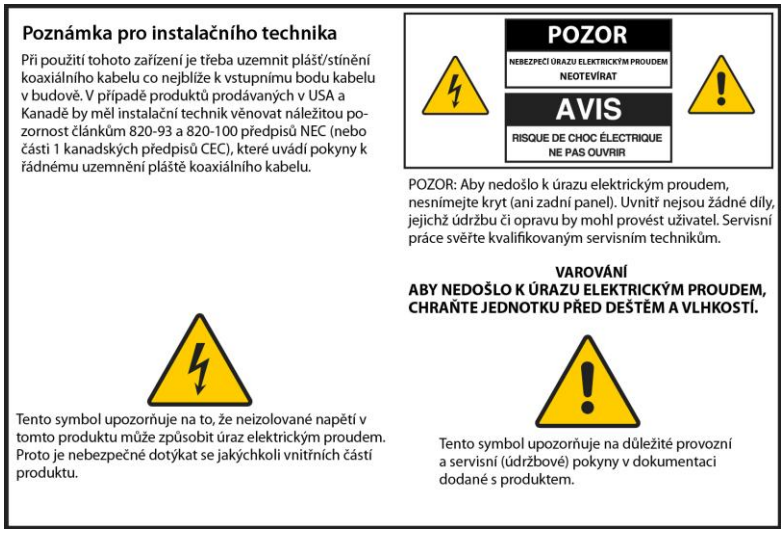
Uživatelská příručka pro bezdrátovou domácí bránu Cisco DPC3925 a EPC3925 8x4 DOCSIS 3.0 s integrovaným digitálním hlasovým adaptérem

Obsah dokumentu

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

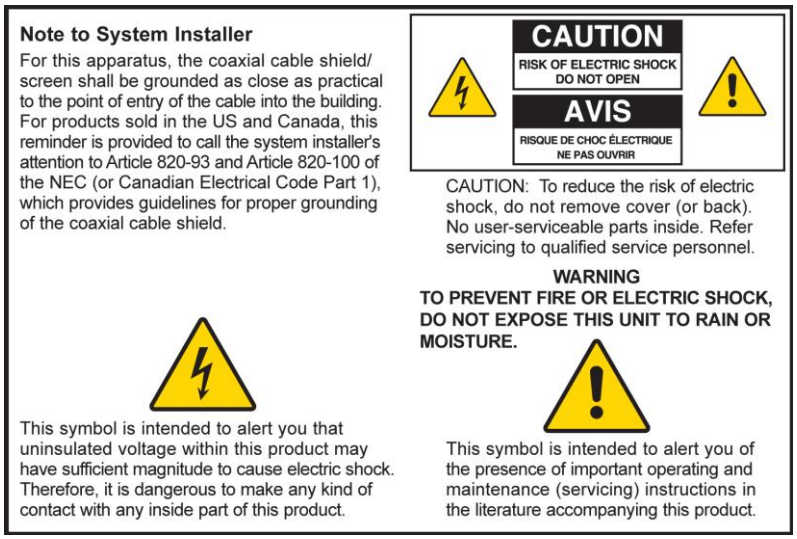
Upozornění pro instalační techniky

Servisní pokyny uvedené v tomto upozornění jsou určeny pouze pro kvalifikovaný servisní personál. Pokud nemáte odpovídající kvalifikaci, nikdy neprovádějte jiné servisní úkony, než ty popsané v provozních pokynech. Jinak byste mohli být zasaženi elektrickým proudem.



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

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

1) Přečtěte si tyto pokyny.
2) Uschovejte tyto pokyny.
3) Respektujte všechna varování.
4) Řiďte se všemi pokyny.
5) Nepoužívejte toto zařízení v blízkosti vody.
6) Čistěte jej pouze suchým hadříkem.
7) Neblokujte větrací otvory. Zařízení instalujte přesně podle pokynů výrobce.
8) Neinstalujte v blízkosti zdrojů tepla, jako jsou radiátory, tepelné vývody, sporáky či jiná zařízení (včetně zesilovačů), která produkují teplo.
9) Neobcházejte bezpečnostní funkce polarizovaných či zemnicích zástrček. Polarizovaná zástrčka má dvě vidlice, z nichž jedna je širší. Zemnicí zástrčka má dvě vidlice a zemnicí kolík. Široká vidlice nebo třetí kolík mají ochranou funkci. Pokud dodanou zástrčku nelze zasunout do zásuvky, požádejte elektrikáře o výměnu zastaralé zásuvky.
10) Napájecí kabel veďte tak, aby se na něj nešlapalo a aby nebyl nikde skřípnut, především v blízkosti zástrček a zásuvek a v místě, kde je vyveden ze zařízení.
11) Používejte pouze příslušenství doporučené výrobcem.

12) Používejte jen s vozíkem, stojanem, stativem, konzolou nebo stolem doporučenými výrobcem nebo dodanými se zařízením. Pokud zařízení používáte na vozíku, přesunujte jej velmi opatrně, aby nedošlo k poranění při převrácení vozíku.
13) Pokud je bouřka nebo pokud zařízení nebudete delší dobu používat, odpojte jej od sítě.
14) Veškeré servisní práce svěřte kvalifikovaným servisním technikům. Servis je nutný, pokud je zařízení jakkoli poškozeno, například pokud je poškozen zdroj napájení nebo napájecí zástrčka, do zařízení pronikla tekutina nebo do něj zapadly cizí předměty, pokud bylo zařízení vystaveno dešti nebo vlhku, nefunguje normálně nebo pokud upadlo.

Varování ke zdroji napájení

Štítek na tomto produktu označuje správný zdroj napájení pro tento produkt. Tento produkt připojujte pouze k elektrické zásuvce s napětím a kmitočtem uvedeným na produktovém štítku. Pokud si nejste jisti, jaký typ zdroje napájení máte doma či ve firmě, obraťte se na poskytovatele služeb nebo místní společnost zajišťující dodávku proudu.

Zásuvka střídavého proudu na jednotce musí být neustále přístupná a provozuschopná.

Uzemněte produkt

VAROVÁNÍ: Dávejte pozor, aby nedošlo k úrazu elektrickým proudem nebo požáru. Pokud se tento produkt připojuje ke koaxiálnímu kabelu, je třeba použít uzemněný kabelový systém. Uzemnění poskytuje určitý stupeň ochrany před napěťovými rázy a nahromaděnou statickou elektřinou.

Chraňte produkt před bleskem

Odpojte napájení střídavým proudem ze zásuvky a také signálové vstupy.

Ověřte přítomnost napájení pomocí indikátoru vypínače

Zařízení může být připojeno ke zdroji napájení, i když indikátor vypínače nesvítí. Indikátor může po vypnutí zařízení zhasnout, přestože je zařízení stále připojeno ke zdroji napájení střídavým proudem.

Nepřetěžujte elektrickou síť

VAROVÁNÍ: Dávejte pozor, aby nedošlo k úrazu elektrickým proudem nebo požáru. Nepřetěžujte elektrickou síť, zásuvky ani prodlužovací kabely. V případě produktů, jejich provoz vyžaduje napájení z baterie nebo jiného zdroje napájení, nahlédněte do příslušných pokynů k obsluze.

Zajistěte větrání a vyberte místo

- Před připojením produktu ke zdroji napájení odstraňte veškerý balicí materiál.
- Neumísťuje zařízení na postel, pohovku, pokrývku ani jiný podobný povrch.
- Neumísťuje zařízení na nestabilní povrch.
- Neinstalujte zařízení do uzavřeného prostoru, jako je například knihovna nebo police, pokud by v takovém případě nebylo zajištěno správné větrání.
- Nepokládejte na produkt přehrávače (např. videorekordéry, přehrávače DVD), lampy, knihy, vázy s tekutinami ani jiné předměty.
- Nezakrývejte větrací otvory.

Chraňte zařízení před vlhkostí a cizími předměty

VAROVÁNÍ: Dávejte pozor, aby nedošlo k úrazu elektrickým proudem nebo požáru. Do produktu nesmí proniknout voda, déšť ani jiná vlhkost. Nikdy na zařízení nepokládejte nádoby s tekutinami, například vázy.

VAROVÁNÍ: Dávejte pozor, aby nedošlo k úrazu elektrickým proudem nebo požáru. Před čištěním produkt vždy odpojte od zdroje napájení. Nepoužívejte tekuté čisticí prostředky ani aerosoly. K čištění produktu nepoužívejte magnetická/statická čisticí zařízení (odstraňovače prachu).

VAROVÁNÍ: Dávejte pozor, aby nedošlo k úrazu elektrickým proudem nebo požáru. Do otvorů v produktu nikdy nevkládejte žádné předměty. Cizí předměty by mohly způsobit elektrický zkrat a v důsledku toho úraz elektrickým proudem či požár.

Varování k servisu

VAROVÁNÍ: Dávejte pozor, aby nedošlo k úrazu elektrickým proudem. Nikdy neotevírejte kryt produktu. Při otevření nebo sejmutí krytu můžete být vystaveni nebezpečnému napětí. Otevření krytu znamená zrušení platnosti záruky. Tento produkt neobsahuje žádné díly, jejichž údržbu či opravu by mohl provést uživatel.

Kontrolujte bezpečnost produktu

Po dokončení servisních prací nebo oprav tohoto produktu musí servisní technik pomocí bezpečnostních kontrol vždy ověřit, zda je produkt v řádném provozním stavu.

Při přemísťování zajistěte ochranu produktu

Před přemístěním zařízení nebo připojením či odpojením kabelů vždy odpojte zdroj napájení.

Upozornění k telefonnímu zařízení

Při použití telefonního zařízení vždy dodržujte základní bezpečnostní pokyny, aby nedošlo k požáru či úrazu elektrickým proudem. Jde především o tyto zásady:

1. Nepoužívejte zařízení v blízkosti vody, například u vany, umyvadla, kuchyňského dřezu, ve vlhkém sklepě nebo v blízkosti bazénu.

2. Nepoužívejte telefon (jiný než bezdrátový) za bouřky. Při blýskání hrozí určité nebezpečí zasažení elektrickým proudem.

3. Nepoužívejte telefon k nahlášení úniku plynu v blízkosti místa úniku.

POZOR: Aby se snížilo riziko požáru, používejte pouze kabel telekomunikační linky č. 26 AWG nebo větší.

TYTO POKYNY SI ULOŽTE.

20090915_Modem No Battery_Safety

Soulad s americkými předpisy FCC

Toto zařízení bylo testováno a vyhodnoceno jako vyhovující **s** omezením jako digitální zařízení třídy B, podle odstavce 15 pravidel FCC. Omezení byla navržena za účelem zajištění přiměřené ochrany proti škodlivému rušení instalací v obytných oblastech. Toto zařízení vytváří, využívá a může vyzařovat vysokofrekvenční energii. Pokud není nainstalováno a používáno podle pokynů, může způsobovat rušení rádiového spojení. Nelze však zaručit, že při konkrétní instalaci rušení způsobovat nebude. Pokud toto zařízení způsobuje nežádoucí rušení rádiového a televizního příjmu, což lze ověřit jeho zapnutím a vypnutím, doporučujeme uživateli, aby se pokusil rušení odstranit pomocí jednoho nebo několika z následujících opatření:

- Přesměrujte nebo přemístěte přijímací anténu.
- Zvyšte vzdálenost mezi zařízením a přijímačem.
- Zapojte zařízení do elektrické zásuvky jiného okruhu, než je ten, k němuž je připojen přijímač.
- Požádejte o pomoc poskytovatele služeb nebo zkušeného radiotelevizního technika.

V případě provedení jakýchkoli změn nebo úprav, které nejsou výslovně povoleny společností Cisco Systems, Inc., může uživatel pozbýt práva používat zařízení.

Níže uvedený odstavec s prohlášením o shodě s předpisy FCC představuje požadavek úřadu FCC a informuje o schválení zařízení podle předpisů FFC. *Uvedená telefonní čísla jsou určena pouze pro dotazy týkající se předpisů FCC. Nejsou tedy určena pro dotazy ohledně zapojení nebo použití tohoto zařízení. Máte-li jakékoli otázky k použití a instalaci zařízení, kontaktujte poskytovatele služeb.*

FC Prohlášení o shodě

Toto zařízení vyhovuje části 15 předpisů FCC. Provoz zařízení je možný za následujících dvou podmínek: 1) Zařízení nesmí způsobovat škodlivé rušení. 2) Zařízení musí přijímat veškeré rušení, včetně toho, které může mít nežádoucí vliv na jeho chod.

Domácí brána DOCSIS
Model: DPC3925/EPC3925
Výrobce:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044 USA
Telefon: +1 770 236 1077

Kanadské směrnice EMI

Toto digitální zařízení třídy B splňuje požadavky kanadské směrnice ICES-003.

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

Dvoupásmové frekvence DFS

Tento produkt může být při určité konfiguraci provozován v pásmech 5 150–5 250 MHz a 5 470–5 725 MHz. Pokud zvolíte kanál v rámci těchto rozsahů frekvencí, produkt bude podle předpisů FCC možné používat pouze uvnitř budov. Venkovní použití tohoto produktu na uvedených frekvencích znamená porušení směrnic a předpisů FCC.

Prohlášení o vystavení účinkům záření

Poznámka: Tento vysílač nesmí být umístěn ani používán na stejném místě jako jiná anténa nebo vysílač. Toto zařízení musí být nainstalováno a provozováno tak, aby mezi vysílačem a tělem uživatele byla vzdálenost minimálně 20 cm.

USA

Tento systém byl hodnocen z hlediska vystavení osob vlivům rádiových frekvencí s ohledem na omezení ANSI C 95.1 (American National Standards Institute). Vyhodnocení vychází z bulletinu FCC OET 65C rev. 01.01 ve shodě s částí 2.1091 a částí 15.27. Za účelem zajištění shody je třeba zajistit, aby mezi anténou a všemi osobami byla vzdálenost minimálně 20 cm.

Kanada

Tento systém byl hodnocen z hlediska vystavení osob vlivům rádiových frekvencí s ohledem na omezení ANSI C 95.1. Vyhodnocení vychází z vyhodnocení podle předpisů RSS-102 rev. 2. Za účelem zajištění shody je třeba zajistit, aby mezi anténou a všemi osobami byla vzdálenost minimálně 20 cm.

Evropská unie

Tento systém byl hodnocen z hlediska vystavení osob vlivům rádiových frekvencí s ohledem na omezení ICNIRP (International Commission on Non-Ionizing Radiation Protection). Vyhodnocení vychází z produktové normy EN 50385 pro prokázání shody rádiových stanic a pevných terminálů pro systémy bezdrátové komunikace se základními omezeními nebo referenčními úrovněmi, které se týkají vystavení osob vlivům vysokofrekvenčních elektromagnetických polí v rozsahu 300 MHz až 40 GHz. Mezi anténou a všemi osobami musí být vzdálenost minimálně 20 cm.

Austrálie

Tento systém byl hodnocen z hlediska vystavení osob vlivům rádiových frekvencí s ohledem na normu ARP (Australian Radiation Protection) a podle limitů ICNIRP (International Commission on Non-Ionizing Radiation Protection). Mezi anténou a všemi osobami musí být vzdálenost minimálně 20 cm.

20091016 FCC DomandIntl

Shoda CE

Prohlášení o shodě s ohledem na směrnici EU 1999/5/ES (směrnice R&TTE)

Toto prohlášení platí pouze pro konfigurace (kombinace softwaru, firmwaru a hardwaru) podporované nebo poskytované společností Cisco Systems pro použití v zemích EU. Použití softwaru nebo firmwaru nepodporovaného ani neposkytovaného společností Cisco Systems může znamenat porušení shody zařízení s požadavky předpisů.

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.

Poznámka: Úplné prohlášení o shodě k tomuto produktu najdete v části Declarations of Conformity and Regulatory Information v příslušném průvodci instalací hardwaru produktu na webu Cisco.com.

Při posuzování produktu s ohledem na požadavky směrnice 1999/5/ES byly uplatněny tyto normy:

- Rádiové záření: EN 300 328
- Elektromagnetická kompatibilita: EN 301 489-1 a EN 301 489-17
- Bezpečnost: EN 60950 a EN 50385

Produkt a jeho obal jsou opatřeny značkou CE a identifikátorem 2. třídy. Tento produkt je v souladu s těmito evropskými směrnicemi:

CE ① -1999/5/ES

Národní omezení

Tento produkt je určen pouze pro použití v budovách.

Francie

V případě frekvence 2,4 GHz je výstupní výkon při venkovním použití produktu v pásmu 2 454–2 483,5 MHz omezen na 10 mW EIRP. Pro použití v jiných částech pásma 2,4 GHz neplatí žádná omezení. Více informací najdete na adrese 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.

Itálie

Tento produkt splňuje specifikace National Radio Interface a požadavky uvedené v tabulce NTFA pro Itálii. Pokud tento produkt bezdrátové sítě LAN nebude provozován pouze v prostoru, který je majetkem jeho vlastníka, jeho použití vyžaduje „obecnou autorizaci“. Více informací najdete na adrese 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.

Lotyšsko

Venkovní použití pásma 2,4 GHz vyžaduje povolení úřadu pro elektronickou komunikaci. Více informací najdete na adrese http://www.esd.lv.

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

Poznámka: Předepsané limity pro maximální výstupní výkon jsou specifikovány ve formě výkonu EIRP. Úroveň výkonu EIRP zařízení lze vypočítat přičtením zisku použité antény (v dBi) k výstupnímu výkonu na konektoru (v dBm).

Antény

Používejte pouze anténu dodanou s produktem.

20090312 CE_Gateway

Úvod

Vítejte ve vzrušujícím světě vysokorychlostního Internetu a vysoce kvalitních digitálních telefonních služeb. Nové bezdrátové domácí brány Cisco® DPC3925 DOCSIS® 3.0 a EPC3925 EuroDOCSIS™ s integrovaným digitálním hlasovým adaptérem jsou kabelové modemy, které plně odpovídají oborovým normám pro vysokorychlostní datové připojení a spolehlivou digitální telefonní službu. Domácí brány DPC3925 a EPC3925 nabízí datové a hlasové funkce a ethernetové a bezdrátové připojení pro různá zařízení doma nebo v malé kanceláři. Podporují vysokorychlostní datový přístup a hlasové služby za dobrou cenu – to vše prostřednictvím jednoho zařízení. S domácí bránou DPC3925 nebo EPC3925 získáte kvalitní připojení k Internetu a další možnosti komunikace doma či ve firmě – a to se nepochybně pozitivně odrazí na vaší produktivitě.

V této příručce naleznete postupy a doporučení k umístění, instalaci, konfiguraci a používání domácích bran DPC3925 a EPC3925 pro vysokorychlostní internetové připojení a digitální telefonní službu doma či v kanceláři a také řešení případných problémů. Vyhledejte vždy konkrétní kapitolu, která se týká vaší situace. Podrobné informace o získání služeb vám sdělí poskytovatel těchto služeb.

Výhody a vlastnosti

Domácí brány DPC3925 a EPC3925 nabízejí jedinečné výhody a vlastnosti:

- kompatibilita se standardem DOCSIS 3.0, 2.0 a 1.x a specifikacemi PacketCable™ a EuroPacketCable™ zaručující špičkový výkon a spolehlivost;
- vysoce výkonné širokopásmové připojení k Internetu pro maximální možnosti online;
- dvoulinkový integrovaný digitální hlasový adaptér pro kabelovou telefonní službu;
- čtyři ethernetové porty 1000/100/10BASE-T pro kabelové připojení;
- bezdrátový přístupový bod 802.11n;
- funkce WPS pro snadné a bezpečné nastavení bezdrátového připojení plus tlačítko pro aktivaci této funkce;
- nastavitelná rodičovská kontrola umožňuje blokování nevhodných internetových stránek;
- pokročilá brána firewall identifikuje hackery a chrání domácí síť před neoprávněným přístupem;
- atraktivní kompaktní design umožňuje vertikální či horizontální umístění i upevnění na stěnu;

- barevné značení portů rozhraní a kabelů maximálně usnadňuje instalaci a nastavení;
- označení a funkce indikátorů v souladu s normou DOCSIS-5 nabízí uživatelům a technikům snadný způsob kontroly provozního stavu a pomáhá při řešení problémů;
- možnost automatické aktualizace softwaru od poskytovatele služeb.

Co je v krabici?

Jakmile obdržíte novou bezdrátovou domácí bránu, zkontrolujte zařízení a příslušenství a ověřte, zda některá z položek nechybí nebo není poškozena. Krabice obsahuje tyto položky:

Jeden z modelů domácí brány DOCSIS (DPC3925 nebo EPC3925)

Jeden napájecí adaptér (u modelů vyžadujících externí zdroj napájení)

Jeden ethernetový kabel (CAT5/RJ-45)

Jeden disk CD-ROM

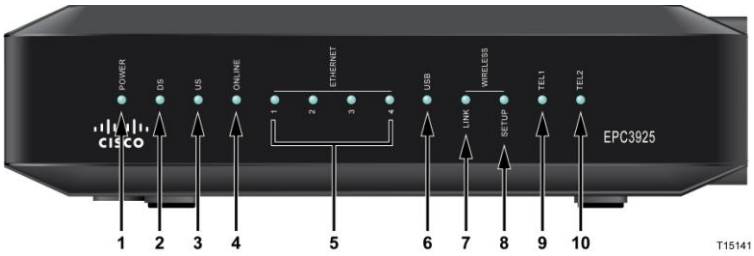
Pokud některá z těchto položek chybí nebo je poškozena, obraťte se na svého poskytovatele služeb.

Poznámky:

- Pokud chcete ke kabelovému připojení, které využívá bezdrátová domácí brána, připojit videorekordér, systém DHCT, set-top konvertor nebo televizor, budete potřebovat volitelný rozdělovač kabelového signálu a další standardní koaxiální kabely RF.
- Kabely a další vybavení pro telefonní službu je třeba zakoupit samostatně. Informace o potřebném vybavení a kabelech pro telefonní službu získáte od poskytovatele služeb.

Popis předního panelu

Na předním panelu domácí brány jsou indikátory stavu, které informují o tom, jak kvalitně domácí brána funguje a v jakém je stavu. Více informací o funkcích indikátorů stavu na předním panelu najdete v části ***Funkce indikátorů stavu na předním panelu*** (str. 103).



Na obrázku je model EPC3925.

1 **POWER** (Napájení): Když SVÍTÍ, napájení bezdrátové domácí brány je zapnuto.

2 **DS** (Příchozí připojení): Když SVÍTÍ, bezdrátová domácí brána přijímá data z kabelové sítě.

3 **US** (Odchozí připojení): Když SVÍTÍ, bezdrátová domácí brána odesílá data do kabelové sítě.

4 **ONLINE**: Když SVÍTÍ, bezdrátová domácí brána je zaregistrována v síti a je plně funkční.

5 **ETHERNET 1–4**: Když SVÍTÍ, zařízení je připojeno k jednomu z ethernetových portů. Když BLIKÁ, prostřednictvím ethernetového připojení jsou přenášena data.

6 **USB**: Když SVÍTÍ, zařízení je připojeno k portu USB. Když BLIKÁ, prostřednictvím připojení USB jsou přenášena data.

7 **WIRELESS LINK** (Bezdrátové připojení): Když SVÍTÍ, bezdrátový přístupový bod je funkční. Když BLIKÁ, prostřednictvím bezdrátového připojení jsou přenášena data. Když NESVÍTÍ, uživatel zakázal bezdrátový přístupový bod.

8 **WIRELESS SETUP** (Nastavení bezdrátového připojení): Když NESVÍTÍ (normální stav), nastavení bezdrátového připojení není aktivní. Když BLIKÁ, uživatel aktivoval nastavení bezdrátového připojení, aby mohl do bezdrátové sítě přidat nové bezdrátové klienty.

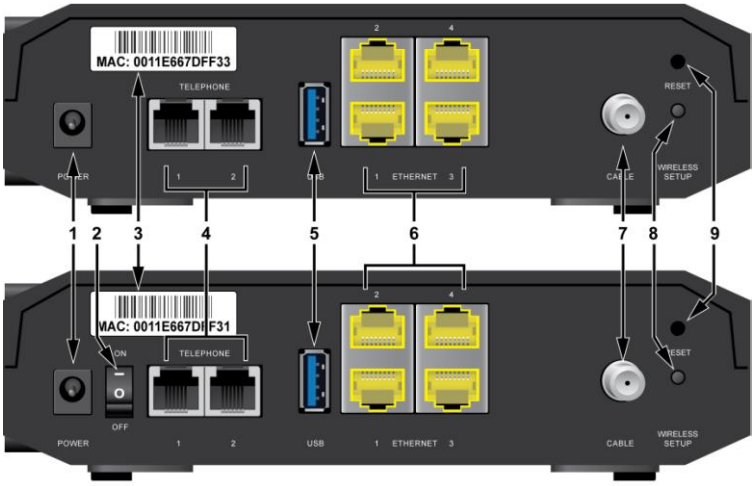
9 **TEL1**: Když SVÍTÍ, je povolena telefonní služba. Když BLIKÁ, linka 1 se používá. Když NESVÍTÍ, telefonní služba TEL 1 není povolena.

10 **TEL2**: Když SVÍTÍ, je povolena telefonní služba. Když BLIKÁ, linka 2 se používá. Když NESVÍTÍ, telefonní služba TEL 2 není povolena.

Popis zadního panelu

V následující části jsou popsány a vysvětleny prvky zadního panelu domácí brány Cisco EPC3925.

Model DPC3925



Model EPC3925

1 **POWER** (Napájení): Slouží k připojení domácí brány k dodanému adaptéru napájení střídavým proudem.

> **POZOR:**
>
> **Dejte pozor, abyste zařízení nepoškodili. Používejte pouze zdroj napájení dodaný s domácí branou.**

2 **VYPÍNAČ (jen u evropských modelů)**: Umožňuje vypnutí domácí brány bez odpojení napájecího kabelu.

3 **ŠTÍTEK S ADRESOU MAC**: Uvádí adresu MAC domácí brány.

4 **TELEPHONE 1 A 2** (Telefon 1 a 2): Telefonní konektory RJ-11 pro připojení k domácímu telefonnímu vedení nebo ke klasickému telefonu a faxu

5 **USB**: Port pro připojení vybraných klientských zařízení

6 **ETHERNET**: Čtyři ethernetové porty RJ-45 pro propojení s ethernetovým portem počítače nebo domácí sítě

7 **CABLE** (Kabel): F-konektor pro připojení aktivního kabelového signálu od poskytovatele služeb

8 **WIRELESS SETUP** (Nastavení bezdrátového připojení): Stisknutím tohoto spínače lze zahájit nastavení bezdrátového připojení. Tato funkce umožňuje přidávat do domácí sítě nové bezdrátové klienty WPS.

9 **RESET** (Restartování): Stisknutím a podržením tohoto tlačítka na 1–2 sekundy lze restartovat adaptér EMTA. Pokud toto tlačítko stisknete a podržíte déle než deset sekund, nejprve se obnoví výchozí nastavení výrobce a potom bude brána restartována.

POZOR:

Tlačítko Reset (Restartování) je určeno jen pro účely údržby. Nepoužívejte jej, pokud vás k tomu nevyzve poskytovatel kabelových nebo telefonních služeb. Jinak by se mohla vymazat všechna vámi vybraná nastavení kabelového modemu.

Jaké jsou systémové požadavky pro internetovou službu?

Aby domácí brána umožňovala skutečně efektivní použití služby vysokorychlostního Internetu, je třeba, aby všechna internetová zařízení v systému odpovídala následujícím minimálním požadavkům na hardware a software.

Poznámka: Dále je třeba také aktivní kabelová vstupní linka a internetové připojení.

Minimální systémové požadavky pro počítače typu PC

- procesor Pentium MMX 133 nebo výkonnější,
- 32 MB paměti RAM,
- webový prohlížeč,
- jednotka CD-ROM.

Minimální systémové požadavky pro počítače Macintosh

- systém MAC OS 7.5 nebo novější,
- 32 MB paměti RAM.

Systémové požadavky pro ethernetové připojení

- počítač PC s operačním systémem Microsoft Windows 2000 (nebo novějším) a s nainstalovaným protokolem TCP/IP nebo počítač Apple Macintosh s nainstalovaným protokolem TCP/IP,
- nainstalovaná aktivní ethernetová karta 10/100/1000BASE-T.

Jak získat vysokorychlostní Internet a telefonní službu?

Aby bylo možné domácí bránu používat, je třeba mít účet pro přístup k vysokorychlostnímu Internetu. Pokud účet pro přístup k vysokorychlostnímu Internetu nemáte, zřiďte si jej u místního poskytovatele služeb. Zvolte jednu z možností v této části.

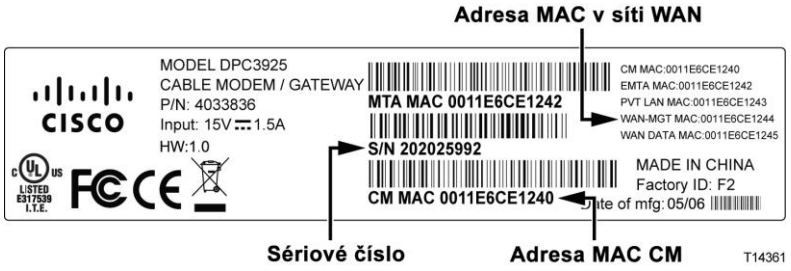
Nemám účet pro přístup k vysokorychlostnímu Internetu

Pokud *nemáte* účet pro přístup k vysokorychlostnímu Internetu, zřiďte si jej u poskytovatele služeb Internetu. Díky přístupu k Internetu budete moci odesílat a přijímat e-maily, prohlížet webové stránky a využívat další internetové služby.

Poskytovatel služeb bude potřebovat tyto informace:

- sériové číslo modemu,
- adresu MAC modemu (CM MAC),
- v případě potřeby další adresy MAC.

Tato čísla najdete na štítku s čárovým kódem na domácí bráně. Sériové číslo je řada alfanumerických znaků uvedená za kódem **S/N**. Adresa MAC je řada alfanumerických znaků uvedená za kódem **CM MAC**. Na níže uvedeném obrázku vidíte vzorový štítek s čárovým kódem.



Zapište čísla svého zařízení na následující řádky.

Sériové číslo _____

Adresa MAC _____

Účet pro přístup k vysokorychlostnímu Internetu již mám

Pokud již účet pro přístup k vysokorychlostnímu Internetu máte, je třeba poskytovateli služeb sdělit sériové číslo a adresu MAC domácí brány. Bližší informace o sériovém čísle a adrese MAC naleznete výše.

Pro telefonní službu chci používat aplikační server

Chcete-li domácí bránu používat pro telefonní službu, je třeba u místního poskytovatele služeb zřídit telefonní účet. Poskytovatel služeb vám buď umožní přenést vaše stávající telefonní čísla, nebo vám pro každou stávající nebo další aktivní telefonní linku přiřadí nové číslo. Podrobné informace o těchto možnostech získáte od poskytovatele telefonních služeb.

Kam umístit domácí bránu DOCSIS?

Domácí bránu je vhodné umístit tak, aby ji bylo možné snadno připojit k zásuvkám a dalším zařízením. Představte si rozmístění nábytku a zařízení doma nebo v kanceláři a vyberte spolu s poskytovatelem služeb optimální místo. Než se rozhodnete, kam domácí bránu umístíte, důkladně si přečtěte tuto uživatelskou příručku.

Vezměte v úvahu následující doporučení:

- Pokud budete domácí bránu používat i pro vysokorychlostní připojení k Internetu, zvolte místo blízko počítače.
- Zvolte místo blízko stávajícího koaxiálního připojení RF, abyste nemuseli používat další koaxiální zásuvku RF.
- Pokud používáte jen jedno či dvě telefonní zařízení, umístěte domácí bránu do jejich blízkosti.

  Poznámka: Pokud domácí bránu chcete použít k zajištění služeb pro více telefonů, instalační technik ji může připojit ke stávajícímu domácímu telefonnímu vedení. Abyste domácí telefonní vedení nemuseli zásadním způsobem měnit, umístěte domácí bránu poblíž stávající telefonní zásuvky.
- Zvolte místo, které je relativně chráněno před náhodným narušením nebo poškozením, například komoru, suterén či jiný chráněný kout.
- Zvolte takové místo, aby bylo možné vést kabely od modemu tak, aby nebyly namáhány nebo ohnuty.
- Vždy musí být zajištěno volné proudění vzduchu okolo domácí brány.
- Před instalací domácí brány si pečlivě přečtěte tuto příručku.

Jak modem upevnit na stěnu? (volitelné)

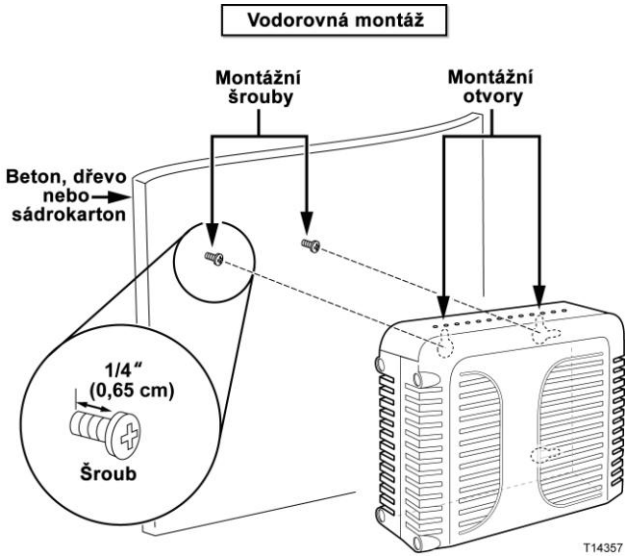
Domácí bránu je možné pomocí dvou kotvicích šroubů (hmoždinek), dvou šroubů a montážních otvorů na jednotce upevnit na stěnu. Modem lze upevnit svisle nebo vodorovně.

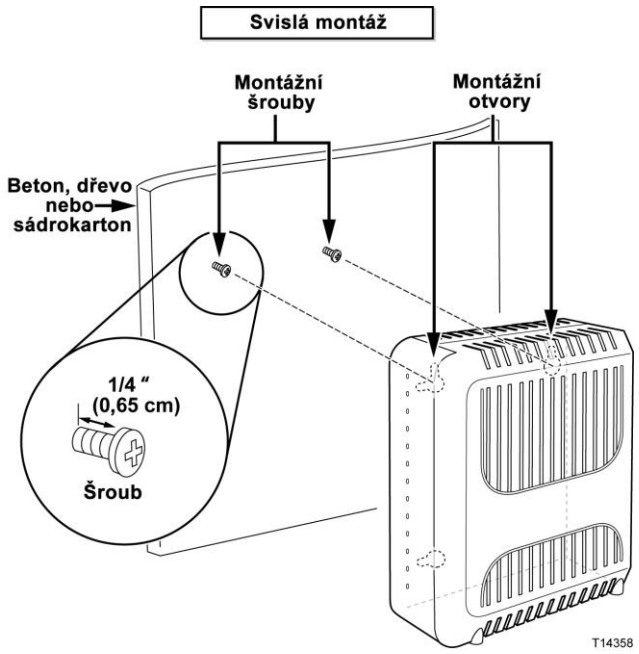
Než začnete

Nejprve vyberte vhodné místo. Stěna může být cementová, dřevěná nebo sádrokartonová. Místo montáže musí být ze všech stran dobře přístupné a kabely domácí brány musí být možné vést tak, aby nebyly namáhány. Mezi spodní stranou domácí brány a podlahou či policemi pod ní musí být dostatečný prostor pro přístup ke kabelům. Všechny kabely musí být dostatečně volné, aby bylo možné domácí bránu při provádění údržby posunout, aniž by bylo nutné kabely odpojovat. Dále ověřte, zda máte:

- dva kotvicí šrouby (hmoždinky) pro 1" šrouby č. 8,
- dva 1" křížové šrouby č. 8,
- vrtačku s 3/16" vrtákem do dřeva nebo zdiva (podle potřeby),
- schémata pro montáž na stěnu uvedená na následujících stránkách.

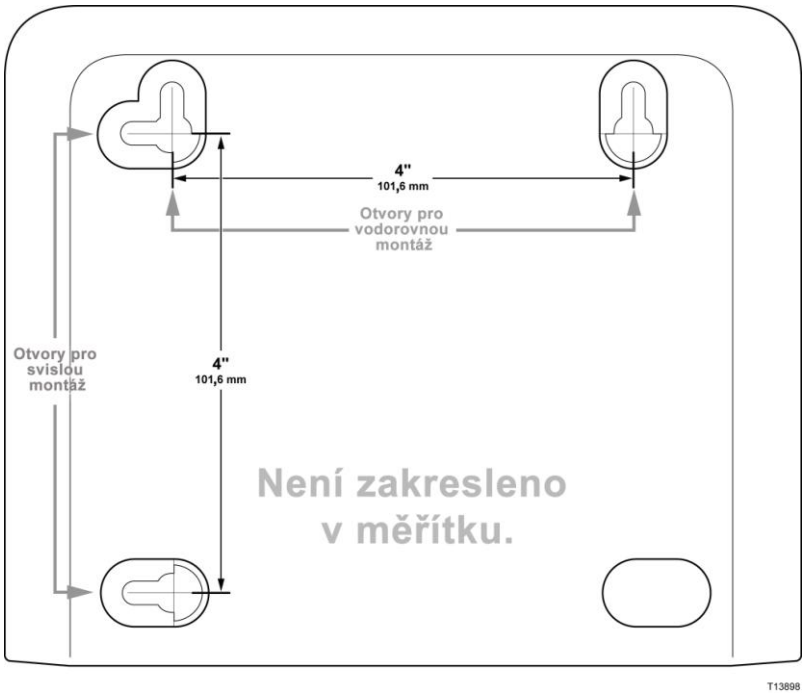
Upevněte modem podle jednoho z následujících obrázků.





Umístění a rozměry otvorů pro montáž na stěnu

Na níže uvedeném obrázku je vyznačeno umístění montážních otvorů na spodní straně modemu a jejich rozměry. Tyto informace vám usnadní montáž modemu na stěnu.



Montáž domácí brány na stěnu)

1 Vrtačkou s 3/16" vrtákem vyvrtejte ve stejné výšce, 10,2 cm od sebe dva otvory.

Poznámka: Umístění montážních otvorů na zadní straně domácí brány je vyznačeno na obrázku výše.

2 Upevňujete domácí bránu na sádrokartonový nebo betonový povrch s dřevěným sloupkem?

- Pokud **ano**, přejděte ke kroku 3.
- Pokud **ne**, navrtejte do stěny kotvicí šrouby a zašroubujte do nich montážní šrouby. Mezi hlavou šroubu a stěnou ponechte mezeru přibližně 0,6 cm. Potom přejděte ke kroku 4.

3 Zašroubujte montážní šrouby do stěny a mezi hlavou šroubu a stěnou ponechte mezeru přibližně 0,6 cm. Potom přejděte ke kroku 4.

4 Zkontrolujte, zda k domácí bráně nejsou připojeny žádné kabely ani vodiče.

5 Zvedněte domácí bránu do montážní pozice. Nasaďte širší konec montážních otvorů na zadní straně domácí brány na montážní šrouby a poté domácí bránu posuňte směrem dolů tak, aby úzký konec otvorů dosedl na šrouby.

Důležité: Než domácí bránu pustíte, ujistěte se, že ji montážní šrouby pevně drží.

Jaké jsou požadavky pro telefonní službu?

Počet telefonních zařízení

Každý telefonní konektor RJ-11 na domácí bráně může zajistit telefonní služby pro několik telefonů, faxů a analogových modemů.

Maximální počet telefonních zařízení, které lze připojit ke každému konektoru RJ-11, je omezen celkovým počtem čísel připojených telefonních zařízení (REN). Hodnota REN se uvádí na mnoha telefonních zařízeních. Každý telefonní port na domácí bráně podporuje až 5 čísel REN.

Součet čísel REN všech telefonních zařízení připojených k jednotlivým portům nesmí překročit 5.

Typy telefonních zařízení

S domácí bránou lze používat i telefonní zařízení bez vyznačeného čísla REN. V takovém případě však není možné přesně určit maximální počet telefonních zařízení, které lze připojit. Používáte-li neoznačená telefonní zařízení, po připojení každého zařízení ověřte, zda funguje vyzvánění. Teprve potom můžete připojit další zařízení. Pokud připojíte příliš mnoho telefonních zařízení a přestane se ozývat vyzvánění, postupně zařízení odpojujte, dokud vyzvánění opět nebude fungovat, jak má.

Aby bylo možné k telefonním portům domácí brány připojit telefony, faxy a jiná telefonní zařízení, tato zařízení musí mít uprostřed konektorů RJ-11 2 kontakty. Některé telefony jsou vybaveny konektory RJ-11 s jinými kontakty – v takovém případě je třeba použít adaptér.

Požadavky na vytáčení

Ve všech telefonech nastavte tónovou volbu. Využití pulzní volby poskytovatelé služeb obvykle neumožňují.

Požadavky na telefonní vedení

Domácí brána umožňuje připojení k vnitřnímu telefonnímu vedení. Lze ji však připojit také přímo k telefonu nebo faxu. Vzdálenost mezi jednotkou a nejvzdálenějším telefonním zařízením nesmí být větší než 300 metrů. Pro telefonní vedení použijte kroucený pár č. 26 nebo větší.

Důležité: Připojení ke stávající nebo nové pevně instalované domácí telefonní síti musí provést kvalifikovaný technik.

Jak bránu připojit k Internetu a telefonní službě?

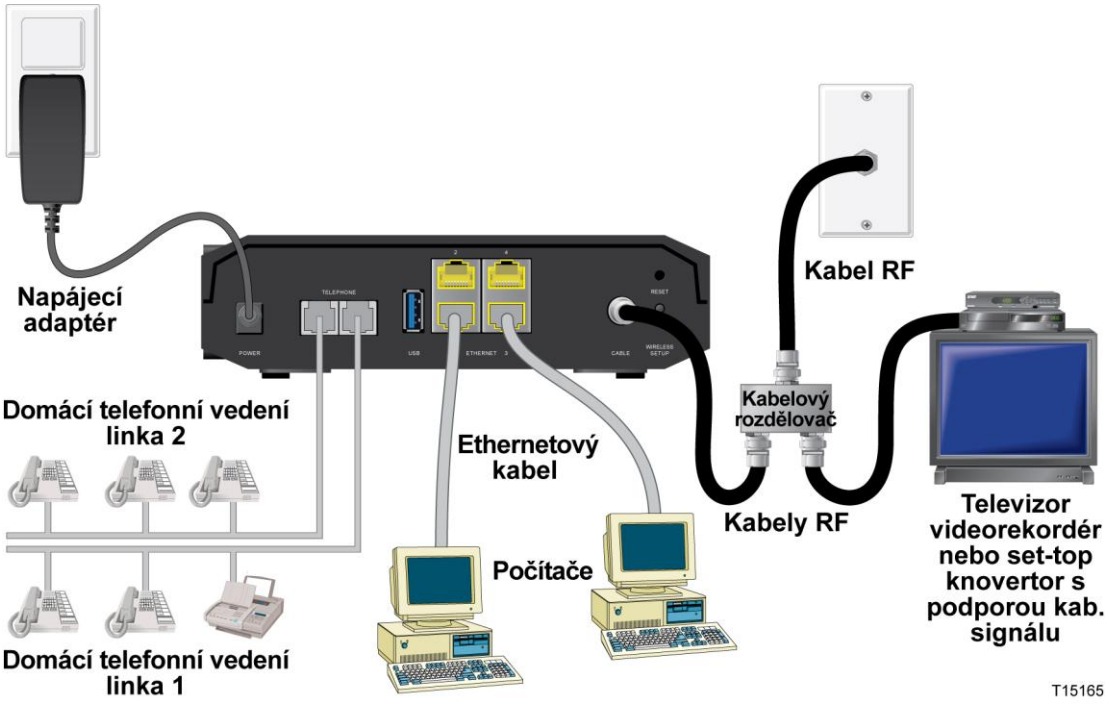
Domácí brána může poskytovat přístup k telefonní službě i Internetu. Přístup k Internetu lze použít pro několik zařízení doma či v kanceláři. Použití jednoho připojení pro více zařízení se označuje jako použití v síti.

Připojení a instalace internetových zařízení

Instalaci je zpravidla možné svěřit do rukou odborníků. Obraťte se na místního poskytovatele služeb.

Připojení zařízení

V následujícím schématu jsou naznačeny různé možnosti síťového řešení, které máte k dispozici.



Připojení domácí brány pro použití vysokorychlostního datového připojení a telefonní služby

V této části je popsán postup instalace, který zaručuje správné nastavení a konfiguraci domácí brány.

1 Zvolte vhodné a bezpečné místo pro instalaci domácí brány – blízko zdroje napájení, aktivního kabelového připojení, počítače (chcete-li používat vysokorychlostní Internet) a telefonních linek (chcete-li používat služby VoIP).

VAROVÁNÍ:

- **Abyste se nezranili, postupujte podle pokynů k instalaci v uvedeném pořadí.**
- **Aby nedošlo k poškození zařízení, před připojením kabelového modemu k vedení odpojte jakékoli jiné telefonní služby k němu připojené.**
- **Na telefonních portech domácí brány a také na všech připojených kabelech, například ethernetovém, telefonním nebo koaxiálním kabelu, může být nebezpečné elektrické napětí.**
- **Telefonní vedení a připojení musí být řádně izolována, aby nemohlo dojít k úrazu elektrickým proudem.**
- **Telefonní připojení k nainstalované domácí telefonní kabelové síti musí provést kvalifikovaný technik. Odbornou instalaci a připojení k domácí telefonní kabelové síti může nabízet přímo poskytovatel kabelových telefonních služeb. Tato služba může být zpoplatněna.**
- **Kabely a připojení musí být řádně izolovány, aby nemohlo dojít k úrazu elektrickým proudem.**
- **Před připojením jakéhokoli zařízení odpojte domácí bránu od napájení.**

2. Vypněte počítač a další síťová zařízení a odpojte je od zdroje napájení.
3. Do koaxiálního konektoru **CABLE** (Kabel) na zadní straně domácí brány zapojte aktivní koaxiální kabel RF od poskytovatele služeb.

   Poznámka: Chcete-li prostřednictvím stejného kabelového připojení připojit televizor, systém DHCT, set-top konvertor nebo videorekordér, je třeba nainstalovat rozdělovač kabelového signálu (není součástí dodávky). Rozdělovač může zhoršit kvalitu signálu. Proto se před jeho použitím nejprve poraďte s poskytovatelem služeb.
4. Jedním z následujících způsobů připojte k domácí bráně počítač.
   - **Ethernetové připojení:** Jeden konec žlutého ethernetového kabelu připojte k ethernetovému portu na počítači a druhý konec ke žlutému portu **ETHERNET** na zadní straně domácí brány.

     Poznámka: Chcete-li nainstalovat více ethernetových zařízení, než je portů na domácí bráně, použijte externí víceportové ethernetové přepínače.
   - **Bezdrátové připojení:** Ověřte, zda je zapnuto bezdrátové zařízení. Jakmile bude brána zprovozněna, bude třeba s ní bezdrátové zařízení propojit. Při připojování zařízení k bezdrátovému přístupovému bodu postupujte podle pokynů dodaných s tímto zařízením.

     Více informací o výchozí konfiguraci bezdrátové brány najdete v části ***Konfigurace bezdrátového nastavení*** (str. 39) v této příručce.
5. Připojte jeden konec telefonního propojovacího kabelu (není součástí dodávky) k telefonní zásuvce nebo k telefonu či faxu. Druhý konec propojovacího kabelu potom připojte k požadovanému portu RJ-11 **TELEPHONE** (Telefon) na zadní straně domácí brány. Telefonní porty jsou světle šedé a v závislosti na oblasti, kde je domácí brána používána, jsou označeny jako 1/2 a 2 nebo 1 a 2.

Poznámky:

- Dejte pozor, abyste telefonní službu připojili ke správnému portu RJ-11. Pro službu s jednou telefonní linkou použijte port 1/2 nebo 1.
- V Severní Americe domácí brány na telefonním portu RJ-11 1/2 podporují více linek. Linka 1 je na portu 1/2 na kontaktech 3 a 4 a linka 2 na kontaktech 2 a 5. V Evropě domácí brány podporují jen jednu linku na port. Linka 1 je na portu 1 a linka 2 na portu 2.
- Telefony vybavené jinými konektory než RJ-11 mohou vyžadovat použití externího adaptéru (prodává se samostatně).

6 Vezměte kabel napájení střídavým proudem dodaný s domácí bránou. Jeden konec tohoto kabelu zapojte do konektoru napájení střídavým proudem na zadní straně domácí brány. Potom kabel zapojte do zásuvky napájení střídavým proudem. Domácí brána je nyní napájena. Domácí brána automaticky vyhledá širokopásmovou datovou síť a přihlásí se k ní. Tento proces může trvat 2–5 minut. Jakmile indikátory **POWER** (Napájení), **DS** (Příchozí připojení), **US** (Odchozí připojení) a **ONLINE** na předním panelu domácí brány přestanou blikat a začnou svítit, modem je připraven k použití.

7 Zapojte počítač a další zařízení v domácí síti do zásuvky a zapněte je. Indikátor **LINK** (Připojení) na domácí bráně odpovídající připojenému zařízení by měl svítit nebo blikat.

8 Jakmile bude domácí brána online, většina internetových zařízení bude mít okamžitý přístup k Internetu.

Poznámka: Pokud počítač nemá přístup k Internetu, nahlédněte do části ***Nejčastější dotazy*** (str. 97), kde najdete informace o konfiguraci počítače pro použití protokolu TCP/IP. V případě jiných internetových zařízení než počítače vyhledejte v uživatelské příručce pro dané zařízení část o konfiguraci serveru DHCP nebo adresy IP.

Jak nakonfigurovat domácí bránu DOCSIS?

Chcete-li domácí bránu nakonfigurovat, je třeba otevřít konfigurační stránky WebWizard. V této části jsou uvedeny podrobné pokyny a postupy pro otevření stránek WebWizard a správnou konfiguraci domácí brány. Najdete zde také příklady a popis všech konfiguračních stránek WebWizard. Doporučujeme vám nepoužívat výchozí nastavení, ale přizpůsobit nastavení domácí brány vašim konkrétním potřebám pomocí stránek WebWizard. Stránky WebWizard v této části jsou uspořádány v pořadí, v jaké jsou uvedeny na stránce **Nastavení**.

Důležité: Stránky WebWizard a uvedené příklady v této části slouží jen pro informační účely. Stránky, které se vám zobrazí, se mohou od stránek v této příručce lišit. Na stránkách zobrazených v této příručce jsou uvedeny výchozí hodnoty nastavení zařízení.

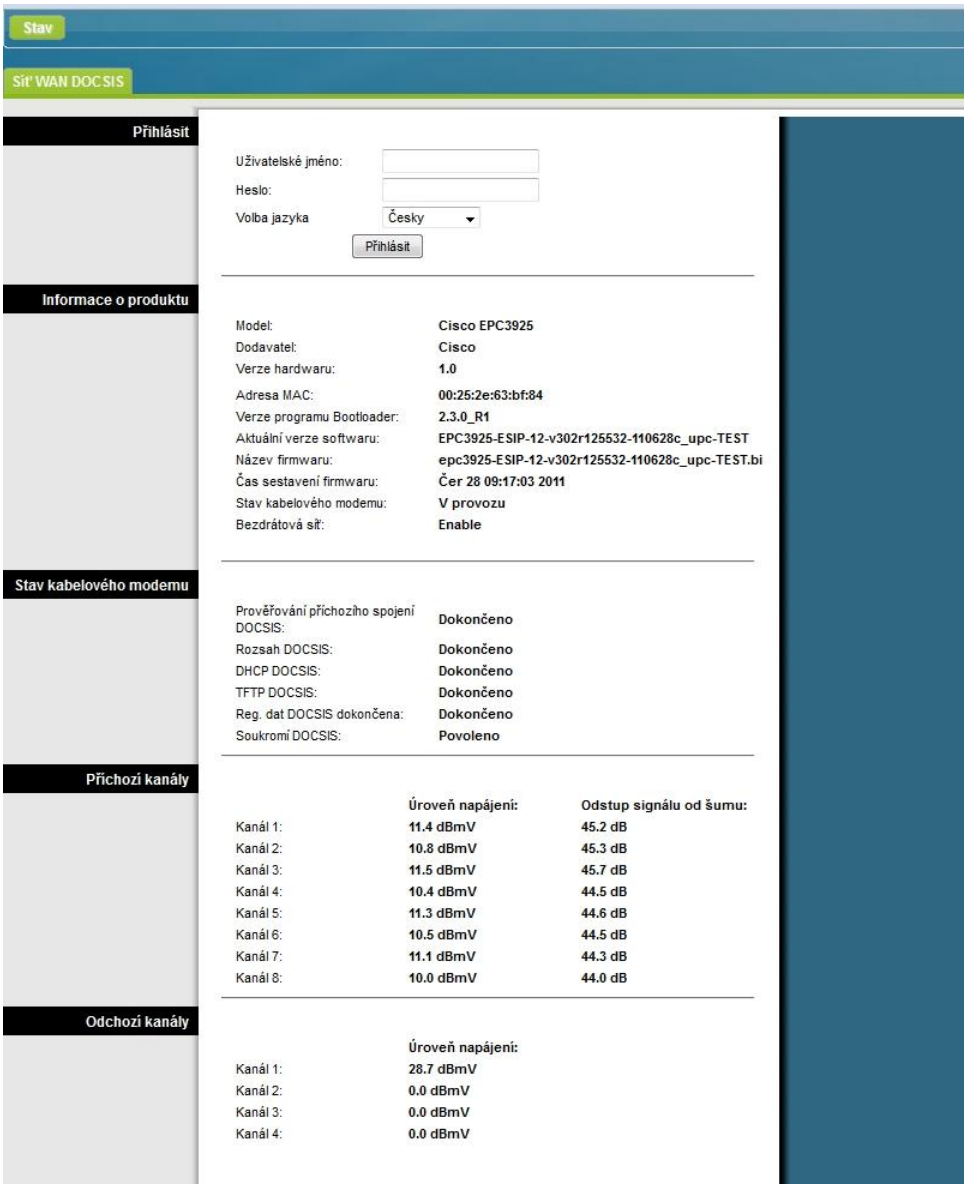
Poznámka: Pokud nemáte zkušenosti s konfigurací sítě popsanou v této části, před změnou jakéhokoli výchozího nastavení domácí brány kontaktujte poskytovatele služeb.

První přihlášení k bráně

Výchozí konfigurace brány používá adresu IP 192.168.0.1. Pokud je brána správně připojena a pokud je správně nastaven počítač, přihlaste se k bráně pomocí těchto kroků jako správce.

1 Spusťte v počítači požadovaný webový prohlížeč.

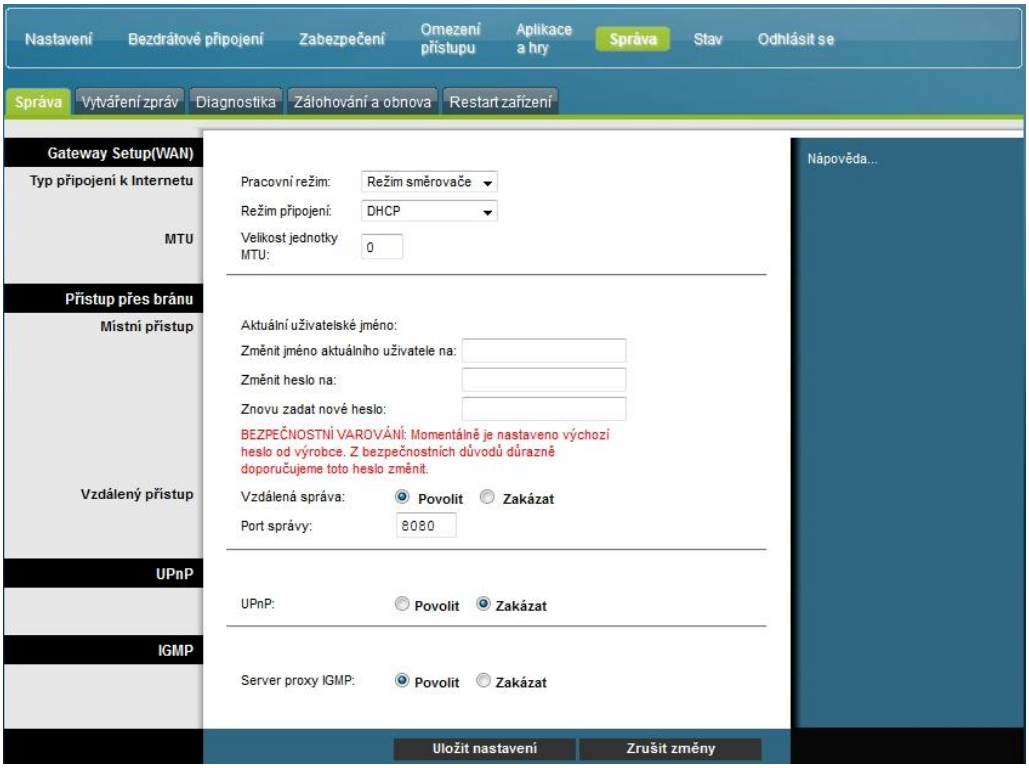
2 Do pole pro adresu zadejte tuto adresu IP: **192.168.0.1**. Otevře se stavová přihlašovací stránka DOCSIS WAN podobná následující stránce.



3 Na stavové stránce DOCSIS WAN ponechte pole Uživatelské jméno a Heslo prázdná a klikněte na tlačítko **Přihlásit**. Otevře se brána s vybranou stránkou pro správu. Pomocí stránky pro správu můžete změnit své uživatelské jméno a heslo.

V tomto okamžiku jste k bráně přihlášeni. Můžete vybrat jakoukoli webovou stránku pro nastavení a správu. To, že se otevřela stránka pro správu, je však signál, že je vhodné nastavit nové heslo.

Důležité: Doporučujeme, abyste si nové heslo nastavili. Ochráníte se tak před internetovými útoky cílenými na zařízení používající známá či výchozí uživatelská jména nebo hesla.



4 Na stránce pro správu vytvořte uživatelské jméno a heslo a klikněte na možnost **Uložit nastavení**. Po uložení nastavení uživatelského jména a hesla na stránce pro správu se otevře stránka Nastavení > Quick Setup (Rychlé nastavení).

Důležité: Pole pro heslo můžete ponechat prázdné (výchozí nastavení). Pokud však uživatelské jméno a heslo nezměníte, při každém přihlašování k bráně se bude otevírat stránka pro správu. Ta slouží jako upozornění, že je třeba nastavit vlastní heslo.

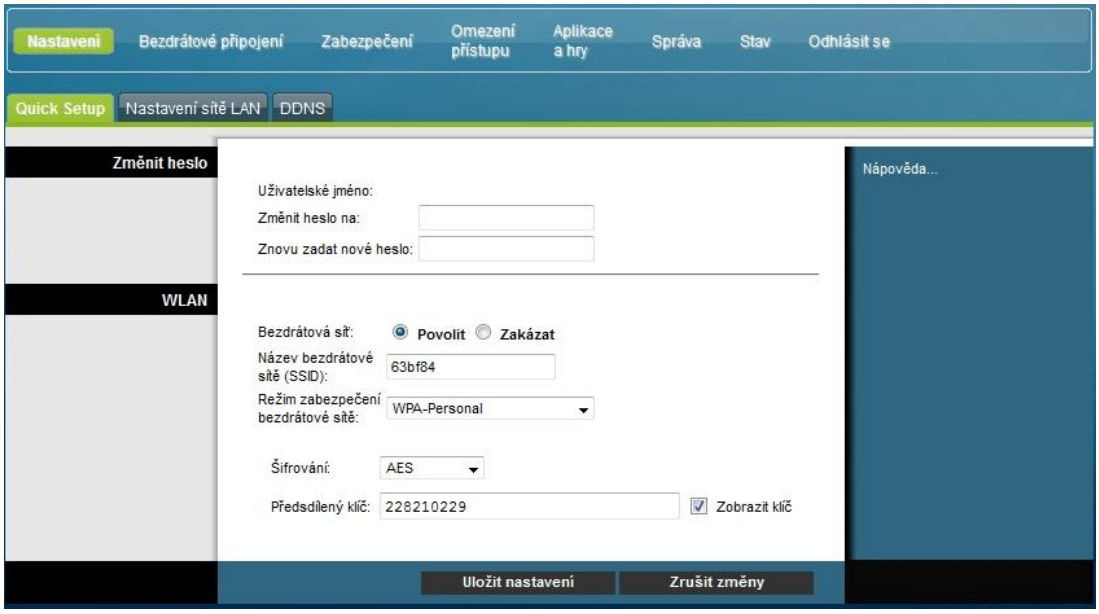
Pokud nastavíte vlastní heslo, při každém dalším přihlášení se otevře stránka Nastavení > Quick Setup (Rychlé nastavení).

5 Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Nastavení > Quick Setup (Rychlé nastavení)

Stránka Nastavení > Quick Setup (Rychlé nastavení) je první stránka, která se otevře po přihlášení k bráně. Nastavení na této stránce umožňují změnit heslo a nakonfigurovat síť WLAN.

Důležité: Nastavení na této stránce jsou pro vaše zařízení jedinečná. Nastavení na této stránce není nutné měnit. Tato výchozí nastavení plně zajišťují bezpečný provoz bezdrátové sítě.



Konfigurace rychlého nastavení

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci síťového nastavení pro zařízení. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Změnit heslo	**Uživatelské jméno** Zde se zobrazuje uživatelské jméno aktuálně přihlášeného uživatele. **Změnit heslo na** Umožňuje změnit heslo. **Znovu zadat nové heslo** Umožňuje opětovné zadání nového hesla. Je třeba zadat stejné heslo, jaké jste zadali do pole **Změnit heslo na.**

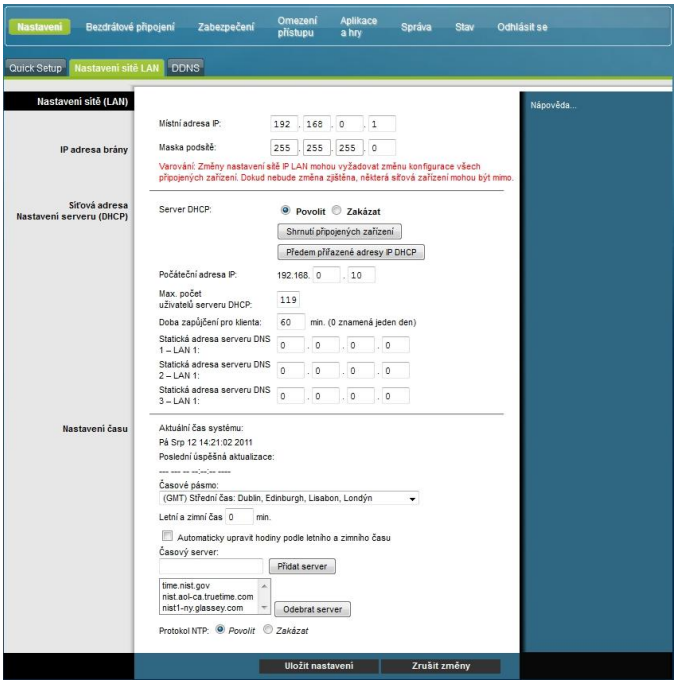
Část	Popis pole
WLAN	**Bezdrátová síť** Umožňuje zapnout nebo vypnout bezdrátovou síť. Vyberte požadovanou možnost: ■ Povolit ■ Zakázat **Název bezdrátové sítě (SSID)** Umožňuje zadat název bezdrátové sítě nebo použít výchozí název. Zadaná hodnota se bude zobrazovat v počítačích a jiných bezdrátových klientských zařízeních. **Poznámka:** Výchozí identifikátor SSID obvykle obsahuje posledních 6 znaků adresy CM MAC. Adresa CM MAC je uvedena na typovém štítku na bezdrátové bráně. **Režim zabezpečení bezdrátové sítě** Umožňuje volbu režimu zabezpečení sítě. Pokud vyberete možnost **Zakázat**, bezdrátová síť nebude zabezpečená a bude se k ní moci připojit jakékoli bezdrátové zařízení v dosahu. Podrobný popis režimů bezdrátového zabezpečení najdete v části ***Zabezpečení bezdrátové sítě*** (str. 43). **Poznámka:** Výchozím režimem bezdrátového zabezpečení je WPA nebo WPA2-Personal. **Šifrování** Umožňuje vybrat úroveň šifrování podle vybraného režimu bezdrátového zabezpečení. Podrobný popis šifrování najdete v části ***Zabezpečení bezdrátové sítě*** (str. 43). **Předsdílený klíč** Předsdílený klíč zařízení. Může obsahovat 8 až 63 znaků. Výchozí předsdílený klíč je stejný jako 9místné sériové číslo brány. Sériové číslo je uvedeno na typovém štítku na bezdrátové bráně. **Poznámka:** Váš poskytovatel služeb vám může dodat kartu pro konfiguraci bezdrátové sítě obsahující identifikátor SSID a informace o konfiguraci bezdrátového zabezpečení pro domácí síť, které se mohou od výše uvedeného popisu lišit.

Nastavení > Nastavení sítě LAN

Stránka Nastavení > Nastavení sítě LAN umožňuje nakonfigurovat nastavení pro síť LAN. Jde například o nastavení rozsahu adres IP, které definuje vlastní síť LAN, a také způsob přiřazování adres (automaticky serverem DHCP nebo ručně) při přidávání nových zařízení do sítě.

Důležité: Pokud nejste dobře obeznámeni se správou adres IP, doporučujeme tato nastavení neměnit. Pokud byste tyto hodnoty změnili nevhodně, mohl by být znemožněn přístup k Internetu.

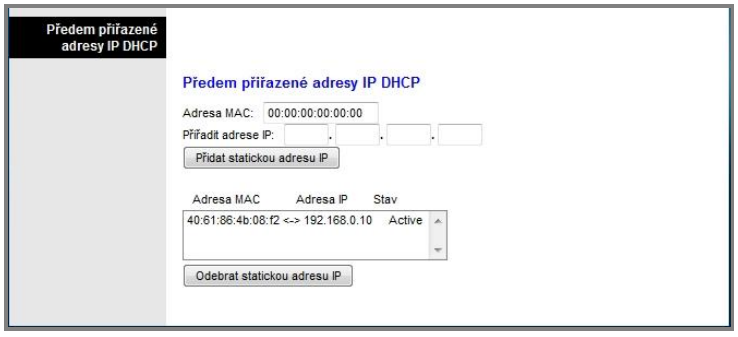
Zvolením karty **Nastavení sítě LAN** otevřete stránku Nastavení > Nastavení sítě LAN.



Konfigurace nastavení sítě

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci síťového nastavení pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Nastavení sítě (LAN)	**Místní adresa IP**
IP adresa brány	Základní adresa IP privátní domácí sítě LAN. Výchozí adresa IP sítě LAN je 192.168.0.1.
	Maska podsítě
	Maska podsítě sítě LAN

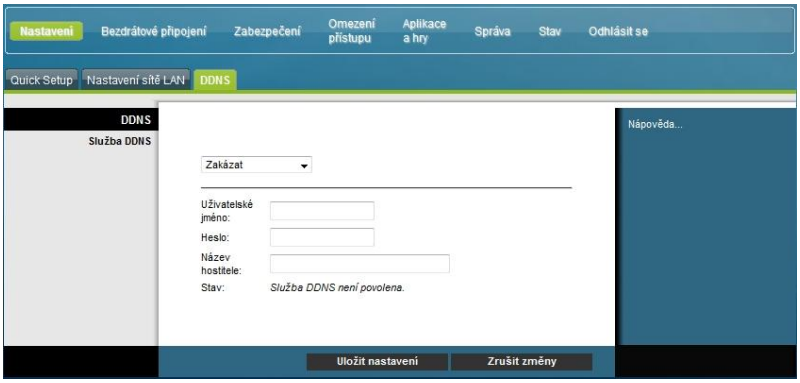
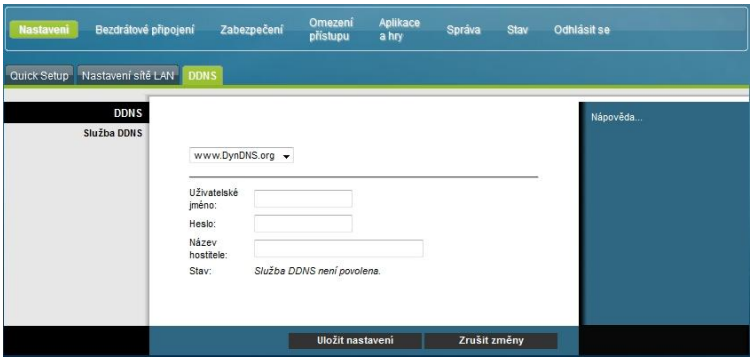
Část	Popis pole
Síťová adresa – Nastavení serveru (DHCP)	**Server DHCP** Umožňuje zapnout či vypnout server DHCP v domácí bráně. Server DHCP zajišťuje automatické přidělování adres IP zařízením připojovaným do domácí sítě. ■ **Stránka Shrnutí připojených zařízení** Klikněte na možnost **Shrnutí připojených zařízení** na stránce Nastavení sítě LAN. Otevře se stránka Shrnutí připojených zařízení. Jde o místní okno, v němž jsou zobrazeny adresy MAC a IP zařízení připojených k domácí bráně.  ■ **Stránka Předem přiřazené adresy IP DHCP** Klikněte na možnost **Předem přiřazené adresy IP DHCP** na stránce Nastavení sítě LAN. Otevře se stránka Předem přiřazené adresy IP DHCP. Tato stránka umožňuje přiřadit počítači či jinému zařízení požadujícímu adresu IP prostřednictvím serveru DHCP konkrétní adresu IP. Pomocí této funkce lze vyhradit pouze adresy v rozsahu fondu adres DHCP brány.  **Poznámky:** – Tlačítkem **Přidat statickou adresu IP** přidáte statickou adresu IP do seznamu předem přiřazených adres IP. – Tlačítkem **Odebrat statickou adresu IP** statickou adresu IP ze seznamu předem přiřazených adres IP odeberete.

Část	Popis pole
	Počáteční adresa IP Zde se zobrazuje počáteční adresa, kterou integrovaný server DHCP používá k distribuci adres IP v privátní síti LAN. Výchozí adresa IP brány je **192.168.0.1**, takže počáteční adresa IP musí být **192.168.0.2** nebo vyšší, ale zároveň nižší než **192.168.0.253**. Výchozí počáteční adresa IP je **192.168.0.10.** **Max. počet uživatelů serveru DHCP** Zde je možné zadat maximální počet uživatelů, kterým může server DHCP přiřadit adresu IP pro použití v síti LAN. Tento počet nesmí překročit hodnotu 254 minus počáteční adresa IP popsaná výše. **Doba zapůjčení pro klienta** Doba zapůjčení pro klienta je doba, po kterou platí přiřazená adresa IP. Počítače a jiná zařízení, která adresu IP získávají prostřednictvím serveru DHCP, zapůjčení adresy IP automaticky obnovují. Pokud platnost zapůjčení skončí, adresa IP je vrácena do fondu dostupných adres IP, které může server DHCP přiřadit zařízením, která jsou nově přidána do sítě. Pokud je brána online, výchozí doba je 60 minut. **Statická adresa serveru DNS LAN 1–3** Prostřednictvím serveru DNS zjišťují počítače či jiná klientská zařízení veřejnou adresu IP přiřazenou k adrese URL nebo názvu webu. Zadáním adres IP těchto serverů do těchto polí můžete ručně určit, které servery DNS mají zařízení v síti používat. Jinak bude brána předávat informace serveru DNCS od poskytovatele služeb automaticky. Ve výchozím nastavení jsou tato pole prázdná.
Nastavení času	**Časové pásmo** Vyberte požadované časové pásmo. Pokud se ve vaší oblasti používá zimní a letní čas, vyberte možnost **Automaticky upravit hodiny podle letního a zimního času**.

Nastavení > DDNS

Služba DDNS poskytuje domácí bráně (která může mít dynamickou adresu IP) název hostitele nebo adresu URL, které dokážou síťové aplikace přeložit pomocí standardních dotazů DNS. Služba DDNS je užitečná, pokud za zařízením hostujete vlastní webovou stránku, server FTP či jiný server. Aby bylo možné tuto funkci použít, je třeba se zaregistrovat k odběru služby DDNS.

Zvolením karty **DDNS** otevřete stránku Nastavení > DDNS.

Část	Popis pole
Služba DDNS	**Vypnutí služby DDNS** (výchozí nastavení) Chcete-li službu DDNS vypnout, vyberte v rozevíracím seznamu možnost **Zakázáno** a klikněte na možnost **Uložit nastavení**.  **Zapnutí služby DDNS** **Poznámka:** Chcete-li funkci DDNS použít, nejprve si zřiďte účet a vytvořte adresu URL prostřednictvím webu www.DynDNS.org. Bez platného účtu nebude funkce DDNS fungovat. Chcete-li si zřídit účet DDNS, spusťte prohlížeč a do pole pro adresu zadejte adresu www.DynDNS.org. Vytvořte účet podle pokynů na webu. Službu DDNS zapnete podle následujících pokynů. **1** Na stránce DDNS vyberte server DDNS **www.DynDNS.org**.  **2** Nastavte následující pole: ■ Uživatelské jméno, ■ Heslo, ■ Název hostitele. **3** Klikněte na možnost **Uložit nastavení**. Zařízení nyní bude službu DDNS informovat o aktuální adrese IP WAN (Internet), kdykoli dojde k její změně. **Důležité:** Oblast Stav v tomto okně bude zobrazovat stav připojení ke službě DDNS.

Konfigurace bezdrátového nastavení

V této části jsou popsány možnosti dostupné na stránce Bezdrátové připojení, které lze použít ke konfiguraci parametrů sítě WAN podle požadavků uživatele.

Bezdrátové připojení > Základní nastavení

Nastavení domácí brány pro bezdrátovou komunikaci umožňuje připojení k Internetu z jakéhokoli místa v dosahu sítě WAN bez použití kabelů. Zvolením karty **Základní nastavení** otevřete stránku Bezdrátové připojení > Základní nastavení.

Na stránce Bezdrátové připojení > Základní nastavení můžete zvolit režim bezdrátové sítě a další základní funkce.

- Bezdrátová síť: Povolit, nebo Zakázat,
- Konfigurace bezdrátové sítě: Ručně, nebo WPS,
- Síťový režim,
- Vysílací pásmo,
- Šířka kanálu,
- Standardní kanál,
- Název bezdrátové sítě (SSID).

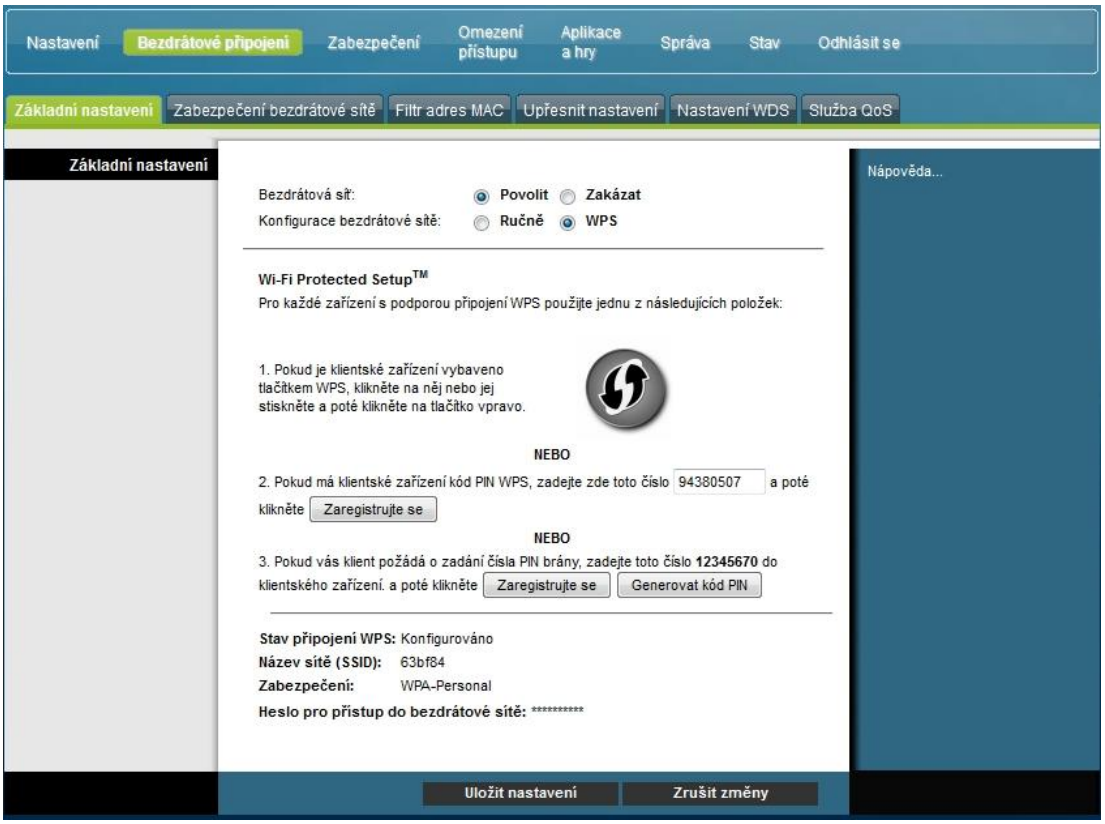
Wi-Fi Protected Setup (WPS)

Pokud pro konfiguraci bezdrátového připojení vyberete nastavení WPS, řada parametrů se nastaví automaticky. Funkce WPS umožňuje snadné připojení nových zařízení WPA do sítě.

Důležité: Při použití režimu WPS není podporováno zabezpečení WEP. Pokud je třeba použít šifrování WEP, je nutné funkci WPS vypnout nastavením konfigurace bezdrátového připojení na možnost **Ručně**.

Poznámka: Ve výchozím nastavení je funkce WPS zapnuta.

Příklad nastavení WPS pro konfiguraci bezdrátového připojení



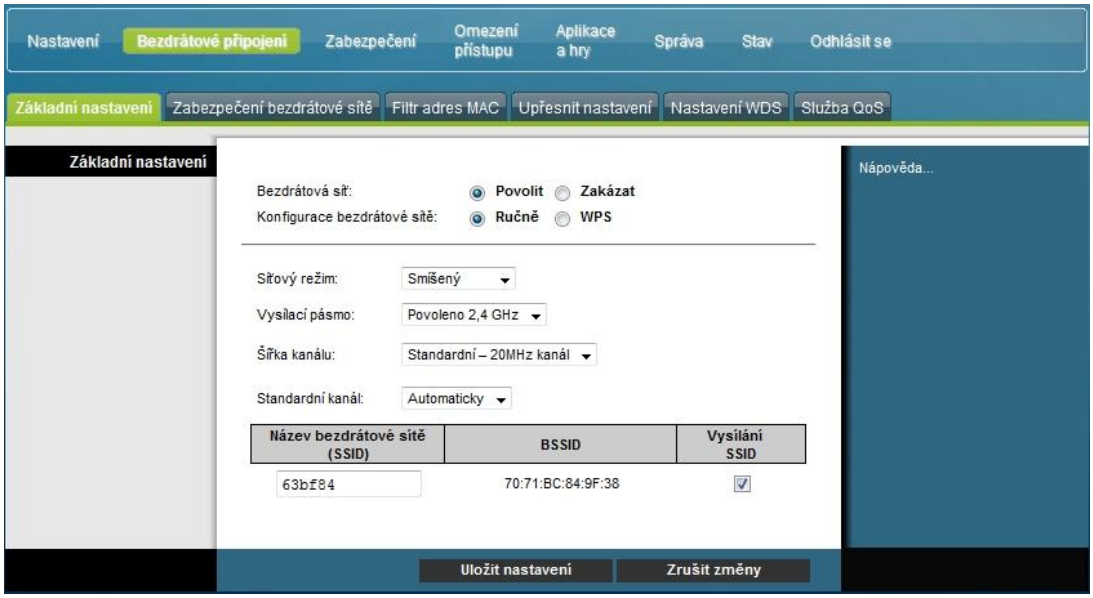
Popis stránky nastavení WPS pro konfiguraci bezdrátového připojení

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci základního nastavení funkce WPS domácí brány. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení** případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Základní nastavení	Bezdrátovou síť můžete **Povolit** či **Zakázat**. **Konfigurace funkce Wi-Fi Protected Setup** Funkce WPS automaticky nastaví šifrovanou bezdrátovou síť. Abyste funkci WPS mohli použít, musí být v síti alespoň jedno zařízení, které ji podporuje. Až nakonfigurujete zařízení WPS, můžete ručně nastavit další zařízení. **Nastavení tlačítka WPS (možnost 1)** Chcete-li na bráně zaregistrovat bezdrátového klienta, stiskněte tlačítko WPS na stránce Bezdrátové připojení > Základní nastavení nebo tlačítko na zadním panelu brány. Současně se stisknutím tlačítka WPS na bráně stiskněte softwarové tlačítko WPS na klientovi. Připojení se automaticky vytvoří.

Část	Popis pole
	Funkce WPS za použití kódu PIN adaptéru Wi-Fi (možnost 2) Toto je nejbezpečnější způsob registrace bezdrátového klienta na bráně. Budete potřebovat kód PIN WPS, který lze zjistit pomocí nástroje WPS klienta. K bráně se můžete připojit po zadání kódu PIN WPS. **Funkce WPS za použití kódu PIN brány (možnost 3)** Poznamenejte si kód PIN WPS brány, který se zobrazuje na stránce WPS. Klikněte na tlačítko Zaregistrujte se u možnosti 3. Pomocí nástroje WPS klienta nebo systému Microsoft Vista zadejte do klientského zařízení kód PIN WPS brány. Registrace je dokončena.

Ukázka stránky ruční konfigurace bezdrátového připojení



Popis stránky Bezdrátové připojení > Základní nastavení

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci základního nastavení bezdrátové komunikace domácí brány. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Základní nastavení	**Bezdrátová síť** Bezdrátovou síť můžete **Povolit** či **Zakázat**. **Konfigurace bezdrátové sítě** Výchozí nastavení je **WPS**. Více informací o použití funkce WPS najdete v části ***Wi-Fi Protected Setup (WPS)*** (str. 39). Chcete-li pomocí této možnosti nastavit síť ručně, vyberte možnost **Ručně**.

Část	Popis pole
	Síťový režim Vyberte jednu z těchto možností režimu sítě: **Pouze G, Smíšený B/G, Smíšený B/G/N** (výchozí nastavení) **Důležité:** Pokud vyberete jen ověřování TKIP, smíšený režim sítě B/G/N nebude dostupný. **Vysílací pásmo** Vyberte možnost **Povoleno 2,4 GHz** (výchozí) nebo **Povoleno 5 GHz.** **Poznámka:** Některé modely nemusí vysílací pásmo 5 GHz podporovat. **Šířka kanálu** Vyberte možnost **Standardní – 20MHz kanál nebo Široký – 40MHz kanál.** **Standardní kanál** Vyberte v rozevíracím seznamu kanál odpovídající nastavení sítě. Aby spolu všechna zařízení v bezdrátové síti mohla komunikovat, musí vysílat na stejném kanálu. Automatickou volbu kanálu můžete nastavit volbou možnosti **Automaticky** (výchozí).
	Název bezdrátové sítě (SSID) Identifikátor SSID je název vaší bezdrátové sítě. Bezdrátová technologie na základě tohoto identifikátoru odlišuje vaši síť od jiných bezdrátových sítí v dané oblasti. Identifikátor SSID může obsahovat až 32 znaků. Výchozí identifikátor SSID zpravidla obsahuje posledních 6 znaků adresy CM MAC, která je uvedena na typovém štítku na spodní straně brány. Identifikátor SSID je zcela jedinečný a není třeba jej měnit. Poskytovatel služeb vám může dodat informace o nastavení bezdrátové sítě, která vyžadují jiný identifikátor SSID. **BSSID** Zde se zobrazuje identifikátor BSSID bezdrátové sítě. Identifikátor BSSID je obvykle adresa MAC bezdrátového přístupového bodu. **Poznámka:** Nemusí se jednat o stejnou adresu MAC, jako je adresa CM MAC používaná k určení výchozího identifikátoru SSID. **Vysílání SSID** Pokud je toto políčko zaškrtnuto (výchozí nastavení), brána odesílá do ostatních bezdrátových zařízení informace o své přítomnosti. Je-li odesílání tohoto signálu povoleno, klientská zařízení mohou automaticky zjistit přístupový bod. Pokud chcete síť před bezdrátovými klienty skrýt, zrušte zaškrtnutí tohoto políčka. Pokud síť skryjete, každé bezdrátové klientské zařízení bude třeba nastavit ručně. **Důležité:** Zaškrtávací políčko **Povolit** se aktuálně nepoužívá a na funkci brány nemá vliv.

Bezdrátové připojení > Zabezpečení bezdrátové sítě

Volba režimu bezdrátového zabezpečení pomáhá chránit síť. Pokud vyberete možnost **Zakázat**, bezdrátová síť nebude zabezpečená a bude se moci k ní připojit jakékoli bezdrátové zařízení v dosahu.

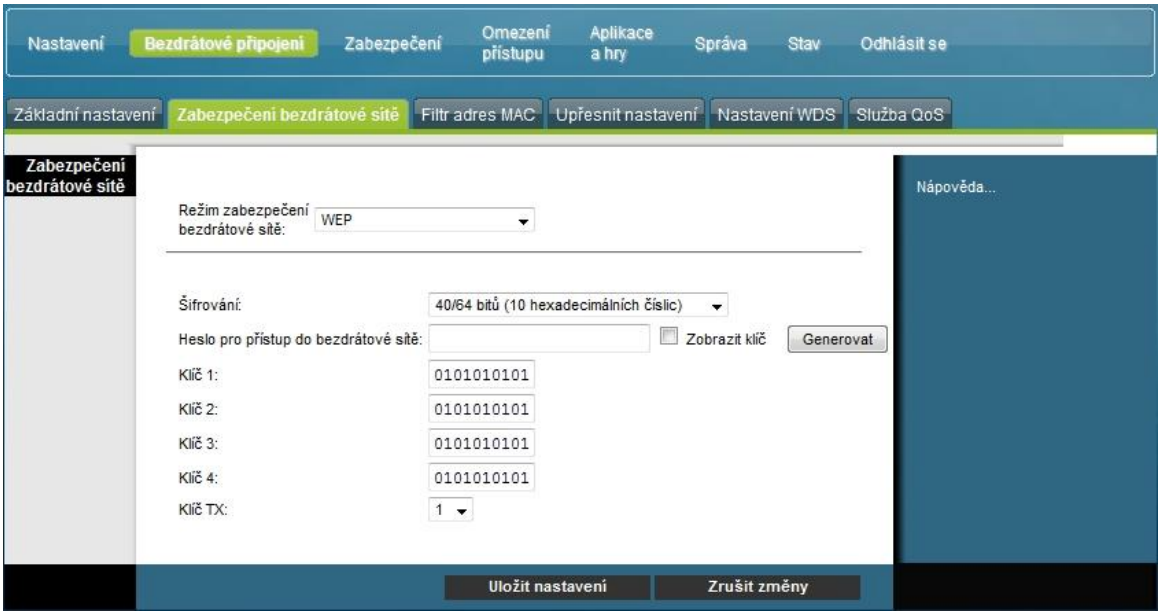
Chcete-li bezdrátovou síť ochránit před narušiteli, nakonfigurujte na stránce Zabezpečení bezdrátové sítě parametry zabezpečení, například režim zabezpečení (úroveň šifrování), šifrovací klíče a další nastavení.

Zvolením karty **Zabezpečení bezdrátové sítě** otevřete stránku Zabezpečení bezdrátové sítě. Následující tabulka obsahuje příklady ze stránky Zabezpečení bezdrátové sítě s různými vybranými režimy bezdrátového zabezpečení.

Popis stránky Zabezpečení bezdrátové sítě

Popisy a pokyny uvedené v této tabulce vám usnadní konfiguraci bezdrátového zabezpečení domácí brány. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Zabezpečení bezdrátové sítě	**Režim zabezpečení bezdrátové sítě** Vyberte jeden z režimů zabezpečení: **WEP** Režim zabezpečení WEP je definován v původním standardu IEEE 802.11. Použití tohoto režimu již nedoporučujeme, protože nabízí pouze nízkou úroveň ochrany. Doporučujeme používat zabezpečení WPA-Personal nebo WPA2-Personal. **Poznámka:** Režim WPS v tomto zařízení zabezpečení WEP nepodporuje.



Popisy polí

- **Šifrování.** Vyberte úroveň šifrování WEP: 40/64 bitů (10 hexadecimálních číslic) nebo 104/128 bitů (26 hexadecimálních číslic).
- **Heslo pro přístup do bezdrátové sítě**. Při nastavování bezdrátového zabezpečení je třeba vybrat heslo pro přístup do bezdrátové sítě, které si snadno zapamatujete, ale které ostatní nebudou moci snadno uhodnout. Při prvním připojení nového bezdrátového zařízení do sítě bude třeba toto heslo zadat v příslušné části nastavení připojovaného zařízení. Aby nedošlo k ohrožení zabezpečení sítě, nesdělujte své přístupové heslo neoprávněným uživatelům. Zadejte řetězec s čísly a/nebo písmeny o délce 4–24 znaků. Potom vytvořte přístupové heslo kliknutím na možnost **Generovat**.
- **Klíč 1–4**. Chcete-li ručně zadat klíče WEP, vyplňte příslušná pole. Každý klíč WEP může obsahovat písmena A–F a čísla 0–9. Při zadání 10 znaků bude použito 40/64bitové šifrování a při zadání 26 znaků 104/128bitové šifrování.
- **Klíč TX**. Vyberte přenosový klíč (TX) 1 až 4. Klíč TX se bude používat k šifrování vašich dat. Vytvořit je možné čtyři klíče, k šifrování dat však lze použít jen jeden z nich. Vyberte pro šifrování WEP jeden ze čtyř klíčů. Vybraný klíč TX použijte k nastavení bezdrátových klientů.

Část	Popis pole

WPA

Zabezpečení osobních sítí – režimy WPA nebo WPA2 Personal

Ochrana Wi-Fi Protected Access (WPA) pro bezdrátové sítě je bezpečnější než zabezpečení WEP. Zabezpečení WPA lze použít pro firemní (podnikové aplikace) i osobní (domácí sítě) bezdrátové sítě. Pro vaši domácí síť doporučujeme zvolit zabezpečení WPA-Personal nebo WPA2-Personal, podle toho, jaký režim podporují bezdrátový adaptér v počítači a bezdrátoví klienti.

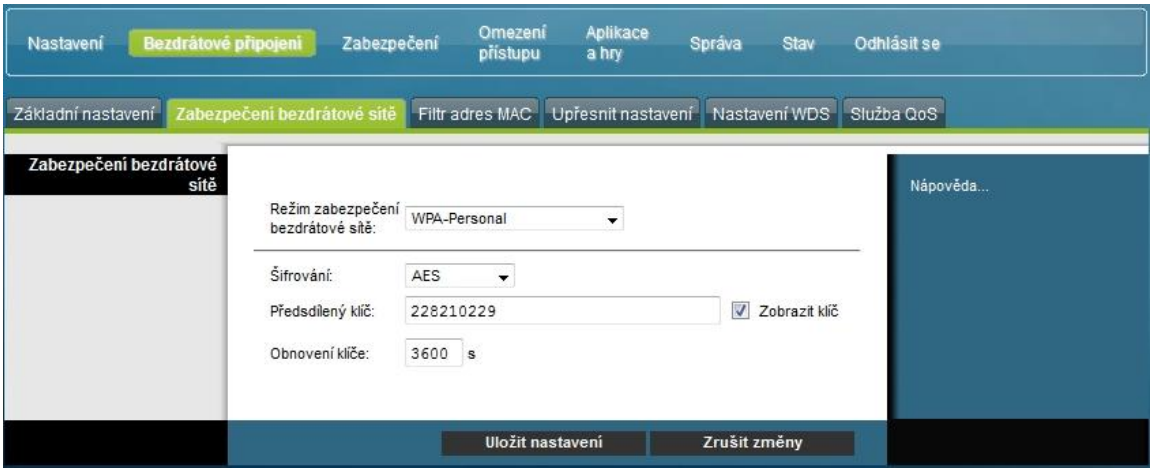
Varianta WPA-Personal (tzv. WPA-PSK nebo WPA-Pre-Shared Key) nabízí vyšší zabezpečení bezdrátové sítě než zabezpečení WEP. Zabezpečení WPA-Personal používá uživatelské ověřování TKIP a silnější šifrovací klíče než zabezpečení WEP.

Zabezpečení WPA2-Personal (tzv. WPA2-PSK nebo WPA2-Pre-Shared Key) zajišťuje nejvyšší úroveň ochrany bezdrátových síti založenou na standardech. Zabezpečení WPA2-Personal zahrnuje standard AES pro přenos dat.

Poznámka: Některé bezdrátové adaptéry nepodporují zabezpečení WPA2. Zabezpečení WPA však podporuje široká škála zařízení. Ať už použijete zabezpečení WPA, nebo WPA2, vždy zvolte silné přístupové heslo. Silné přístupové heslo je řetězec obsahující alespoň 21 náhodných znaků.

Vyberte jeden z těchto tří režimů zabezpečení WPA nebo WPA2:

- **WPA-Personal,**
- **WPA2-Personal,**
- **WPA nebo WPA2-Personal.**



Popisy polí

- **Šifrování**. Výchozí nastavení je TKIP+AES.
- **Předsdílený klíč**. Zadejte klíč o délce 8–63 znaků.
- **Obnovení klíče**. Zadejte interval obnovení klíče, který určuje, jak často má zařízení měnit šifrovací klíče. Výchozí nastavení je **3 600** sekund.

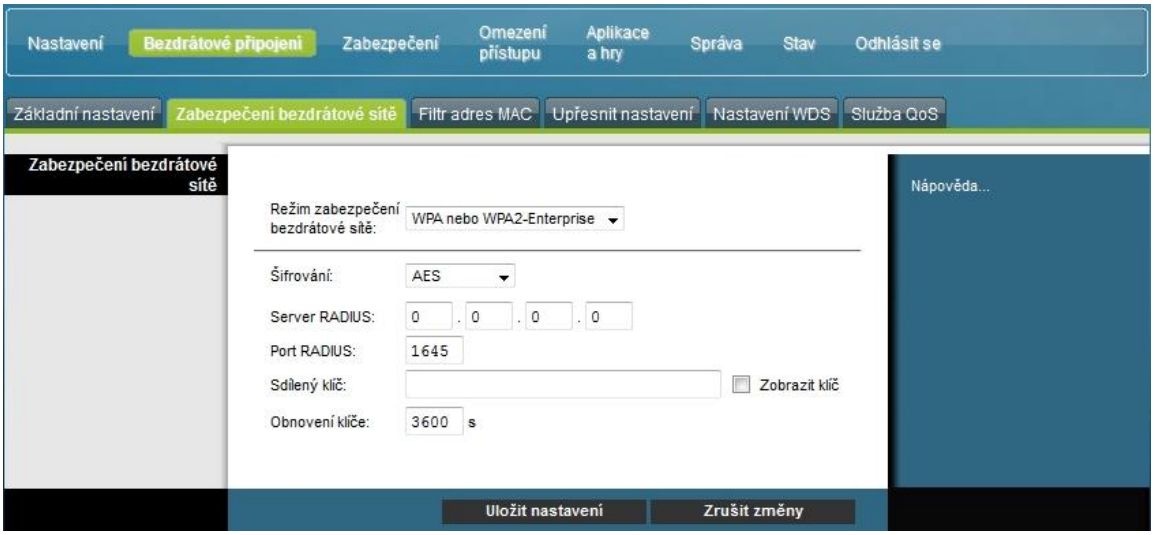
Část	Popis pole

Zabezpečení podnikových sítí – režimy WPA-Enterprise

Tato funkce nabízí zabezpečení WPA používané společně se serverem RADIUS k ověřování klientů. (Tuto možnost použijte, pouze pokud je k zařízení připojen server RADIUS.)

Zvolte jeden z těchto tří režimů zabezpečení WPA nebo WPA2 Enterprise:

- **WPA-Enterprise,**
- **WPA2-Enterprise,**
- **WPA nebo WPA2-Enterprise.**



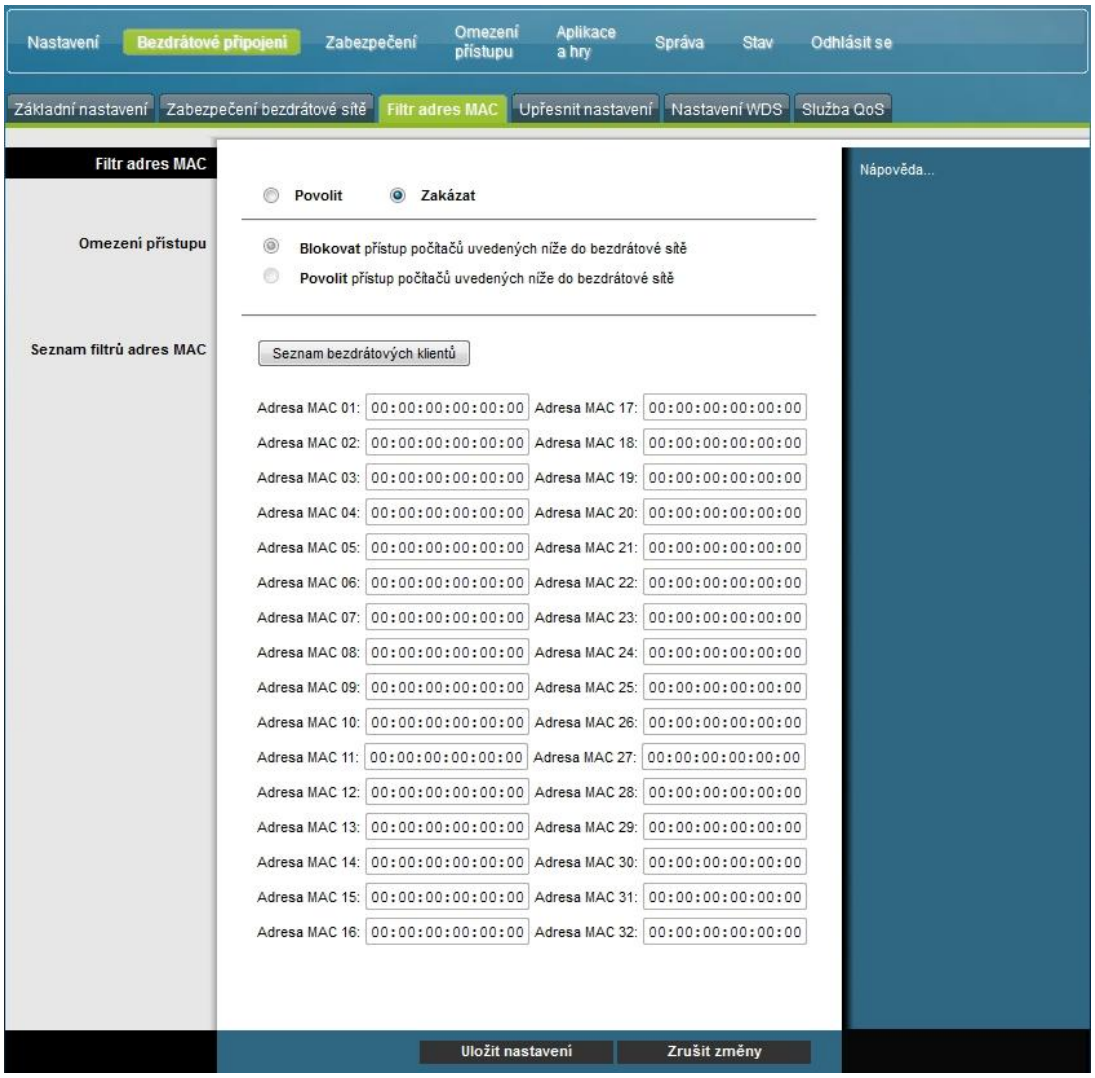
Popisy polí

- **Šifrování**. Výchozí nastavení je TKIP+AES.
- **Server RADIUS**. Zadejte adresu IP serveru RADIUS.
- **Port RADIUS**. Zadejte číslo portu používané serverem RADIUS. Výchozí hodnota je **1 812**.
- **Sdílený klíč**. Zadejte klíč používaný zařízením a serverem RADIUS.
- **Obnovení klíče.** Zadejte interval obnovení klíče, který určuje, jak často má zařízení měnit šifrovací klíče. Výchozí nastavení je **3 600** sekund.

Bezdrátové připojení > Filtr adres MAC

Funkce filtru adres MAC umožňuje povolení nebo blokování přístupu do bezdrátové sítě LAN na základě adresy MAC bezdrátového klientského zařízení. Funkce filtru adres MAC, označovaná též jako přístupový seznam, pomáhá chránit bezdrátovou síť před neoprávněnými uživateli.

Zvolením možnosti **Filtr adres MAC** otevřete stránku Bezdrátové připojení > Filtr adres MAC.



Popis stránky Bezdrátové připojení > Filtr adres MAC

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci filtrování adres MAC pro bezdrátovou síť domácí brány. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Filtr adres MAC	Umožňuje **Povolit** nebo **Zakázat** filtrování adres MAC pro domácí bránu.
Omezení přístupu	**Omezení přístupu** Umožňuje povolit nebo blokovat přístup počítačů do bezdrátové sítě. Toto nastavení se vztahuje na všechny adresy uvedené na této stránce. Vyberte jednu z těchto možností: ■ Blokovat přístup počítačů uvedených níže do bezdrátové sítě. Zvolením této možnosti zamítnete internetový přístup pro zařízení s adresami MAC uvedenými v tabulce. Pro ostatní zařízení bude internetový přístup povolen. ■ Povolit přístup počítačů uvedených níže do bezdrátové sítě. Zvolením této možnosti povolíte internetový přístup pouze pro zařízení s adresami MAC uvedenými v tabulce. Všem zařízením, jejichž adresy MAC v tabulce uvedeny nejsou, bude internetový přístup zamítnut.
Seznam filtrů adres MAC	**Seznam filtrů adres MAC** V seznamu filtrů adres MAC jsou uvedeni uživatelé, jejichž přístup do bezdrátové sítě chcete řídit. Kliknutím na tlačítko **Seznam bezdrátových klientů** zobrazíte seznam uživatelů sítě podle adres MAC. Pomocí rozevírací nabídky Řadit podle můžete tabulku seřadit podle adresy IP, adresy MAC, stavu, rozhraní nebo názvu klienta. Chcete-li zobrazit aktuální informace, klikněte na tlačítko Aktualizovat.

Bezdrátové připojení > Upřesnit nastavení

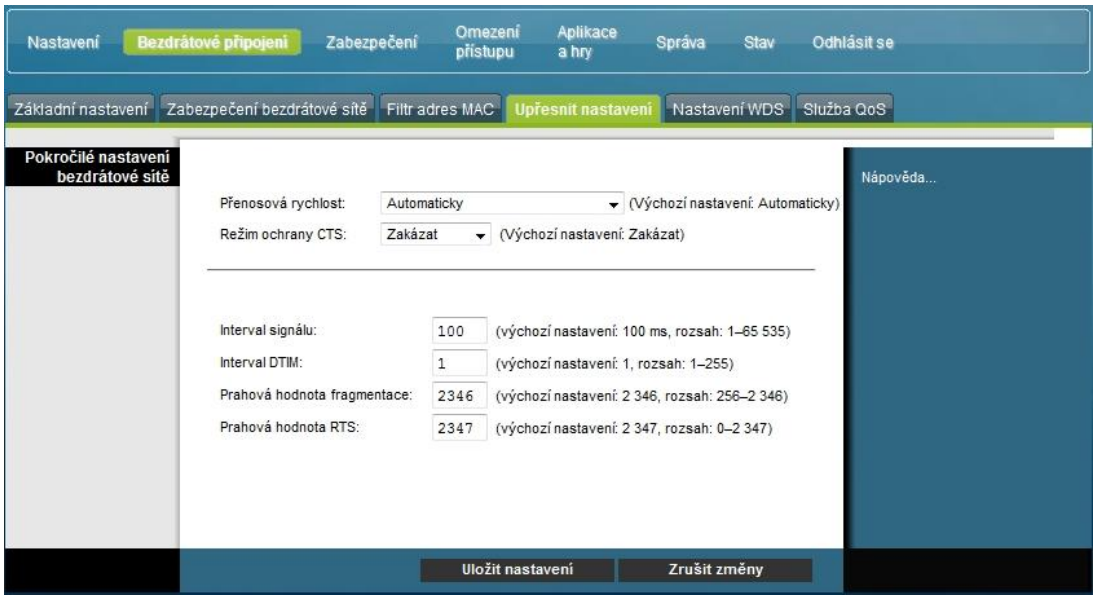
Upřesňující nastavení bezdrátového připojení umožňují pro bezdrátovou síť domácí brány nastavit další úroveň zabezpečení. Na této stránce můžete nastavit pokročilé funkce bezdrátového připojení. Tato nastavení by měl upravovat pouze zkušený správce. Nesprávné nastavení může mít vliv na fungování a výkon bezdrátové sítě.

Zvolením karty **Upřesnit nastavení** otevřete stránku Bezdrátové připojení > Upřesnit nastavení.

Na této stránce můžete nastavit následující možnosti:

- Přenosová rychlost N,
- Režim ochrany CTS,

- Interval signálu,
- Interval DTIM,
- Prahová hodnota fragmentace,
- Prahová hodnota RTS.



Popis stránky Bezdrátové připojení > Upřesnit nastavení

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci upřesňujícího nastavení domácí brány. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

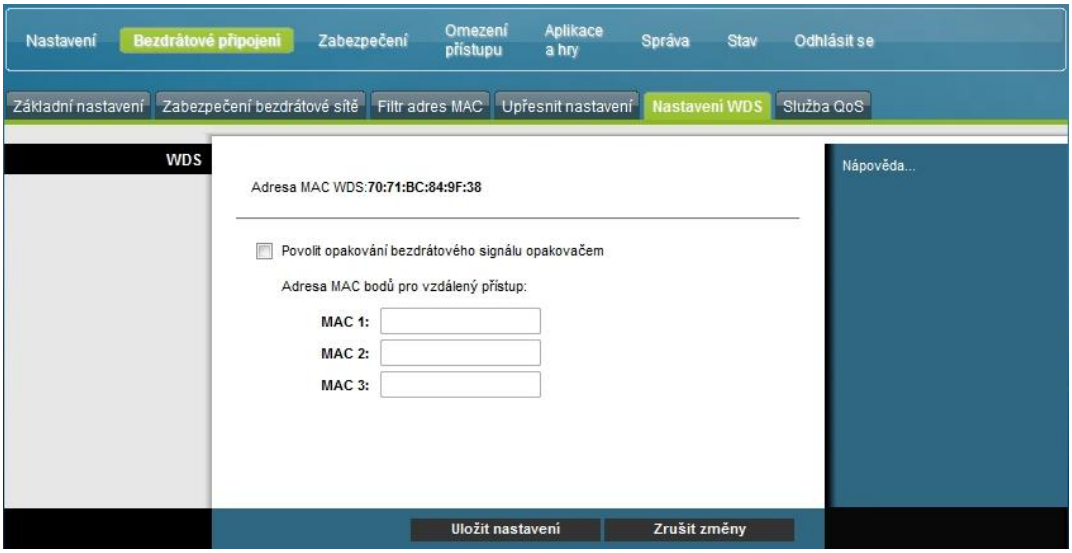
Část	Popis pole
Pokročilé nastavení bezdrátové sítě	**Přenosová rychlost N** Rychlost přenosu dat by měla být nastavena podle rychlosti bezdrátového připojení N. Volit můžete z řady přenosových rychlostí. Dále můžete vybrat nastavení **Automaticky**, pokud chcete, aby zařízení vybralo nejvyšší možnou rychlost přenosu dat, a povolit funkci Automatické snížení rychlosti. Funkce Automatické snížení rychlosti zjišťuje nejvyšší možnou rychlost připojení mezi zařízením a bezdrátovým klientem. Výchozí nastavení je **Automaticky**. Vyberte jednu z těchto možností nastavení přenosové rychlosti: ■ Automaticky (výchozí), ■ Použít starší přenosovou rychlost, ■ 0: 6,5 nebo 13,5 Mb/s, ■ 1: 13 nebo 27 Mb/s, ■ 2: 19,5 nebo 40,5 Mb/s, ■ 3: 26 nebo 54 Mb/s, ■ 4: 39 nebo 81 Mb/s, ■ 5: 52 nebo 108 Mb/s, ■ 6: 58,5 nebo 121,5 Mb/s, ■ 7: 65 nebo 135 Mb/s, ■ 8: 13 nebo 27 Mb/s, ■ 9: 26 nebo 54 Mb/s, ■ 10: 39 nebo 81 Mb/s, ■ 11: 52 nebo 108 Mb/s, ■ 12: 78 nebo 162 Mb/s, ■ 13: 104 nebo 216 Mb/s, ■ 14: 117 nebo 243 Mb/s, ■ 15: 130 nebo 270 Mb/s.
	Režim ochrany CTS Režim ochrany CTS zvyšuje efektivitu zařízení při zachycování všech bezdrátových přenosů, může však výrazně snížit výkon. Chcete-li, aby se funkce používala podle potřeby, jestliže produkty s podporou bezdrátového připojení N/G nedokážou přenést data do zařízení v prostředí s velkým provozem 802.11b, vyberte možnost **Automaticky**. Chcete-li tuto funkci trvale zakázat, vyberte možnost **Zakázat**.

Část	Popis pole
	Interval signálu Hodnota intervalu signálu označuje frekvenci signálu. Signál je paket vysílaný zařízením za účelem synchronizace bezdrátové sítě. (Výchozí hodnota: 100 ms, rozsah: 20-1 000)
	Interval DTIM Interval DTIM je interval mezi vysíláním / všesměrovým vysíláním. Pole DTIM je odpočítávací pole, které informuje klienty o další možnosti pro zjišťování zpráv vysílání a všesměrového vysílání. Pokud má zařízení ve vyrovnávací paměti uloženy zprávy vysílání nebo všesměrového vysílání pro přiřazené klienty, odešle další zprávu DTIM s hodnotou intervalu DTIM. Pokud klienti zjistí tyto signály, probudí se a přijmou zprávy vysílání a všesměrového vysílání. (Výchozí hodnota: 1, rozsah: 1–255)
	Prahová hodnota fragmentace Prahová hodnota fragmentace určuje maximální velikost paketu. Je-li tato velikost překročena, data jsou fragmentována na více paketů. Pokud zjistíte velkou míru chyb paketů, zkuste prahovou hodnotu fragmentace mírně zvýšit. Nastavení příliš nízké prahové hodnoty fragmentace může zhoršit fungování sítě. Doporučujeme provést pouze mírné snížení výchozí hodnoty. Ve většině případů by měla být ponechána výchozí hodnota 2 346.
	Prahová hodnota RTS Prahová hodnota RTS určuje, od jaké velikosti paketu má být vyvolán mechanismus RTS/CTS. Pokud zjistíte nekonzistentní tok dat, doporučujeme provést pouze mírné snížení výchozí hodnoty 2 346. Pokud je síťový paket menší než přednastavená velikost prahové hodnoty RTS, mechanismus RTS/CTS nebude povolen. Zařízení odesílá rámce RTS do určité přijímající stanice a vyjednává odeslání datového rámce. Po přijetí požadavku RTS bude bezdrátová stanice reagovat rámcem CTS, čímž potvrdí, že může zahájit přenos. Měla by být ponechána výchozí prahová hodnota RTS 2 347.

Bezdrátové připojení > Nastavení WDS

Stránka Nastavení WDS umožňuje rozšířit pokrytí bezdrátové sítě zavedením opakovačů signálu. Všechna nastavení s povoleným systémem WDS musí mít stejné nastavení kanálu.

Zvolením karty **Nastavení WDS** otevřete stránku Bezdrátové připojení > Nastavení WDS. Na této stránce můžete nakonfigurovat nastavení WDS.



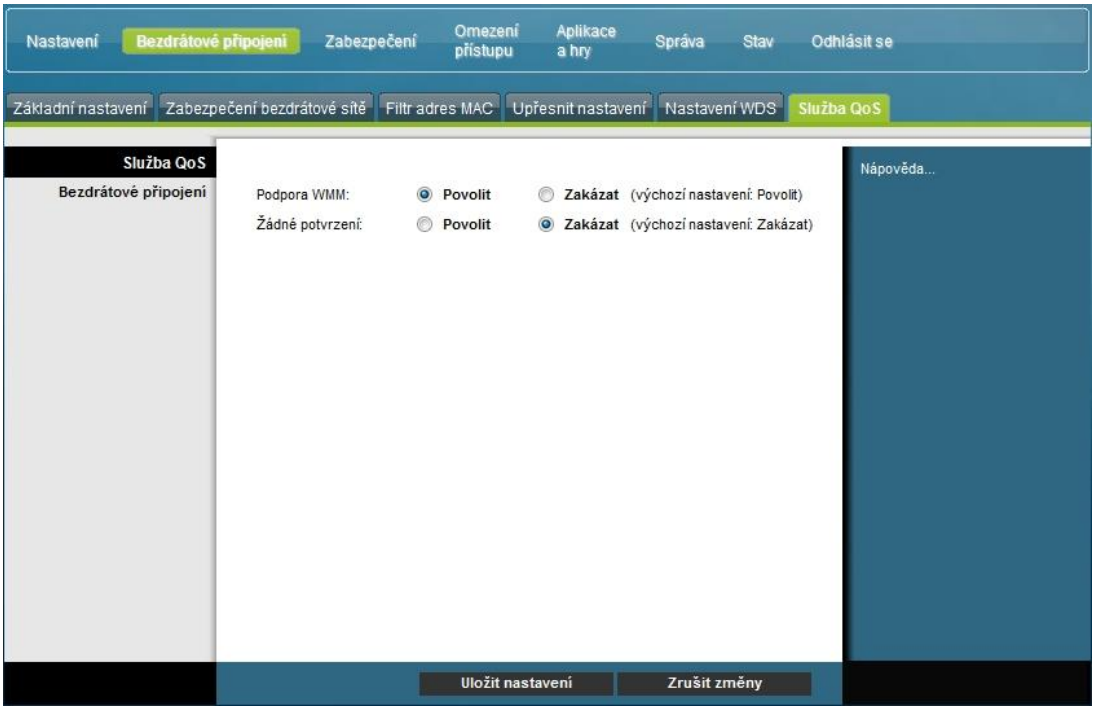
Popis stránky Bezdrátové připojení > Nastavení WDS

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci nastavení WDS pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
WDS	**Adresa MAC WDS** Zde se zobrazuje adresa MAC WDS (nebo BSSID) přístupového bodu brány.
	Povolit opakování bezdrátového signálu opakovačem Zaškrtnutím tohoto políčka umožníte připojení bezdrátového klienta k opakovači a směrování provozu mezi bezdrátovým klientem a opakovačem. Použít lze maximálně 3 opakovače.
	Adresa MAC bodů pro vzdálený přístup (MAC 1 až 3) Do těchto tří polí (MAC 1, 2 a 3) lze zadat adresy MAC opakovačů.

Bezdrátové připojení > Služba QoS

Služba QoS zvyšuje kvalitu služby pro síťový provoz s vysokou prioritou, například náročné aplikace pracující v reálném čase, jako jsou videokonference. Nastavení služby QoS umožňují určit prioritu různých typů provozu. Provoz s nižší prioritou bude zpomalen, aby byla zajištěna vyšší propustnost nebo zkráceno zpoždění provozu s vyšší prioritou. Zvolením karty **Služba QOS** otevřete stránku Bezdrátové připojení > Služba QoS.



Popis stránky Bezdrátové připojení > Služba QoS

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci každého nastavení služby QoS. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Služba QoS	
Bezdrátové připojení	**Podpora WMM** Pokud vaši bezdrátoví klienti podporují funkci WMM, při povolení této funkce získá provoz s hlasovými daty a multimédii vyšší prioritu než ostatní typy provozu. Vyberte požadovanou možnost: ■ **Povolit** (výchozí), ■ **Zakázat.**

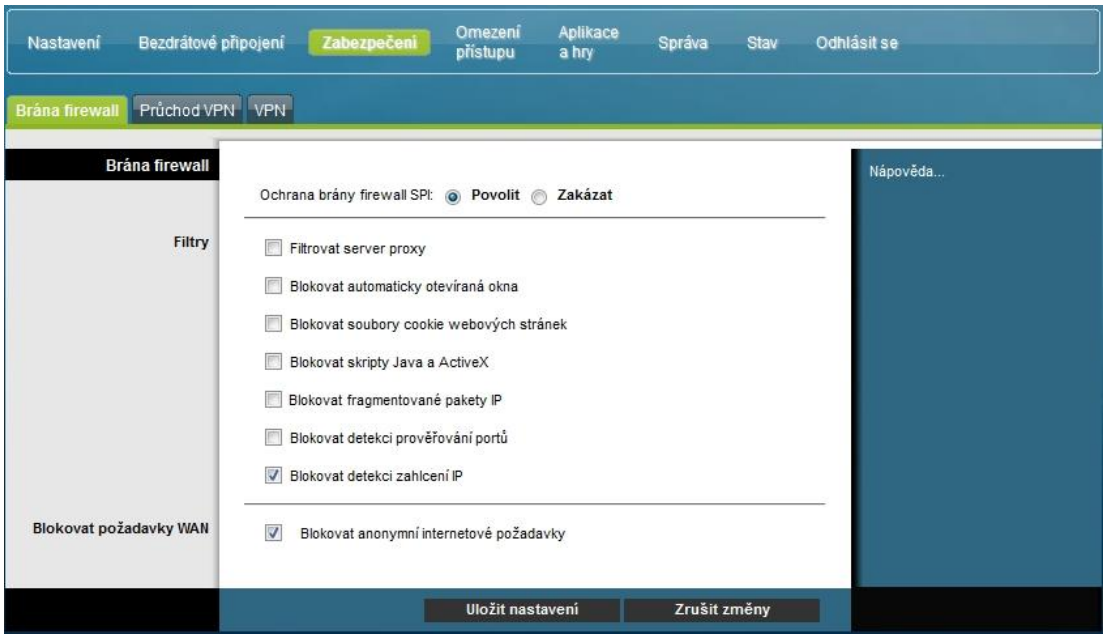
Část	Popis pole
	Žádné potvrzení Zde je možné v klientském počítači povolit nebo zakázat možnost Žádné potvrzení. Tato funkce je vhodná pro datové služby, u nichž je důležitá rychlost přenosu a u nichž je do určité míry přípustná ztráta paketů. Pokud vyberete možnost **Zakázat**, potvrzovací paket bude vrácen pro každý přijatý paket. Tím se zvýší spolehlivost přenosu, ale zároveň se zvyšuje zatížení sítě, a tudíž se snižuje výkon. Vyberte požadovanou možnost: ■ **Povolit,** ■ **Zakázat** (výchozí).

Konfigurace zabezpečení

Zabezpečení > Brána firewall

Pokročilá brána firewall detekuje hackery a chrání domácí síť před neoprávněným přístupem. Na této stránce lze nakonfigurovat bránu firewall, která dokáže filtrovat různé typy nežádoucího provozu v místní síti brány.

Zvolením karty **Brána firewall** otevřete stránku Zabezpečení > Brána firewall.



Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci brány firewall pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

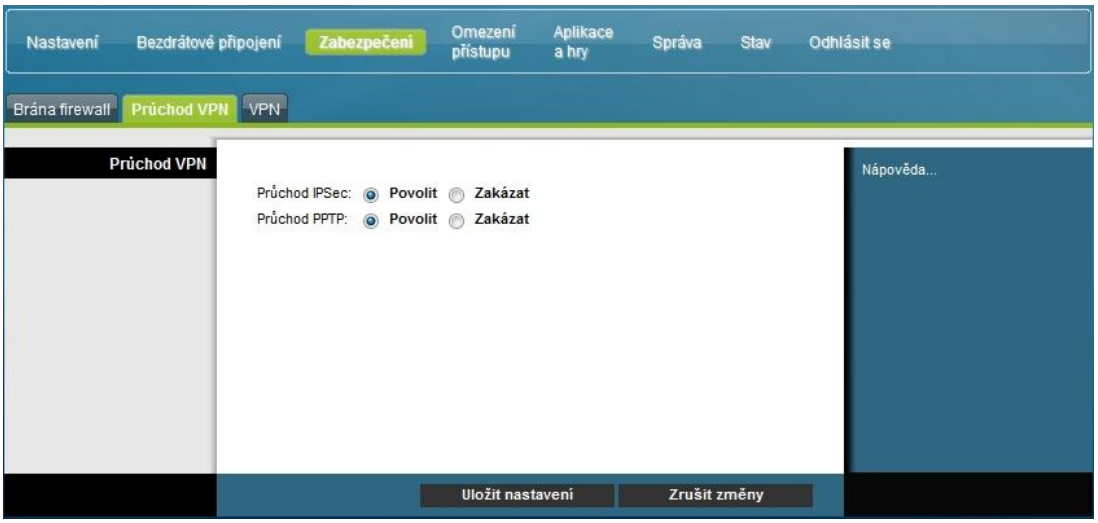
Část	Popis pole
Brána firewall	**Ochrana brány firewall SPI** Ochrana brány firewall SPI blokuje útoky DoS. Cílem útoku DoS není odcizení dat ani poškození počítače, ale přetížení internetového připojení tak, aby bylo nepoužitelné. Vyberte požadovanou možnost: ■ **Povolit** (výchozí), ■ **Zakázat.**

Část	Popis pole
Filtry	**Filtrovat server proxy** Umožňuje povolit či zakázat filtrování serveru proxy. Pokud místní uživatelé mají přístup k serverům proxy sítě WAN, mohou obejít filtry obsahu a získat přístup k webům, které jsou zařízením blokovány. Pokud vyberete možnost Filtrovat server proxy, bude zablokován přístup k jakémukoli serveru proxy sítě WAN. **Blokovat automaticky otevíraná okna** Umožňuje povolit či zakázat automaticky otevíraná okna. Součástí některých běžně používaných aplikací jsou automaticky otevíraná okna. Pokud tato okna zakážete, fungování některých takových aplikací může být narušeno. **Blokovat soubory cookie webových stránek** Umožňuje povolit nebo zakázat blokování souborů cookie. Tato funkce filtruje nežádoucí doručování souborů cookie do zařízení v privátní místní síti. Soubory cookie jsou počítačové soubory obsahující osobní údaje nebo data o chování uživatelů na webu. **Blokovat skripty Java a ActiveX** Umožňuje povolit nebo zakázat applety Java a skripty ActiveX. Tato funkce chrání zařízení v privátní síti před obtížnými nebo nebezpečnými applety Java, které jsou do těchto zařízení odesílány bez vyžádání z Internetu. Tyto applety se v počítači po přijetí automaticky spouští. Java je programovací jazyk pro webové stránky. Pokud vyberete možnost Filtrovat applety Java, riskujete, že nebudete mít přístup k internetovým stránkám, které byly vytvořeny pomocí tohoto programovacího jazyka. Tato funkce chrání zařízení v privátní síti také před obtížnými nebo nebezpečnými ovládacími prvky ActiveX, které jsou do těchto zařízení odesílány bez vyžádání z Internetu. Ovládací prvky ActiveX se v počítači po přijetí automaticky spouští. **Blokovat fragmentované pakety IP** Umožňuje povolit či zakázat filtrování fragmentovaných paketů IP. Tato funkce chrání privátní místní síť před internetovými útoky DoS. **Blokovat detekci prověřování portů** Umožňuje povolit či zakázat, aby brána reagovala na internetové prověřování portů. Tato funkce chrání privátní místní síť před internetovými hackery, kteří se pokoušejí detekovat otevřené porty IP na bráně a získat tak neoprávněný přístup do sítě. **Blokovat detekci zahlcení IP** (zaškrtnuto – výchozí nastavení) Tato funkce blokuje nebezpečná zařízení, která se pokouší zahltit vaše zařízení nebo sítě pomocí paketů nezákonného vysílání. Toto chování se označuje také jako „bouře vysílání“.

Část	Popis pole
Blokovat požadavky WAN	**Blokovat anonymní internetové požadavky** (zaškrtnuto – výchozí nastavení) Pokud zapnete tuto funkci, do vaší sítě nebude možné odesílat příkazy ping a síť nebude zjistitelná jinými uživateli Internetu. Možnost Blokovat anonymní internetové požadavky skryje také síťové porty. Obě funkce ztěžují vnějším uživatelům vstup do sítě.

Zabezpečení > Průchod VPN

Tato stránka slouží ke konfiguraci podpory sítě VPN. Povolením nastavení na této stránce umožníte průchod tunelů VPN přes bránu firewall brány pomocí protokolu IPsec nebo PPTP. Zvolením karty **Průchod VPN** otevřete stránku Zabezpečení > Průchod VPN.



Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci průchodu VPN pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Průchod VPN	**Průchod IPSec** Umožňuje povolit nebo zakázat protokol IPsec. IPSec je řada protokolů používaných k implementaci zabezpečené výměny paketů na úrovni IP. Pokud povolíte průchod IPSec, aplikace používající protokol IPsec budou moci proniknout přes bránu firewall. Chcete-li průchod IPSec vypnout, zvolte možnost **Zakázat**. Vyberte požadovanou možnost: ■ **Povolit** (výchozí), ■ **Zakázat.**

Část	Popis pole
	Průchod PPTP Umožňuje povolit nebo zakázat protokol PPTP. Protokol PPTP umožňuje tunelování protokolu PPP přes síť IP. Pokud povolíte průchod PPTP, aplikace používající protokol PPTP budou moci proniknout přes bránu firewall. Chcete-li průchod PPTP vypnout, vyberte možnost **Zakázat**. Vyberte požadovanou možnost: ■ **Povolit** (výchozí), ■ **Zakázat**

Zabezpečení > VPN

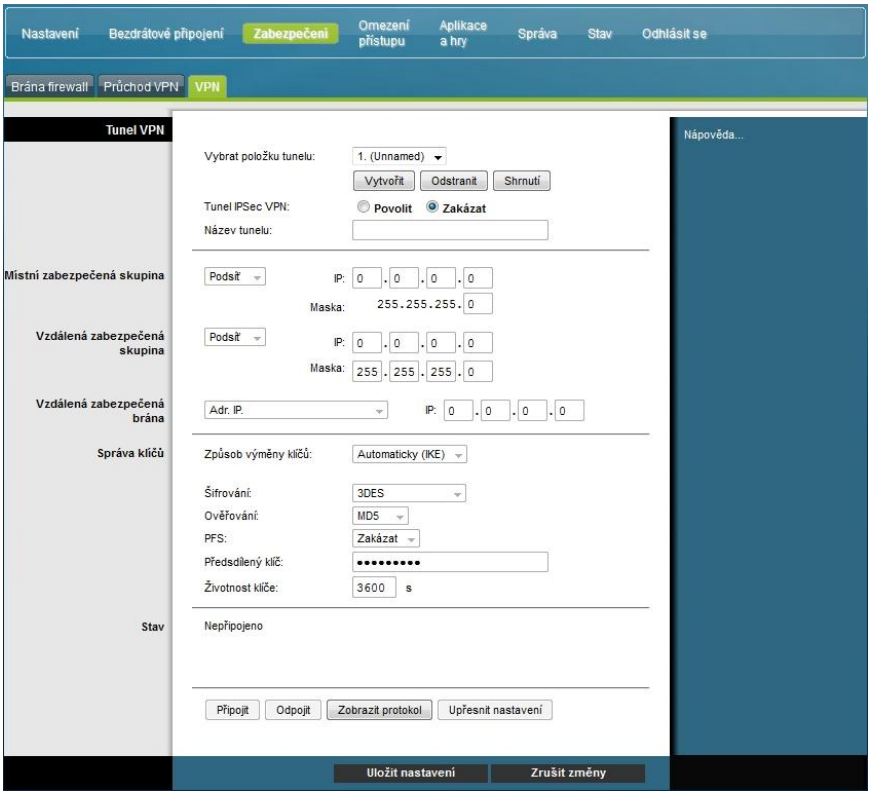
Síť VPN je propojení dvou koncových bodů v různých sítích, které umožňuje bezpečné odesílání dat prostřednictvím veřejných sítí nebo jiných privátních sítí. Za tím účelem se vytváří „tunel VPN“. Tunel VPN propojuje dva počítače nebo sítě a umožňuje přenos dat přes Internet tak, jako by byla v privátní síti. Tunel VPN data odesílaná mezi dvěma koncovými body šifruje pomocí protokolu IPsec a uzavírá je do normálního ethernetového/IP rámce. To umožňuje bezpečný a bezproblémový průchod dat mezi sítěmi.

Použití sítě VPN je úspornější a bezpečnější alternativou k používání privátní, vyhrazené, pronajaté linky pro privátní síť. Síť VPN IPsec vytváří pomocí standardních metod šifrování a ověřování bezpečné připojení, které funguje stejně, jako byste byli připojeni přímo k místní privátní síti.

Síť VPN například umožňuje, aby se uživatelé připojili z domova k firemní síti a získali adresu IP v privátní síti stejně, jako kdyby seděli ve své kanceláři a byli připojeni k firemní síti LAN.

Zvolením karty **VPN** otevřete stránku Zabezpečení > VPN.

Na této stránce můžete nakonfigurovat síť VPN pro domácí bránu.



Popis stránky Zabezpečení > Tunel VPN

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci tunelu VPN pro bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Tunel VPN	**Vybrat položku tunelu** Zde se zobrazuje seznam vytvořených tunelů VPN. **Tlačítko Vytvořit** Kliknutím na toto tlačítko vytvoříte nový tunel. **Tlačítko Odstranit** Kliknutím na toto tlačítko odstraníte veškerá nastavení pro vybraný tunel. **Tlačítko Shrnutí** Kliknutím na toto tlačítko zobrazíte nastavení a stav všech povolených tunelů. **Tunel IPSec VPN** Umožňuje povolit nebo zakázat protokol IPSec pro tunel VPN. **Název tunelu** Zadejte název tunelu.

Část	Popis pole
Místní zabezpečená skupina	Vyberte uživatele sítě LAN, kteří mohou používat tento tunel VPN. Může se jednat o jednu adresu IP nebo podsíť. Místní zabezpečená skupina se musí shodovat se vzdálenou zabezpečenou skupinou brány. **IP** Zadejte adresu IP místní sítě. **Maska** Pokud vyberete možnost Podsíť, zadáním masky určete adresu IP v místní síti.
Vzdálená zabezpečená skupina	Vyberte vzdálené uživatele sítě LAN za vzdálenou bránou, kteří mohou používat tento tunel VPN. Může se jednat o jednu adresu IP, podsíť nebo jakoukoli adresu. Pokud vyberete nastavení „Jakákoli“, brána bude fungovat jako respondér a přijímat požadavky od jakéhokoli vzdáleného uživatele. Vzdálená zabezpečená skupina se musí shodovat s místní zabezpečenou skupinou vzdálené brány. **IP** Zadejte adresu IP vzdálené sítě. **Maska** Pokud vyberete možnost Podsíť, zadáním masky určete adresy IP ve vzdálené síti.
Vzdálená zabezpečená brána	Vyberte požadovanou možnost: **Adr. IP**, **Jakákoli** nebo **Úplný doménový název**. Pokud má vzdálená brána dynamickou adresu IP, vyberte možnost **Jakákoli** nebo **Úplný doménový název**. Pokud vyberete možnost **Jakákoli**, brána bude přijímat požadavky z jakékoli adresy IP. **Úplný doménový název (FQDN)** Pokud vyberete možnost **Úplný doménový název**, zadejte název domény vzdálené brány, aby brána mohla najít aktuální adresu IP pomocí služby DDNS. **IP** Adresa IP v tomto poli se musí shodovat s veřejnou adresou IP (WAN nebo Internet) vzdálené brány na druhém konci tunelu.
Správa klíčů	**Způsob výměny klíčů** Brána podporuje automatickou i ruční správu klíčů. Pokud vyberete automatickou správu klíčů, protokoly IKE budou používány k vyjednávání materiálů klíčů pro přidružení zabezpečení. Pokud vyberete ruční správu klíčů, není nutné používat žádné vyjednávání klíčů. Ruční správa klíčů se v zásadě používá v malých statických prostředích nebo pro účely odstraňování potíží. Pamatujte si, že obě strany musí používat stejnou metodu správy klíčů.

Část	Popis pole
Správa klíčů (pokračování)	Vyberte jeden z následujících způsobů výměny klíčů: ■ **Automaticky (IKE)** – **Šifrování:** Způsob šifrování určuje délku klíče používaného k šifrování a dešifrování paketů ESP. Obě strany musí používat stejnou metodu. – **Ověřování:** Metoda ověřování kontroluje pakety ESP. Vyberte možnost **MD5** nebo **SHA**. Obě strany (koncové body VPN) musí používat stejnou metodu. ▪ MD5: Jednosměrný algoritmus hash produkující 128bitový kontrolní součet ▪ SHA: Jednosměrný algoritmus hash produkující 160bitový kontrolní součet – **PFS**: Pokud je povolena metoda PFS, vyjednávání 2. fáze protokolu IKE vygeneruje materiály nových klíčů pro šifrování a ověřování provozu IP. Metodu PFS musí mít povolenou obě strany. – **Předsdílený klíč:** Protokol IKE používá předsdílený klíč k ověřování vzdálených systémů peer s protokolem IKE. V tomto poli lze použít znaky a hexadecimální hodnoty, například „Moje_@123“ nebo „0x4d795f40313233“. Obě strany musí používat stejný předsdílený klíč. – **Životnost klíče:** Toto pole určuje životnost vygenerovaného klíče IKE. Po uplynutí životnosti je automaticky vygenerován nový klíč. Životnost klíče může být v rozsahu 300 až 100 000 000 sekund. Výchozí životnost je **3 600** sekund. ■ **Ručně** – **Šifrování:** Způsob šifrování určuje délku klíče používaného k šifrování a dešifrování paketů ESP. Obě strany musí používat stejnou metodu. – **Šifrovací klíč:** Toto pole určuje klíč používaný k šifrování a dešifrování provozu IP. V tomto poli lze použít znaky a hexadecimální hodnoty. Obě strany musí používat stejný šifrovací klíč. – **Ověřování:** Metoda ověřování kontroluje pakety ESP. Vyberte možnost MD5 nebo SHA. Obě strany (koncové body VPN) musí používat stejnou metodu. ▪ MD5: Jednosměrný algoritmus hash produkující 128bitový kontrolní součet ▪ SHA: Jednosměrný algoritmus hash produkující 160bitový kontrolní součet – **Ověřovací klíč:** Toto pole určuje klíč používaný k ověřování provozu IP. V tomto poli lze použít znaky a hexadecimální hodnoty. Obě strany musí používat stejný ověřovací klíč. – **Příchozí index SPI / Odchozí index SPI:** Index SPI je přenášen v hlavičce ESP. Díky tomu může přijímač vybrat přidružení zabezpečení, pomocí kterého má být zpracován paket. Index SPI je 32bitová hodnota. Lze použít desítkovou i hexadecimální hodnotu, například „987654321“ nebo „0x3ade68b1“. Každý tunel musí mít jedinečný příchozí a odchozí index SPI. Žádné dva tunely nesmí mít stejný index SPI. Příchozí index SPI se musí shodovat s ochozím indexem SPI vzdálené brány a naopak.

Část	Popis pole
Stav	Toto pole informuje o stavu připojení vybraného tunelu. Může se jednat o stav **Připojeno** nebo **Odpojeno**.
Tlačítka	**Připojit** Kliknutím na toto tlačítko vytvoříte připojení pro aktuální tunel VPN. Pokud jste provedli nějaké změny, nejprve je zaveďte kliknutím na tlačítko **Uložit nastavení**. **Odpojit** Kliknutím na toto tlačítko přerušíte připojení pro aktuální tunel VPN. **Zobrazit protokol** Kliknutím na toto tlačítko zobrazíte protokol VPN obsahující podrobnosti o vytvořeném tunelu. **Upřesnit nastavení** Pokud je použita metoda výměny klíčů Automaticky (IKE), toto tlačítko umožní přístup k dalšímu nastavení, které se týká protokolu IKE. Na toto tlačítko klikněte, pokud brána nedokáže vytvořit tunel VPN ke vzdálené bráně, a ověřte, že se upřesňující nastavení shodují s nastaveními ve vzdálené bráně. ■ **Fáze 1 – Provozní režim** Vyberte vhodnou metodu pro vzdálený koncový bod VPN. – **Hlavní**: Hlavní režim je pomalejší, ale bezpečnější. – **Agresivní**: Agresivní režim je rychlejší, ale méně bezpečný. ■ **Místní identita** Vyberte požadovanou možnost odpovídající nastavení vzdálené identity na druhém konci tunelu. – Místní adresa IP: Adresa IP sítě WAN (Internet) – Název: Název domény ■ **Vzdálená identita** Vyberte požadovanou možnost odpovídající nastavení místní identity na druhém konci tunelu. – Místní adresa IP: Adresa IP sítě WAN (Internet) vzdáleného koncového bodu VPN – Název: Název domény vzdáleného koncového bodu VPN ■ **Šifrování** Toto je šifrovací algoritmus používaný pro přidružení zabezpečení IKE. Musí se shodovat s nastavením používaným na druhém konci tunelu.

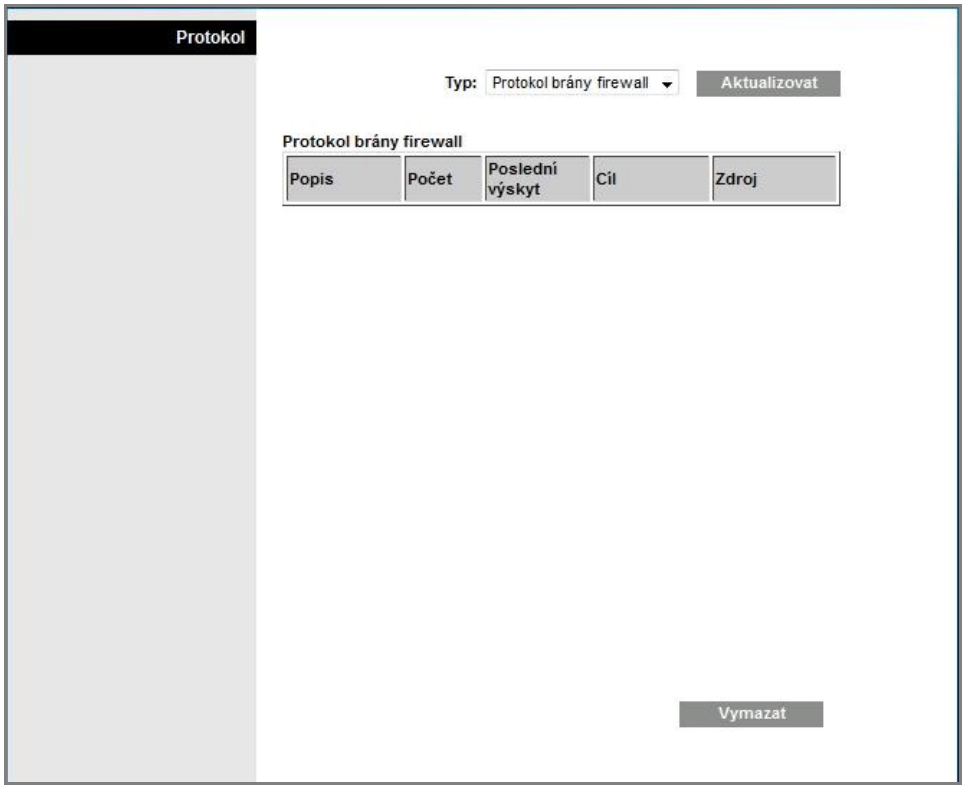
Zobrazení protokolu

Na stránce Zabezpečení > VPN > Zobrazit protokol jsou uvedeny události zachycené branou firewall. Protokol obsahuje tyto položky:

- popis události;
- počet událostí, k nimž došlo;
- poslední událost, k níž došlo;
- cílové a zdrojové adresy.

Prostřednictvím této stránky lze zobrazit následující protokoly:

- protokol přístupů,
- protokol brány firewall,
- protokol sítě VPN,
- protokol rodičovské kontroly.



Kliknutím na možnost **Vymazat** smažete data protokolu.

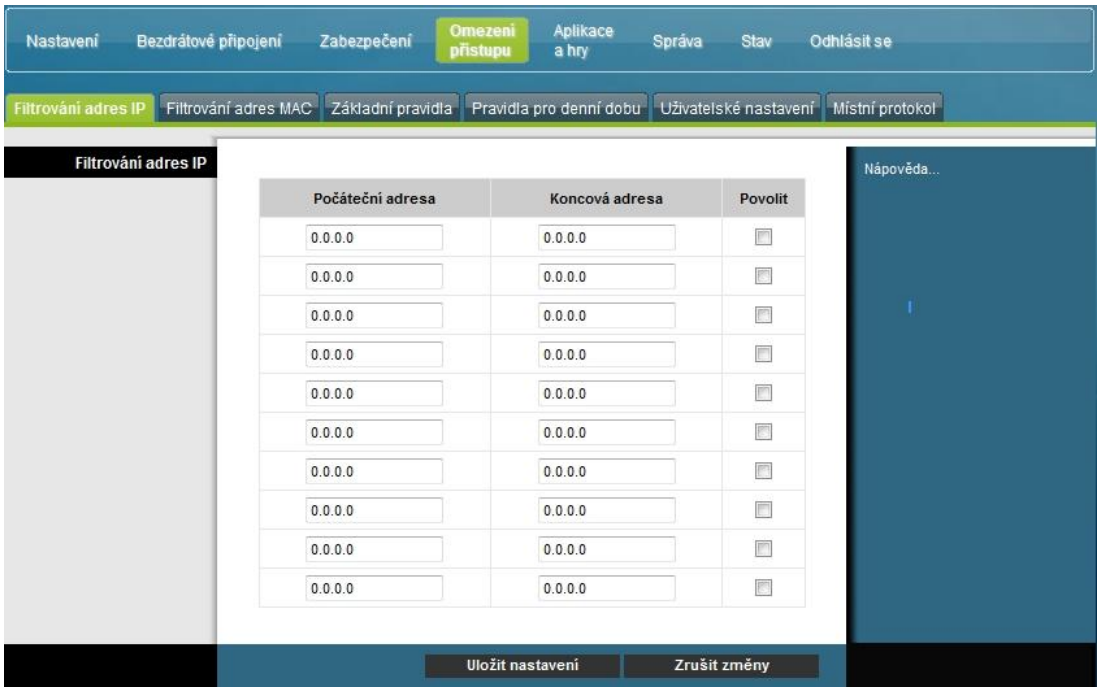
Řízení přístupu k bráně

Omezení přístupu > Filtrování adres IP

Stránka Omezení přístupu > Filtrování adres IP slouží ke konfiguraci filtrů adres IP. Tyto filtry blokují přístup k Internetu pro adresy IP v určitém rozsahu.

Poznámka: Pokud nejste s pokročilým nastavením v této části dostatečně obeznámeni, před změnou jakéhokoli výchozího nastavení filtrování adres IP domácí brány kontaktujte poskytovatele služeb.

Zvolením karty **Filtrování adres IP** otevřete stránku Omezení přístupu > Filtrování adres IP. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

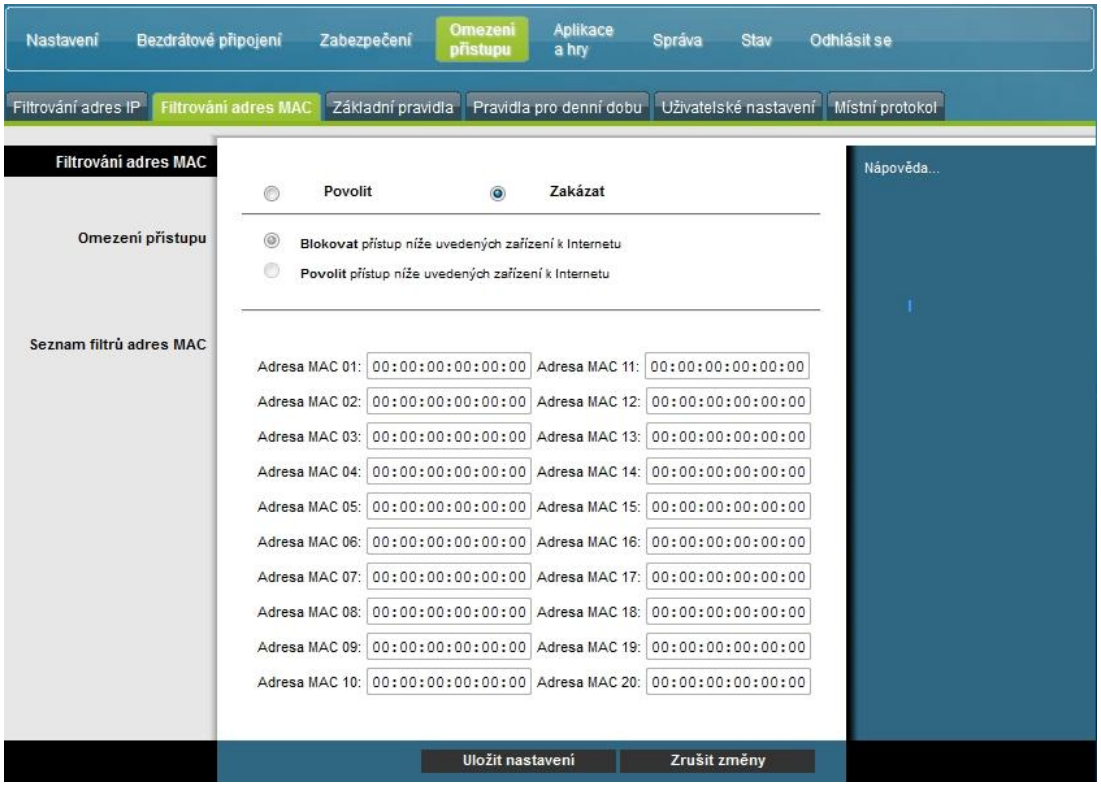


Omezení přístupu > Filtrování adres MAC

Stránka Omezení přístupu > Filtrování adres MAC slouží ke konfiguraci filtrů adres MAC. Tyto filtry umožňují povolit nebo blokovat přístup adres MAC v určitém rozsahu k Internetu.

Poznámka: Pokud nejste s pokročilým nastavením v této části dostatečně obeznámeni, před změnou jakéhokoli výchozího nastavení filtrování adres IP domácí brány kontaktujte poskytovatele služeb.

Zvolením karty **Filtrování adres MAC** otevřete stránku Omezení přístupu > Filtrování adres MAC.



Rozevírací nabídka Blokovat/povolit umožňuje blokovat nebo povolit internetový přístup pro zařízení s adresami MAC zadanými do tabulky filtrů adres MAC. Funkce rozevírací nabídky Blokovat/povolit je popsána v následující tabulce. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Název pole	Popis
Filtrování adres MAC	**Na seznamu blokovaných (výchozí)** Možnost **Na seznamu blokovaných** vyberte, chcete-li zamítnout internetový přístup zařízením s adresami MAC uvedenými v tabulce. Pro ostatní zařízení bude internetový přístup povolen.
	Na seznamu povolených Možnost **Na seznamu povolených** vyberte, chcete-li povolit internetový přístup pouze zařízením s adresami MAC uvedenými v tabulce. Všem zařízením, jejichž adresy MAC v tabulce uvedeny *nejsou*, bude internetový přístup zamítnut.

Funkční tlačítka

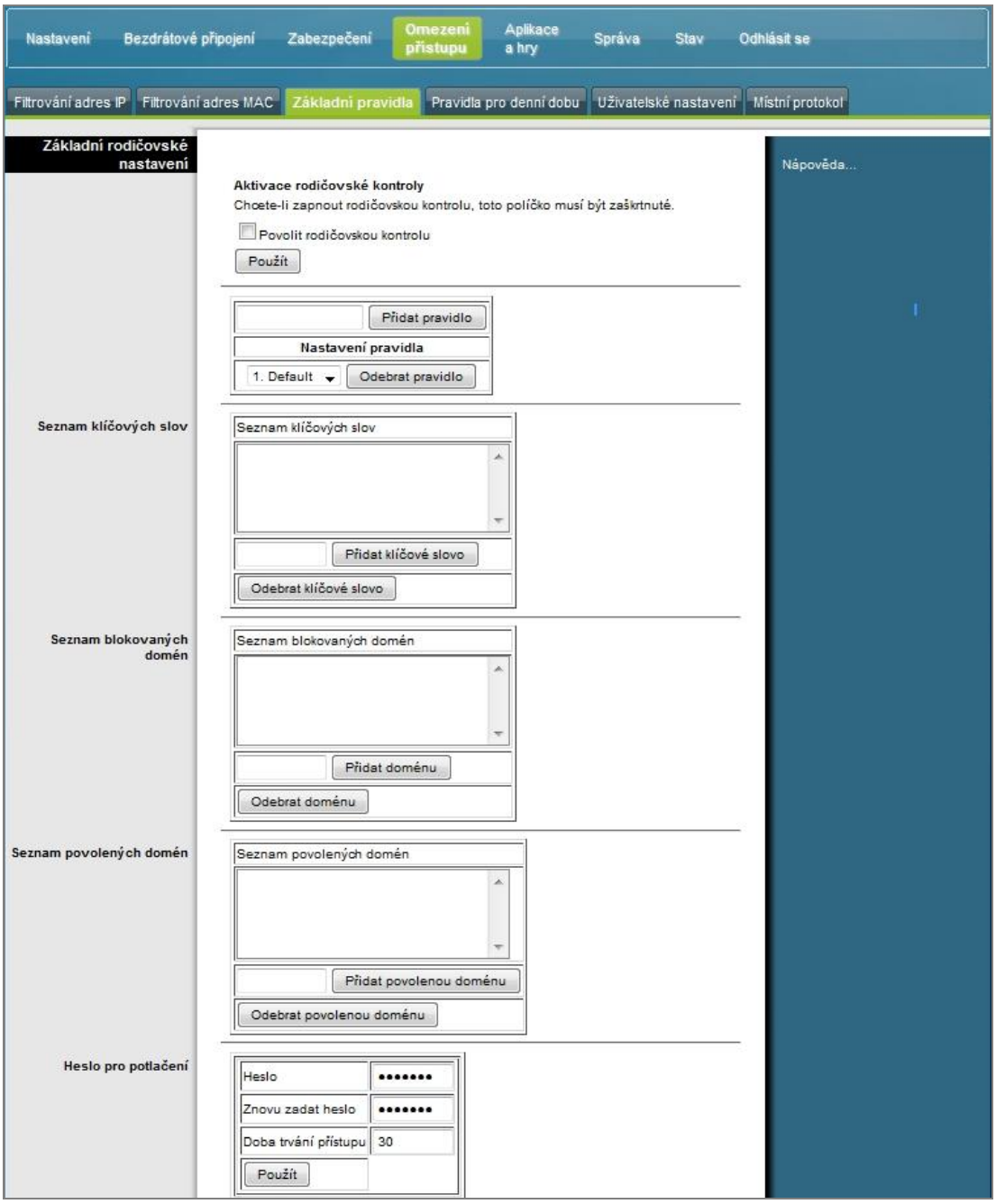
Na stránce Upřesnit nastavení > Filtrování adres MAC jsou k dispozici následující funkční tlačítka.

Tlačítko	Popis
Použít	Uloží hodnoty zadané do polí, aniž by se zavřela stránka.
Přidat adresu MAC	Uloží adresu MAC zadanou do příslušného textového pole.
Odebrat adresu MAC	Odebere vybranou adresu MAC.
Vymazat vše	Odebere všechny definované adresy MAC.

Omezení přístupu > Základní pravidla

Omezení přístupu umožňuje blokovat nebo povolit konkrétní způsoby využití Internetu a konkrétní provoz, například přístup k Internetu, určené aplikace, weby a příchozí provoz v určité dny a v určitou dobu. Na stránce Omezení přístupu > Základní pravidla můžete nakonfigurovat rodičovskou kontrolu na domácí bráně a zobrazit uživatele, kteří jsou oprávněni rodičovskou kontrolu nastavovat.

Zvolením karty **Základní pravidla** otevřete stránku Omezení přístupu > Základní pravidla.



Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci základních pravidel omezení přístupu pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Základní rodičovské nastavení	**Aktivace rodičovské kontroly** Umožňuje povolit nebo zakázat rodičovskou kontrolu. Chcete-li rodičovskou kontrolu povolit, zaškrtněte políčko **Povolit rodičovskou kontrolu** a klikněte na tlačítko **Použít**. Chcete-li rodičovskou kontrolu zakázat, zrušte zaškrtnutí políčka **Povolit rodičovskou kontrolu** a klikněte na tlačítko **Použít**. **Přidat pravidlo** Přidá a uloží nové pravidlo do seznamu pravidel pro obsah. **Odebrat pravidlo** Odebere vybrané pravidlo ze seznamu pravidel pro obsah.
Seznam klíčových slov	**Seznam klíčových slov** Umožňuje vytvoření seznamu klíčových slov. Brána zablokuje každý pokus o přístup k adrese URL obsahující některé z klíčových slov uvedených v tomto seznamu. **Přidat klíčové slovo / Odebrat klíčové slovo** Tato tlačítka umožňují přidat do seznamu nové klíčové slovo, respektive ze seznamu odstranit vybraná klíčová slova.
Seznam blokovaných domén	**Seznam blokovaných domén** Umožňuje vytvořit seznam domén, ke kterým má brána blokovat přístup. Brána zablokuje každý pokus o přístup k doméně uvedené na seznamu. **Přidat doménu / Odebrat doménu** Tato tlačítka umožňují přidat do seznamu nové domény, respektive ze seznamu odstranit vybrané domény.
Seznam povolených domén	**Seznam povolených domén** Umožňuje vytvořit seznam domén, ke kterým má brána povolit přístup. **Přidat povoleno doménu / Odebrat povolenou doménu** Tato tlačítka umožňují přidat do seznamu nové domény, respektive ze seznamu odstranit vybrané domény.

Část	Popis pole
Heslo pro potlačení	**Heslo** Umožňuje vytvořit heslo pro dočasné potlačení omezení uživatelského přístupu k blokovanému webu. **Znovu zadat heslo** Do tohoto pole znovu zadejte heslo pro potlačení, které jste zadali v předchozím poli. **Doba trvání přístupu** Umožňuje určit dobu v minutách, na jakou heslo pro potlačení umožní dočasný přístup k zakázanému webu. **Použít** Uloží všechny přidané položky, úpravy a změny.

Použití klíčových slov a blokování domén

Klíčová slova a blokování domén umožňují blokování přístupu k internetovým stránkám na základě slova nebo textového řetězce obsaženého v adrese URL, která slouží pro přechod na stránku.

Blokování domén umožňuje zamezit přístup na webové stránky na základě názvu jejich domény. Název domény je část adresy URL před příponou, jako je například .COM, .ORG nebo .GOV.

Blokování na základě klíčového slova umožňuje blokovat přístup na Internetové stránky podle klíčového slova nebo textového řetězce kdekoli v adrese URL, nikoli jen v názvu domény.

Poznámka: Funkce blokování domén blokuje přístup k doménám uvedeným na seznamu domén. Dále blokuje domény, jejichž část se shoduje s některou z položek v seznamu.

Pokud například zadáte doménu **priklad.cz**, bude blokována každá stránka obsahující řetězec „priklad.cz“. Do názvu domény není vhodné zahrnovat úvodní sekvenci „www.“, protože v takovém případě by byla blokována pouze stránka, která se přesně shoduje s názvem domény. Pokud byste do seznamu zadali například řetězec „www.priklad.cz“, brána by zablokovala jen stránku s tímto názvem. Pokud úvodní sekvenci „www.“ nezahrnete, budou blokovány všechny stránky v rámci domény „priklad.cz“ a stránky s ní spojené.

Blokování přístupu na weby

Pokud chcete zablokovat přístup na webové stránky, použijte možnost **Seznam blokovaných domén** nebo **Seznam klíčových slov**.

Chcete-li použít možnost **Seznam blokovaných domén**, zadejte adresy URL nebo názvy domén webů, které chcete blokovat.

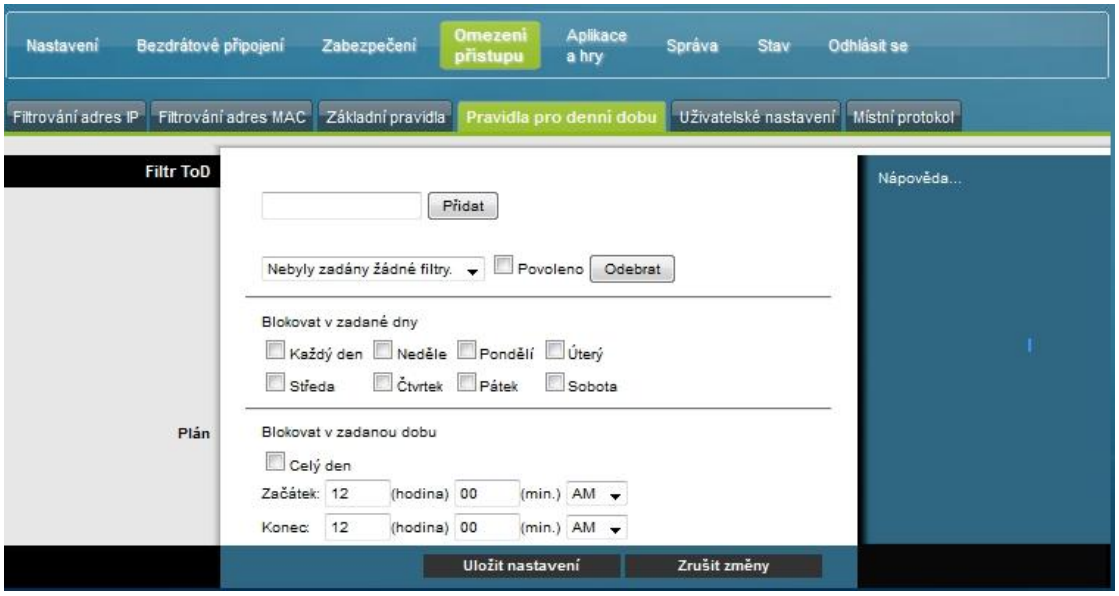
Pomocí možnosti **Seznam klíčových slov** zadejte klíčová slova, která chcete blokovat. Pokud se některé z těchto klíčových slov objeví v adrese URL webu, přístup na tento web bude zablokován. Kontroluje se pouze adresa URL, nikoli obsah webových stránek.

Omezení přístupu > Pravidla pro denní dobu

Stránka Omezení přístupu > Pravidla pro denní dobu umožňuje konfiguraci filtrů pro přístup na web, pomocí nichž lze blokovat veškerý internetový provoz mezi konkrétními síťovými zařízeními na základě vybraného dne v týdnu a času.

Zvolením karty **Pravidla pro denní dobu** otevřete stránku Omezení přístupu > Pravidla pro denní dobu. Na obrázku níže vidíte příklad stránky Omezení přístupu > Pravidla pro denní dobu.

Poznámka: Domácí brána používá síťový čas spravovaný poskytovatelem datových služeb. Aby funkce fungovala správně, hodiny musí být přesné a musí ukazovat čas pro vaše časové pásmo. Ověřte, že se na stránkách Stav a Nastavit čas zobrazuje správný časový údaj. Pokud správný není, kontaktujte svého poskytovatele datových služeb. Rozdíl lze eliminovat také úpravou vašeho nastavení.



Popis stránky Omezení přístupu > Pravidla pro denní dobu

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci pravidel pro denní dobu pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Filtr ToD	**Přidat** Umožňuje přidat nový přístupový filtr nebo pravidlo pro denní dobu. Zadejte název filtru a kliknutím na tlačítko **Přidat** filtr přidejte na seznam. Pravidla pro denní dobu se používají k zakázání přístupu na Internet podle dne a doby. **Odebrat** Odebere vybraný filtr ze seznamu filtrů pro denní dobu.
Plán	**Blokovat v zadané dny** Umožňuje řídit přístup podle dne v týdnu. **Blokovat v zadanou dobu** Umožňuje řídit přístup podle času.

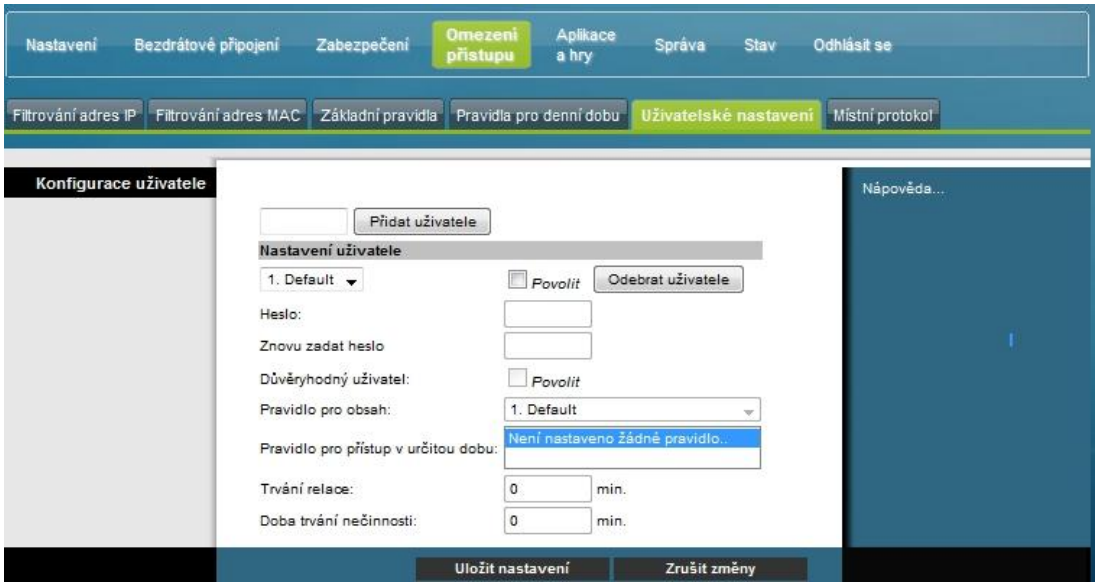
Omezení přístupu > Uživatelské nastavení

Stránka Omezení přístupu > Uživatelské nastavení umožňuje nastavení dalších účtů a uživatelských profilů pro členy domácnosti. Každému profilu lze pomocí pravidel přístupu přiřadit zvláštní úrovně internetového přístupu.

Důležité: Tyto další účty nemají oprávnění správce pro přístup k bráně.

Poznámka: Až definujete a povolíte uživatelské profily, všichni uživatelé se při každém přístupu k Internetu budou muset přihlásit. Přihlašovat se mohou pomocí přihlašovací obrazovky, která se otevře v jejich webovém prohlížeči. Aby získali přístup k Internetu, musí zadat správné uživatelské jméno a heslo.

Zvolením karty **Uživatelské nastavení** otevřete stránku Omezení přístupu > Uživatelské nastavení.



Popis stránky Omezení přístupu > Uživatelské nastavení

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci uživatelů pro domácí bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení** , případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Konfigurace uživatele	**Přidat uživatele** Umožňuje přidat profil nového uživatele. Zadejte jméno uživatele a kliknutím na tlačítko **Přidat uživatele** uživatele přidejte na seznam. **Nastavení uživatele** Umožňuje upravit profil uživatele pomocí rozevírací nabídky. Požadovaný profil lze zobrazit pomocí rozevírací nabídky. V uživatelských jménech a heslech se rozlišují malá a velká písmena. Profil uživatele je třeba aktivovat zaškrtnutím políčka **Povolit**. Pokud profil není aktivní, daný uživatel nemá přístup k Internetu. Chcete-li některý z uživatelských profilů odebrat, pomocí rozevírací nabídky vyberte požadovaného uživatele a klikněte na tlačítko **Odebrat uživatele**. **Heslo** Do tohoto pole zadejte heslo pro vybraného uživatele. Uživatelé musí své uživatelské jméno a heslo zadat při každém přístupu k Internetu. V uživatelských jménech a heslech se rozlišují malá a velká písmena. **Poznámka:** Domácí brána umožní uživatelům přístup k Internetu podle pravidel, která pro ně nastavíte na jejich stránce. **Znovu zadat heslo** Do tohoto pole znovu zadejte heslo, které jste zadali v předchozím poli. **Důvěryhodný uživatel** Toto políčko zaškrtněte, pokud chcete aktuálně vybraného uživatele určit jako důvěryhodného. Na důvěryhodné uživatele se nevztahují pravidla pro internetový přístup. **Pravidlo pro obsah** Zde vyberte pravidlo pro obsah pro aktuální uživatelský profil. Pravidla pro obsah je třeba nejprve definovat na stránce pro konfiguraci pravidel. Stránku pro konfiguraci pravidel otevřete kliknutím na kartu Základní pravidla na této stránce. **Pravidlo pro přístup v určitou dobu** Zde vyberte pravidlo pro přístup v určitou dobu pro aktuální uživatelský profil. Pravidlo pro přístup v určitou dobu je třeba nejprve definovat na stránce Pravidla pro denní dobu. Na stránku Pravidla pro denní dobu přejdete kliknutím na kartu Pravidla pro denní dobu na této stránce.

Část	Popis pole
Konfigurace uživatele	**Trvání relace** 1 440 minut (Výchozí nastavení při vytvoření uživatele. Jinak je nastavena hodnota 0.) Zadejte dobu v minutách, po kterou má mít uživatel přístup k Internetu od momentu, kdy se přihlásí pomocí svého uživatelského jména a hesla. **Poznámka:** Aby nemohlo dojít k vypršení limitu relace, nastavte trvání relace na hodnotu 0.
	Doba trvání nečinnosti 60 minut (Výchozí nastavení při vytvoření uživatele. Jinak je nastavena hodnota 0.) Zadejte dobu nečinnosti při připojení k Internetu, podle níž má systém určit, že uživatel již není online. Pokud bude spuštěn časovač nečinnosti, relace uživatele bude automaticky ukončena. Pokud se uživatel bude chtít znovu připojit k Internetu, bude se muset znovu přihlásit pomocí svého uživatelského jména a hesla. **Poznámka:** Aby nemohlo dojít k vypršení limitu relace, nastavte dobu nečinnosti na hodnotu 0.

Omezení přístupu > Místní protokol

Tato stránka umožňuje sledovat pokusy jednotlivých uživatelů o přístup k zakázaným internetovým stránkám. Dále je zde možné zobrazit události zachycené funkcí rodičovské kontroly pro hlášení událostí.

Zvolením karty **Místní protokol** otevřete stránku Omezení přístupu > Místní protokol.

Na obrázku níže vidíte příklad stránky Omezení přístupu > Místní protokol.

Část	Popis pole
Místní protokol	**Poslední výskyt**
Rodičovská kontrola – protokol událostí	Čas posledního pokusu o otevření zakázané internetové stránky
	Akce
	Akce, kterou provedl systém
	Cíl
	Adresa URL zakázané stránky
	Uživatel
	Jméno uživatele, který se pokusil otevřít zakázanou stránku
	Zdroj
	Adresa IP počítače, pomocí něhož se uživatel pokusil otevřít zakázanou webovou stránku

Konfigurace aplikací a nastavení pro hraní her

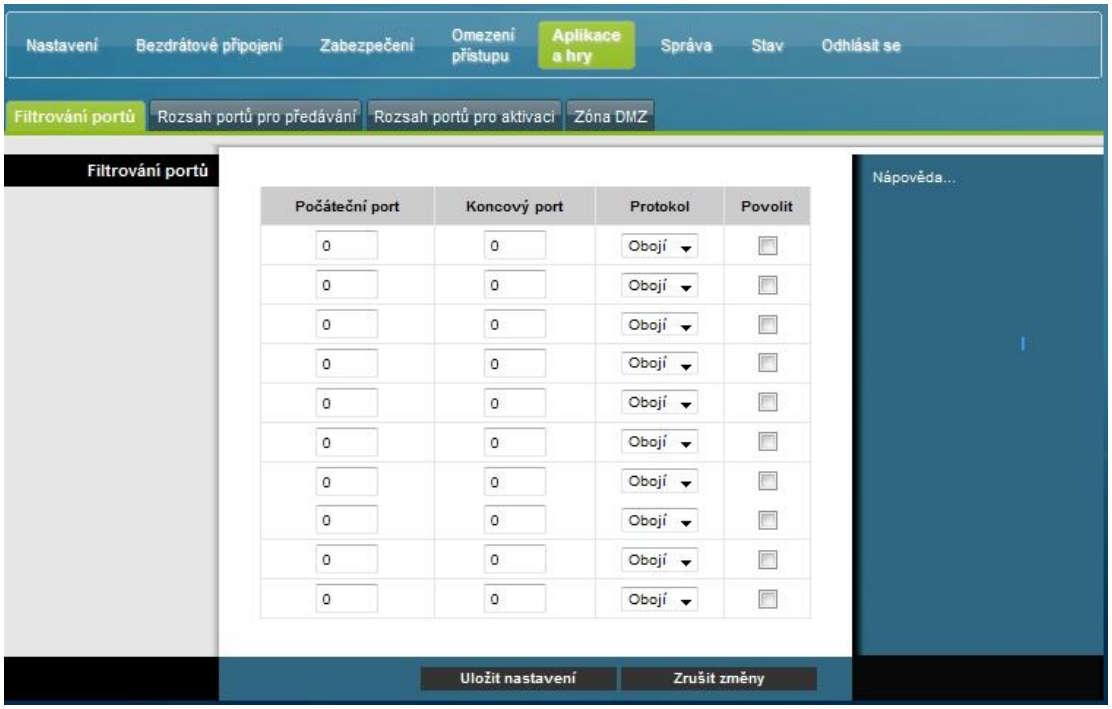
Přehled

Brány aplikační vrstvy podporují nejznámější internetové aplikace. Brány aplikační vrstvy automaticky upravují bránu firewall brány tak, aby umožňovala průchod dat, aniž by bylo nutné přizpůsobit nastavení. Než provedete jakékoli změny v této části, doporučujeme nejprve otestovat konkrétní aplikaci.

Aplikace a hry > Filtrování portů

V tomto okně lze nakonfigurovat filtry portů TCP a UDP. Tyto filtry blokují přístup k Internetu pro rozsah portů TCP a UDP. Dále je možné zakázat, aby počítače odesílaly data TCP/UDP do sítě WAN na určitých portech IP. Tento filtr není určen pro konkrétní adresy IP ani MAC. Systém blokuje určený rozsah portů pro všechny počítače.

Zvolením karty **Filtrování portů** otevřete stránku Aplikace a hry > Filtrování portů.



Popis stránky Aplikace a hry > Filtrování portů

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci filtrování portů pro aplikace a hry používané na domácí bráně. Chcete-li povolit předávání portů pro danou aplikaci, zaškrtněte příslušné políčko **Povolit**. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Filtrování portů	**Počáteční port:** Toto je začátek rozsahu portů. Zadejte počáteční hodnotu rozsahu čísel portů (externí porty) používaných serverem nebo internetovou aplikací. V případě potřeby nahlédněte do dokumentace internetové aplikace, kde najdete více informací.
	Koncový port: Toto je konec rozsahu portů. Zadejte koncovou hodnotu rozsahu čísel portů (externí porty) používaných serverem nebo internetovou aplikací. V případě potřeby nahlédněte do dokumentace internetové aplikace, kde najdete více informací.
	Protokol Vyberte jeden z následujících protokolů: ■ **TCP,** ■ **UDP,** ■ **Obojí.**
	Povolit: Zaškrtnutím tohoto políčka aktivujete filtrování na určených portech.

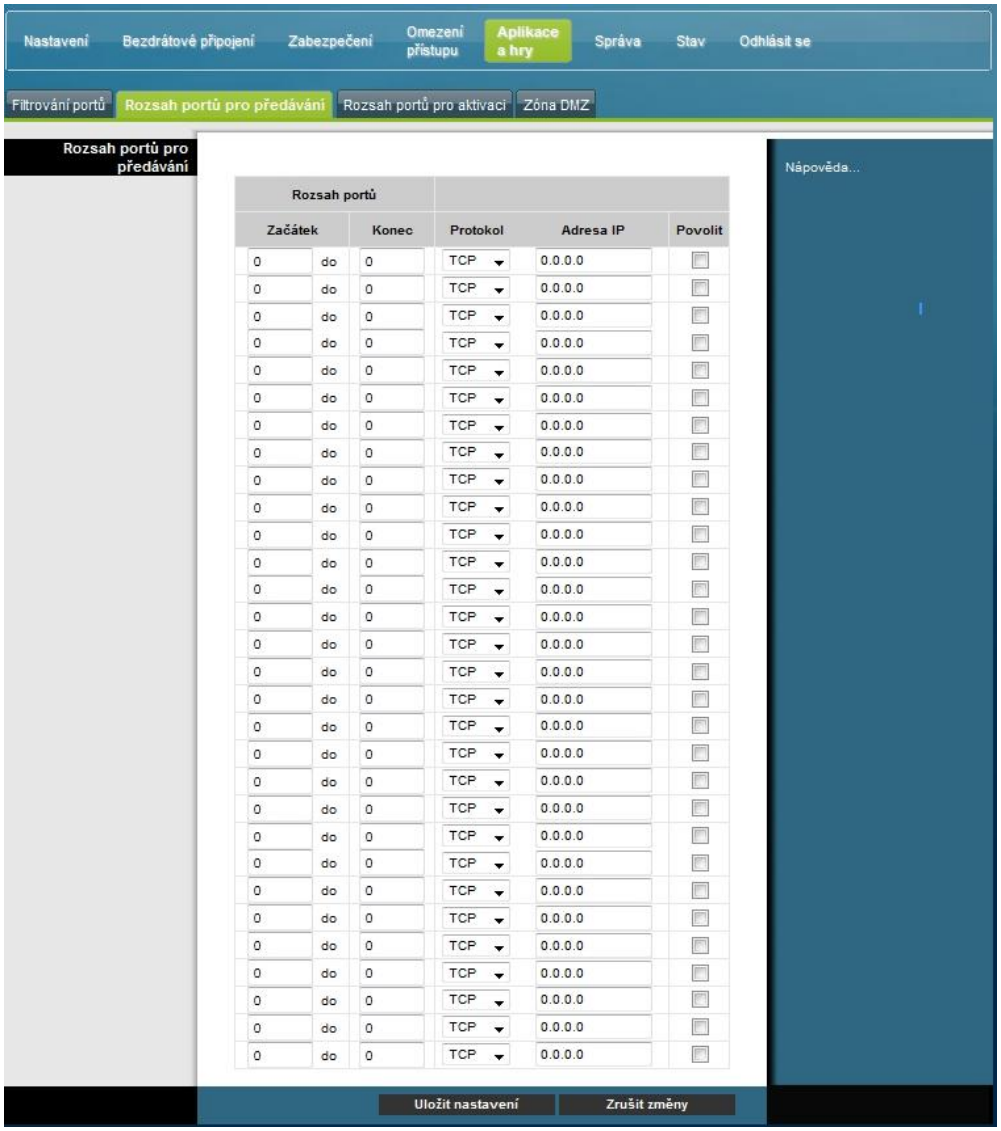
Aplikace a hry > Rozsah portů pro předávání

Důležité: Brána obvykle nabízí funkci označovanou jako překlad portů. Tato funkce sleduje, které porty jsou skutečně využívány počítači a jinými zařízeními v síti LAN. Toto sledování představuje další úroveň zabezpečení přesahující úroveň zabezpečení, kterou poskytuje brána firewall. Některé aplikace však vyžadují, aby brána pro internetové připojení používala konkrétní porty.

Funkce Rozsah portů pro předávání umožňuje předávání portů z veřejného Internetu na konkrétní adresy IP v místní síti. Zvolením karty **Rozsah portů pro předávání** otevřete stránku Aplikace a hry > Rozsah portů pro předávání.

Jako počáteční a koncový port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat. Zadejte do obou polí číslo portu nebo rozsah portů. Do pole Adresa IP zadejte požadovanou adresu IP počítače.

Poznámka: Při použití funkce Rozsah portů pro předávání jsou vybrané porty trvale viditelné pro veřejnou síť Internet. To znamená, že brána firewall brány není v případě těchto portů aktivní. Zařízení s adresou IP pro předávání mohou být při předávání portů v daném rozsahu vystavena útokům hackerů.



Popis stránky Aplikace a hry > Rozsah portů pro předávání

Popisy a pokyny uvedené v této tabulce vám usnadní konfiguraci předávání portů v daném rozsahu pro domácí bránu. Pro každou položku zaškrtněte políčko Povolit. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

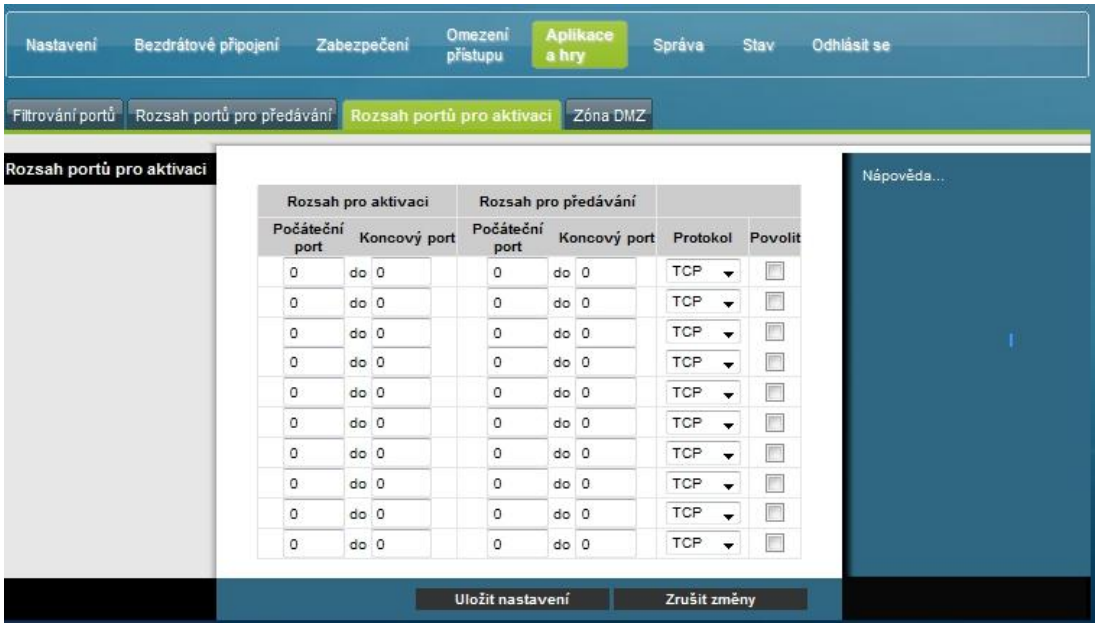
Část	Popis pole
Rozsah portů pro předávání	**Začátek** Jako počáteční port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat.

Část	Popis pole
	Konec Jako koncový port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat.
	Protokol Vyberte jeden z následujících protokolů: ■ TCP, ■ UDP, ■ Obojí.
	Adresa IP Zadejte adresu IP požadovaného počítače.
	Povolit Zaškrtnutím tohoto políčka povolíte předávání portů pro určené porty a adresy IP.

Aplikace a hry > Rozsah portů pro aktivaci

Funkce Rozsah portů pro aktivaci umožňuje dynamické předávání portů do počítačů v síti LAN, které je potřebují v určitou dobu. Jde o dobu, kdy je spuštěna konkrétní aplikace spouštějící určitou událost, která spouští směrovač. Touto událostí musí být odchozí komunikace na portu v určitém rozsahu.

Zvolením karty **Rozsah portů pro aktivaci** otevřete stránku Aplikace a hry > Rozsah portů pro aktivaci.



Popis stránky Aplikace a hry > Rozsah portů pro aktivaci

Popisy a pokyny uvedené v této tabulce vám usnadní konfiguraci aktivace portů v daném rozsahu pro domácí bránu. Pro každou položku zaškrtněte políčko Povolit. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

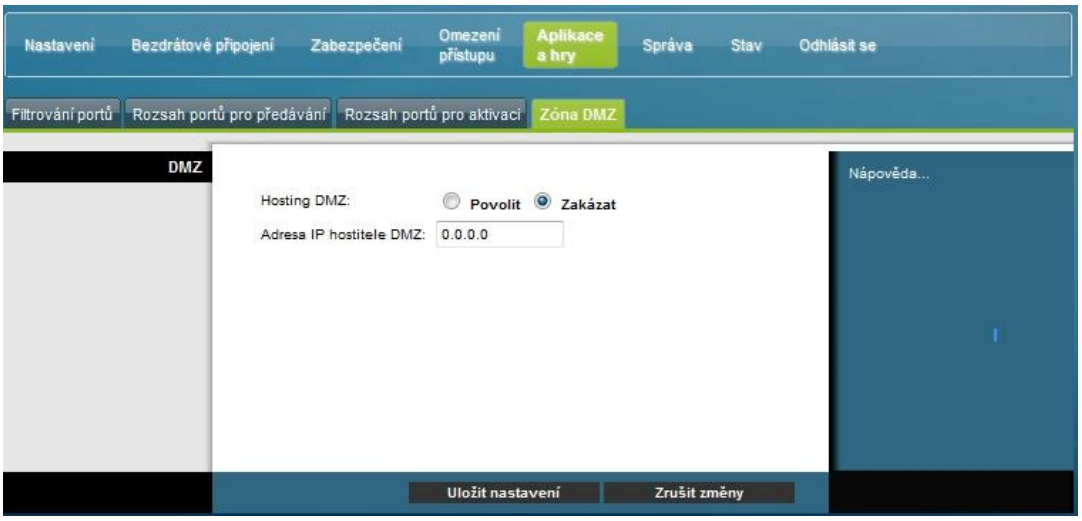
Část	Popis pole
Rozsah portů pro aktivaci	
Rozsah pro aktivaci	**Počáteční port** Jako počáteční port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat.
	Koncový port Jako koncový port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat.
Rozsah pro předávání	**Počáteční port** Jako počáteční port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat.
	Koncový port Jako koncový port vyberte port z doporučeného rozsahu 49 152–65 535. Programy používají konkrétní porty, takže zkontrolujte, které porty je třeba pro daný program předávat.
	Protokol Vyberte jeden z následujících protokolů: ■ TCP, ■ UDP, ■ Obojí.
	Povolit Zaškrtnutím políčka Povolit povolíte aktivaci portů pro danou aplikaci.

Aplikace a hry > Zóna DMZ

Tato stránka umožňuje konfiguraci adresy IP, jejíž porty jsou přímo přístupné pro veřejný Internet a síť WAN. Hostování DMZ se běžně označuje jako „odhalený hostitel“. Umožňuje určit příjemce provozu sítě WAN, které metoda NAT nedokáže přeložit pro známý místní počítač.

Zónu DMZ obvykle používají společnosti, které chtějí hostovat vlastní internetový server. Zóna DMZ umožňuje umístění jedné adresy IP na internetovou stranu brány firewall brány, zatímco ostatní adresy jsou chráněny branou firewall.

Zóna DMZ umožňuje přímý přístup k zařízení z Internetu, například z webového serveru (HTTP), serveru FTP, serveru SMTP (pošta) nebo serveru DNS. Zvolením karty **Zóna DMZ** otevřete stránku Aplikace a hry > Zóna DMZ.



Popis stránky Aplikace a hry > Zóna DMZ

Popisy a pokyny uvedené v této tabulce vám usnadní konfiguraci aktivace portů v daném rozsahu pro domácí bránu. Pro každou adresu IP hostitele DMZ zaškrtněte možnost Povolit. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

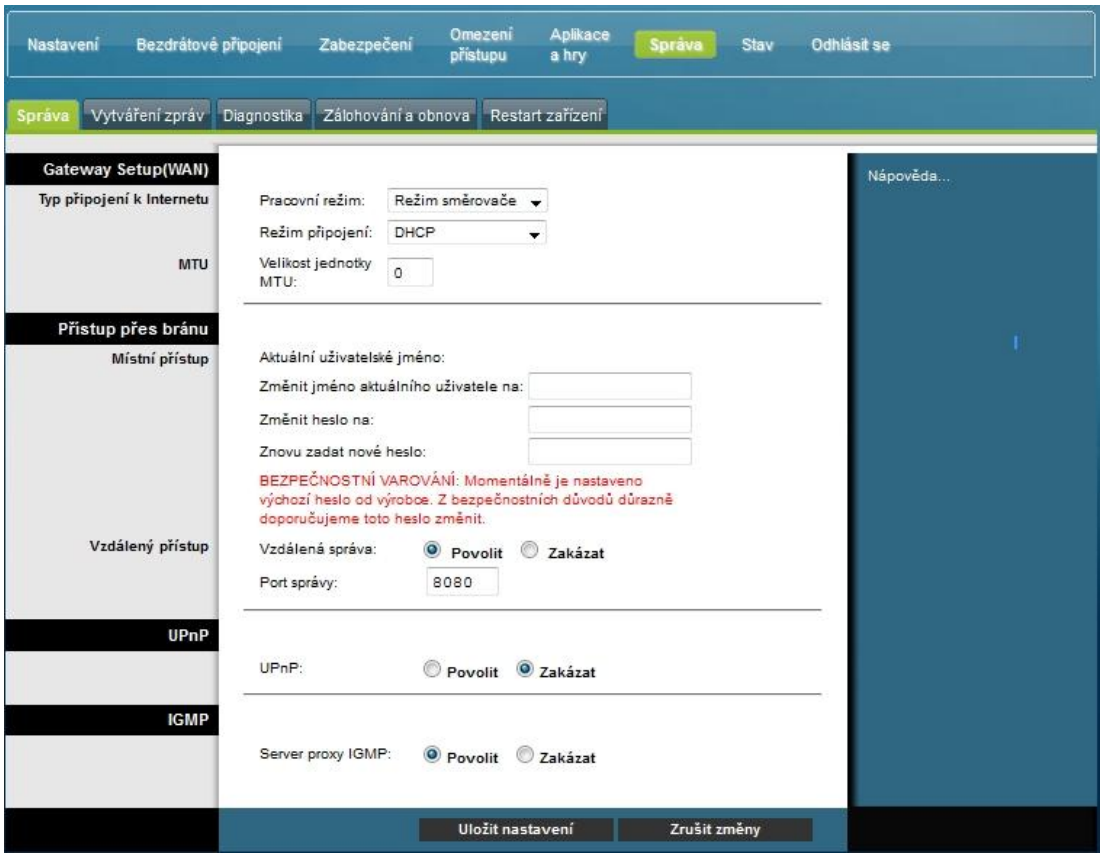
Část	Popis pole
Zóna DMZ	**Hosting DMZ** Vyberte požadovanou možnost: ■ **Povolit,** ■ **Zakázat** (výchozí).
	Adresa IP hostitele DMZ Zóna DMZ umožňuje nastavit jednu adresu IP jako nechráněnou, zatímco ostatní adresy zůstávají chráněné. Do tohoto pole zadejte adresu IP počítače, kterou chcete nastavit jako nechráněnou.

Správa brány

Správa > Správa

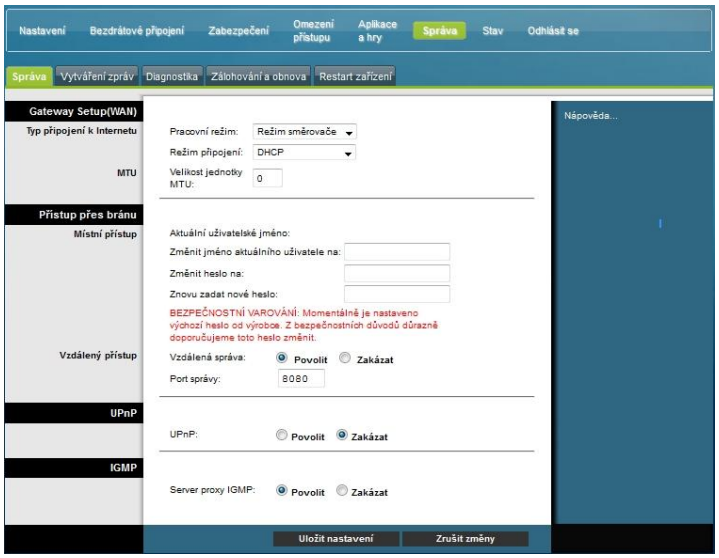
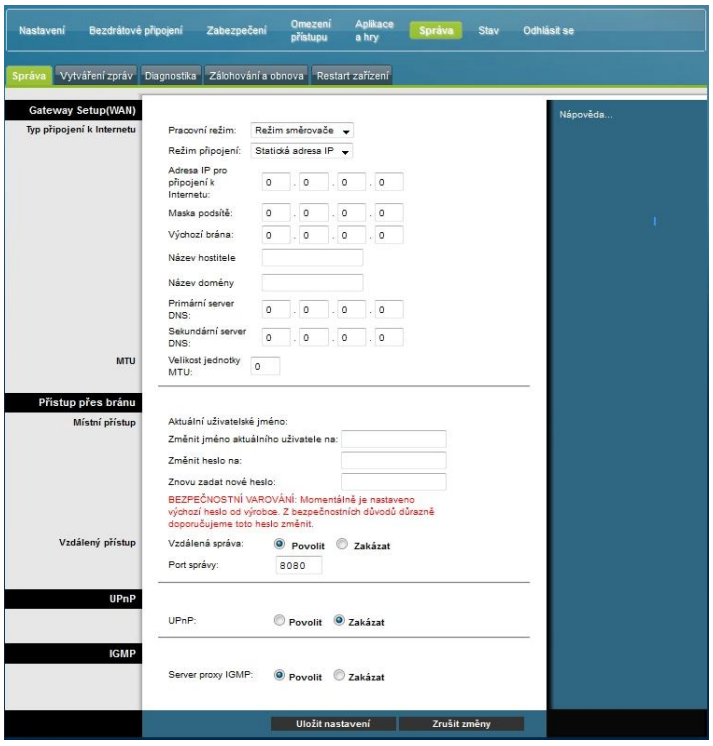
Stránka Správa > Správa umožňuje správci sítě spravovat určité funkce brány pro přístup a zabezpečení. Zvolením karty **Správa** otevřete stránku Správa > Správa.

Důležité: Následující stránka se zobrazí, pokud je v režimu připojení zvoleno nastavení **DHCP** (výchozí). Stránka, která se zobrazí při zvolení možnosti **Statická adresa IP**, je zobrazena a popsána dále.



Popis stránky Správa > Správa

Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci správy pro domácí bránu při zvolení režimu připojení DHCP nebo připojení pomocí statické adresy IP. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Pole	Popis
Gateway Setup (WAN) (Nastavení brány (WAN)) **Typ připojení k Internetu**	**Režim připojení.** Toto nastavení umožňuje určit způsob, jakým má síť WAN (nebo internetové rozhraní brány) získávat adresu IP. **DHCP** (výchozí) Umožní bráně automaticky získávat veřejnou adresu IP.  **Statická adresa IP** Umožňuje určit adresu IP sítě WAN a příslušné informace o serveru jako statické nebo pevné hodnoty, které mají být použity, kdykoli je brána online. 

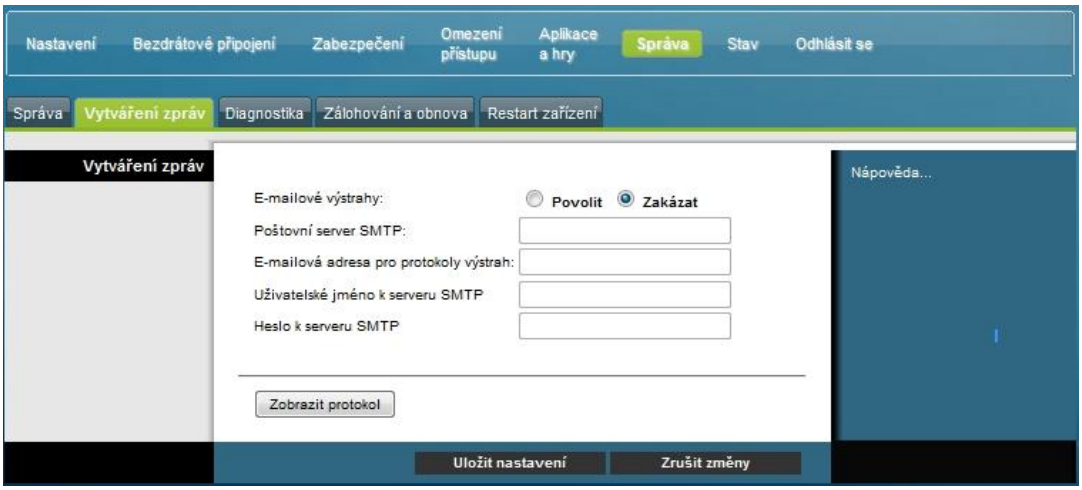
Pole	Popis
	Adresa IP pro připojení k Internetu Zadejte adresu IP brány (tak, jak se zobrazuje na Internetu). **Maska podsítě** Zadejte masku podsítě brány (tak, jak se zobrazuje na Internetu, včetně poskytovatele služeb). **Výchozí brána** Zadejte výchozí bránu serveru poskytovatele služeb. **Primární server DNS** Zadejte adresy IP primárního serveru DNS, které jste získali od poskytovatele služeb. Toto je povinná položka. **Sekundární server DNS** Zadejte adresy IP sekundárního serveru DNS, které jste získali od poskytovatele služeb. Toto je volitelná položka.
MTU	**Velikost jednotky MTU** MTU je maximální přenosová jednotka. Určuje největší dovolenou velikost paketu pro přenos prostřednictvím Internetu. Výchozí nastavení = 0 (1 500 bajtů).
Přístup přes bránu **Místní přístup**	**Aktuální uživatelské jméno** Označuje aktuálně přihlášeného uživatele. **Změnit jméno aktuálního uživatele na** Umožňuje změnit uživatelské jméno. Chcete-li změnit své uživatelské jméno, zadejte do tohoto pole nové uživatelské jméno a uložte jej kliknutím na možnost **Uložit nastavení**. **Poznámka:** Ve výchozím nastavení je pole pro uživatelské jméno prázdné. **Změnit heslo na** Umožňuje změnit heslo. Chcete-li změnit své heslo, zadejte do tohoto pole nové heslo. Potom toto heslo zadejte ještě jednou do pole **Znovu zadat nové heslo** a uložte změnu kliknutím na možnost **Uložit nastavení**. **Poznámka:** Ve výchozím nastavení je pole pro heslo prázdné. **Znovu zadat nové heslo** Do tohoto pole se znovu zadává nové heslo. Je třeba zadat stejné heslo, jaké jste zadali do pole **Změnit heslo na.** Až podruhé zadáte nové heslo, uložte změnu kliknutím na možnost **Uložit nastavení**.

Pole	Popis
Vzdálený přístup	**Vzdálená správa** Umožňuje povolit nebo zakázat vzdálenou správu. Tato funkce umožňuje otevřít a spravovat nastavení brány prostřednictvím Internetu, když nejste přímo u svého počítače. Chcete-li vzdálený přístup povolit, vyberte možnost **Povolit**. Jinak ponechte výchozí nastavení **Zakázat**. Vzdálená správa vyžaduje protokol HTTP. Chcete-li se k zařízení připojit prostřednictvím vzdáleného přístupu, zadejte do pole **Adresa** ve webovém prohlížeči řetězec https://xxx.xxx.xxx.xxx:8080 (znaky „x“ představují veřejnou internetovou adresu zařízení a číslo „8080“ určený port). **Port správy** Zadejte číslo portu, který má být otevřený pro vnější přístup. Výchozí nastavení je 8080. Tento port je nutné použít při vytváření vzdáleného připojení.
UPnP	**UPnP** Funkce UPnP umožňuje automatickou konfiguraci brány pro různé internetové aplikace, jako jsou například hry a videokonference, v systémech Windows XP a Vista. Chcete-li funkci UPnP použít, ponechte výchozí nastavení **Povolit**. Jinak vyberte možnost **Zakázat**.
IGMP	**Server proxy IGMP** Protokol IGMP slouží k vytvoření členství ve skupině vícesměrového vysílání a běžně se používá pro aplikace pro vícesměrové vysílání datových proudů. Může jít například o televizor IPTV s více set-top boxy ve stejné místní síti. Tyto set-top boxy současně přehrávají různé datové proudy videa, a proto je třeba použít funkci IGMP směrovače. Předávání IGMP je systém, který vylepšuje vícesměrové vysílání klientů na straně sítě LAN. Pokud klienti tuto možnost podporují, ponechte výchozí nastavení **Povolit**. Jinak vyberte možnost **Zakázat**.

Správa > Vytváření zpráv

Pomocí zpráv pro správu je možné na zadanou e-mailovou adresu zasílat informace o různých činnostech systému.

Zvolením karty **Vytváření správ** otevřete stránku Správa > Vytváření správ.



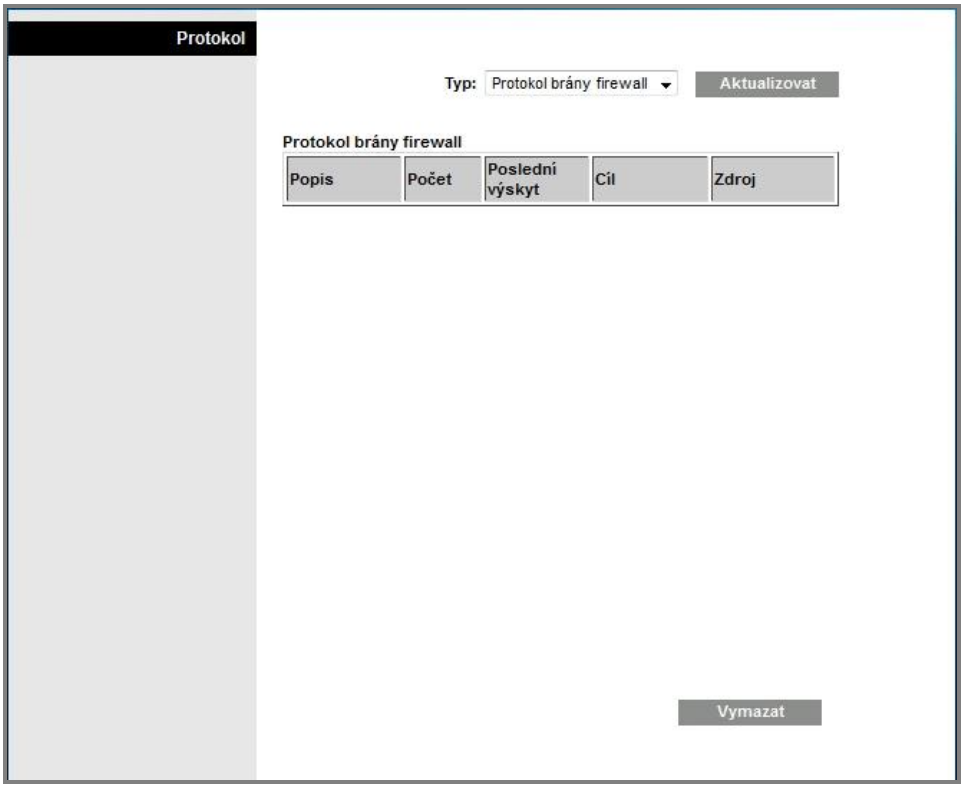
Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci funkce vytváření správ pro bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Vytváření zpráv	**E-mailové výstrahy** Pokud tuto funkci povolíte, okamžitě po zjištění jakékoli události, kterou je třeba nahlásit, bude odeslán e-mail. Chcete-li tuto funkci použít, zadejte požadovanou e-mailovou adresu.
	Poštovní server SMTP Zadejte adresu (název domény) nebo adresu IP serveru SMTP, který používáte pro odchozí poštu.
	E-mailová adresa pro protokoly výstrah Zadejte e-mailovou adresu, na kterou se mají odesílat protokoly.

Zobrazení protokolu

Chcete-li zobrazit protokoly, postupujte níže popsaným způsobem.

1 Klikněte na možnost **Zobrazit protokol**. Otevře se nové okno se stránkou dat protokolů.



2 Chcete-li zobrazit konkrétní protokol, vyberte v rozevírací nabídce Typ jednu z následujících možností:

- Vše,
- Protokol přístupů,
- Protokol brány firewall,
- Protokol sítě VPN.

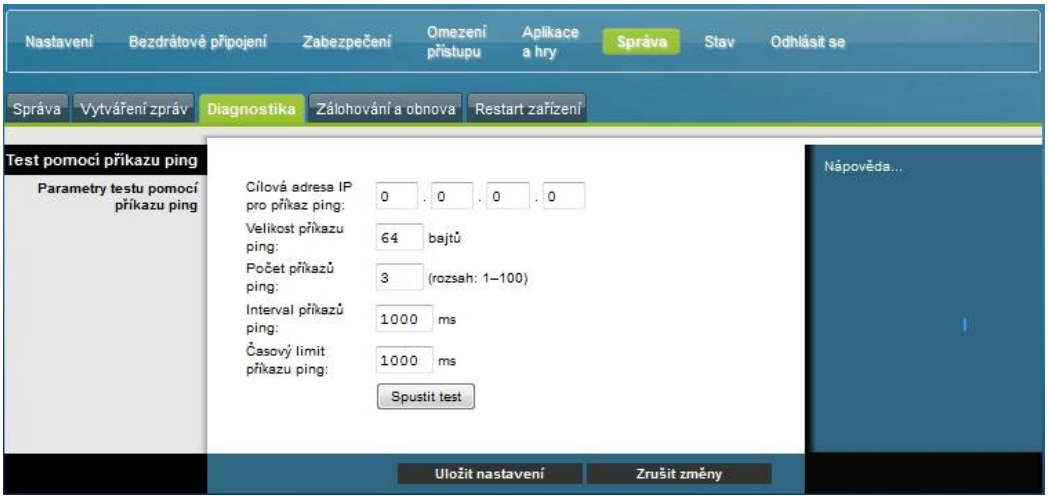
3 Až se data protokolu zobrazí, můžete použít některou z těchto možností:

- Kliknutím na tlačítko **Aktualizace stránky** aktualizujete protokol.
- Kliknutím na tlačítko **Vymazat** smažete všechny informace v aktuálním protokolu.
- Kliknutím na tlačítko **Předchozí strana** zobrazíte dříve zobrazené informace.
- Kliknutím na tlačítko **Další strana** zobrazíte další část protokolu (je-li k dispozici).

Správa > Diagnostika

V části Diagnostika lze kontrolovat stav internetového připojení pomocí testu ping.

Zvolením karty **Diagnostika** otevřete stránku Správa > Diagnostika.



Popisy a pokyny uvedené v následující tabulce vám usnadní konfiguraci funkce diagnostiky pro bránu. Až provedete požadovaná nastavení, uložte změny kliknutím na možnost **Uložit nastavení**, případně klikněte na možnost **Zrušit změny**.

Část	Popis pole
Test pomocí příkazu ping **Parametry testu pomocí příkazu ping**	**Cílová adresa IP pro příkaz ping** Adresa IP, na kterou se má odeslat příkaz ping. **Velikost příkazu ping** Zadejte požadovanou velikost paketu. **Počet příkazů ping** Určete, kolikrát chcete odeslat příkaz ping k cílovému zařízení. **Interval příkazů ping** Zadejte dobu (ms), která má uplynout mezi jednotlivými příkazy ping. **Časový limit příkazu ping** Zadejte požadovaný časový limit příkazu v milisekundách. Pokud během této doby nebude přijata žádná odezva, test pomocí příkazu ping bude považován za neúspěšný.

Část	Popis pole
	Spustit test Test lze spustit pomocí následujících kroků. **1** Zahajte test kliknutím na možnost **Spustit test**. Zobrazí se nová stránka se souhrnem výsledků testu. **2** Kliknutím na možnost **Uložit nastavení** výsledky testu uložte, případně je zrušte kliknutím na možnost **Zrušit změny**.

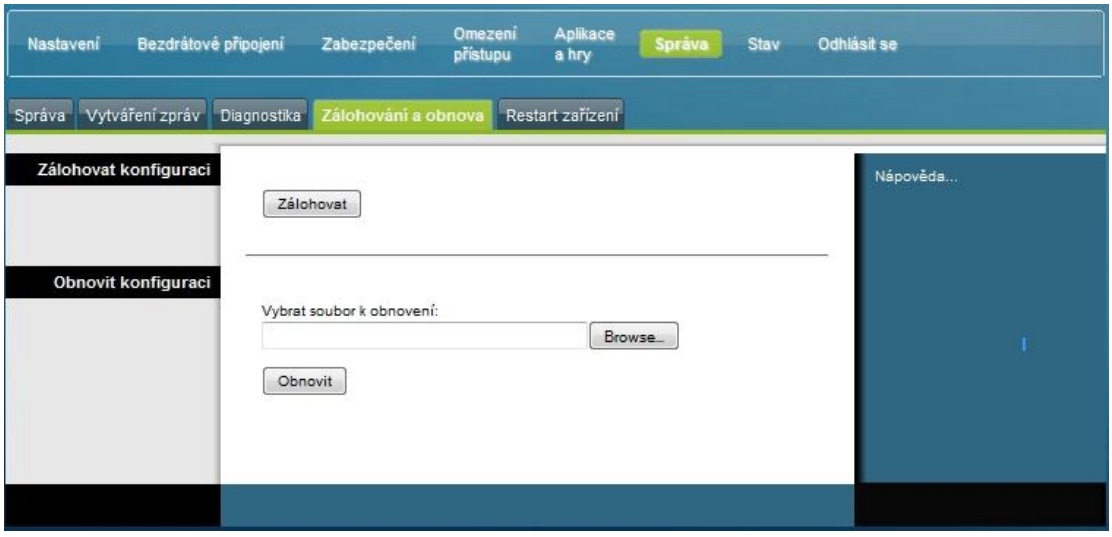
Správa > Zálohování a obnova

Funkce Zálohování a obnova umožňuje zálohovat konfiguraci brány a uložit ji do počítače. Soubor zálohy pak lze použít k obnovení dříve uložené konfigurace brány.

Zvolením karty **Zálohování a obnova** otevřete stránku Správa > Zálohování a obnova.

POZOR:

Obnovením souboru konfigurace se vymažou (přepíší) všechna stávající nastavení.



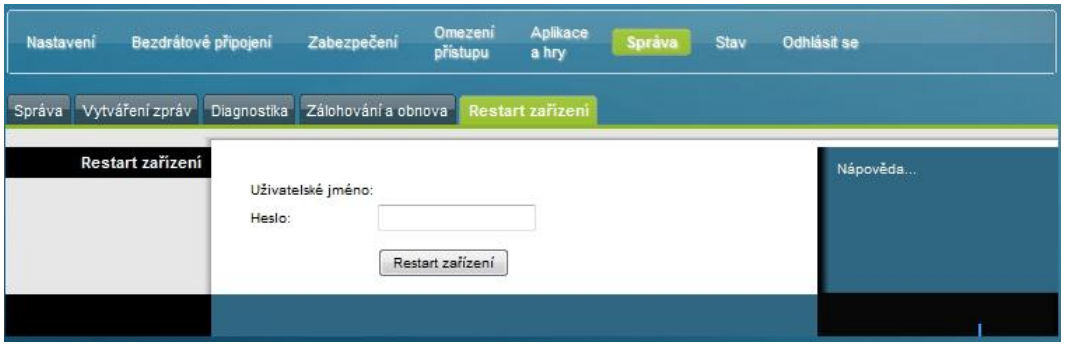
Část	Popis pole
Zálohovat konfiguraci	Funkce Zálohovat konfiguraci slouží k uložení kopie aktuální konfigurace do souboru v počítači. Zálohování spustíte kliknutím na možnost **Zálohovat**.
Obnovit konfiguraci	Funkce Obnovit konfiguraci slouží k obnovení dříve uložené konfigurace. Klikněte na možnost **Browse** (Procházet) a vyberte soubor konfigurace. Kliknutím na možnost **Obnovit** načtěte soubor konfigurace do zařízení.

Správa > Výchozí nastavení výrobce

Prostřednictvím stránky Správa > Výchozí nastavení výrobce lze obnovit výchozí nastavení od výrobce. Zvolením karty **Výchozí nastavení výrobce** otevřete stránku Správa > Výchozí nastavení výrobce.

POZOR:

Pokud obnovíte výchozí nastavení, vymažou se všechna nastavení brány, která jste zadali. Proto si, než výchozí nastavení brány obnovíte, poznamenejte všechna vlastní nastavení. Po obnovení výchozího nastavení bude třeba všechna vlastní nastavení zadat znovu.



Obnovit výchozí nastavení výrobce

Chcete-li obnovit výchozí nastavení, klikněte na možnost **Obnovit výchozí nastavení výrobce**. Všechna nastavení konfigurace se změní na výchozí hodnoty. Při obnově výchozího nastavení se vymažou všechna vámi uložená nastavení.

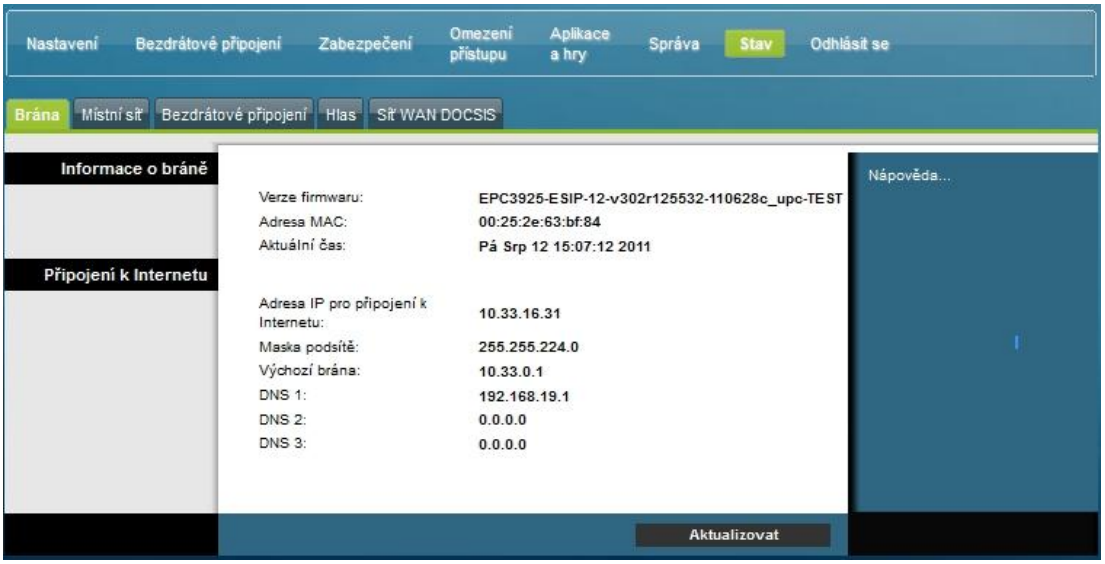
Sledování stavu brány

V této části jsou popsány možnosti dostupné na kartě Stav, pomocí níž lze sledovat stav domácí brány a provádět diagnostiku zařízení a sítě.

Stav > Brána

Na stránce Stav > Brána se zobrazují informace o bráně a jejím aktuálním nastavení. Zobrazené informace se liší podle používaného typu připojení k Internetu.

Zvolením karty **Brána** otevřete obrazovku Stav > Brána. Kliknutím na možnost **Aktualizovat** aktualizujte data na obrazovce.



Popisy uvedené v následující tabulce vám usnadní kontrolu stavu brány a internetového připojení.

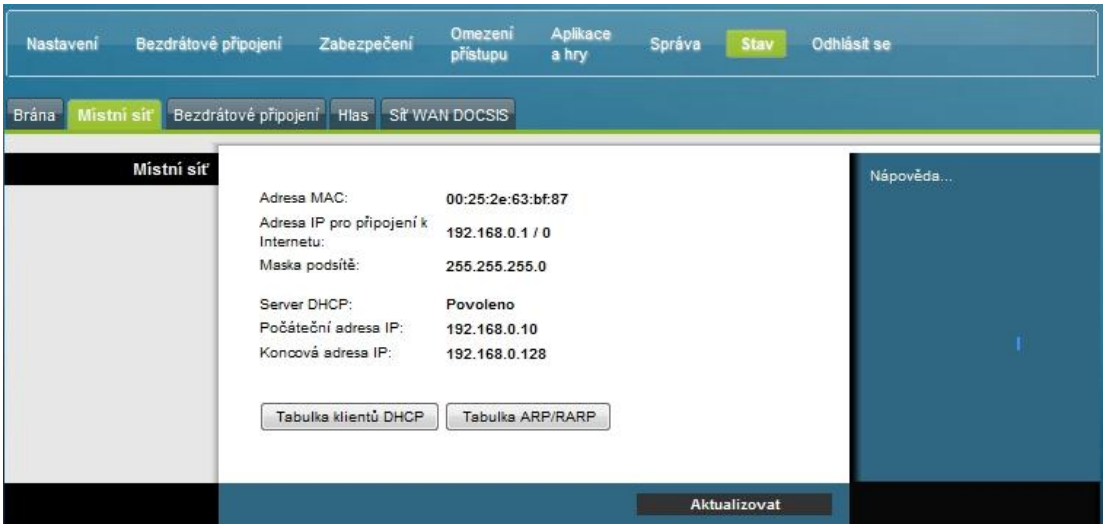
Část	Popis pole
Informace o bráně	**Verze firmwaru** Číslo verze firmwaru **Adresa MAC (adresa CM MAC)** Jedinečná alfanumerická adresa koaxiálního rozhraní kabelového modemu, která slouží k připojení systému CMTS. Adresa MAC je hardwarová adresa, jež jednoznačně určuje každý uzel v síti. **Aktuální čas** Čas podle časového pásma, které jste vybrali na stránce Základní nastavení

Část	Popis pole
Připojení k Internetu	**Adresa IP** Adresa IP rozhraní sítě WAN. Tato adresa je bráně přiřazena při přechodu do stavu online. **Maska podsítě** Maska podsítě portu sítě WAN. Tuto adresu přiřazuje portu sítě WAN automaticky poskytovatel služeb Internetu při nastavení statické adresy IP. **Výchozí brána** Adresa IP výchozí brány poskytovatele služeb Internetu **DNS 1–3** Adresy IP serveru DNS aktuálně používané bránou **WINS** Adresa IP serveru WINS aktuálně používaná bránou

Stav > Místní síť

Na stránce Stav > Místní síť se zobrazují informace o stavu místní sítě.

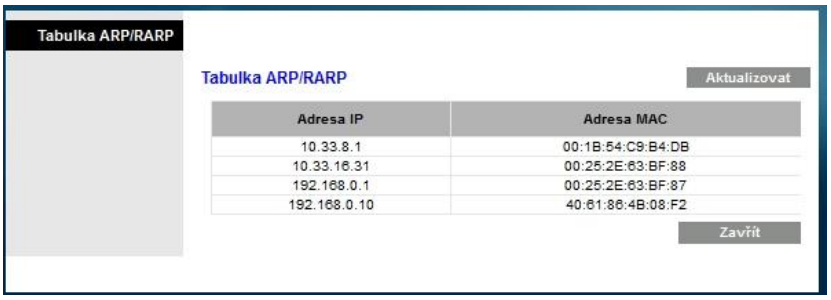
Zvolením karty **Místní síť** otevřete stránku Stav > Místní síť. Kliknutím na možnost **Aktualizovat** aktualizujte data na stránce.



Následující tabulka vám usnadní kontrolu stavu brány a internetového připojení.

Část	Popis pole
Místní síť	**Adresa MAC** Jedinečná alfanumerická adresa privátní domácí sítě LAN. Adresa

Část	Popis pole
	MAC je hardwarová adresa jednoznačně určující každý uzel v síti. **Adresa IP** Adresa IP podsítě LAN **Maska podsítě** Maska podsítě sítě LAN **Server DHCP** Stav místního serveru DHCP (Povoleno nebo Zakázáno) **Počáteční adresa IP** Počáteční adresa IP rozsahu, kterou používá server DHCP v bráně **Koncová adresa IP** Koncová adresa IP rozsahu, kterou používá server DHCP v bráně
Tabulka klientů DHCP	Kliknutím na možnost **Tabulka klientů DHCP** zobrazíte zařízení, která jsou připojena do sítě LAN a kterým server DHCP brány přiřadil adresy IP. Na stránce Tabulka klientů DHCP je uveden seznam klientů DHCP (počítačů a jiných síťových zařízení) s následujícími informacemi: názvy hostitelů klientů, adresy IP, adresy MAC a doba skončení platnosti adres IP přiřazených zařízením. Chcete-li načíst aktuální informace, klikněte na možnost **Aktualizovat**. Chcete-li stránku zavřít a přejít zpět na stránku Místní síť, klikněte na možnost **Zavřít**. Na následujícím obrázku vidíte ukázku stránky Tabulka klientů DHCP. 

Část	Popis pole
Tabulka ARP/RARP	Kliknutím na možnost **Tabulka ARP/RARP** zobrazíte seznam všech zařízení připojených do sítě. Chcete-li načíst aktuální informace, klikněte na možnost **Aktualizovat**. Chcete-li stránku zavřít a přejít zpět na stránku Místní síť, klikněte na možnost **Zavřít**. Na následujícím obrázku vidíte ukázku stránky Tabulka ARP/RARP. 

Stav > Bezdrátové připojení

Na stránce Stav > Bezdrátové připojení jsou uvedeny základní informace o bezdrátové síti brány.

Zvolením karty **Bezdrátové připojení** otevřete stránku Stav > Bezdrátové připojení. Kliknutím na možnost **Aktualizovat** aktualizujte data na stránce.

Popis stránky Stav > Bezdrátové připojení

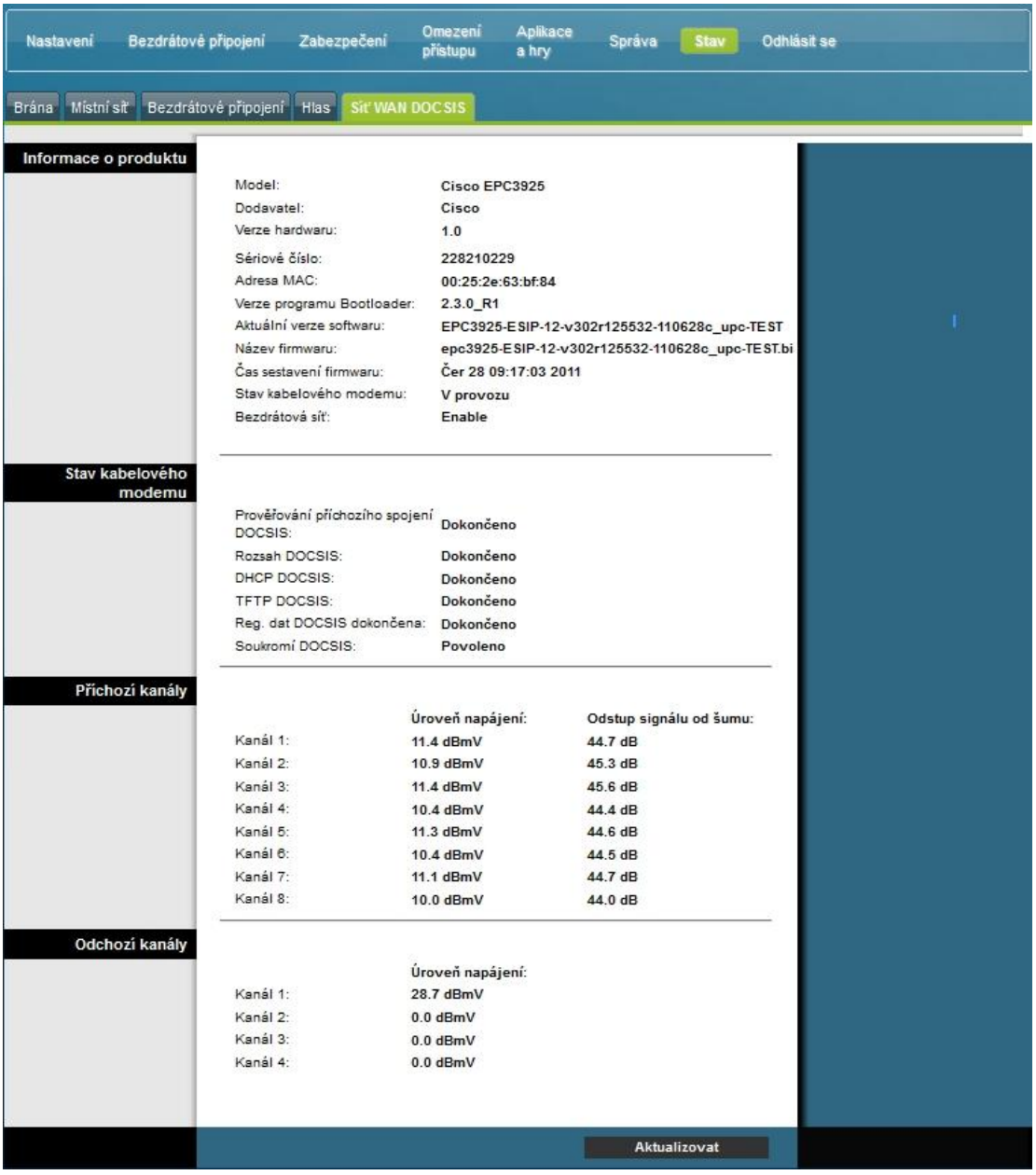
Následující tabulka vám usnadní kontrolu stavu bezdrátové sítě.

Část	Popis pole
Bezdrátová síť	**Adresa MAC** Adresa MAC místního bezdrátového přístupového bodu brány **Vysílací pásmo** Zde se zobrazuje aktuálně používaná vysílací frekvence – jedna z následujících možností: ■ 2,4 GHz, ■ 5 GHz, ■ 2,4 a 5 GHz. **Poznámka:** Některé produkty vysílací pásmo 5 GHz nepodporují. **Název sítě (SSID)** Identifikátor SSID bezdrátového přístupového bodu **Šířka kanálu** Zde se zobrazuje šířka pásma kanálu vybraná na stránce Bezdrátové připojení > Základní nastavení. **Široký kanál** Zde se zobrazuje nastavení Široký kanál vybrané na stránce Bezdrátové připojení > Základní nastavení. **Standardní kanál** Zde se zobrazuje nastavení Standardní kanál vybrané na stránce Bezdrátové připojení > Základní nastavení. **Zabezpečení** Zde se zobrazuje způsob zabezpečení používaný v bezdrátové síti. **Vysílání SSID** Zde se zobrazuje stav funkce Vysílání SSID brány.

Stav > Síť WAN DOCSIS

Na stránce Stav > Síť WAN DOCSIS se zobrazují informace o systému kabelového modemu.

Zvolením karty **Síť WAN DOCSIS** otevřete stránku Stav > Síť WAN DOCSIS.



Popis stránky Stav > Síť WAN DOCSIS

Popisy uvedené v následující tabulce vám usnadní kontrolu stavu sítě WAN DOCSIS.

Část	Popis pole
Informace o produktu	**Model** Název domácí brány
	Dodavatel Výrobce domácí brány
	Verze hardwaru Verze obvodové desky
	Sériové číslo Jedinečné sériové číslo domácí brány
	Adresa MAC (adresa CM MAC) Adresa MAC CM. Adresa MAC CM je jedinečná alfanumerická adresa koaxiálního rozhraní kabelového modemu, které slouží k připojení systému CMTS. Adresa MAC je hardwarová adresa jednoznačně určující každý uzel v síti.
	Verze programu Bootloader Verze kódu spouštěcího programu
	Aktuální verze softwaru Verze firmwaru
	Název firmwaru Název firmwaru
	Čas sestavení firmwaru Datum a čas sestavení firmwaru
	Stav kabelového modemu Zde se zobrazuje jeden z možných stavů brány.
Příchozí kanály	**Kanály 1–8** Zde se zobrazuje úroveň napájení a odstup signálu od šumu aktivních příchozích kanálů.
Odchozí kanály	**Kanály 1–4** Zde se zobrazuje úroveň napájení aktivních příchozích kanálů.

Nejčastější dotazy

Otázka: Jak se nastaví protokol TCP/IP?

Odpověď: Aby bylo možné nastavit protokol TCP/IP, musí být v systému nainstalována síťová karta s komunikačním protokolem TCP/IP. TCP/IP je komunikační protokol používaný pro přístup k Internetu. V následující části jsou uvedeny pokyny k nastavení protokolu TCP/IP v internetových zařízeních pro použití domácí brány v prostředí systému Microsoft Windows a Macintosh.

Protokol TCP/IP pro prostředí systému Microsoft Windows se liší podle používaného operačního systému. Postupujte podle pokynů pro váš operační systém.

Konfigurace protokolu TCP/IP v systému Windows 2000

1. Klikněte na tlačítko **Start**, vyberte možnost **Nastavení** a poté zvolte možnost **Síťová a telefonická připojení**.
2. V okně Síťová a telefonická připojení dvakrát klikněte na ikonu **Připojení k místní síti**.
3. V okně Připojení k místní síti – stav klikněte na možnost **Vlastnosti**.
4. V okně Připojení k místní síti – vlastnosti klikněte na možnost **Protokol sítě Internet (TCP/IP)** a poté klikněte na možnost **Vlastnosti**.
5. V okně Vlastnosti protokolu sítě Internet (TCP/IP) vyberte možnosti **Automaticky získat adresu IP** a **Získat adresu serveru DNS automaticky** a klikněte na tlačítko **OK**.
6. Až se otevře okno Místní síť, kliknutím na tlačítko **Ano** zvolte, že se počítač má restartovat. Počítač se restartuje. V počítači je nyní nakonfigurován protokol TCP/IP a ethernetová zařízení jsou připravena k použití.
7. Zkuste se připojit k Internetu. Pokud se připojení k Internetu nedaří navázat, požádejte o pomoc svého poskytovatele služeb.

Konfigurace protokolu TCP/IP v systému Windows XP

1. Klikněte na tlačítko **Start** a podle nastavení nabídky Start vyberte jednu z těchto možností:
   - Pokud používáte výchozí nabídku Start systému Windows XP, vyberte možnost **Připojit k**, dále zvolte možnost **Zobrazit všechna připojení** a přejděte ke kroku 2.
   - Pokud používáte klasickou nabídku Start systému Windows XP, vyberte možnost **Nastavení**, zvolte možnost **Síťová připojení**, klikněte na možnost **Připojení k místní síti** a přejděte ke kroku 3.
2. V části LAN nebo vysokorychlostní Internet v okně Síťová připojení dvakrát klikněte na ikonu **Připojení k místní síti**.

3 V okně Připojení k místní síti – stav klikněte na možnost **Vlastnosti**.

4 V okně Připojení k místní síti – vlastnosti klikněte na možnost **Protokol sítě Internet (TCP/IP)** a potom na možnost **Vlastnosti**.

5 V okně Vlastnosti protokolu sítě Internet (TCP/IP) vyberte možnosti **Automaticky získat adresu IP** a **Získat adresu serveru DNS automaticky** a klikněte na tlačítko **OK**.

6 Až se otevře okno Místní síť, kliknutím na tlačítko **Ano** zvolte, že se počítač má restartovat. Počítač se restartuje. V počítači je nyní nakonfigurován protokol TCP/IP a ethernetová zařízení jsou připravena k použití.

7 Zkuste se připojit k Internetu. Pokud se připojení k Internetu nedaří navázat, požádejte o pomoc svého poskytovatele služeb.

Konfigurace protokolu TCP/IP v systémech Macintosh

1 Klikněte na ikonu **Apple** v horním levém rohu aplikace Finder. Přejděte na možnost **Ovládací panely** a klikněte na možnost **TCP/IP**.

2 Klikněte na možnost **Upravit** v nástroji Finder v horní části stránky. Přejděte k dolní části nabídky a klikněte na možnost **Uživatelský režim**.

3 V okně Uživatelský režim klikněte na možnost **Pokročilé** a potom klikněte na tlačítko **OK**.

4 Klikněte na šipky selektoru nahoru/dolů vpravo od části Připojit přes v okně TCP/IP a potom klikněte na možnost **Pomocí serveru DHCP**.

5 Klikněte na možnost **Volby** v okně TCP/IP a potom na možnost **Aktivní** v okně Volby TCP/IP.

Poznámka: Políčko **Načíst, jen pokud to je třeba** musí zůstat *nezaškrtnuté*.

6 Ověřte, že možnost **Použít 802.3** v pravém horním rohu okna TCP/IP není zaškrtnuta. Pokud zaškrtnuta je, zrušte zaškrtnutí a levém dolním rohu klikněte na možnost **Informace**.

7 Je v tomto okně uvedena hardwarová adresa?

- Pokud **ano**, klikněte na tlačítko **OK**. Klikněte na možnost **Soubor**, přejděte níže, klikněte na tlačítko **Zavřít** a zavřete ovládací panel TCP/IP. Postup je dokončen.
- Pokud **ne**, vypněte počítač.

8 Až bude počítač vypnutý, stiskněte současně klávesy **Command (Apple)**, **Option**, **P** a **R**. Držte tyto klávesy stisknuté a znovu počítač zapněte. Klávesy uvolněte, teprve až alespoň třikrát zazní zvuk Apple. Poté se počítač spustí.

9 Jakmile bude počítač zcela spuštěn, proveďte znovu kroky 1 až 7 a ověřte, zda jsou všechna nastavení protokolu TCP/IP správná. Pokud počítač stále nemá hardwarovou adresu, kontaktujte autorizovaného prodejce nebo technickou podporu produktů Apple.

Otázka: Jak se obnoví adresa IP v počítači?

Odpověď: Pokud se prostřednictvím počítače nelze připojit k Internetu, přestože je domácí brána online, je možné, že počítač neobnovil adresu IP. Postupujte podle pokynů pro váš operační systém v této části a obnovte adresu IP v počítači.

Obnovení adresy IP v systémech Windows 95, 98, 98SE a ME

1. Klikněte na tlačítko **Start** a potom kliknutím na možnost **Spustit** otevřete okno Spustit.
2. Do pole Otevřít zadejte řetězec **winipcfg** a kliknutím na tlačítko **OK** spusťte příkaz winipcfg. Otevře se okno Konfigurace protokolu IP.
3. Klikněte na šipku dolů vpravo vedle horního pole a vyberte síťový adaptér, který je nainstalovaný v počítači. V okně Konfigurace protokolu IP se zobrazí informace o síťovém adaptéru.
4. Klikněte na možnost **Uvolnění** a potom na možnost **Obnovit**. V okně Konfigurace protokolu IP se zobrazí nová adresa IP.
5. Kliknutím na tlačítko **OK** zavřete okno Konfigurace protokolu IP. Postup byl dokončen.

   Poznámka: Pokud se připojení k Internetu stále nedaří navázat, požádejte o pomoc svého poskytovatele služeb.

Obnova adresy IP v systémech Windows NT, 2000 nebo XP

1. Klikněte na tlačítko **Start** a potom na možnost **Spustit**. Otevře se okno Spustit.
2. Do pole Otevřít zadejte řetězec **cmd** a klikněte na tlačítko **OK**. Otevře se okno s příkazovým řádkem.
3. Zadejte na řádek C:/ řetězec **ipconfig/release** a stiskněte klávesu **Enter**. Systém uvolní adresu IP.
4. Zadejte na řádek C:/ řetězec **ipconfig/renew** a stiskněte klávesu **Enter**. Systém zobrazí novou adresu IP.
5. Kliknutím na tlačítko **X** v pravém horním rohu zavřete okno s příkazovým řádkem. Postup je dokončen.

   Poznámka: Pokud se připojení k Internetu stále nedaří navázat, požádejte o pomoc svého poskytovatele služeb.

Otázka: Co když si nepořídím odběr kabelové televize?

Odpověď: Pokud je ve vaší oblasti kabelová televize, je možné, že datové služby lze získat i bez odběru služeb kabelové televize. Podrobné informace o kabelových službách získáte od místního poskytovatele služeb.

Otázka: Jak mohu zajistit instalaci?

Odpověď: Informace o odborné instalaci vám sdělí váš poskytovatel služeb. Profesionální instalace je zárukou řádného připojení kabelu k modemu a počítači a správné konfigurace všech nastavení hardwaru a softwaru. Více informací o instalaci získáte od svého poskytovatele služeb.

Otázka: Jak se domácí brána připojuje k počítači?

Odpověď: Domácí brána se k počítači připojuje pomocí bezdrátového připojení nebo ethernetového portu 10/100/1000BASE-T na počítači. Síťovou kartu potřebnou pro připojení prostřednictvím ethernetového rozhraní získáte u místního prodejce počítačů nebo poskytovatele služeb. Nejvyššího výkonu ethernetového připojení dosáhnete při instalaci gigabitové ethernetové karty.

Otázka: Jak se po připojení domácí brány připojím k Internetu?

Odpověď: Místní poskytovatel služeb se stane vaším poskytovatelem služeb Internetu. Nabídne vám širokou škálu služeb, například e-mailovou službu, chat, odběr zpráv a informací apod. Kromě toho zajistí potřebný software.

Otázka: Mohu současně sledovat televizi a procházet Internet?

Odpověď: Samozřejmě. Pokud si pořídíte odběr kabelové televize, můžete současně sledovat televizi a používat domácí bránu. Stačí televizor a domácí bránu připojit ke kabelové síti pomocí volitelného rozdělovače kabelového signálu.

Řešení běžných problémů

Nerozumím významu indikátorů stavu na předním panelu

Přejděte k části ***Funkce indikátorů stavu na předním panelu*** (str. 103), kde najdete podrobnější informace o funkcích těchto indikátorů.

Domácí brána neregistruje ethernetové připojení

- Ověřte, že je v počítači ethernetová karta a že je řádně nainstalován síťový ovladač. Při instalaci zakoupené ethernetové karty se pečlivě řiďte příslušnými pokyny.
- Zkontrolujte stav indikátorů stavu na předním panelu.

Domácí brána po připojení k rozbočovači neregistruje ethernetové připojení

Pokud k domácí bráně připojujete více počítačů, nejprve modem pomocí správného propojovacího kabelu připojte k odchozímu portu. Rozsvítí se indikátor LINK (Připojení) na rozbočovači.

Domácí brána neregistruje kabelové připojení

- Modem funguje se standardním 75ohmovým koaxiálním kabelem RF. Pokud použijete jiný kabel, domácí brána nebude fungovat správně. Kontaktujte poskytovatele kabelových služeb a ověřte, zda používáte správný kabel.
- Dále je možné, že nefunguje správně síťová karta nebo rozhraní USB. Pokyny k řešení těchto problémů najdete v dokumentaci ke kartě či rozhraní USB.

Tipy pro vylepšení výkonu

Co je třeba zkontrolovat a opravit

Pokud domácí brána nefunguje podle očekávání, vyzkoušejte následující tipy. Potřebujete-li pomoc, kontaktujte svého poskytovatele služeb.

- Zkontrolujte, zda je zástrčka napájení domácí brány správně zapojena do elektrické zásuvky.
- Zkontrolujte, zda napájecí kabel domácí brány není připojen k elektrické zásuvce ovládané přepínačem. Pokud ano, ověřte, že je přepínač v poloze **ZAPNUTO**.
- Zkontrolujte, zda svítí indikátor stavu **ONLINE** na předním panelu domácí brány.
- Zkontrolujte, zda je kabelová služba aktivní a podporuje obousměrný provoz.
- Zkontrolujte, zda jsou správně připojeny všechny kabely a že používáte správné kabely.
- Pokud používáte ethernetové připojení, zkontrolujte, zda je správně nainstalován a nastaven protokol TCP/IP.
- Ověřte, zda jste poskytovateli služeb sdělili sériové číslo a adresu MAC domácí brány.
- Pokud používáte rozdělovač kabelového signálu, abyste mohli domácí bránu připojit k jiným zařízením, odeberte rozdělovač a připojte domácí bránu přímo ke kabelovému vstupu. Pokud nyní domácí brána funguje správně, rozdělovač kabelového signálu je zřejmě vadný a je třeba jej vyměnit.
- Nejvyššího výkonu ethernetového připojení dosáhnete při instalaci gigabitové ethernetové karty.

Funkce indikátorů stavu na předním panelu

První zapnutí, kalibrace a registrace (při použití napájení střídavým proudem)

V následující tabulce jsou uvedeny sekvence kroků a odpovídající chování indikátorů stavu na předním panelu domácí brány během jejího zapnutí, kalibrace a registrace v síti při použití napájení střídavým proudem. Tato tabulka vám pomůže při řešení problémů se zapnutím, kalibrací a registrací domácí brány.

Poznámka: Jakmile domácí brána dokončí krok 11 (Registrace telefonní služby dokončena), modem začne normálně fungovat. Další informace naleznete v části ***Normální provoz (při použití napájení střídavým proudem)*** (str. 105).

Indikátory stavu na předním panelu během prvního zapnutí, kalibrace a registrace brány							
		Část 1 – registrace vysokorychlostního datového připojení					
Krok:		**1**	**2**	**3**	**4**	**5**	**6**
Indikátor na předním panelu		**Samo-činný test**	**Zjišťování příchozích dat**	**Zámek příchozího signálu**	**Prohledá-vání rozsahu**	**Žádost o adresu IP**	**Žádost o soubor pro zajištění služby vysokorychlostníh o datového připojení**
1	POWER (Napájení)	Svítí	Svítí	Svítí	Svítí	Svítí	Svítí
2	DS (Příchozí připojení)	Svítí	Bliká	Svítí	Svítí	Svítí	Svítí
3	US (Odchozí připojení)	Svítí	Nesvítí	Nesvítí	Bliká	Svítí	Svítí
4	ONLINE	Svítí	Nesvítí	Nesvítí	Nesvítí	Nesvítí	Bliká
5	ETHERNET 1–4	Svítí	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
6	USB	Svítí	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
7	WIRELESS LINK (Bezdrátové připojení)	Nesvítí	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
8	WIRELESS SETUP (Nastavení bezdrátového připojení)	Nesvítí	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
9	TEL 1	Svítí	Nesvítí	Nesvítí	Nesvítí	Nesvítí	Nesvítí
10	TEL 2	Svítí	Nesvítí	Nesvítí	Nesvítí	Nesvítí	Nesvítí

Indikátory stavu na předním panelu během prvního zapnutí, kalibrace a registrace brány						
Část 2 – registrace telefonní služby						
Krok		**7**	**8**	**9**	**10**	**11**
Indikátor na předním panelu		**Registrace síťových dat dokončena**	**Žádost o adresu IP telefonní služby**	**Žádost o soubor pro zajištění telefonní služby**	**Restartování hlasové služby**	**Registrace telefonní služby dokončena**
1	POWER (Napájení)	Svítí	Svítí	Svítí	Svítí	Svítí
2	DS (Příchozí připojení)	Svítí	Svítí	Svítí	Svítí	Svítí
3	US (Odchozí připojení)	Svítí	Svítí	Svítí	Svítí	Svítí
4	ONLINE	Svítí	Svítí	Svítí	Svítí	Svítí
5	ETHERNET 1–4	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
6	USB	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
7	WIRELESS LINK (Bezdrátové připojení)	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká	Svítí nebo bliká
8	WIRELESS SETUP (Nastavení bezdrátového připojení)	Nesvítí	Nesvítí	Nesvítí	Svítí nebo bliká	Svítí nebo bliká
9	TEL 1	Nesvítí	Bliká	Nesvítí	Bliká	Svítí
10	TEL 2	Nesvítí	Nesvítí	Bliká	Bliká	Svítí

Normální provoz (při použití napájení střídavým proudem)

V následující tabulce je popsáno chování indikátorů stavu na předním panelu domácí brány během normálního provozu.

Indikátory stavu na předním panelu za normálního provozního stavu		
Indikátor na předním panelu		**Normální provozní stav**
1	POWER (Napájení)	Svítí
2	DS (Příchozí připojení)	Svítí
3	US (Odchozí připojení)	Svítí
4	ONLINE	Svítí
5	ETHERNET 1–4	■ Svítí: K ethernetovému portu je připojeno jedno zařízení a do modemu ani z modemu nejsou odesílána žádná data. ■ Bliká: Je připojeno pouze jedno ethernetové zařízení a mezi zařízením uživatele a bezdrátovou domácí bránou probíhá přenos dat. ■ Nesvítí: K ethernetovým portům nejsou připojena žádná zařízení.
6	USB	■ Svítí: K portu USB je připojeno jedno zařízení a do modemu ani z modemu nejsou odesílána žádná data. ■ Bliká: Je připojeno pouze jedno zařízení USB a mezi zařízením uživatele a bezdrátovou domácí bránou probíhá přenos dat. ■ Nesvítí: K portům USB nejsou připojena žádná zařízení.
7	WIRELESS LINK (Bezdrátové připojení)	■ Svítí: Je povolen bezdrátový přístupový bod a tento bod je aktivní. ■ Bliká: Mezi zařízením uživatele a bezdrátovou domácí bránou probíhá přenos dat. ■ Nesvítí: Uživatel zakázal bezdrátový přístupový bod.
8	WIRELESS SETUP (Nastavení bezdrátového připojení)	■ Nesvítí: Nastavení bezdrátového připojení není aktivní. ■ Bliká: Nastavení bezdrátového připojení je aktivní a do bezdrátové sítě je možné přidat nové bezdrátové klienty.
9	TEL 1	■ Svítí: Je povolena telefonní služba. ■ Bliká: Používá se linka 1.
10	TEL 2	■ Svítí: Je povolena telefonní služba. ■ Bliká: Používá se linka 2.

Zvláštní stavy

V následující tabulce je popsáno chování indikátorů stavu na předním panelu kabelového modemu za zvláštních situací, kdy je zamítnut přístup k síti.

Indikátory stavu na předním panelu za zvláštních provozních stavů		
Indikátor na předním panelu		**Zamítnutí přístupu k síti**
1	POWER (Napájení)	Pomalé blikání 1x za sekundu
2	DS (Příchozí připojení)	Pomalé blikání 1x za sekundu
3	US (Odchozí připojení)	Pomalé blikání 1x za sekundu
4	ONLINE	Pomalé blikání 1x za sekundu
5	ETHERNET 1–4	Pomalé blikání 1x za sekundu
6	USB	Pomalé blikání 1x za sekundu
7	WIRELESS LINK (Bezdrátové připojení)	Pomalé blikání 1x za sekundu
8	WIRELESS SETUP (Nastavení bezdrátového připojení)	Pomalé blikání 1x za sekundu
9	TEL 1	Nesvítí
10	TEL 2	Nesvítí

Oznámení

Ochranné známky

Cisco a logo Cisco jsou ochranné známky nebo registrované ochranné známky společnosti Cisco nebo jejích dceřiných společností v USA a dalších zemích. Seznam ochranných známek společnosti Cisco najdete na adrese **www.cisco.com/go/trademarks**.
DOCSIS je registrovaná ochranná známka společnosti Cable Television Laboratories, Inc. EuroDOCSIS, EuroPacketCable a PacketCable jsou ochranné známky společnosti Cable Television Laboratories, Inc.

Jiné ochranné známky třetích stran zmíněné v tomto dokumentu jsou majetkem příslušných vlastníků. Použití výrazu „partner“ nevyjadřuje partnerský vztah mezi společností Cisco a jakoukoli jinou společností. (1009R)

Právní prohlášení

Společnost Cisco Systems, Inc., neodpovídá za chyby ani opomenutí v této příručce. Vyhrazujeme si právo tuto příručku kdykoli a bez předchozího upozornění změnit.

Oznámení týkající se autorských práv na dokumentaci

Informace uvedené v tomto dokumentu mohou být bez upozornění změněny. Žádnou část tohoto dokumentu není dovoleno bez výslovného písemného souhlasu společnosti Cisco Systems, Inc., jakýmkoli způsobem reprodukovat.

Použití softwaru a firmwaru

Software popsaný v tomto dokumentu je chráněn autorským zákonem a uživatelům je poskytován na základě licenčního ujednání. Tento software je povoleno používat a kopírovat pouze v souladu s licenčním ujednáním.

Firmware v tomto zařízení je chráněn autorským zákonem. Je povoleno jej používat pouze v zařízení, ve kterém je dodán. Jakákoli reprodukce nebo distribuce tohoto firmwaru nebo jakékoli jeho části bez výslovného písemného souhlasu je zakázána.

Další informace

Dotazy

Máte-li jakékoli technické dotazy, obraťte se na oddělení služeb společnosti Cisco. Se servisních technikem budete spojeni po zvolení příslušných možností z nabídky.

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

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

Srpen 2011 Výrobní číslo 4041324 Rev. A