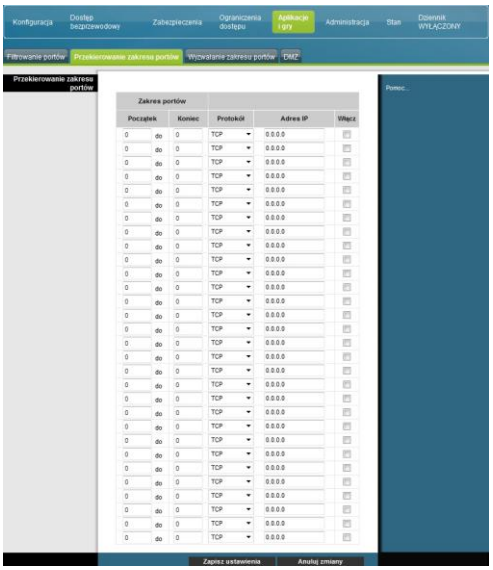
Aplikacje i gry > Przekierowanie zakresu portów

Ważne: W bramie zwykle jest wykorzystywana funkcja translacji portów. Funkcja ta monitoruje bieżące użycie portów przez komputery i inne urządzenia w sieci LAN. Zapewnia to dodatkowy poziom zabezpieczeń, oprócz zapory. Jednak niektóre aplikacje wymagają użycia przez bramę określonych portów w celu nawiązania połączenia przez Internet.

Należy użyć funkcji Przekierowanie zakresu portów, aby przekierować porty używane przez Internet do określonych adresów IP w sieci lokalnej. Wybierz kartę **Przekierowanie zakresu portów**, aby przejść do strony Aplikacje i gry > Przekierowanie zakresu portów.

W polach Port początkowy i Port końcowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program. Wpisz numer portu lub zakres portów w obu polach. W polu Adres IP wpisz adres IP komputera, którego ma dotyczyć reguła.

Uwaga: Funkcja Przekierowanie zakresu portów powoduje ciągłe udostępnianie wybranych portów w Internecie. Oznacza to, że na tych portach nie będzie działać zapora bramy. Podczas przekierowywania zakresu portów urządzenie o wskazanym adresie IP może być narażone na ataki hakerów.



Opis strony Aplikacje i gry > Przekierowanie zakresu portów

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania funkcji przekierowania zakresu portów bramy domowej. Zaznacz pole Włącz dla poszczególnych pozycji. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Przekierowanie zakresu portów	**Początek** Jako port początkowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program.
	Koniec Jako port końcowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program.
	Protokół Wybierz jeden z następujących protokołów: ■ TCP ■ UDP ■ Obie opcje
	Adres IP Wprowadź adres IP komputera, którego dotyczy reguła.

Sekcja	Opis pola
	Włącz Zaznacz to pole wyboru, aby włączyć przekierowanie portów dla określonych portów i adresów IP.

Aplikacje i gry > Wyzwalanie zakresu portów

Wyzwalanie zakresu portów to sposób na dynamiczne przekierowanie portów do komputera w sieci LAN, który potrzebuje ich użyć w konkretnym czasie. Wtedy, gdy zostaje uruchomiona określona aplikacja generująca zdarzenie wyzwalane przez router. Tym zdarzeniem musi być wygenerowanie ruchu wychodzącego dla określonego zakresu portów.

Wybierz kartę **Wyzwalanie zakresu portów**, aby przejść do strony Aplikacje i gry > Wyzwalanie zakresu portów.

Opis strony Aplikacje i gry > Wyzwalanie zakresu portów

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji wyzwalania zakresu portów bramy domowej. Zaznacz pole Włącz dla poszczególnych pozycji. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Wyzwalanie zakresu portów	
Zakres wyzwolonych	**Port początkowy** Jako port początkowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program.

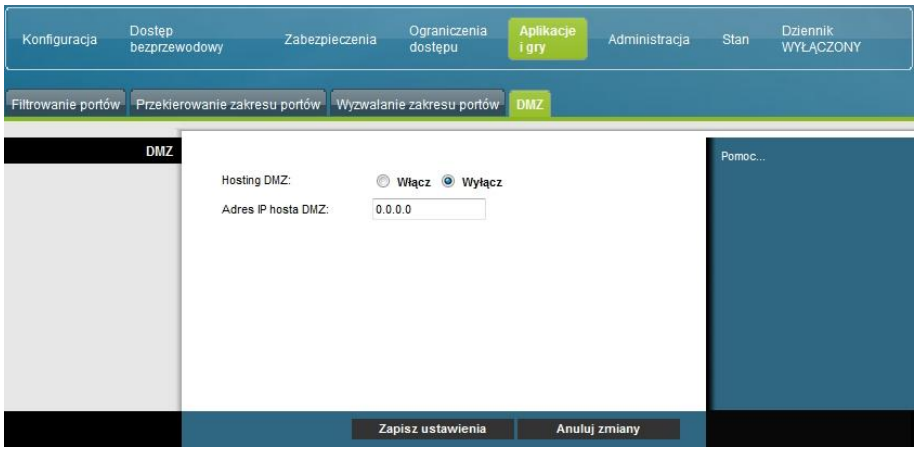
Sekcja	Opis pola
	Port końcowy Jako port końcowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program.
Zakres przekierowanych	**Port początkowy** Jako port początkowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program.
	Port końcowy Jako port końcowy wybierz numer portu z zalecanego zakresu 49152–65535. Należy pamiętać o tym, że używane porty zależą od programu, więc należy sprawdzić, których portów wymaga dany program.
	Protokół Wybierz jeden z następujących protokołów: ■ TCP ■ UDP ■ Obie opcje
	Włącz Kliknij pole wyboru Włącz, aby włączyć wyzwalanie zakresu portów dla odpowiedniej aplikacji.

Aplikacje i gry > DMZ

Ta strona służy do konfigurowania adresu IP, którego porty będą bezpośrednio dostępne z Internetu lub z sieci WAN (Wide Area Network). Hosting DMZ (Demilitarized Zone) jest często określany jako „wystawienie hosta” i umożliwia określenie adresata ruchu z sieci WAN, dla którego funkcja NAT (Network Address Translation) nie może określić znanego lokalnego komputera.

Funkcja DMZ jest zwykle używana przez firmy, które chcą używać własnego serwera internetowego. Ta funkcja umożliwia umieszczenie jednego adresu IP po tej samej stronie zapory bramy, co Internet, podczas gdy pozostałe są chronione przez zaporę.

Funkcja DMZ umożliwia urządzeniu bezpośredni dostęp do ruchu internetowego, takiego jak ruch do serwera WWW (HTTP), FTP, SMTP (poczta e-mail) czy DNS (Domain Name System). Wybierz kartę **DMZ**, aby przejść do strony Aplikacje i gry > DMZ.



Opis strony Aplikacje i gry > DMZ

Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfiguracji wyzwalania zakresu portów bramy domowej. Zaznacz pole Włącz dla adresu IP każdego hosta DMZ. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

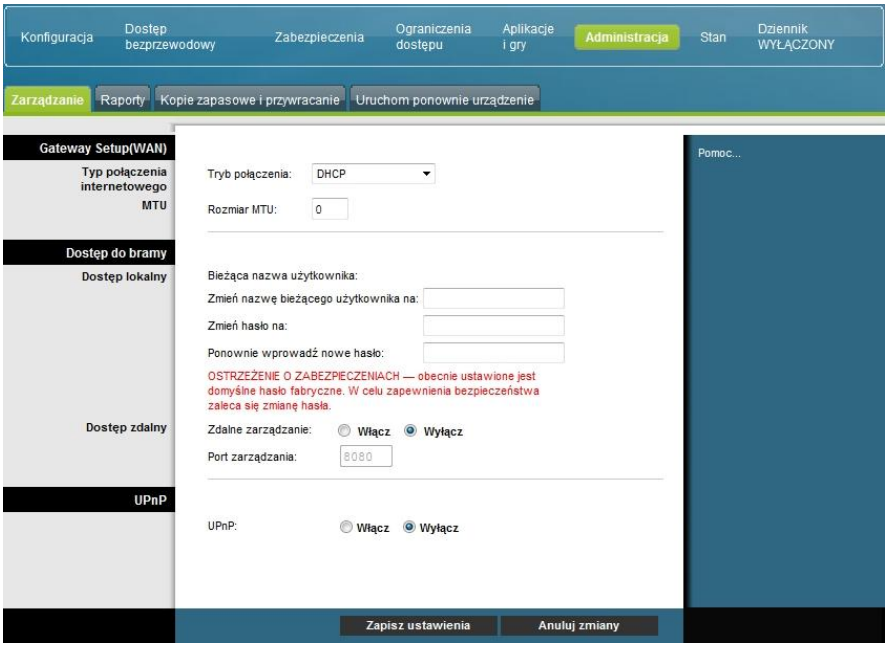
Sekcja	Opis pola
DMZ	**Hosting DMZ** Wybierz żądaną opcję: ■ **Włącz** ■ **Wyłącz** (domyślne ustawienie fabryczne)
	Adres IP hosta DMZ Funkcja DMZ umożliwia pozostawienie jednego adresu IP bez ochrony, podczas gdy pozostałe są chronione. Wprowadź w tym polu adres IP komputera, który chcesz udostępnić w Internecie.

Zarządzanie bramą

Administracja > Zarządzanie

Strona Administracja > Zarządzanie umożliwia administratorowi sieci zarządzanie określonymi funkcjami bramy związanymi z dostępem i zabezpieczeniami. Wybierz kartę **Zarządzanie**, aby przejść do strony Administracja > Zarządzanie.

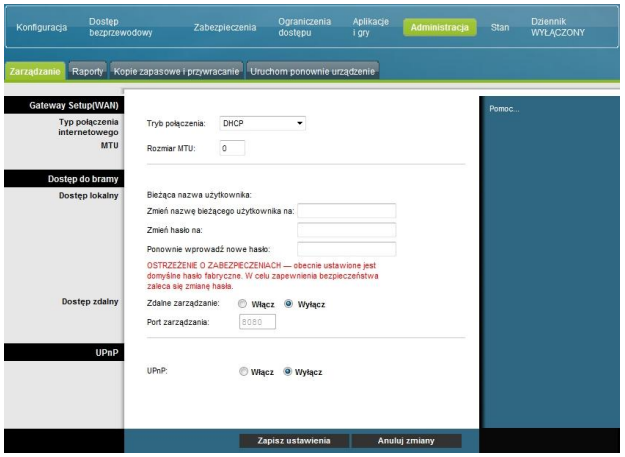
Ważne: Następująca strona jest wyświetlana, gdy jako Tryb połączenia zostanie wybrana wartość **DHCP** (domyślne ustawienie fabryczne). Strona wyświetlana po wybraniu trybu **Statyczny adres IP** jest pokazana i opisana w dalszej części sekcji.



Opis strony Administracja > Zarządzanie

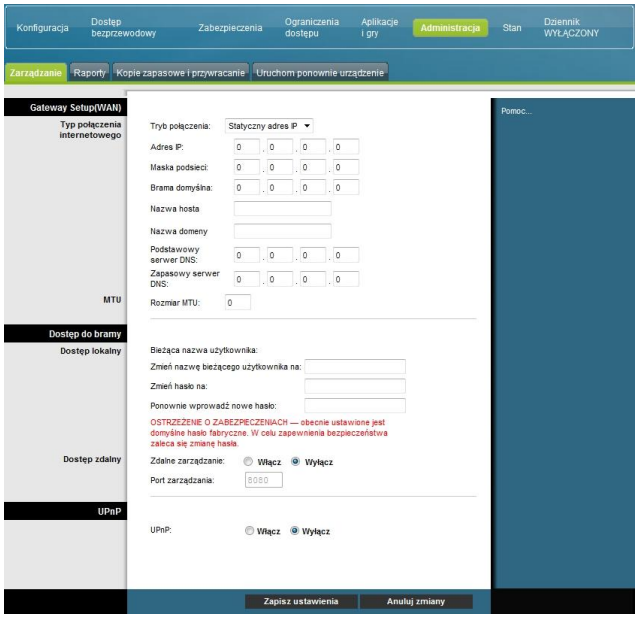
Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania funkcji zarządzania bramą domową, gdy jako tryb połączenia zostanie wybrana opcja DHCP lub Statyczny adres IP. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Pole	Opis
Gateway Setup (WAN)	**Tryb połączenia** Ta wartość umożliwia określenie sposobu uzyskiwania adresu IP w sieci WAN (lub interfejsu bramy do Internetu).
Typ połączenia internetowego	**DHCP** (domyślne ustawienie fabryczne) Umożliwia bramie automatyczne uzyskiwanie publicznego adresu IP.



Statyczny adres IP

Umożliwia określenie adresu IP w sieci WAN i odpowiednich informacji o serwerze jako statycznych lub ustalonych wartości używanych przy każdym przejściu bramy w tryb online.



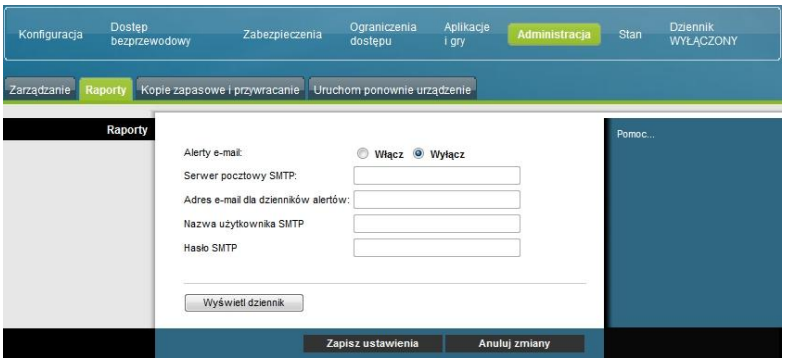
Pole	Opis
	Adres IP Wprowadź adres IP bramy (widoczny w Internecie). **Maska podsieci** Wprowadź maskę podsieci bramy (widoczną w Internecie, w tym przez dostawcę usług). **Brama domyślna** Wprowadź adres bramy domyślnej dla serwera dostawcy usług. **Podstawowy serwer DNS** Wprowadź adresy IP podstawowych serwerów DNS dostarczone przez dostawcę usług. To pole jest wymagane. **Zapasowy serwer DNS** Wprowadź adresy IP zapasowych serwerów DNS dostarczone przez dostawcę usług. Ten parametr jest opcjonalny.
MTU	**Rozmiar MTU** MTU to skrót oznaczający największą jednostkę transmisji (Maximum Transmission Unit). Rozmiar MTU określa maksymalną dozwoloną wielkość pakietu w komunikacji internetowej . Domyślne ustawienie fabryczne to 0 (1500 bajtów).
Dostęp do bramy **Dostęp lokalny**	**Bieżąca nazwa użytkownika** Identyfikuje aktualnie zalogowanego użytkownika. **Zmień nazwę bieżącego użytkownika na** W tym polu możesz zmienić swoją nazwę użytkownika. Aby to zrobić, wpisz nową nazwę i kliknij przycisk **Zapisz ustawienia**. **Uwaga:** Domyślnie pole nazwy użytkownika jest puste. **Zmień hasło na** W tym polu możesz zmienić swoje hasło. Aby to zrobić, wpisz nowe hasło w tym polu. Następnie wpisz je także w polu **Ponownie wprowadź nowe hasło** i kliknij przycisk **Zapisz ustawienia**. **Uwaga:** Domyślnie pole hasła jest puste. **Ponownie wprowadź nowe hasło** To pole służy do ponownego wpisania hasła. Wpisane hasło musi być takie samo, jak hasło w polu **Zmień hasło na**. Po ponownym wpisaniu hasła kliknij przycisk **Zapisz ustawienia**.

Pole	Opis
Dostęp zdalny	**Zdalne zarządzanie** Służy do włączania i wyłączania funkcji zdalnego zarządzania. Po włączeniu funkcji można zarządzać ustawieniami bramy przez Internet — spoza domu. Aby umożliwić dostęp zdalny, wybierz opcję **Włącz**. W przeciwnym razie zachowaj ustawienie domyślne **Wyłącz**. Zdalne zarządzanie wymaga protokołu HTTP. Aby uzyskać zdalny dostęp do urządzenia, w przeglądarce w polu **Adres** wpisz https://xxx.xxx.xxx.xxx:8080 (znaki x oznaczają internetowy adres IP urządzenia, a 8080 to określony port). **Port zarządzania** Wprowadź numer portu, który będzie otwarty dla dostępu z zewnątrz. Domyślne ustawienie fabryczne to 8080. Ten port musi być używany podczas nawiązywania połączenia zdalnego.
UPnP	**UPnP** Technologia Universal Plug and Play (UPnP) umożliwia, w systemach Windows Me i Windows XP, automatyczne konfigurowanie routera pod kątem różnych aplikacji internetowych, takich jak gry czy wideokonferencje. Aby korzystać z funkcjonalności UPnP, zachowaj ustawienie domyślne **Włącz**. W przeciwnym razie wybierz opcję **Wyłącz**.
IGMP	**IGMP Proxy** Protokół IGMP (Internet Group Multicast Protocol) służy do nawiązywania relacji członkowskich w grupie multicast, dlatego jest często wykorzystywany w aplikacjach przesyłających dane strumieniowe multicast. Na przykład w lokalnej sieci może funkcjonować telewizja internetowa (IPTV) docierająca do kilku dekoderów. Na każdym dekoderze powinien być odtwarzany inny strumień wideo, dlatego należy skorzystać z funkcji IGMP dostępnej w routerze. Mechanizm przekazywania (proxy) w usłudze IGMP to system usprawniający multicasting do klientów w sieci LAN. Jeśli urządzenia klienckie obsługują tę opcję, pozostaw zaznaczone ustawienie domyślne **Włącz**. W przeciwnym razie wybierz opcję **Wyłącz**.

Administracja > Raporty

Funkcja raportów administracyjnych umożliwia wysyłanie na swój adres wiadomości e-mail o różnych zdarzeniach zachodzących w systemie.

Kliknij kartę **Raporty**, aby przejść do strony Administracja > Raporty.



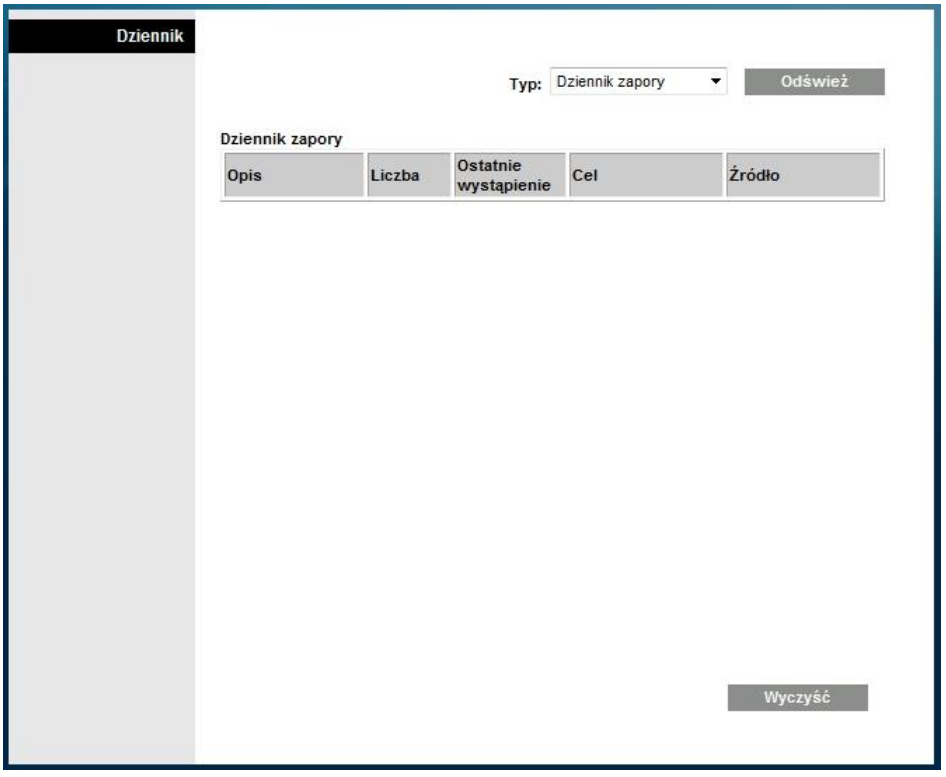
Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania funkcji raportowania w bramie domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Raporty	**Alerty e-mail** Jeśli ta opcja jest włączona, wykrycie zdarzeń podlegających raportowaniu powoduje natychmiastowe wysłanie wiadomości e-mail. Aby korzystać z tej funkcji, należy podać adres e-mail.
	Serwer pocztowy SMTP Wprowadź adres (nazwę domeny) lub IP serwera SMTP (Simple Mail Transport Protocol) używanego do wysyłania poczty e-mail.
	Adres e-mail dla dzienników alertów Wprowadź adres e-mail, pod który mają być wysyłane dzienniki.

Wyświetl dziennik

Aby obejrzeć dzienniki, wykonaj poniższe czynności.

1 Kliknij przycisk **Wyświetl dziennik**. Zostanie otwarte nowe okno ze stroną danych dziennika.



2 Aby wyświetlić konkretny dziennik, w menu rozwijanym Typ zaznacz jedną z poniższych opcji:

- Wszystkie
- Dziennik dostępu
- Dziennik zapory
- Dziennik VPN

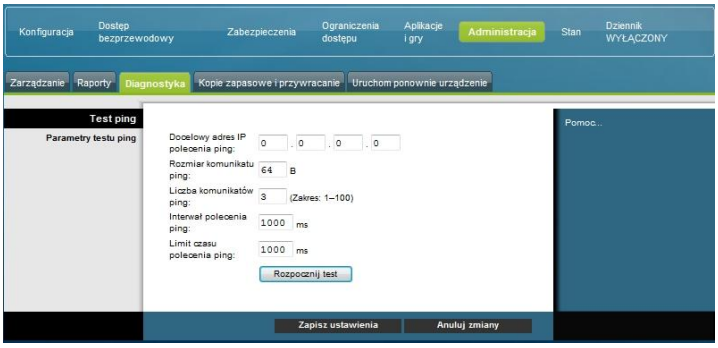
3 Po wyświetleniu danych dziennika dostępne są następujące opcje:

- Kliknij przycisk **Odśwież stronę**, aby zaktualizować dziennik.
- Kliknij przycisk **Wyczyść**, aby usunąć wszystkie informacje z bieżącego dziennika.
- Kliknij przycisk **Poprzednia strona**, aby powrócić do poprzednio wyświetlanych informacji.
- Kliknij przycisk **Następna strona**, aby wyświetlić kolejną sekcję dziennika, jeśli istnieje.

Administracja > Diagnostyka

Funkcja diagnostyki administracyjnej służy do sprawdzania stanu połączenia internetowego za pomocą testu ping.

Kliknij kartę **Diagnostyka**, aby przejść do strony Administracja > Diagnostyka.



Opisy i instrukcje przedstawione w następującej tabeli dotyczą konfigurowania funkcji diagnostyki w bramie domowej. Po wprowadzeniu ustawień kliknij przycisk **Zapisz ustawienia**, aby zastosować zmiany, lub przycisk **Anuluj zmiany**, aby je anulować.

Sekcja	Opis pola
Test ping	
Parametry testu ping	**Docelowy adres IP polecenia ping** Adres IP, do którego ma zostać wysłane polecenie ping. **Rozmiar komunikatu ping** Rozmiar pakietu, którego chcesz użyć. **Liczba komunikatów ping** Liczba komunikatów ping, które mają zostać wysłane do urządzenia docelowego. **Interwał polecenia ping** Okres (w ms) między poszczególnymi komunikatami ping. **Limit czasu polecenia ping** Żądany limit czasu (w ms). Jeśli w tym czasie nie zostanie odebrana odpowiedź, test ping uznaje się za zakończony niepowodzeniem.

Sekcja	Opis pola
	Rozpocznij test Aby zainicjować test, wykonaj następujące czynności. **1** Kliknij przycisk **Rozpocznij test**. Zostanie wyświetlona nowa strona zawierająca podsumowanie wyników testu. **2** Kliknij przycisk **Zapisz ustawienia**, aby zapisać wyniki testu, lub przycisk **Anuluj zmiany**, aby anulować test.

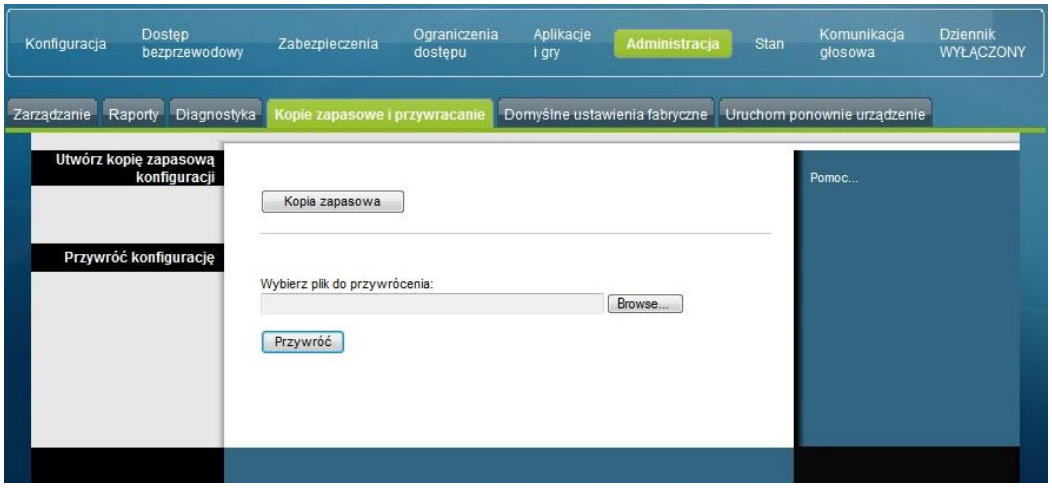
Administracja > Kopie zapasowe i przywracanie

Funkcja Kopie zapasowe i przywracanie służy do wykonywania kopii zapasowej konfiguracji bramy i zapisania jej na komputerze. Za pomocą tego pliku można następnie przywrócić w bramie zapisaną wcześniejszą konfigurację.

Kliknij kartę **Kopie zapasowe i przywracanie**, aby przejść do strony Administracja > Kopie zapasowe i przywracanie.

UWAGA:

Przywrócenie ustawień z pliku konfiguracyjnego spowoduje zniszczenie (zastąpienie) wszystkich istniejących ustawień.



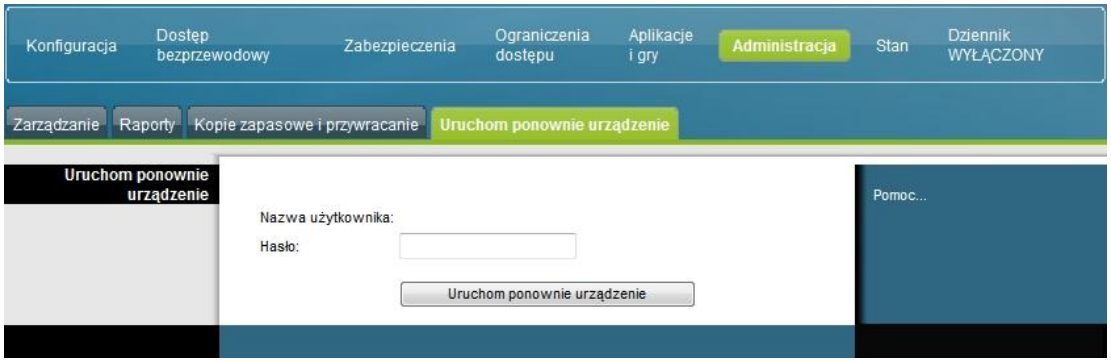
Sekcja	Opis pola
Utwórz kopię zapasową konfiguracji	Funkcja Utwórz kopię zapasową konfiguracji służy do zapisania kopii bieżącej konfiguracji w pliku i zachowania go na komputerze. Aby rozpocząć pobieranie danych konfiguracyjnych, kliknij przycisk **Kopia zapasowa**.
Przywróć konfigurację	Funkcja Przywróć konfigurację służy do przywracania konfiguracji z zapisanego wcześniej pliku. Kliknij przycisk **Przeglądaj**, odszukaj i zaznacz plik konfiguracyjny, a następnie kliknij przycisk **Przywróć**. Plik zostanie załadowany do urządzenia.

Administracja > Uruchom ponownie urządzenie

Za pomocą opcji na stronie Administracja > Uruchom ponownie urządzenie można przywracać domyślne fabryczne ustawienia konfiguracyjne urządzenia. Kliknij kartę **Uruchom ponownie urządzenie**, aby przejść do strony Administracja > Uruchom ponownie urządzenie.

UWAGA:

Ponowne uruchomienie bramy spowoduje utracenie wszystkich dotychczas istniejących ustawień. Przed zresetowaniem bramy do domyślnych ustawień fabrycznych zanotuj wszystkie niestandardowe ustawienia. Po przywróceniu domyślnych ustawień fabrycznych konieczne będzie ponowne wprowadzenie wszystkich ustawień konfiguracji.



Uruchom ponownie urządzenie

Aby przywrócić domyślne ustawienia fabryczne, kliknij przycisk **Uruchom ponownie urządzenie**. Wszystkie ustawienia konfiguracyjne zostaną przywrócone do swoich wartości domyślnych. Po uruchomieniu ponownie urządzenia zostaną utracone wszelkie zapisane ustawienia.

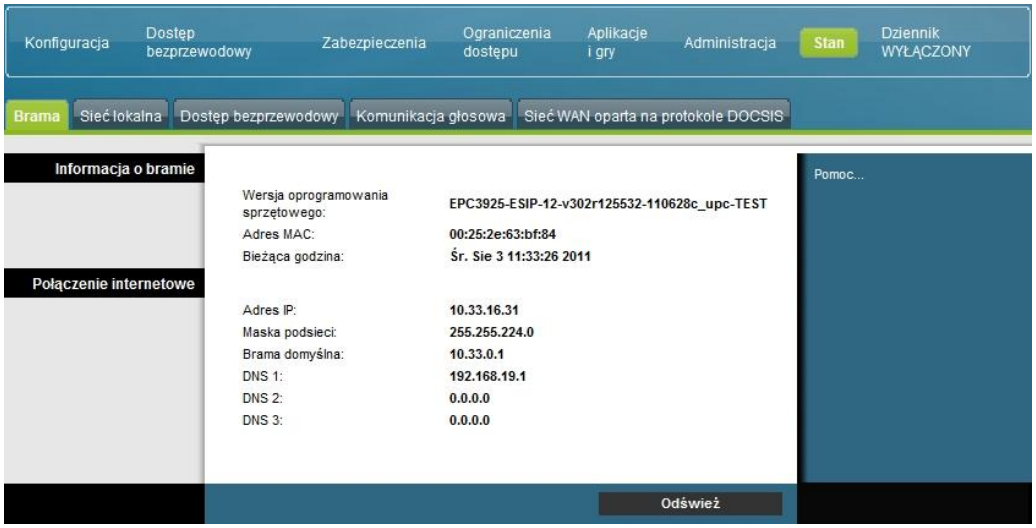
Monitorowanie stanu bramy

W tym rozdziale opisano opcje dostępne na karcie Stan służące do monitorowania stanu urządzenia bramy domowej oraz do diagnozowania urządzenia i całej sieci.

Stan > Brama

Na stronie Stan > Brama znajdują się informacje o bramie i jej aktualnych ustawieniach. Zawartość ekranu zależy od typu używanego połączenia internetowego.

Kliknij kartę **Brama**, aby przejść do strony Stan > Brama. Aby zaktualizować dane wyświetlane na ekranie, kliknij przycisk **Odśwież**.



Korzystając z opisów umieszczonych w tabeli poniżej, można sprawdzić stan bramy i połączenia z Internetem.

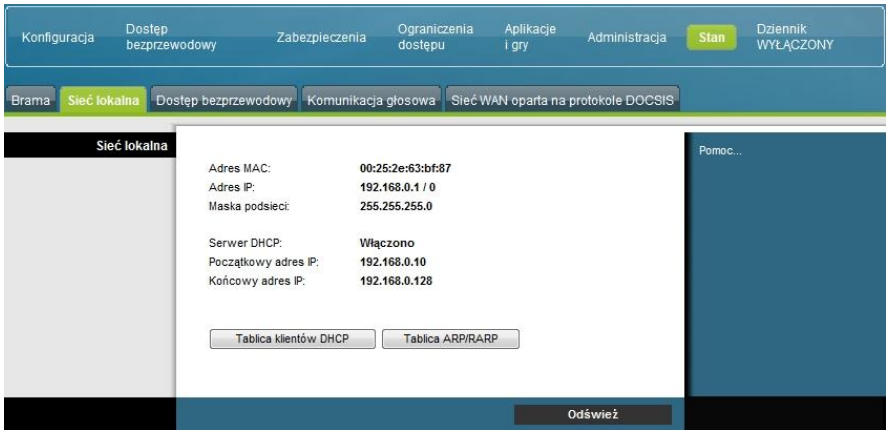
Sekcja	Opis pola
Informacja o bramie	**Wersja oprogramowania sprzętowego** Numer wersji oprogramowania sprzętowego. **Adres MAC (Adres MAC modemu kablowego)** Unikatowy alfanumeryczny adres interfejsu koncentrycznego w modemie kablowym podłączanego do układu zakończenia modemu kablowego (Cable Modem Termination System, CMTS) w stacji nadawczej. Adres sterowania dostępem do nośnika (Media Access Control, MAC) to adres sprzętowy, który w sposób unikatowy identyfikuje każdy węzeł w sieci. **Bieżąca godzina** Wyświetlana jest bieżąca godzina, w oparciu o ustawienia strefy czasowej wprowadzone na stronie Podstawowa konfiguracja.

Sekcja	Opis pola
Połączenie internetowe	**Adres IP** Wyświetlany jest adres IP interfejsu sieci WAN. Adres jest przypisywany do bramy po jej włączeniu. **Maska podsieci** Wyświetlana jest maska podsieci portu sieci WAN. Ten adres jest automatycznie przypisywany do portu sieci WAN przez usługodawcę internetowego, chyba że zdefiniowano statyczny adres IP. **Brama domyślna** Adres IP domyślnej bramy usługodawcy internetowego. **DNS 1-3** Adresy IP serwera DNS używane aktualnie przez bramę. **WINS** Adres IP serwera WINS używany aktualnie przez bramę.

Stan > Sieć lokalna

Na stronie stanu sieci lokalnej są wyświetlane informacje o stanie sieci lokalnej.

Kliknij kartę **Sieć lokalna**, aby przejść do strony Stan > Sieć lokalna. Aby zaktualizować informacje podawane na stronie, kliknij przycisk **Odśwież**.



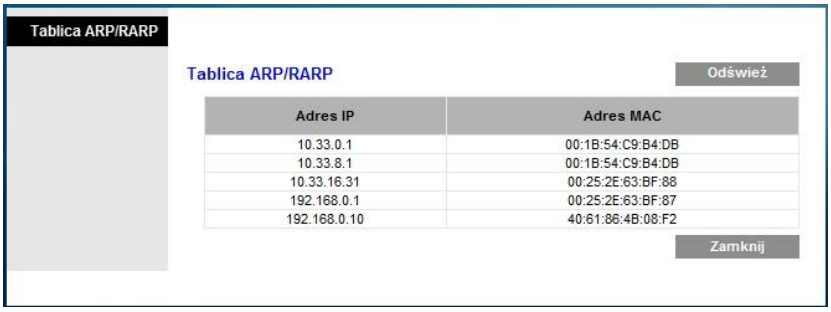
Korzystając z tabeli poniżej, można sprawdzić stan bramy i połączenia z Internetem.

Sekcja	Opis pola
Sieć lokalna	**Adres MAC** Unikatowy alfanumeryczny adres prywatnej sieci domowej LAN. Adres MAC to adres sprzętowy, który w sposób unikatowy identyfikuje każdy węzeł w sieci.

Sekcja	Opis pola
	Adres IP Wyświetlany jest adres IP podsieci LAN. **Maska podsieci** Wyświetlana jest maska podsieci sieci LAN. **Serwer DHCP** Wyświetlany jest stan lokalnego serwera DHCP (Włączony lub Wyłączony). **Początkowy adres IP** Wyświetlany jest początek zakresu adresów IP używanych przez serwer DHCP skonfigurowany w urządzeniu bramy. **Końcowy adres IP** Wyświetlany jest koniec zakresu adresów IP używanych przez serwer DHCP.
Tablica klientów DHCP	Kliknij przycisk **Tablica klientów DHCP**, aby wyświetlić listę urządzeń podłączonych do sieci LAN, które mają adresy IP przypisane przez serwer DHCP skonfigurowany w urządzeniu bramy. Na stronie Tablica klientów DHCP zostanie wyświetlona lista klientów DHCP (komputerów i innych urządzeń sieciowych) oraz następujące informacje: nazwy hostów klientów, adresy IP, adresy MAC oraz czas, jaki pozostał do wygaśnięcia przypisanych im adresów IP. Aby wyświetlić najbardziej aktualne informacje, kliknij przycisk **Odśwież**. Aby opuścić tę stronę i powrócić do strony Sieć lokalna, kliknij przycisk **Zamknij**. Ilustracja poniżej przedstawia przykład tablicy klientów DHCP.

Tablica ARP/RARP Kliknij przycisk **Tablica ARP/RARP**, aby wyświetlić listę wszystkich urządzeń podłączonych do sieci. Aby wyświetlić najbardziej aktualne informacje, kliknij przycisk **Odśwież**. Aby opuścić tę stronę i powrócić do strony Sieć lokalna, kliknij przycisk **Zamknij**.

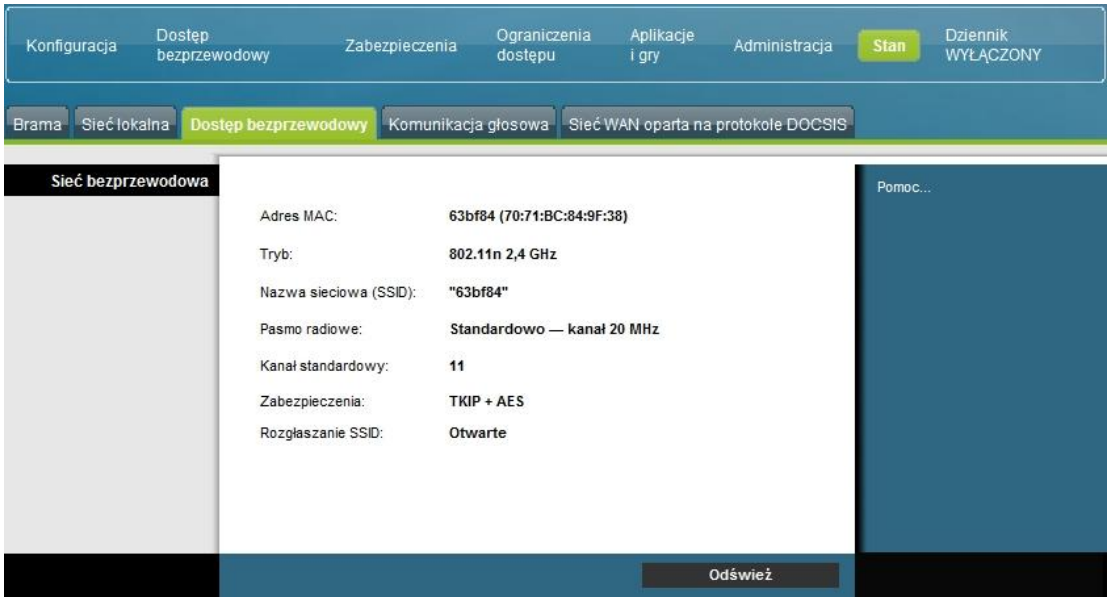
Ilustracja poniżej przedstawia przykład tablicy ARP/RARP.



Stan > Dostęp bezprzewodowy

Strona stanu sieci bezprzewodowej zawiera podstawowe informacje o sieci bezprzewodowej skonfigurowanej w bramie.

Kliknij kartę **Dostęp bezprzewodowy**, aby przejść do strony Stan > Dostęp bezprzewodowy. Aby zaktualizować informacje podawane na stronie, kliknij przycisk **Odśwież**.



Opis strony Stan > Dostęp bezprzewodowy

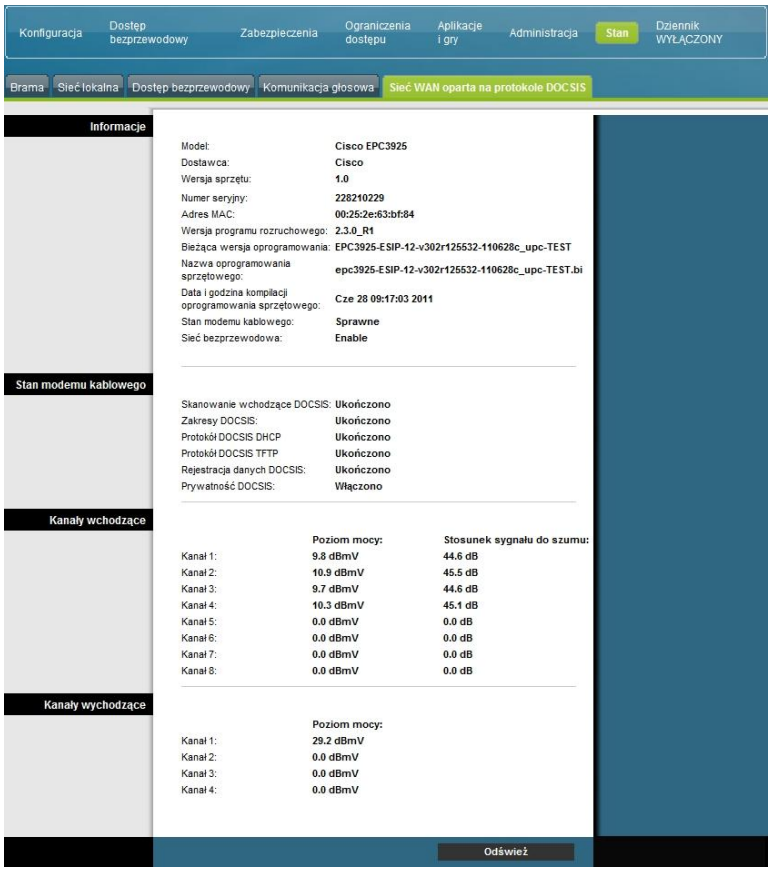
Korzystając z tabeli poniżej, można sprawdzić stan sieci bezprzewodowej.

Sekcja	Opis pola
Sieć bezprzewodowa	**Adres MAC** Wyświetlany jest adres MAC lokalnego punktu dostępu do sieci bezprzewodowej skonfigurowanego w bramie. **Pasmo radiowe** Wyświetlane jest używane pasmo częstotliwości radiowych. Jest to jedna z następujących wartości: ■ 2,4 GHz ■ 5 GHz ■ 2,4 i 5 GHz **Uwaga:** Niektóre urządzenia nie obsługują pasma 5 GHz. **Nazwa sieciowa (SSID)** Wyświetlana jest nazwa zwana identyfikatorem zestawu usług (Service Set Identifier, SSID) punktu dostępu do sieci bezprzewodowej. **Zasięg kanału** Wyświetlana jest wartość ustawienia pasma kanału wybrana na stronie Podstawowe ustawienia sieci bezprzewodowej. **Kanał dla całej sieci** Wyświetlana jest wartość ustawienia kanału dla całej sieci wybrana na stronie Podstawowe ustawienia sieci bezprzewodowej. **Kanał standardowy** Wyświetlana jest wartość ustawienia Kanał standardowy wybrana na stronie Podstawowe ustawienia sieci bezprzewodowej. **Zabezpieczenia** Wyświetlana jest metoda zabezpieczeń używana w sieci bezprzewodowej. **Rozgłaszanie SSID** Wyświetlany jest stan funkcji rozgłaszania identyfikatora SSID skonfigurowanej w bramie.

Stan > Sieć WAN oparta na protokole DOCSIS

W oknie Sieć WAN oparta na protokole DOCSIS są wyświetlane informacje o systemie modemu kablowego.

Kliknij kartę **Sieć WAN oparta na protokole DOCSIS**, aby przejść do strony Stan > Sieć WAN oparta na protokole DOCSIS.



Opis strony Sieć WAN oparta na protokole DOCSIS

Korzystając z opisów umieszczonych w tabeli poniżej, można sprawdzić stan sieci WAN opartej na protokole DOCSIS.

Sekcja	Opis pola
Informacje	**Model** Wyświetlana jest nazwa bramy domowej.
	Dostawca Wyświetlany jest producent bramy domowej.
	Wersja sprzętu Wyświetlana jest wersja płyty głównej urządzenia.

Sekcja	Opis pola
	Numer seryjny Wyświetlany jest unikatowy numer seryjny bramy domowej.
	Adres MAC (Adres MAC modemu kablowego) Wyświetlany jest adres MAC modemu kablowego. Adres MAC modemu kablowego to unikatowy alfanumeryczny adres interfejsu koncentrycznego w modemie kablowym podłączanego do układu CMTS w stacji nadawczej. Adres MAC to adres sprzętowy, który w sposób unikatowy identyfikuje każdy węzeł w sieci.
	Wersja programu rozruchowego Wyświetlany jest numer wersji kodu źródłowego programu rozruchowego.
	Bieżąca wersja oprogramowania Wyświetlany jest numer wersji oprogramowania sprzętowego.
	Nazwa oprogramowania sprzętowego Wyświetlana jest nazwa oprogramowania sprzętowego.
	Data i godzina kompilacji oprogramowania sprzętowego Wyświetlana jest data i godzina skompilowania oprogramowania sprzętowego.
	Stan modemu kablowego Wyświetlana jest aktualna wartość stanu urządzenia bramy.
Kanały wchodzące	**Kanały 1-8** Wyświetlany jest poziom mocy oraz stosunek siły sygnału do natężenia szumów w aktywnych kanałach wchodzących.
Kanały wychodzące	**Kanały 1-4** Wyświetlany jest poziom mocy aktywnych kanałów wychodzących.

Najczęściej zadawane pytania

P. Jak skonfigurować protokół TCP/IP?

O. Aby można było skonfigurować protokół TCP/IP, w komputerze musi być zainstalowana karta Ethernet (Ethernet Network Interface Card, NIC) obsługująca protokół komunikacyjny TCP/IP. TCP/IP to protokół komunikacyjny używany w celu uzyskania dostępu do Internetu. W tej sekcji zamieszczono instrukcje konfigurowania protokołu TCP/IP dla urządzeń internetowych współpracujących z bramą domową w środowisku systemu operacyjnego Microsoft Windows lub Macintosh.

Ustawienia protokołu TCP/IP różnią się dla poszczególnych wersji systemu Microsoft Windows. Dlatego poniżej należy odszukać sekcję odpowiednią dla używanego systemu.

Konfigurowanie protokołu TCP/IP w systemach Windows 2000

1. Kliknij przycisk **Start**, a następnie wybierz kolejno polecenia **Ustawienia** oraz **Połączenia sieciowe i telefoniczne**.
2. W oknie Połączenia sieciowe i telefoniczne kliknij dwukrotnie ikonę **Połączenie lokalne**.
3. W oknie Stan: Połączenie lokalne kliknij przycisk **Właściwości**.
4. W oknie Właściwości: Połączenie lokalne zaznacz pozycję **Protokół internetowy (TCP/IP)** i kliknij przycisk **Właściwości**.
5. W oknie Właściwości: Protokół internetowy (TCP/IP) zaznacz pola wyboru **Uzyskaj adres IP automatycznie** i **Uzyskaj adres serwera DNS automatycznie**, a następnie kliknij przycisk **OK**.
6. W wyświetlonym oknie Sieć lokalna kliknij przycisk **Tak**, aby zrestartować komputer. Komputer zostanie ponownie uruchomiony. Protokół TCP/IP jest skonfigurowany na komputerze, a urządzenia w sieci Ethernet są gotowe do pracy.
7. Spróbuj uzyskać dostęp do Internetu. Jeśli są problemy z nawiązaniem połączenia z Internetem, poproś o pomoc usługodawcę.

Konfigurowanie protokołu TCP/IP w systemach Windows XP

1. Kliknij przycisk **Start**, a następnie zależnie od konfiguracji menu wybierz jedną z następujących opcji:
   - Jeśli używasz domyślnej konfiguracji menu Start, wybierz kolejno polecenia **Połącz z** i **Pokaż wszystkie połączenia**, a następnie przejdź do kroku 2.
   - Jeśli używasz klasycznego menu Start, wybierz kolejno polecenia **Ustawienia**, **Połączenia sieciowe** i **Połączenie lokalne**, a następnie przejdź do kroku 3.

2 W oknie Połączenia sieciowe w sekcji Sieć LAN lub szybki Internet kliknij dwukrotnie ikonę **Połączenie lokalne**.

3 W oknie Stan: Połączenie lokalne kliknij przycisk **Właściwości**.

4 Zaznacz pozycję **Protokół internetowy (TCP/IP)** i w oknie Właściwości: Połączenie lokalne kliknij przycisk **Właściwości**.

5 W oknie Właściwości: Protokół internetowy (TCP/IP) zaznacz pola wyboru **Uzyskaj adres IP automatycznie** i **Uzyskaj adres serwera DNS automatycznie**, a następnie kliknij przycisk **OK**.

6 W wyświetlonym oknie Sieć lokalna kliknij przycisk **Tak**, aby zrestartować komputer. Komputer zostanie ponownie uruchomiony. Protokół TCP/IP jest skonfigurowany na komputerze, a urządzenia w sieci Ethernet są gotowe do pracy.

7 Spróbuj uzyskać dostęp do Internetu. Jeśli są problemy z nawiązaniem połączenia z Internetem, poproś o pomoc usługodawcę.

Konfigurowanie protokołu TCP/IP na komputerach Macintosh

1 W prawym górnym rogu aplikacji Finder kliknij ikonę **Apple**. Przejdź do sekcji **Tablice kontrolne** i kliknij pozycję **TCP/IP**.

2 U góry strony w aplikacji Finder kliknij przycisk **Edycja**. Przejdź do dołu menu i kliknij pozycję **Tryb użytkownika**.

3 W oknie Tryb użytkownika kliknij kolejno przyciski **Zaawansowane** i **OK**.

4 W oknie TCP/IP z prawej strony sekcji Połącz przez za pomocą strzałek w górę/w dół zaznacz pozycję **Używanie serwera DHCP**.

5 W oknie TCP/IP kliknij przycisk **Opcje**, a następnie przycisk **Aktywny**.

Uwaga: Upewnij się, że opcja **Ładuj opcję tylko w razie potrzeby** jest *niezaznaczona*.

6 Upewnij się, że opcja **Używaj standardu 802.3** znajdująca się w prawym górnym rogu okna TCP/IP jest niezaznaczona. Jeśli obok opcji widać znacznik wyboru, usuń go, a następnie w lewym dolnym rogu kliknij przycisk **Informacje**.

7 Czy w oknie widać pozycję Adres sprzętowy?

- Jeśli **tak**, kliknij przycisk **OK**. Aby zamknąć okno panelu sterowania dla protokołu TCP/IP, kliknij menu **Plik**, przewiń w dół i kliknij przycisk **Zamknij**. Procedura została ukończona.
- Jeśli **nie**, wyłącz komputer.

8 Przy wyłączonym zasilaniu naciśnij i przytrzymaj jednocześnie klawisze **Command (Apple)**, **Option**, **P** i **R**. Trzymając te klawisze naciśnięte, włącz komputer. Nie puszczaj klawiszy, aż usłyszysz co najmniej trzy sygnały dzwonka. Wtedy puść klawisze i zezwól na kontynuowanie uruchamiania.

9 Gdy komputer zostanie w pełni uruchomiony, powtórz kroki od 1 do 7 i sprawdź, czy wszystkie ustawienia protokołu TCP/IP są poprawne. Jeśli komputer wciąż nie zgłasza przypisania adresu sprzętowego, poproś o pomoc autoryzowanego sprzedawcę lub serwis techniczny firmy Apple.

P. Jak odnowić adres IP na komputerze?

O. Jeśli z komputera nie można uzyskać dostępu do Internetu, a brama domowa jest włączona, być może nie nastąpiło odnowienie adresu IP komputera. W celu odnowienia adresu postępuj zgodnie z instrukcjami zawartymi w sekcji odpowiedniej dla używanego systemu operacyjnego.

Odnawianie adresu IP w systemach Windows 95, 98, 98SE i ME

1. Kliknij przycisk **Start** i wybierz polecenie **Uruchom**. Zostanie wyświetlone okno Uruchamianie.
2. W polu Otwórz wpisz polecenie **winipcfg** i kliknij przycisk **OK**, aby wykonać polecenie winipcfg. Zostanie otwarte okno Konfiguracja IP.
3. Kliknij strzałkę w dół umieszczoną z prawej strony górnego pola i zaznacz kartę sieci Ethernet, która jest zainstalowana w komputerze. W oknie Konfiguracja IP zostaną wyświetlone informacje o tej karcie.
4. Kliknij kolejno przyciski **Zwolnij** i **Odnów**. W oknie Konfiguracja IP pojawi się nowy adres IP.
5. Kliknij przycisk **OK**, aby zamknąć okno Konfiguracja IP. Procedura została zakończona.

   Uwaga: Jeśli są problemy z nawiązaniem połączenia z Internetem, poproś o pomoc usługodawcę.

Odnawianie adresu IP w systemach Windows NT, 2000 i XP

1. Kliknij przycisk **Start** i wybierz polecenie **Uruchom**. Zostanie otwarte okno Uruchamianie.
2. W polu Otwórz wpisz polecenie **cmd** i kliknij przycisk **OK**. Zostanie otwarte okno z wierszem poleceń.
3. W wierszu monitu C:\ wpisz polecenie **ipconfig/release** i naciśnij klawisz **Enter**. Adres IP zostanie w systemie zwolniony.
4. W wierszu monitu C:\ wpisz polecenie **ipconfig/renew** i naciśnij klawisz **Enter**. Zostanie wyświetlony nowy adres IP.
5. W prawym górnym rogu okna wiersza poleceń kliknij ikonę **X**, aby zamknąć okno. Procedura została ukończona.

   Uwaga: Jeśli są problemy z nawiązaniem połączenia z Internetem, poproś o pomoc usługodawcę.

P. Co w przypadku, gdy nie subskrybuję usług telewizji kablowej?

O. Jeśli w miejscu Twojego zamieszkania są oferowane usługi telewizji kablowej, usługi transmisji danych mogą być dostępne nawet bez subskrybowania samej usługi telewizyjnej. Skontaktuj się z usługodawcą i szczegółowo dopytaj o oferowane przez niego usługi kablowe, w tym o szybki dostęp do Internetu.

P. Jak zamówić instalację urządzenia?

O. Zadzwoń do usługodawcy i zapytaj o usługę profesjonalnego montażu. Specjalista zadba o poprawne podłączenie do modemu i komputera oraz o skonfigurowanie wszystkich ustawień sprzętowych i programowych. Aby uzyskać więcej informacji o ofercie instalacyjnej, skontaktuj się z usługodawcą.

P. W jaki sposób brama domowa łączy się z komputerem?

O. Brama domowa łączy się z komputerem za pośrednictwem sieci bezprzewodowej lub portu sieci Ethernet 10/100/1000BASE-T umieszczonego w komputerze. Jeśli chcesz używać interfejsu Ethernet, kup kartę sieci Ethernet w sklepie albo u dostawcy usług i zainstaluj ją w komputerze. Aby połączenie Ethernet było wydajne, zastosuj kartę Gigabit Ethernet.

P. Moja brama domowa jest już podłączona. Jak uzyskać dostęp do Internetu?

O. Lokalny dostawca usług staje się usługodawcą internetowym (ISP). Oferuje on cały szereg usług, w tym poczta e-mail, rozmowy sieciowe, wiadomości i serwisy informacyjne. Usługodawca dostarcza również wszelkie potrzebne oprogramowanie.

P. Czy mogę jednocześnie oglądać telewizję i przeglądać strony internetowe?

O. Jak najbardziej! Jeśli subskrybujesz usługę telewizji kablowej, możesz w tym samym czasie oglądać telewizję i korzystać z bramy domowej. Wystarczy podłączyć telewizor i bramę do tej samej sieci kablowej za pomocą opcjonalnego rozgałęźnika.

Rozwiązywanie typowych problemów

Nie rozumiem wskazań kontrolek stanu wyświetlanych na przednim panelu

Dokładniejsze informacje o działaniu i funkcjach wskaźników diodowych na panelu przednim można znaleźć w sekcji ***Funkcje diodowego wskaźnika stanu na panelu przednim*** (na stronie 109).

Brama domowa nie rejestruje połączenia z siecią Ethernet

- Upewnij się, że komputer jest wyposażony w kartę Ethernet, a oprogramowanie sterownika karty jest poprawnie zainstalowane. Jeśli karta została kupiona i zamontowana samodzielnie, upewnij się, że przestrzegano wszystkich instrukcji instalacji.
- Sprawdź wskaźniki stanu na przednim panelu.

Brama domowa nie rejestruje połączenia z siecią Ethernet po podłączeniu do koncentratora

Jeśli chcesz podłączyć do bramy domowej kilka komputerów, najpierw za pomocą odpowiedniego kabla krosowego podłącz modem do portu ruchu wychodzącego w koncentratorze. Wskaźnik LINK na koncentratorze powinien zacząć świecić w sposób ciągły.

Brama domowa nie rejestruje połączenia kablowego

- Modem współpracuje ze standardowymi kablami koncentrycznymi RF o impedancji 75 omów. Jeśli zostanie użyty inny kabel, brama domowa nie będzie działała poprawnie. Aby ustalić, czy używasz właściwego kabla, skontaktuj się z dostawcą usług kablowych.
- Być może karta sieciowa albo interfejs USB działa wadliwie. Zajrzyj do dokumentacji karty NIC i interfejsu USB, do części poświęconych rozwiązywaniu problemów.

Porady dotyczące poprawy wydajności

Sprawdź i popraw

Jeśli brama domowa nie działa zgodnie z oczekiwaniami, skorzystaj z porad zamieszczonych poniżej. W razie potrzeby dodatkowej pomocy udzieli dostawca usług.

- Upewnij się, że wtyczka przewodu zasilania bramy prądem zmiennym jest poprawnie umieszczona w gnieździe elektrycznym.
- Upewnij się, że przewód zasilania bramy prądem zmiennym nie jest podłączony do gniazda elektrycznego włączanego i wyłączanego przełącznikiem ściennym. Jeśli gniazdem steruje przełącznik, upewnij się, że jest on ustawiony w pozycji **Włączony**.
- Upewnij się, że wskaźnik **ONLINE** na przednim panelu bramy domowej świeci się.
- Upewnij się, że usługa kablowa jest aktywna i obsługuje komunikację dwukierunkową.
- Upewnij się, że wszystkie kable są poprawnie podłączone i że używasz odpowiednich kabli.
- Jeśli korzystasz z połączenia Ethernet, upewnij się, że oprogramowanie protokołu TCP/IP jest poprawnie zainstalowane i skonfigurowane.
- Pamiętaj, aby skontaktować się z dostawcą usług i podać mu numer seryjny oraz adres MAC swojej bramy domowej.
- Jeśli używasz rozgałęźnika kablowego umożliwiającego podłączenie bramy domowej do innych urządzeń, odłącz go i podłącz kable tak, aby brama łączyła się bezpośrednio ze źródłem sygnału kablowego. Jeśli po takim przełączeniu urządzenie bramy działa poprawnie, być może rozgałęźnik jest uszkodzony i trzeba go wymienić.
- Aby połączenie Ethernet było wydajne, zastosuj kartę Gigabit Ethernet.

Funkcje diodowego wskaźnika stanu na panelu przednim

Uruchomienie, kalibracja i rejestracja (urządzenie zasilane prądem zmiennym)

W tabeli poniżej opisano kolejne kroki i odpowiadające im zachowanie wskaźników stanu na przednim panelu bramy domowej podczas uruchamiania, kalibrowania i rejestrowania bramy w sieci po podłączeniu zasilania prądem zmiennym. Będzie ona pomocna przy rozwiązywaniu problemów występujących w trakcie włączania, kalibrowania i rejestrowania bramy domowej.

Uwaga: Po zakończeniu kroku 11 (Rejestracja przez telefon ukończona) modem automatycznie przechodzi do trybu normalnej pracy. Zobacz sekcję ***Normalna praca (urządzenie zasilane prądem zmiennym)*** (na stronie 101).

Wskaźniki stanu na przednim panelu podczas uruchamiania, kalibracji i rejestracji							
		Część 1: Rejestracja przez łącze szerokopasmowe					
Krok:		**1**	**2**	**3**	**4**	**5**	**6**
Wskaźnik na panelu przednim		**Autotest**	**Skanowanie ruchu przychodzącego**	**Blokada ruchu przychodzącego**	**Ustalanie zakresu**	**Żądanie adresu IP**	**Żądanie pliku obsługi transmisji szerokopasmowej**
1	POWER	Włączony	Włączony	Włączony	Włączony	Włączony	Włączony
2	DS	Włączony	Miga	Włączony	Włączony	Włączony	Włączony
3	US	Włączony	Wyłączony	Wyłączony	Miga	Włączony	Włączony
4	ONLINE	Włączony	Wyłączony	Wyłączony	Wyłączony	Wyłączony	Miga
5	ETHERNET 1-4	Włączony	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
6	USB	Włączony	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
7	WIRELESS LINK	Wyłączony	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
8	WIRELESS SETUP	Wyłączony	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
9	TEL 1	Włączony	Wyłączony	Wyłączony	Wyłączony	Wyłączony	Wyłączony
10	TEL 2	Włączony	Wyłączony	Wyłączony	Wyłączony	Wyłączony	Wyłączony

Wskaźniki stanu na przednim panelu podczas uruchamiania, kalibracji i rejestracji						
Część 2: Rejestracja przez telefon						
Krok		**7**	**8**	**9**	**10**	**11**
Wskaźnik na panelu przednim		**Rejestracja w sieci transmisji danych ukończona**	**Żądanie adresu IP telefonu**	**Żądanie pliku obsługi łączności telefonicznej**	**Uruchamianie usługi głosowej**	**Rejestracja przez telefon ukończona**
1	POWER	Włączony	Włączony	Włączony	Włączony	Włączony
2	DS	Włączony	Włączony	Włączony	Włączony	Włączony
3	US	Włączony	Włączony	Włączony	Włączony	Włączony
4	ONLINE	Włączony	Włączony	Włączony	Włączony	Włączony
5	ETHERNET 1 - 4	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
6	USB	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
7	WIRELESS LINK	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga	Włączony lub miga
8	WIRELESS SETUP	Wyłączony	Wyłączony	Wyłączony	Włączony lub miga	Włączony lub miga
9	TEL 1	Wyłączony	Miga	Wyłączony	Miga	Włączony
10	TEL 2	Wyłączony	Wyłączony	Miga	Miga	Włączony

Normalna praca (urządzenie zasilane prądem zmiennym)

W tabeli poniżej opisano wygląd wskaźników stanu na przednim panelu bramy domowej podczas jej normalnej pracy po podłączeniu zasilania prądem zmiennym.

Wskaźniki stanu na przednim panelu podczas normalnej pracy		
Wskaźnik na panelu przednim		**Normalna praca**
1	POWER	Włączony
2	DS	Włączony
3	US	Włączony
4	ONLINE	Włączony
5	ETHERNET 1 - 4	■ Włączony — gdy to portu Ethernet jest podłączone jedno urządzenie, a do lub z modemu nie są wysyłane żadne dane ■ Miga — gdy do portu sieci Ethernet jest podłączone tylko jedno urządzenie oraz trwa przesyłanie danych między urządzeniem abonenckim w siedzibie użytkownika (CPE) a bezprzewodową bramą domową ■ Wyłączony — gdy do portów sieci Ethernet nie są podłączone żadne urządzenia
6	USB	■ Włączony — gdy to portu USB jest podłączone jedno urządzenie, a do lub z modemu nie są wysyłane żadne dane ■ Miga — gdy do portu USB jest podłączone tylko jedno urządzenie oraz trwa przesyłanie danych między urządzeniem abonenckim w siedzibie użytkownika (CPE) a bezprzewodową bramą domową ■ Wyłączony — gdy do portów USB nie są podłączone żadne urządzenia
7	WIRELESS LINK	■ Włączony — gdy punkt dostępu bezprzewodowego jest włączony i aktywny ■ Miga — gdy trwa przesyłanie danych między urządzeniem abonenckim CPE a bezprzewodową bramą domową ■ Wyłączony — gdy użytkownik wyłączył punkt dostępu bezprzewodowego
8	WIRELESS SETUP	■ Wyłączony — gdy funkcja konfigurowania łączności bezprzewodowej jest nieaktywna ■ Miga — gdy włączono funkcję konfigurowania łączności bezprzewodowej w celu dodania nowych klientów bezprzewodowych do sieci bezprzewodowej
9	TEL 1	■ Włączony — gdy usługa telefonii jest włączona ■ Miga — gdy jest używana linia 1
10	TEL 2	■ Włączony — gdy usługa telefonii jest włączona ■ Miga — gdy jest używana linia 2

Szczególne okoliczności

W tabeli poniżej opisano wygląd wskaźników stanu na przednim panelu modemu kablowego po wystąpieniu szczególnych okoliczności powodujących odmowę dostępu do sieci.

Wskaźniki stanu na przednim panelu po wystąpieniu szczególnych okoliczności		
Wskaźnik na panelu przednim		**Odmowa dostępu do sieci**
1	POWER	Wolne miganie 1 raz na sekundę
2	DS	Wolne miganie 1 raz na sekundę
3	US	Wolne miganie 1 raz na sekundę
4	ONLINE	Wolne miganie 1 raz na sekundę
5	ETHERNET 1 - 4	Wolne miganie 1 raz na sekundę
6	USB	Wolne miganie 1 raz na sekundę
7	WIRELESS LINK	Wolne miganie 1 raz na sekundę
8	WIRELESS SETUP	Wolne miganie 1 raz na sekundę
9	TEL 1	Wyłączony
10	TEL 2	Wyłączony

Uwagi

Znaki towarowe

Nazwa i logo Cisco są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco i/lub jej spółek zależnych w Stanach Zjednoczonych i innych krajach. Lista znaków towarowych firmy Cisco znajduje się na stronie **www.cisco.com/go/trademarks**.
DOCSIS jest zastrzeżonym znakiem towarowym firmy Cable Television Laboratories, Inc.EuroDOCSIS, EuroPacketCable i PacketCable są znakami towarowymi firmy Cable Television Laboratories, Inc.

Znaki towarowe innych firm są własnością ich właścicieli. Użycie słowa „partner" nie oznacza stosunku partnerstwa między firmą Cisco a jakąkolwiek inną firmą. (1009R)

Ostrzeżenie

Firma Cisco Systems, Inc. nie ponosi odpowiedzialności za ewentualne błędy lub pominięcia występujące w tym podręczniku. Zastrzegamy sobie prawo do wprowadzania zmian w podręczniku bez wcześniejszego powiadomienia.

Informacja o prawach autorskich do dokumentacji

Informacje zawarte w tym dokumencie mogą ulec zmianie bez wcześniejszego powiadomienia. Żadna część tego dokumentu nie może być powielana w jakiejkolwiek formie bez jednoznacznej pisemnej zgody firmy Cisco Systems, Inc.

Korzystanie z oprogramowania i oprogramowania sprzętowego

Oprogramowanie opisane w tym dokumencie podlega ochronie prawami autorskimi wymienionymi w umowie licencyjnej. Korzystanie z oprogramowania i jego kopiowanie jest dozwolone wyłącznie na warunkach podanych w umowie licencyjnej.

Oprogramowanie sprzętowe urządzenia podlega ochronie prawami autorskimi. Można z niego korzystać wyłącznie w urządzeniu, do którego jest dołączone. Jakiekolwiek powielanie lub rozpowszechnianie oprogramowania sprzętowego w całości albo części bez naszej jednoznacznej pisemnej zgody jest zabronione.

Więcej informacji

Jeśli masz pytania

Wszelkie pytania techniczne należy kierować do działu Cisco Services. W celu zainicjowania rozmowy z serwisantem użyj odpowiednich opcji w menu.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

+1-678-277-1120
+1-800-722-2009
www.cisco.com

W niniejszym dokumencie wymieniono różne znaki towarowe firmy Cisco Systems, Inc. Pełna lista znaków towarowych firmy Cisco Systems, Inc. użytych w dokumencie znajduje się w sekcji Uwagi.

Dostępność produktów i usług może ulec zmianie bez wcześniejszego powiadomienia.

© 2011 Cisco i/lub podmioty stowarzyszone. Wszelkie prawa zastrzeżone.

Sierpień 2011

Numer części 4041327 wer. A