



Ghid de utilizare a gateway-ului rezidențial wireless cu adaptor vocal digital încorporat Cisco Model DPC3925 și EPC3925 8x4 DOCSIS 3.0









În acest document

■ INSTRUCȚIUNI IMPORTANTE PENTRU SIGURANȚĂ	2
■ Introducere	13
■ Ce se află în cutie?.....	15
■ Descrierea panoului frontal.....	16
■ Descrierea panoului din spate	18
■ Care sunt cerințele de sistem pentru serviciile Internet?	20
■ Cum mă abonez la serviciile de Internet de mare viteză și de telefonie?	21
■ Care este cea mai bună locație pentru gateway-ul meu rezidențial DOCSIS?	23
■ Cum montez modemul pe perete? (Opțional).....	24
■ Care sunt cerințele pentru serviciile de telefonie?	28
■ Cum conectez gateway-ul pentru serviciile de Internet și telefonie?.....	29
■ Cum configurez gateway-ul rezidențial DOCSIS?.....	33
■ Configurarea setărilor wireless.....	44
■ Configurare securitate.....	61
■ Controlarea accesului la gateway	71
■ Configurarea aplicațiilor și a jocurilor	82
■ Gestionarea gateway-ului.....	89
■ Monitorizarea stării gateway-ului.....	99
■ Întrebări frecvente	107
■ Sfaturi pentru performanță îmbunătățită.....	112
■ Funcții ale indicatorilor de stare cu LED de pe panoul frontal	113
■ Note	117
■ Pentru informații.....	118

INSTRUCȚIUNI IMPORTANTE PENTRU SIGURANȚĂ









Notă pentru instalatori

Instrucțiunile privind operațiile de service din această notă sunt destinate utilizării exclusive de către personal de service calificat. Pentru a reduce riscul electrocutării, nu efectuați nicio altă operație de service în afara celor conținute în instrucțiunile de utilizare dacă nu dețineți calificările necesare.

<p>Notă pentru instalatorul sistemului</p> <p>Pentru acest aparat, blindajul cablului coaxial trebuie împământat cât se poate de aproape de punctul de intrare a cablului în clădire. Pentru produsele comercializate în S.U.A. și Canada, această notă este furnizată pentru a atrage atenția instalatorului asupra Articolului 820-93 și a Articolului 820-100 din NEC (sau Codul Electric Canadian, Partea 1), care oferă îndrumări pentru împământarea corespunzătoare a blindajului cablului coaxial.</p>  <p>Acest simbol are scopul de a vă alerta asupra faptului că tensiunea neizolată din acest produs poate avea o magnitudine suficientă pentru a cauza electrocutarea. Prin urmare, este periculos să se realizeze orice fel de contact cu vreo piesă din interiorul acestui produs.</p>	<table border="1"><tr><td data-bbox="748 470 841 625"></td><td data-bbox="841 470 1019 625"><p>ATENȚIE</p><p>RISQUE DE ELECTROCUTARE A NU SE DESCHIDE</p></td><td data-bbox="1019 470 1110 625"></td></tr><tr><td colspan="3" data-bbox="841 625 1019 716"><p>AVIS</p><p>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</p></td></tr></table> <p>ATENȚIE: Pentru a reduce riscul de electrocutare, nu îndepărtați capacul (sau partea din spate). Nu conține piese ce pot fi reparate de către utilizator. Intervențiile de service trebuie efectuate doar de către personal de service calificat.</p> <p>AVERTISMENT PENTRU PREVENIREA INCENDIILOR SAU A ELECTROCUTĂRII, NU EXPUNEȚI ACEASTĂ UNITATE LA PLOAIE SAU UMEZEALĂ.</p>  <p>Acest simbol are drept scop să vă alerteze cu privire la existența unor instrucțiuni importante de funcționare și întreținere (service) în documentația care însoțește acest produs.</p>		<p>ATENȚIE</p> <p>RISQUE DE ELECTROCUTARE A NU SE DESCHIDE</p>		<p>AVIS</p> <p>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</p>		
	<p>ATENȚIE</p> <p>RISQUE DE ELECTROCUTARE A NU SE DESCHIDE</p>						
<p>AVIS</p> <p>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</p>							

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.

<p>Note to System Installer</p> <p>For this apparatus, the coaxial cable shield/ screen shall be grounded as close as practical to the point of entry of the cable into the building. For products sold in the US and Canada, this reminder is provided to call the system installer's attention to Article 820-93 and Article 820-100 of the NEC (or Canadian Electrical Code Part 1), which provides guidelines for proper grounding of the coaxial cable shield.</p>  <p>This symbol is intended to alert you that uninsulated voltage within this product may have sufficient magnitude to cause electric shock. Therefore, it is dangerous to make any kind of contact with any inside part of this product.</p>	<table border="1"><tr><td data-bbox="748 1201 841 1356"></td><td data-bbox="841 1201 1019 1356"><p>CAUTION</p><p>RISK OF ELECTRIC SHOCK DO NOT OPEN</p></td><td data-bbox="1019 1201 1110 1356"></td></tr><tr><td colspan="3" data-bbox="841 1356 1019 1446"><p>AVIS</p><p>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</p></td></tr></table> <p>CAUTION: To reduce the risk of electric shock, do not remove cover (or back). No user-serviceable parts inside. Refer servicing to qualified service personnel.</p> <p>WARNING TO PREVENT FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS UNIT TO RAIN OR MOISTURE.</p>  <p>This symbol is intended to alert you of the presence of important operating and maintenance (servicing) instructions in the literature accompanying this product.</p>		<p>CAUTION</p> <p>RISK OF ELECTRIC SHOCK DO NOT OPEN</p>		<p>AVIS</p> <p>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</p>		
	<p>CAUTION</p> <p>RISK OF ELECTRIC SHOCK DO NOT OPEN</p>						
<p>AVIS</p> <p>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</p>							



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.

<p>Remarque à l'attention de l'installateur du système</p> <p>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.</p>  <p>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.</p>	<table border="1"> <tr> <td data-bbox="764 428 833 489"></td> <td data-bbox="846 394 1003 533"> <p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> <p>ATTENTION DANGER ÉLECTRIQUE NE PAS OUVRIR</p> </td> <td data-bbox="1016 428 1084 489"></td> </tr> </table> <p>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.</p> <p>AVERTISSEMENT POUR ÉVITER LES INCENDIES OU LES CHOCs ÉLECTRIQUES, NE PAS EXPOSER L'APPAREIL À LA PLUIE OU À L'HUMIDITÉ.</p>  <p>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.</p>		<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> <p>ATTENTION DANGER ÉLECTRIQUE NE PAS OUVRIR</p>	
	<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> <p>ATTENTION DANGER ÉLECTRIQUE NE PAS OUVRIR</p>			

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.

<p>Mitteilung an den Systemtechniker</p> <p>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 Koaxialkabelschirms festgehalten sind.</p>  <p>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.</p>	<table border="1"> <tr> <td data-bbox="764 1140 833 1201"></td> <td data-bbox="846 1106 1003 1245"> <p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> <p>ACHTUNG STROMSCHLAGEGFAHR, NICHT ÖFFNEN</p> </td> <td data-bbox="1016 1140 1084 1201"></td> </tr> </table> <p>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.</p> <p>WARNUNG DAS GERÄT NICHT REGEN ODER FEUCHTIGKEIT AUSSETZEN, UM STROMSCHLAG ODER DURCH EINEN KURZSCHLUSS VERURSACHTEN BRAND ZU VERMEIDEN.</p>  <p>Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.</p>		<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> <p>ACHTUNG STROMSCHLAGEGFAHR, NICHT ÖFFNEN</p>	
	<p>CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN</p> <p>ACHTUNG STROMSCHLAGEGFAHR, NICHT ÖFFNEN</p>			

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

INSTRUCȚIUNI IMPORTANTE PENTRU SIGURANȚĂ

- 1) Citiți aceste instrucțiuni.
- 2) Păstrați aceste instrucțiuni.
- 3) Acordați atenție tuturor avertismentelor.
- 4) Urmați toate instrucțiunile.
- 5) Nu utilizați acest aparat în apropierea apei.
- 6) Curățați-l doar cu o cârpă uscată.
- 7) Nu blocați niciun orificiu de ventilare. Instalați aparatul în conformitate cu instrucțiunile producătorului.
- 8) Nu instalați aparatul în apropierea surselor de căldură, precum radiatoare, grilaje de încălzire, sobe sau alte aparate (inclusiv amplificatoare) ce produc căldură.
- 9) Nu alterați destinația de siguranță a fișei polarizate sau a celei de împământare. O fișă polarizată are două lamele, una mai lată decât cealaltă. O fișă de împământare are două lamele și un știft de împământare. Lamela lată sau știftul de împământare are drept scop siguranța dumneavoastră. Dacă fișa furnizată nu se potrivește în priză, consultați un electrician pentru a înlocui priza veche.
- 10) Protejați cablul de alimentare pentru a nu se călca pe el și pentru a nu fi ciupit, în special în zona fișelor, a prizelor și în locul în care iese din aparat.
- 11) Utilizați doar atașamentele/accesoriile specificate de producător.
- 12) Utilizați aparatul doar cu căruciorul, suportul, trepiedul, consola sau masa specificate de producător sau vândute împreună cu aparatul. Când se utilizează un cărucior, manevrați cu grijă ansamblul cărucior/aparat, pentru a evita eventualele vătămări cauzate de răsturnare.
- 13) Deconectați aparatul de la priză în timpul furtunilor cu fulgere sau când nu îl utilizați perioade mai îndelungate.
- 14) Toate intervențiile de service trebuie efectuate doar de către personal de service calificat. Intervențiile de service sunt necesare atunci când aparatul a fost deteriorat în orice mod, dacă a fost deteriorat cablul de alimentare sau fișa electrică, dacă s-au vărsat lichide pe aparat sau dacă au căzut obiecte în acesta, dacă aparatul a fost expus la ploaie sau la umezeală, dacă nu funcționează normal sau dacă a căzut.



Avertisment cu privire la sursa de alimentare

O etichetă de pe acest produs indică sursa de alimentare corectă pentru acest produs. Utilizați acest produs doar cu alimentare de la o priză electrică cu tensiunea și frecvența indicate pe eticheta produsului. Dacă nu sunteți sigur de tipul alimentării electrice de acasă sau de la serviciu, consultați furnizorul de servicii sau compania electrică locală.

Intrarea CA de pe unitate trebuie să rămână accesibilă și operabilă în orice moment.

Efectuați împământarea produsului



AVERTISMENT: Evitați pericolele de electrocutare și incendiu! Dacă acest produs se conectează la un cablaj format din cabluri coaxiale, asigurați-vă că sistemul de cabluri este legat la masă (împământat). Împământarea asigură un anumit grad de protecție împotriva supratensiunii tranzitorii și a sarcinilor statice acumulate.

Protejați produsul împotriva fulgerelor

Pe lângă deconectarea alimentării CA de la priza de perete, deconectați intrările de semnal.

Verificați sursa de alimentare de la indicatorul luminos de alimentare pornit/oprit

Dacă indicatorul luminos de alimentare pornit/oprit nu este aprins, este posibil ca aparatul să fie în continuare conectat la sursa de alimentare. Lumina se poate stinge atunci când aparatul este oprit, indiferent dacă mai este conectat la sursa de alimentare CA sau nu.

Eliminați supraîncărcarea rețelei CA



AVERTISMENT: Evitați pericolele de electrocutare și incendiu! Nu supraîncărcați rețeaua CA, prizele, prelungitoarele sau prizele integrale. Pentru produsele care necesită alimentare de la baterii sau alte surse de alimentare pentru a funcționa, consultați instrucțiunile de utilizare pentru produsele respective.

Asigurați ventilarea și alegeți o locație

- Îndepărtați toate ambalajele înainte de a pune produsul sub tensiune.
- Nu puneți acest aparat pe pat, pe canapea, pe covor sau pe o suprafață similară.
- Nu puneți acest aparat pe o suprafață instabilă.
- Nu instalați acest aparat într-un spațiu închis, precum o bibliotecă sau un raft, dacă instalarea nu asigură ventilarea corespunzătoare.
- Nu puneți dispozitive de divertisment (precum dispozitive VCR sau DVD), veioze, cărți, vase cu lichide sau alte obiecte pe acest produs.
- Nu blocați orificiile de ventilare.

Protejați aparatul împotriva expunerii la umezeală și obiecte străine



AVERTISMENT: Evitați pericolele de electrocutare și incendiu! Evitați stropirea aparatului și posibilitatea ca pe acesta să se scurgă lichide și nu îl expuneți la ploaie sau umezeală. Pe acest aparat nu trebuie puse obiecte umplute cu lichide, precum vase.



AVERTISMENT: Evitați pericolele de electrocutare și incendiu! Deconectați acest produs înainte de curățare. Nu utilizați un agent de curățare lichid sau unul cu aerosoli. Nu utilizați un dispozitiv de curățare magnetic/static (aspirator) pentru a curăța acest produs.



AVERTISMENT: Evitați pericolele de electrocutare și incendiu! Nu introduceți niciodată obiecte prin orificiile acestui produs. Obiectele străine pot cauza scurtcircuite electrice, care pot duce la electrocutare sau incendiu.

Avertismente pentru service



AVERTISMENT: Evitați electrocutarea! Nu deschideți capacul acestui produs. Deschiderea sau îndepărtarea capacului vă poate expune la tensiuni periculoase. Dacă deschideți capacul, garanția va fi anulată. Acest produs nu conține piese ce pot fi reparate de către utilizator.

Verificați siguranța produsului

După finalizarea intervențiilor de service sau a reparațiilor asupra acestui produs, tehnicianul de service trebuie să efectueze verificări de siguranță pentru a stabili dacă produsul se află în stare de funcționare corespunzătoare.

Protejați produsul atunci când îl mutați

Deconectați întotdeauna sursa de alimentare atunci când mutați aparatul sau când conectați sau deconectați cablurile.

Notă cu privire la echipamentele telefonice

Când utilizați echipamentul telefonic, trebuie respectate întotdeauna precauțiile de siguranță de bază pentru a reduce riscul de incendiu, electrocutare și vătămare a persoanelor, inclusiv următoarele:

1. Nu utilizați acest produs în apropierea apei, de exemplu, în apropierea unei căzi, a unui lavoar, a unei chiuvete de bucătărie sau a unei căzi de spălat rufe, într-un subsol umed sau în apropierea unei piscine.
2. Evitați utilizarea telefonului (altul decât tipul wireless) în timpul unei furtuni cu descărcări electrice. Există, în mică măsură, un risc de electrocutare de la fulgere.
3. Nu utilizați telefonul pentru a raporta o scurgere de gaze în apropierea scurgerii respective.



ATENȚIE: Pentru a reduce riscul de incendiu, utilizați doar un cablu pentru linii de telecomunicații nr. 26 AWG sau mai mare.

PĂSTRAȚI ACESTE INSTRUCȚIUNI

Conformitatea cu FCC (Comisia Federală de Comunicații) a Statelor Unite

Acest dispozitiv a fost testat și s-a dovedit a fi conform cu limitele pentru un dispozitiv digital din Clasa B, în conformitate cu capitolul 15 al Regulilor FCC. Scopul acestor limite este de a asigura o protecție rezonabilă împotriva unor astfel de interferențe în cazul unei instalări rezidențiale. Acest echipament generează, utilizează și poate radia energie cu frecvență radio. Dacă nu este instalat și utilizat în conformitate cu instrucțiunile, poate cauza interferențe dăunătoare comunicațiilor radio. Totuși, nu există nicio garanție că nu vor avea loc interferențe în cazul unei instalări specifice. Dacă acest echipament cauzează, totuși, interferențe dăunătoare recepției radio sau TV, lucru care poate fi stabilit prin oprirea și pornirea echipamentului, utilizatorul este încurajat să încerce să remedieze interferența, luând una sau mai multe dintre următoarele măsuri:

- Reorientați sau re poziționați antena de recepție.
- Măriți distanța dintre echipament și receptor.
- Conectați echipamentul la o priză aflată într-un circuit diferit de cel la care este conectat receptorul.
- Consultați furnizorul de servicii sau un tehnician radio/TV experimentat pentru ajutor.

Orice schimbare sau modificare neaprobata în mod expres de către Cisco Systems, Inc. poate anula dreptul utilizatorului de a folosi echipamentul.

Informațiile prezentate în paragraful Declarație de conformitate cu FCC de mai jos reprezintă o cerință a FCC și au drept scop furnizarea de informații cu privire la aprobarea de către FCC a acestui dispozitiv. *Numerele de telefon listate sunt doar pentru întrebări legate de FCC și nu pentru întrebări privind conectarea sau funcționarea acestui dispozitiv. Contactați furnizorul de servicii dacă aveți întrebări legate de funcționarea sau instalarea acestui dispozitiv.*

FCC Declarație de conformitate

Acest dispozitiv este conform cu Capitolul 15 al Regulilor FCC. Funcționarea este restricționată de următoarele două condiții: 1) dispozitivul nu poate cauza interferențe dăunătoare și 2) dispozitivul trebuie să accepte orice interferență primită, inclusiv interferențele ce pot cauza funcționarea într-un mod nedorit.

<p>Gateway rezidențial DOCSIS Model: DPC3925/EPC3925 Produs de: Cisco Systems, Inc. 5030 Sugarloaf Parkway Lawrenceville, Georgia 30044 S.U.A. Telefon: +1 770 236-1077</p>

Reglementare privind interferențele electromagnetice pentru Canada

Acest aparat digital din Clasa B este conform cu reglementarea canadiană ICES-003.

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

Frecvențe de bandă dublă cu selectare dinamică a frecvenței (DFS)

Este posibil ca unele configurații ale acestui produs să funcționeze în benzile de 5.150 - 5.250 MHz și 5.470 - 5.725 MHz. Dacă selectați un canal în aceste intervale de frecvență, produsul este restricționat la funcționarea în interior doar în baza îndrumării FCC. Utilizarea acestui produs pe frecvențele afectate atunci când se află în exterior nu respectă reglementările și îndrumările FCC.

Declarații cu privire la expunerea la radiații

Notă: Acest transmițător nu trebuie amplasat și nici utilizat în legătură cu o altă antenă sau un alt transmițător. Acest echipament trebuie instalat și utilizat la o distanță de cel puțin 7,9 inci (20 cm) între radiator și corpul dumneavoastră.

S.U.A.

Acest sistem a fost evaluat din punct de vedere al expunerii la frecvențe radio pentru oameni în raport cu limitele stipulate de ANSI C 95.1 (Institutul Național American de Standarde). Evaluarea a avut la bază Buletinul OET FCC 65C rev 01.01, în conformitate cu Capitolul 2.1091 și Capitolul 15.27. Distanța minimă de separare dintre antenă și persoanele aflate în apropiere este de 7,9 inci (20 cm) pentru menținerea conformității.

Canada

Acest sistem a fost evaluat din punct de vedere al expunerii la frecvențe radio pentru oameni în raport cu limitele stipulate de ANSI C 95.1. Evaluarea s-a bazat pe evaluarea în conformitate cu RSS-102 Rev 2. Distanța minimă de separare dintre antenă și persoanele aflate în apropiere este de 7,9 inci (20 cm) pentru menținerea conformității.

UE

Acest sistem a fost evaluat din punct de vedere al expunerii la frecvențe radio pentru oameni în raport cu limitele stipulate de ICNIRP (Comisia Internațională de Protecție Împotriva Radiațiilor Neionizante). Evaluarea s-a bazat pe Standardul pentru produse EN 50385, pentru demonstrarea conformității stațiilor de radio de bază și a terminalelor fixe pentru sisteme de telecomunicații wireless cu restricțiile de bază sau nivelurile de referință privind expunerea oamenilor la câmpuri electromagnetice cu frecvență radio între 300 MHz și 40 GHz. Distanța minimă de separare dintre antenă și persoanele aflate în apropiere este de 20 cm (7,9 inci).

Australia

Acest sistem a fost evaluat din punct de vedere al expunerii la frecvențe radio, după cum se stipulează în standardul australian pentru protecție împotriva radiațiilor și a fost evaluat în raport cu limitele ICNIRP (Comisia Internațională de Protecție Împotriva Radiațiilor Neionizante). Distanța minimă de separare dintre antenă și persoanele aflate în apropiere este de 20 cm (7,9 inci).

20091016 FCC DomandIntl

Conformitatea cu reglementările CE

Declarație de conformitate cu privire la directiva UE 1999/5/CE (Directiva privind Echipamentele radio și echipamentele terminale de telecomunicații)

Această declarație este valabilă doar pentru configurații (combinații de software, firmware și hardware) acceptate sau furnizate de Cisco Systems pentru a fi utilizate în UE. Utilizarea de componente software sau firmware care nu sunt acceptate sau furnizate de Cisco Systems poate duce la pierderea conformității echipamentului cu cerințele de reglementare.

Bългарски [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/EU 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 así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτό ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές 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 è 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 essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet 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 în conformitate cu cerințele esențiale și 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.

Notă: Textul complet al declarației de conformitate pentru acest produs poate fi găsit în secțiunea Declarații de conformitate și informații de reglementare a ghidului de instalare hardware pentru produsul corespunzător, disponibil pe Cisco.com.

Următoarele standarde au fost aplicate la evaluarea produsului în raport cu cerințele directivei 1999/5/CE:

- Radio: EN 300 328
- Compatibilitate electromagnetică: EN 301 489-1 și EN 301 489-17
- Siguranță: EN 60950 și EN 50385

Marca CE și identificatorul de clasă 2 sunt aplicate pe produs și pe ambalajul acestuia. Acest produs este conform cu următoarele directive europene:



Restricții naționale

Acest produs este destinat exclusiv utilizării în interior.

Franța

Pentru 2,4 GHz, puterea de ieșire este restricționată la 10 mW EIRP, atunci când produsul este utilizat în exterior, în banda 2.454 - 2.483, 5 MHz. Nu există restricții atunci când este utilizat în alte segmente ale benzii de 2,4 GHz. Consultați <http://www.arcep.fr/> pentru mai multe detalii.

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.

Italia

Acest produs respectă cerințele Interfeței Naționale Radio și cerințele specificate în Tabelul de Alocare a Frecvențelor Naționale pentru Italia. În afara cazului în care acest produs LAN wireless funcționează în limitele proprietății proprietarului, utilizarea sa necesită o „autorizare generală”. Consultați <http://www.comunicazioni.it/it/> pentru mai multe detalii.

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.

Letonia

Utilizarea în exterior a benzii de 2,4 GHz necesită o autorizare din partea Biroului de Comunicații Electronice. Consultați <http://www.esd.lv> pentru mai multe detalii.

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

Notă: Limitele de reglementare pentru puterea de ieșire maximă sunt specificate în EIRP. Nivelul EIRP al unui dispozitiv poate fi calculat prin adăugarea amplificării antenei utilizate (specificată în dBi) la puterea de ieșire disponibilă pentru conector (specificată în dBm).

Antene

Utilizați doar antena furnizată împreună cu produsul.

20090312 CE_Gateway

Introducere

Bine ați venit în incitanta lume a serviciilor de Internet de mare viteză și de telefonie digitală de înaltă calitate. Noul dumneavoastră Gateway rezidențial wireless cu adaptor vocal digital încorporat Cisco® Model DPC3925 DOCSIS® 3.0 sau EPC3925 EuroDOCSIS™ este un modem cu cablu care respectă standardele din industrie pentru conectivitate de date de mare viteză, împreună cu un serviciu de telefonie digitală de încredere. Gateway-ul rezidențial DPC3925 și EPC3925 asigură capacități de date, voce și gateway cu fir (Ethernet) sau wireless pentru a conecta o diversitate de dispozitive acasă sau într-un birou mic și pentru a permite acces la date de înaltă viteză și servicii de voce rentabile, toate într-un singur dispozitiv. Cu un gateway rezidențial DPC3925 sau EPC3925, bucuria dumneavoastră de a naviga pe Internet, comunicațiile de acasă și de la serviciu, precum și productivitatea personală vor lua cu siguranță avânt.

Acest ghid furnizează proceduri și recomandări pentru amplasarea, instalarea, configurarea, funcționarea și depanarea gateway-ului rezidențial DPC3925 și EPC3925 pentru servicii de Internet de mare viteză și de telefonie digitală pentru acasă sau pentru birou. Consultați secțiunea corespunzătoare din acest ghid pentru informațiile specifice de care aveți nevoie pentru situația dumneavoastră. Contactați furnizorul de servicii pentru mai multe informații despre abonarea la aceste servicii.

Beneficii și caracteristici

Noul dumneavoastră gateway rezidențial DPC3925 și EPC3925 prezintă următoarele beneficii și caracteristici remarcabile:

- Conformitate cu standardele DOCSIS 3.0, 2.0 și 1.x și cu specificațiile PacketCable™ și EuroPacketCable™ pentru a vă asigura performanță și fiabilitate de vârf
- Conectivitate la Internet de bandă largă de înaltă performanță pentru a vă stimula experiența online
- Adaptor digital de voce cu două linii, încorporat, pentru servicii de telefonie cu fir
- Patru porturi Ethernet 1000/100/10BASE-T pentru a asigura conectivitatea cu fir
- Punct de acces wireless 802.11n
- Configurație protejată Wi-Fi (WPS), inclusiv un comutator cu buton pentru activarea WPS pentru o instalare wireless simplificată și securizată
- Controlul parental configurabil de către utilizator blochează accesul la site-uri Internet nedorite

Introducere

- Tehnologia firewall avansată descurajează hackerii și protejează rețeaua de la domiciliu împotriva accesului neautorizat
- Design compact și atrăgător care permite utilizarea aparatului la verticală, la orizontală sau montat pe perete
- Porturile de interfață codate cu culori și cablurile corespunzătoare simplifică instalarea și configurarea
- Etichetarea și comportamentul în conformitate cu DOCSIS-5 oferă o metodă facilă pentru utilizator și tehnician de a verifica starea de funcționare și acționează ca un instrument de depanare
- Permite upgrade-urile de software automate realizate de furnizorul dumneavoastră de servicii

Ce se află în cutie?

În momentul în care primiți gateway-ul rezidențial wireless, trebuie să verificați echipamentul și accesoriile pentru a vă asigura că fiecare articol se află în cutie și că niciun articol nu este deteriorat. Cutia conține următoarele articole:



Unul dintre modelele de Gateway rezidențial DOCSIS (DPC3925 sau EPC3925)



Un adaptor electric (modelele care necesită alimentare externă cu energie)



Un cablu Ethernet (CAT5/RJ-45)



Un CD-ROM

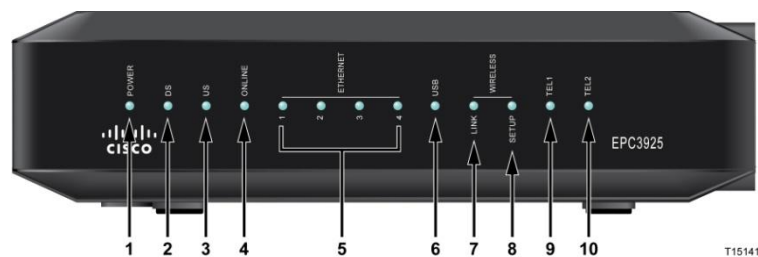
Dacă oricare dintre aceste articole lipsește sau este deteriorat, contactați furnizorul de servicii pentru asistență.

Note:

- Veți avea nevoie de un divizor de semnal prin cablu opțional și de cabluri coaxiale RF standard suplimentare dacă doriți să conectați un VCR, un terminal de comunicații digital pentru domiciliu (DHCT), un set-top box sau un televizor la aceeași conexiune prin cablu ca și gateway-ul rezidențial wireless.
- Cablurile și alte echipamente necesare pentru serviciul telefonic trebuie achiziționate separat. Contactați furnizorul de servicii pentru a afla informații despre echipamentele și cablurile necesare pentru serviciul telefonic.

Descrierea panoului frontal

Panoul frontal al gateway-ului rezidențial oferă indicatori de stare cu LED, care arată cât de bine și în ce stare funcționează gateway-ul dumneavoastră rezidențial. Consultați *Funcții ale indicatorilor de stare cu LED de pe panoul frontal* (la pagina 113) pentru mai multe informații despre funcțiile indicatorilor de stare cu LED de pe panoul frontal.



Aici este prezentat modelul EPC3925

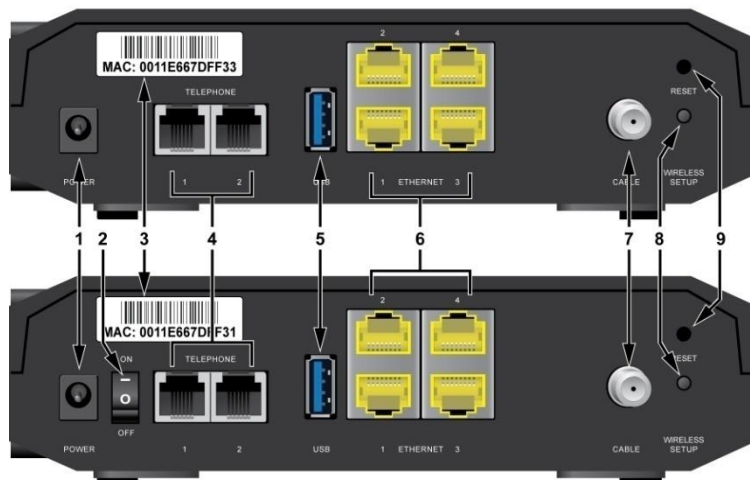
- 1 POWER** – APRINS, gateway-ul rezidențial wireless este alimentat cu curent electric
- 2 DS** – APRINS, gateway-ul rezidențial wireless primește date de la rețeaua prin cablu
- 3 US** – APRINS, gateway-ul rezidențial wireless trimite date către rețeaua prin cablu
- 4 ONLINE** – APRINS, gateway-ul rezidențial wireless este înregistrat în rețea și complet funcțional
- 5 ETHERNET 1 - 4** – APRINS, un dispozitiv este conectat la unul dintre porturile Ethernet. CLIPITUL indică faptul că se transferă date prin intermediul conexiunii Ethernet
- 6 USB** – APRINS, un dispozitiv este conectat la portul USB. CLIPITUL indică faptul că se transferă date prin intermediul conexiunii USB
- 7 WIRELESS LINK** – APRINS, Punctul de acces wireless este funcțional. CLIPITUL indică faptul că se transferă date prin intermediul conexiunii wireless. STINS indică faptul că punctul de acces wireless a fost dezactivat de către utilizator
- 8 WIRELESS SETUP** – STINS (stare normală) configurarea wireless nu este activă. CLIPITUL indică faptul că utilizatorul a activat configurarea wireless pentru a adăuga noi clienți wireless la rețeaua wireless

- 9 **TEL1** – APRINS indică faptul că serviciul de telefonie este activat. Clipește atunci când linia 1 este în uz. STINS indică faptul că serviciul telefonic pentru TEL 1 nu este activat
- 10 **TEL2** – APRINS indică faptul că serviciul de telefonie este activat. Clipește atunci când linia 2 este în uz. STINS indică faptul că serviciul telefonic pentru TEL 2 nu este activat

Descrierea panoului din spate

Următoarele ilustrații prezintă descrierea și funcția componentelor panoului din spate al gateway-ului rezidențial Cisco EPC3925.

Model DPC3925



Model EPC3925

T14517

- 1 **POWER** – Conectează gateway-ul rezidențial la adaptorul electric CA furnizat împreună cu gateway-ul rezidențial



ATENȚIE:

Evitați deteriorarea echipamentului. Utilizați doar sursa de alimentare furnizată împreună cu gateway-ul rezidențial.

- 2 **COMUTATOR ON/OFF (doar pentru modelele din Europa)** – Vă permite să opriți gateway-ul rezidențial fără a scoate cablul de alimentare
- 3 **ETICHETĂ ADRESĂ MAC** – Afișează adresa MAC a gateway-ului rezidențial
- 4 **TELEPHONE 1 și 2** – Porturile RJ-11 pentru linii telefonice ajută la conectarea la sistemul telefonic din casă, la telefoane sau aparate de fax convenționale
- 5 **USB** – Pentru conectarea la dispozitivele client selectate
- 6 **ETHERNET** – Patru porturi Ethernet RJ-45 pentru conectarea la portul Ethernet de pe PC sau la rețeaua de domiciliu
- 7 **CABLE** – Conector F pentru conectarea la un semnal prin cablu activ, primit de la furnizorul dumneavoastră de servicii
- 8 **WIRELESS SETUP** – Apăsând pe acest comutator se inițiază instalarea wireless, această caracteristică permițând utilizatorului să adauge noi clienți wireless ce respectă Configurația protejată Wi-Fi (WPS) la rețeaua de domiciliu

- RESET** – O apăsare scurtă (1 - 2 secunde) a acestui comutator repornește EMTA. Apăsarea comutatorului timp de mai mult de zece secunde cauzează, mai întâi, resetarea tuturor setărilor la valorile implicite din fabrică și apoi reinițializează gateway-ul.



ATENȚIE:

Butonul Reset are doar scop de întreținere. Nu îl utilizați decât dacă vi se indică acest lucru de către furnizorul de servicii de cablu sau telefonie. Utilizarea acestuia poate atrage după sine pierderea setărilor modemului cu cablu selectate.

Care sunt cerințele de sistem pentru serviciile Internet?

Pentru a vă asigura că gateway-ul rezidențial funcționează eficient pentru serviciul de Internet de mare viteză, verificați dacă toate dispozitivele Internet din cadrul sistemului dumneavoastră satisfac sau depășesc următoarele cerințe minime de hardware și software.

Notă: Veți avea nevoie, de asemenea, de o linie de intrare pentru cablu activă și o conexiune la Internet.

Cerințe minime de sistem pentru un PC

- Un PC cu procesor Pentium MMX 133 sau mai puternic
- 32 MO de RAM
- Software de navigare pe Web
- Unitate CD-ROM

Cerințe minime de sistem pentru Macintosh

- MAC OS 7.5 sau ulterior
- 32 MO de RAM

Cerințe de sistem pentru o conexiune Ethernet

- Un PC cu sistem de operare Microsoft Windows 2000 (sau ulterior) cu protocol TCP/IP instalat sau un computer Apple Macintosh cu protocol TCP/IP instalat
- O placă de rețea (NIC) Ethernet 10/100/1000BASE-T activă instalată

Cum mă abonez la serviciile de Internet de mare viteză și telefonie?

Înainte de a putea utiliza gateway-ul rezidențial, trebuie să dețineți un cont de acces la Internet de mare viteză. Dacă nu dețineți un cont de acces la Internet de mare viteză, trebuie să vă înregistrați un cont cu furnizorul dumneavoastră de servicii local. Alegeți una dintre opțiunile din această secțiune.

Nu dețin un cont de acces la Internet de mare viteză

Dacă *nu* dețineți un cont de acces la Internet de mare viteză, furnizorul dumneavoastră de servicii vă va deschide un cont și va deveni furnizorul dumneavoastră de servicii de Internet (ISP). Accesul la Internet vă permite să trimiteți și să primiți e-mailuri, să accesați rețeaua World Wide Web și să primiți alte servicii Internet.

Va trebui să oferiți furnizorului de servicii următoarele informații:

- Numărul de serie al modemului
- Adresa de Control al accesului la media (MAC) a modemului (CM MAC)
- Alte numere de adresă MAC, după caz

Aceste numere apar pe o etichetă cu cod de bare, amplasată pe gateway-ul rezidențial. Numărul de serie constă dintr-o serie de caractere alfanumerice, precedate de **S/N**. Adresa MAC constă dintr-o serie de caractere alfanumerice, precedate de **CM MAC**. Următoarea ilustrație prezintă un exemplu de etichetă cu cod de bare.



Notați aceste numere în spațiul prevăzut aici.

Număr de serie _____

Adresă MAC _____

Cum mă abonez la serviciile de Internet de mare viteză și telefonie?

Dețin deja un cont de acces la Internet de mare viteză

Dacă dețineți un cont de acces la Internet de mare viteză, trebuie să oferiți furnizorului de servicii numărul de serie și adresa MAC ale gateway-ului rezidențial. Consultați informațiile despre numărul de serie și adresa MAC menționate anterior în această secțiune.

Doresc să utilizez serverul aplicației pentru serviciul telefonic

Va trebui să vă deschideți, de asemenea, un cont de telefonie cu furnizorul de servicii local pentru a utiliza gateway-ul rezidențial pentru servicii telefonice. Când contactați furnizorul de servicii, este posibil să vă puteți transfera numerele de telefon existente sau furnizorul de servicii de telefonie prin cablu va aloca un număr de telefon nou pentru fiecare linie telefonică activă curentă sau suplimentară. Discutați aceste opțiuni cu furnizorul dumneavoastră de servicii de telefonie.

Care este cea mai bună locație pentru gateway-ul meu rezidențial DOCSIS?

Locația ideală pentru gateway-ul rezidențial este un loc în care acesta are acces la prize și alte dispozitive. Gândiți-vă la planul casei sau al biroului dumneavoastră și consultați-vă cu furnizorul de servicii pentru a selecta cea mai bună locație pentru gateway-ul rezidențial. Citiți cu atenție acest ghid de utilizare înainte de a decide unde amplasați gateway-ul rezidențial.

Luați în considerare următoarele recomandări:

- Alegeți o locație în apropierea computerului, dacă veți utiliza gateway-ul rezidențial și pentru serviciul de Internet de mare viteză.
- Alegeți o locație în apropierea unei conexiuni coaxiale RF existente pentru a elimina nevoia unei prize coaxiale RF suplimentare.
- Alegeți o locație pentru gateway-ul rezidențial care să se afle lângă echipamentul telefonic, dacă utilizați doar unul sau două echipamente telefonice.
Notă: Dacă utilizați gateway-ul rezidențial pentru a furniza servicii mai multor telefoane, un instalator profesionist poate conecta gateway-ul rezidențial la cablajul telefonic existent în casa dumneavoastră. Pentru a minimiza modificările aduse cablajului telefonic de acasă, vă recomandăm să amplasați gateway-ul rezidențial în apropierea unei prize de telefon existente.
- Alegeți o locație care să fie relativ protejată de deranjamente sau deteriorări accidentale, precum un dulap, un subsol sau altă zonă protejată.
- Alegeți o locație astfel încât să existe suficient spațiu pentru a trage cablurile de la modem fără a le întinde sau îndoi.
- Nu trebuie restricționată circulația aerului în jurul gateway-ului rezidențial.
- Citiți cu atenție acest ghid de utilizare înainte de a instala gateway-ul rezidențial.

Cum montez modemul pe perete? (Opțional)

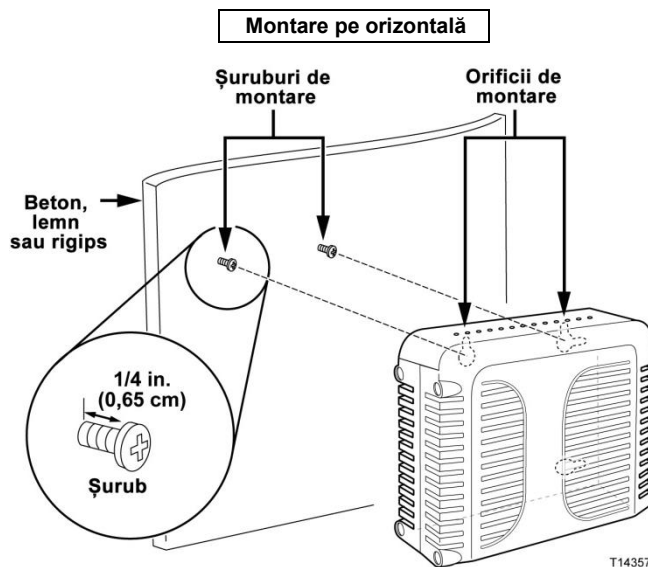
Puteți monta gateway-ul rezidențial pe un perete utilizând două ancore de perete, două șuruburi și orificiile de montare de pe unitate. Modemul poate fi montat pe verticală sau pe orizontală.

Înainte de a începe

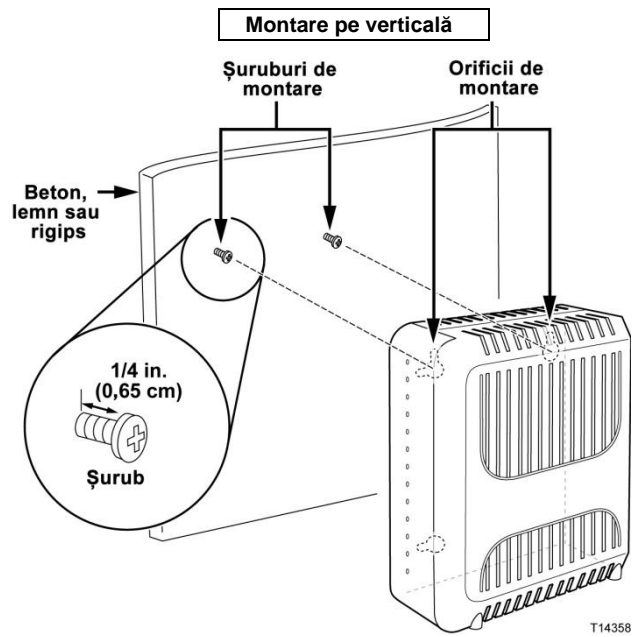
Înainte de a începe, alegeți un loc de montare corespunzător. Peretele poate fi făcut din ciment, lemn sau rigips. Locul de montare trebuie să nu prezinte obstacole pe nicio parte, iar cablurile trebuie să poată ajunge cu ușurință la gateway-ul rezidențial, fără să fie întinse. Lăsați o distanță suficientă între partea de jos a gateway-ului rezidențial și podeaua sau rafturile de dedesubt pentru a permite accesul la cabluri. În plus, nu întindeți la maximum cablurile, astfel încât gateway-ul rezidențial să poată fi îndepărtat pentru intervenții de întreținere necesare fără a deconecta cablurile. De asemenea, verificați dacă dispuneți de următoarele articole:

- Două ancore de perete pentru șuruburi #8 x 1 inci
- Două șuruburi de #8 x 1 inci, din metal, cu cap în cruce
- Burghiu de 3/16 in. pentru lemn sau zidărie, în funcție de compoziția peretelui
- O copie a ilustrațiilor pentru montarea pe perete prezentate în următoarele pagini

Montați modemul după cum se arată într-una din ilustrațiile următoare.

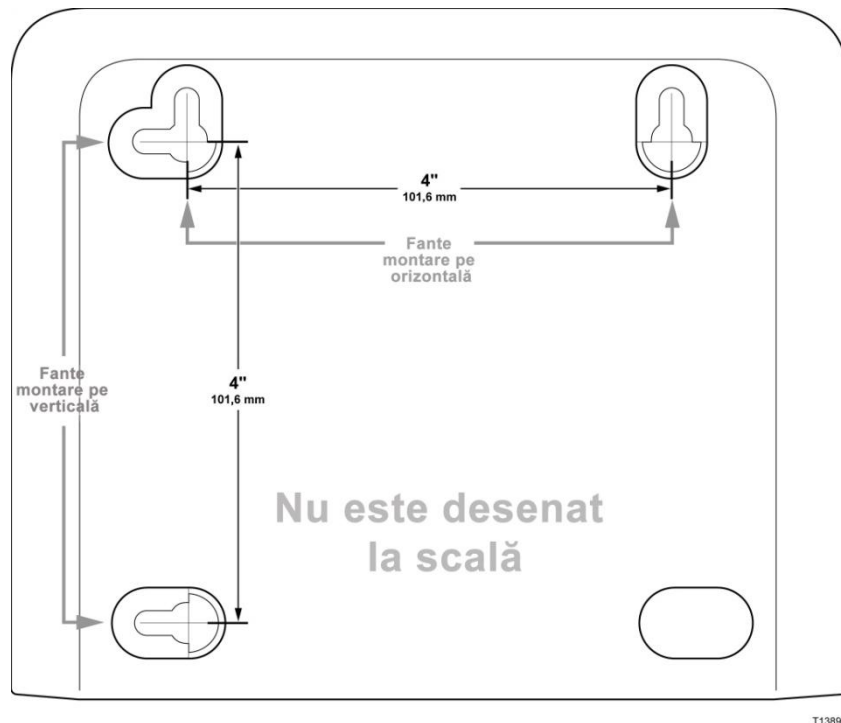


Cum montez modemul pe perete? (Opțional)



Locația și dimensiunile orificiilor pentru montarea pe perete

Următoarea ilustrație prezintă locația și dimensiunile orificiilor pentru montarea pe perete de pe partea de dedesubt a modemului. Utilizați informațiile de pe această pagină drept ghid pentru montarea modemului pe perete.



Montarea gateway-ului rezidențial pe perete

- 1 Cu ajutorul unui burghiu de 3/16 inci, dați două găuri la aceeași înălțime și la distanță de 4 inci (10 cm).
Notă: Graficul precedent ilustrează locația orificiilor de montare de pe spatele gateway-ului rezidențial.
- 2 Montați gateway-ul rezidențial pe o suprafață de rigips sau beton unde există un stâlp de lemn?
 - Dacă **da**, treceți la pasul 3.
 - Dacă **nu**, introduceți diblurile de ancorare în perete și înșurubați șuruburile de montare în diblurile de ancorare; lăsați o distanță de circa 1/4 inci (6 mm) între capul șurubului și perete. Apoi, treceți la pasul 4.

- 3 Introduceți șuruburile de montare în perete; lăsați o distanță de circa 1/4 inci (6 mm) între capul șurubului și perete. Apoi, treceți la pasul 4.
- 4 Asigurați-vă că nu există cabluri sau fire conectate la gateway-ul rezidențial.
- 5 Ridicați gateway-ul rezidențial pe poziție. Glisați capătul larg al ambelor orificii de montare (amplasate pe spatele gateway-ului rezidențial) peste șuruburile de montare și apoi glisați în jos gateway-ul rezidențial, până când capătul îngust al orificiului în formă de gaură de cheie intră în contact cu corpul șurubului.
Important: Verificați dacă șuruburile de montare susțin în siguranță gateway-ul rezidențial înainte de a da drumul unității.

Care sunt cerințele pentru serviciile de telefonie?

Numărul aparatelor telefonice

Conectorii RJ-11 pentru telefonie de pe gateway-ul rezidențial pot furniza fiecare servicii de telefonie pentru mai multe telefoane, aparate de fax și modemi analogice.

Numărul maxim de aparate telefonice conectate la fiecare port RJ-11 este limitat de sarcina totală de sonerie a aparatelor telefonice conectate. Multe aparate telefonice sunt marcate cu un Număr de echivalență a telefonului (REN). Fiecare port de telefon de pe gateway-ul rezidențial poate accepta o sarcină de până la 5 REN.

Suma sarcinilor REN de pe toate aparatele telefonice conectate la fiecare port nu trebuie să depășească 5 REN.

Tipuri de aparate telefonice

Puteți utiliza aparate telefonice care nu sunt etichetate cu un număr REN, însă nu poate fi calculat cu exactitate numărul maxim de aparate telefonice ce pot fi conectate. În cazul aparatelor telefonice care nu sunt etichetate, fiecare aparat trebuie conectat, iar semnalul de sonerie trebuie testat înainte de a adăuga alte aparate. Dacă sunt conectate prea multe aparate telefonice și semnalul de sonerie nu se mai poate auzi, trebuie îndepărtate aparate telefonice până când semnalul de sonerie funcționează în mod corespunzător.

Telefoanele, aparatele de fax și alte aparate telefonice trebuie să utilizeze cei 2 pini centrali ai conectorilor RJ-11 pentru a se conecta la porturile pentru telefon ale gateway-ului rezidențial. Unele telefoane utilizează alți pini de pe conectorii RJ-11 și necesită adaptoare pentru a funcționa.

Cerințe privind apelarea

Toate telefoanele trebuie setate să utilizeze apelarea DTMF. În mod obișnuit, apelarea prin impulsuri nu este activată de furnizorul dumneavoastră local.

Cerințe privind cablajul telefonic

Gateway-ul rezidențial acceptă conectarea la cablajul telefonic interior, precum și conectarea directă la un telefon sau un aparat de fax. Distanța maximă dintre unitate și aparatul telefonic aflat cel mai departe nu trebuie să depășească 1.000 de picioare (300 metri) Utilizați cabluri de telefon răsucite de 26 sau mai mari.

Important: Conectarea la o rețea de domiciliu cu cabluri telefonice existentă sau la una nouă, instalată permanent, trebuie realizată de un instalator calificat.

Cum conectez gateway-ul pentru serviciile de Internet și telefonie?

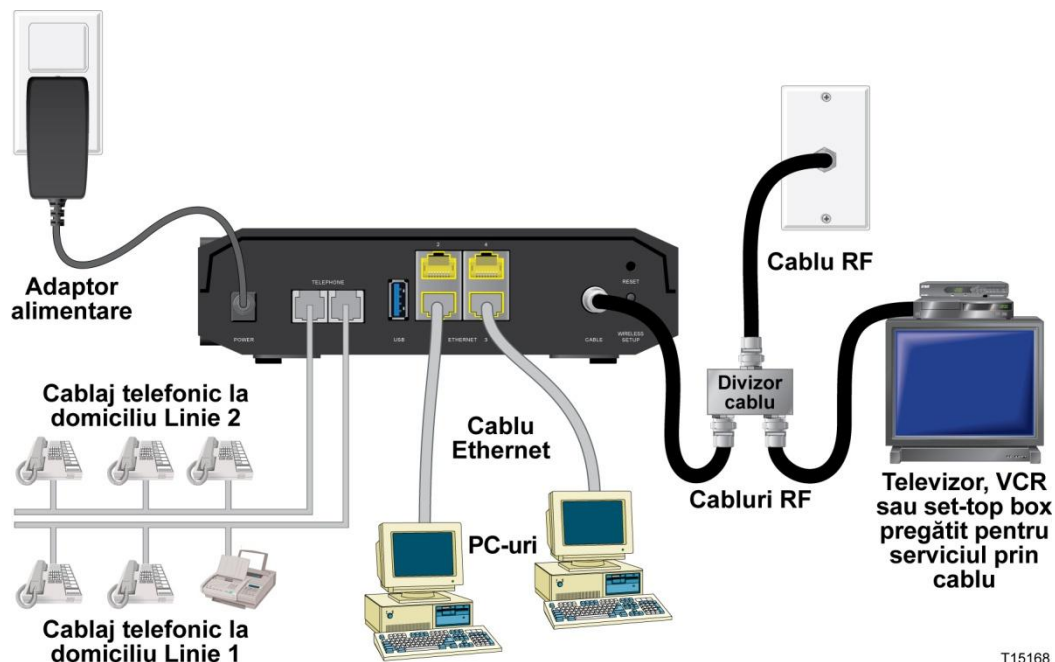
Puteți utiliza gateway-ul rezidențial pentru a vă furniza serviciul telefonic și accesul la Internet și puteți partaja această conexiune la Internet cu alte dispozitive pentru Internet de acasă sau de la birou. Partajarea unei conexiuni între mai multe dispozitive se numește lucru în rețea.

Conectarea și instalarea dispozitivelor pentru Internet

Este posibil să fie disponibil un serviciu de instalare asigurată de specialiști. Contactați furnizorul local de servicii pentru asistență suplimentară.

Pentru a conecta dispozitive

Următoarea diagramă ilustrează una dintre diversele opțiuni de lucru în rețea care vă stau la dispoziție.



T15168

Conectarea gateway-ului rezidențial pentru serviciile de date de mare viteză și telefonie

Următoarea procedură de instalare asigură instalarea și configurarea corespunzătoare pentru gateway-ul rezidențial.

- 1 Alegeți o locație adecvată și sigură pentru a instala gateway-ul rezidențial (în apropierea unei surse de alimentare, a unei conexiuni prin cablu active, a PC-ului - dacă utilizați serviciul de Internet de mare viteză și de liniile telefonice - dacă utilizați VoIP).



AVERTISMENT:

- Pentru a evita vătămarea personală, urmați instrucțiunile de instalare exact în ordinea prezentată.
- Pentru a preveni eventuala deteriorare a echipamentului, deconectați orice alt serviciu telefonic înainte de a conecta modemul cu cablu la aceleași fire.
- Tensiuni electrice periculoase pot fi prezente pe porturile de telefon ale gateway-ului rezidențial și pe orice cabluri conectate, inclusiv cabluri Ethernet, de telefon sau coaxiale.
- Cablurile și conexiunile telefonice trebuie izolate în mod corespunzător pentru a preveni electrocutarea.
- Conexiunile telefonice la o rețea cu cabluri de telefonie instalată acasă trebuie realizate de un instalator calificat. Este posibil ca furnizorul serviciului de telefonie prin cablu să ofere servicii profesionale de instalare și conectare la rețeaua cu cabluri de telefonie de la domiciliu. Se poate percepe o taxă pentru acest serviciu.
- Cablurile și conexiunile trebuie izolate în mod corespunzător pentru a preveni electrocutarea.
- Întrerupeți alimentarea gateway-ului rezidențial înainte de a încerca să îl conectați la orice dispozitiv.

- 2 Opriți PC-ul și alte echipamente din rețea; apoi, deconectați-le de la sursa de alimentare.
- 3 Conectați cablul coaxial RF activ de la furnizorul de servicii la conectorul coaxial etichetat **CABLE** de pe partea din spate a gateway-ului rezidențial.

Notă: Pentru a conecta un televizor, un DHCT, un set-top box sau un VCR de la aceeași conexiune prin cablu, va trebui să montați un divizor de semnal prin cablu (nu este inclus). Consultați-vă întotdeauna cu furnizorul de servicii înainte de a utiliza un divizor, deoarece divizorul poate degrada semnalul.

- 4 Conectați PC-ul la gateway-ul rezidențial utilizând oricare dintre următoarele metode.
 - **Conexiune Ethernet:** Găsiți cablul Ethernet galben, conectați un capăt al cablului Ethernet la portul Ethernet de pe PC și celălalt capăt la portul **ETHERNET** galben de pe partea din spate a gateway-ului rezidențial.
Note: Pentru a instala mai multe dispozitive Ethernet decât porturile prevăzute pe gateway-ul rezidențial, utilizați switchuri Ethernet externe cu mai multe porturi.
 - **Wireless:** Asigurați-vă că dispozitivul wireless este sub tensiune. Va trebui să asociați dispozitivul wireless cu gateway-ul wireless odată ce gateway-ul este operațional. Uurmați îndrumările primite împreună cu dispozitivul wireless pentru asocierea cu un punct de acces wireless.
Mai multe informații despre configurația implicită din fabrică a gateway-ului dumneavoastră wireless pot fi găsite mai departe în acest ghid de utilizare, în secțiunea *Configurarea setărilor wireless* (la pagina 44).
- 5 Conectați un capăt al cablului de conexiune telefonică (nu este inclus) la o priză de telefon de acasă sau la un telefon sau un aparat de fax. Apoi conectați celălalt capăt al cablului de conexiune la portul RJ-11 **TELEPHONE** corespunzător de pe partea din spate a gateway-ului rezidențial. Porturile de telefon sunt de culoare gri deschis și sunt etichetate 1/2 și 2 sau 1 și 2, în funcție de regiunea de pe glob unde este utilizat gateway-ul rezidențial.
Note:
 - Asigurați-vă că ați conectat serviciul telefonic la portul RJ-11 corect. Pentru serviciul de telefonie printr-o singură linie, conectați la portul 1/2 sau 1.
 - În America de Nord, gateway-urile rezidențiale au capacitate pentru mai multe linii pe portul de telefon RJ-11 etichetat cu 1/2. Linia 1 este pe pinii 3 și 4 ai portului 1/2, iar Linia 2 este acceptată pe pinii 2 și 5. În Europa, gateway-urile rezidențiale acceptă doar câte o linie per port. Linia 1 este pe portul 1 și linia 2 este pe portul 2.
 - Telefoanele care necesită alți conectori electrici decât RJ-11 pot avea nevoie un adaptor extern (comercializat separat).
- 6 Găsiți cablul de alimentare CA furnizat împreună cu gateway-ul rezidențial. Introduceți un capăt al cablului de alimentare în conectorul CA de pe partea din spate a gateway-ului rezidențial. Apoi, conectați cablul CA la o priză CA pentru a alimenta gateway-ul rezidențial cu energie electrică. Gateway-ul rezidențial va efectua o căutare automată pentru a localiza și pentru a se conecta la rețeaua de date de bandă largă. Acest proces poate dura între 2 și 5 minute. Modemul va fi pregătit pentru utilizare în momentul în care LED-urile **POWER**, **DS**, **US** și **ONLINE** de pe panoul frontal al gateway-ului rezidențial nu mai clipesc și rămân aprinse.

Cum conectez gateway-ul pentru serviciile de Internet și telefonie?

- 7 Conectați și porniți PC-ul și alte dispozitive din rețeaua de domiciliu. LED-ul **LINK** de pe gateway-ul rezidențial corespunzător dispozitivelor conectate trebuie să fie aprins sau să clipească.
- 8 Odată ce gateway-ul rezidențial este online, majoritatea dispozitivelor pentru Internet vor avea acces imediat la Internet.

Notă: Dacă PC-ul nu are acces la Internet, consultați secțiunea *Întrebări frecvente* (la pagina 107) pentru informații despre modul de configurare a PC-ului pentru TCP/IP. Pentru dispozitive Internet diferite de PC-uri, consultați secțiunea privind configurarea DHCP sau a adresei IP din Ghidul de utilizare sau Manualul de funcționare al dispozitivelor respective.

Cum configurez gateway-ul rezidențial DOCSIS?

Pentru a configura gateway-ul rezidențial, trebuie mai întâi să accesați paginile de configurare WebWizard. Această secțiune oferă instrucțiuni și proceduri detaliate pentru accesarea paginilor WebWizard și pentru configurarea gateway-ului rezidențial în vederea unei funcționări corecte. Această secțiune prezintă, de asemenea, exemple și descrieri ale fiecărei pagini de configurare WebWizard. Utilizați paginile WebWizard pentru a individualiza gateway-ul rezidențial în funcție de nevoile dumneavoastră în loc să utilizați setările implicite. Paginile WebWizard din această secțiune sunt organizate în ordinea prezentată în pagina **Configurare**.

Important: Paginile WebWizard și exemplele prezentate în această secțiune au doar scop ilustrativ. Paginile dumneavoastră pot diferi de cele prezentate în acest ghid. Paginile prezentate în acest ghid reprezintă, de asemenea, valorile implicite pentru dispozitiv.

Notă: Dacă nu sunteți familiarizat cu procedurile de configurare a rețelei detaliate în această secțiune, contactați furnizorul de servicii înainte de a încerca să modificați oricare dintre setările implicite ale gateway-ului rezidențial.

Conectarea pentru prima dată la gateway

Configurația implicită a gateway-ului utilizează adresa IP 192.168.0.1. Dacă ați conectat corect gateway-ul și ați configurat corespunzător computerul, efectuați pașii următori pentru a vă conecta la gateway ca administrator.

- 1 Pe PC, deschideți browserul Web preferat.
- 2 În câmpul de adresă, introduceți următoarea adresă IP: **192.168.0.1**. Se deschide o pagină de log in Stare WAN DOCSIS, similară cu pagina următoare.

Cum configurez gateway-ul rezidențial DOCSIS?

The screenshot displays the WAN DOCSIS configuration interface. It features a sidebar with navigation options: 'Stare' (Status), 'Log in', 'Despre' (About), 'Stare modem de cablu' (Cable modem status), 'Canale de descărcare' (Download channels), and 'Canale de încărcare' (Upload channels). The main content area is divided into several sections:

- Log in:** Fields for 'Nume utilizator:' (Username) and 'Parolă:' (Password), a language dropdown set to 'Română', and a 'Log in' button.
- Despre:** Device information including Model (Cisco EPC3925), Distributor (Cisco), Versiune hardware (1.0), Adresă MAC (00:25:2e:63:bf:84), Versiune Bootloader (2.3.0_R1), Versiune curentă software (EPC3925-ESIP-12-v302r125532-110628c_upc-TEST), Nume firmware (epc3925-ESIP-12-v302r125532-110628c_upc-TEST.bi), Oră generare firmware (lun 28 09:17:03 2011), Stare modem de cablu (Operațional), and Rețea wireless (Enable).
- Stare modem de cablu:** Status of DOCSIS operations: Scanare descărcare DOCSIS (Finalizat), Interval DOCSIS (Finalizat), DHCP DOCSIS (Finalizat), TFTP DOCSIS (Finalizat), Înreg. date DOCSIS finalizată (Finalizat), and Confidențialitate DOCSIS (Activat).
- Canale de descărcare:** A table showing power levels and signal reports for 8 channels.
- Canale de încărcare:** A table showing power levels for 4 channels.

Canal	Nivel alimentare:	Raport semnal - zgomot:
Canal 1:	11.4 dBmV	45.4 dB
Canal 2:	10.8 dBmV	45.3 dB
Canal 3:	11.5 dBmV	45.6 dB
Canal 4:	10.5 dBmV	44.2 dB
Canal 5:	11.3 dBmV	44.4 dB
Canal 6:	10.5 dBmV	44.1 dB
Canal 7:	11.1 dBmV	44.5 dB
Canal 8:	10.0 dBmV	44.3 dB

Canal	Nivel alimentare:
Canal 1:	28.7 dBmV
Canal 2:	0.0 dBmV
Canal 3:	0.0 dBmV
Canal 4:	0.0 dBmV

- Pe pagina Stare WAN DOCSIS, lăsați necompletate câmpurile Nume utilizator și Parolă și faceți clic pe **Log in**. Gateway-ul se deschide cu pagina Administrare - Gestionare în prim-plan. Puteți utiliza pagina Administrare - Gestionare pentru a vă modifica Numele de utilizator și Parola.

- 4 În acest moment, v-ați logat la gateway. Puteți selecta oricare dintre paginile Web de configurare și management. Însă, ați fost direcționat către pagina de Management administrativ pentru a vă aduce aminte să modificați parola.

Important: Vă recomandăm cu tărie să stabiliți o nouă parolă pentru a vă proteja împotriva eventualelor atacuri prin Internet care caută dispozitive ce funcționează cu nume de utilizator și parole binecunoscute sau implicite din fabrică.

- 5 Pe pagina de Administrare - Gestionare, creați un Nume de utilizator și o Parolă și apoi faceți clic pe **Salvare setări**. După ce ați salvat setările pentru numele de utilizator și parolă pe pagina Management al administrării, se deschide pagina Configurare - Quick Setup (Setărilor rapide).

Important: Aveți posibilitatea de a lăsa câmpul pentru parolă necompletat (implicit din fabrică). Totuși, dacă nu vă modificați numele de utilizator și parola, veți fi direcționat la pagina Administrare - Gestionare de fiecare dată când accesați gateway-ul. Acest lucru are drept scop să vă reamintească să vă creați o parolă personalizată.

Odată ce v-ați personalizat parola, orice log in ulterior vă va duce direct la pagina Configurare - Quick Setup (Setărilor rapide).

- 6 După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Configurare > Quick Setup (Setărilor rapide)

Pagina Configurare - Quick Setup (Setărilor rapide) este prima pagină care se deschide după ce vă logați la gateway. Puteți utiliza setările de pe această pagină pentru a vă modifica parola și pentru a configura WLAN.

Important: Setările de pe această pagină sunt unice pentru dispozitivul dumneavoastră. Dacă doriți, nu este nevoie să aduceți nicio modificare setărilor din această pagină. Aceste setări implicite sunt tot ceea ce vă trebuie pentru a utiliza o rețea wireless securizată.

The screenshot shows the 'Quick Setup' configuration page. The top navigation bar includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. Below this, there are sub-tabs for 'Quick Setup', 'Configurare LAN', and 'DDNS'. The main content area is split into two sections: 'Schimbare parolă' and 'WLAN'. The 'Schimbare parolă' section contains three input fields: 'Nume de utilizator:', 'Modificare parolă la:', and 'Introduceți din nou parolă nouă:'. The 'WLAN' section contains radio buttons for 'Rețea wireless' (with 'Activare' selected), a text field for 'Nume rețea wireless (SSID):' with the value '63b84', a dropdown menu for 'Mod securitate wireless:' set to 'WPA-Personal', a dropdown for 'Criptare:' set to 'AES', and a text field for 'Cheie pre-partajată:' with the value '228210229' and a checked 'Afișare cheie' checkbox. At the bottom of the page are two buttons: 'Salvare setări' and 'Revocare modificări'.

Configurarea setărilor rapide

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura setările de rețea pentru dispozitiv. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau faceți clic pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Schimbare parolă	Nume de utilizator Afișează numele de utilizator al operatorului logat în momentul respectiv
	Modificare parolă la Vă permite să modificați parola
	Introduceți din nou parolă nouă Vă permite să reintroduceți parola nouă. Trebuie să introduceți aceeași parolă ca cea introdusă în câmpul Modificare parolă la

Secțiune	Descriere câmp
WLAN	<p data-bbox="613 331 786 359">Rețea wireless</p> <p data-bbox="613 373 1382 436">Vă permite să activați sau să dezactivați rețeaua wireless. Selectați opțiunea dorită:</p> <ul data-bbox="613 451 797 520" style="list-style-type: none"> <li data-bbox="613 451 760 478">■ Activare <li data-bbox="613 493 797 520">■ Dezactivare <p data-bbox="613 535 932 562">Nume rețea wireless (SSID)</p> <p data-bbox="613 577 1382 703">Vă permite să introduceți un nume pentru rețeaua wireless sau să utilizați valoarea implicită. Valoarea introdusă aici va fi văzută pe PC-uri și pe alte dispozitive client wireless ca nume al rețelei wireless.</p> <p data-bbox="613 718 1382 844">Notă: Identificatorul setului de servicii (SSID) implicit din fabrică este egal, în mod obișnuit, cu ultimele 6 caractere ale adresei CM MAC. Adresa CM MAC poate fi găsită pe eticheta de clasificare atașată gateway-ului wireless.</p> <p data-bbox="613 858 899 886">Mod securitate wireless</p> <p data-bbox="613 900 1398 1089">Vă permite să selectați un mod de securitate wireless pentru a ajuta la protejarea rețelei. Dacă selectați Dezactivare, rețeaua dumneavoastră nu este securizată și orice dispozitiv wireless din raza ei se poate conecta la aceasta. Consultați <i>Wireless > Securitate wireless</i> (la pagina 48) pentru descrieri detaliate ale modurilor de securitate wireless.</p> <p data-bbox="613 1104 1422 1167">Notă: Modul de securitate wireless implicit din fabrică este WPA sau WPA2-Personal.</p> <p data-bbox="613 1182 711 1209">Criptare</p> <p data-bbox="613 1224 1414 1308">Vă permite să selectați un nivel de criptare în funcție de modul de securitate wireless pe care îl alegeți. Consultați <i>Wireless > Securitate wireless</i> (la pagina 48) pentru descrieri detaliate ale criptării.</p> <p data-bbox="613 1323 846 1350">Cheie pre-partajată</p> <p data-bbox="613 1365 1422 1524">Cheia pre-partajată pentru dispozitiv. Cheia poate conține între 8 și 63 de caractere. Cheia pre-partajată implicită din fabrică este egală cu numărul de serie din 9 cifre al gateway-ului dumneavoastră. Numărul de serie poate fi găsit pe eticheta de clasificare atașată gateway-ului wireless.</p> <p data-bbox="613 1539 1422 1665">Notă: Este posibil ca furnizorul dumneavoastră de servicii să vă ofere o cartelă pentru configurarea wireless, care să conțină SSID și informații de configurare a securității wireless pentru rețeaua dumneavoastră de acasă și care să difere de cele descrise mai sus.</p>

Configurare > Configurare LAN

Pagina Configurare - Configurare LAN vă permite să configurați setările pentru rețeaua locală (LAN) de la domiciliu. Aceste setări includ intervalul de adrese IP care definesc rețeaua LAN în sine, precum și modul în care adresele sunt alocate (automat, de către DHCP, sau manual) pe măsură ce sunt adăugate dispozitive noi la rețea.

Important: Dacă nu aveți cunoștințe despre administrarea adreselor IP, vă recomandăm să nu modificați aceste setări. Dacă modificați aceste setări în mod incorect, puteți pierde accesul la Internet.

Selectați fila **Configurare LAN** pentru a deschide pagina Configurare - Configurare LAN.

The screenshot displays the 'Configurare rețea (LAN)' page with the following settings:

- Adresă IP locală:** 192 . 168 . 0 . 1
- Mască subrețea:** 255 . 255 . 255 . 0
- Server DHCP:** Activare Dezactivare
- Început adrese IP:** 192.168.0.10
- Număr maxim de utilizatori DHCP:** 119
- Termen atribuire client:** 60 minute (0 înseamnă o zi)
- LAN 1 DNS 1 static:** 0 . 0 . 0 . 0
- LAN 1 DNS 2 static:** 0 . 0 . 0 . 0
- LAN 1 DNS 3 static:** 0 . 0 . 0 . 0
- Oră locală sistem:** Vi Aug 12 17:03:26 2011
- Fus orar:** (GMT) Ora centrală Greenwich: Dublin, Edinburgh, Lisabona, Londra
- Ora de vară:** 0 minute
- Adaptare automată la ora de vară:**
- Server de oră:** time.nist.gov, nist.aol-ca.truetime.com, nist1-ny.glassey.com
- NTP:** Activare Dezactivare

Configurarea setărilor de rețea

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura setările de rețea pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau faceți clic pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Configurare rețea (LAN) IP gateway	Adresă IP locală Adresa IP de bază a rețelei dumneavoastră LAN de la domiciliu. Adresa IP LAN implicită din fabrică este 192.168.0.1.
	Mască subrețea Masca de subrețea pentru LAN

Setări adresă server de rețea (DHCP)	<p>Server DHCP</p> <p>Vă permite să activați sau să dezactivați serverul DHCP din gateway-ul rezidențial. Serverul DHCP este utilizat pentru a aloca în mod automat adrese IP dispozitivelor, pe măsură ce acestea sunt adăugate în rețeaua dumneavoastră de domiciliu.</p>
---	--

- **Pagină Rezumat dispozitive conectate**

Faceți clic pe **Rezumat dispozitive conectate** din pagina Configurare LAN. Se deschide pagina Rezumat dispozitive conectate. Această pagină este o fereastră pop-up care afișează adresa MAC și adresa IP ale dispozitivelor conectate la gateway-ul rezidențial.

Rezumat dispozitive conectate		
Rezumat dispozitive conectate		
Conectat la	Adresă MAC	Atribuire adresă IP
Eth-Switch Lan(1)	40:61:86:4b:08:f2	192.168.0.10

Reimprospătare Închidere

Secțiune

Descriere câmp

Setări adresă server de rețea (DHCP)

■ Pagina Adrese IP DHCP pre-atribuite

Faceți clic pe **Adrese IP DHCP pre-atribuite** din pagina Configurare LAN. Se deschide pagina Adrese IP DHCP pre-alocate. Această pagină vă permite să alocați o adresă IP specifică unui PC sau unui alt dispozitiv, atunci când acesta solicită o adresă IP utilizând DHCP. Cu această caracteristică pot fi rezervate doar adrese din intervalul de adrese DHCP al gateway-ului.

Adrese IP DHCP pre-atribuite

Adresă IP DHCP pre-atribuite

Adresă MAC: 00:00:00:00:00:00

Atribuire adresei IP: [] [] [] []

Adăugare IP static

Adresă MAC	Adresă IP	Stare
40:61:86:4b:08:f2 <->	192.168.0.10	Active

Eliminare IP static

Note:

- Butonul **Adăugare IP static** adaugă adresa IP statică la lista de adrese IP pre-alocate.
- Butonul **Eliminare IP static** elimină adresa IP statică din lista de adrese IP pre-alocate.

Început adrese IP

Afișează adresa de început utilizată de serverul DHCP încorporat pentru a distribui adrese IP LAN private. Întrucât adresa IP implicită a gateway-ului este **192.168.1.1**, adresa IP de început trebuie să fie **192.168.1.2** sau mai mare, dar mai mică decât **192.168.0.253**. Adresa IP implicită de început este **192.168.0.10**.

Număr maxim de utilizatori DHCP

Introduceți numărul maxim de utilizatori cărora serverul DHCP le poate aloca adrese IP pentru utilizarea în cadrul rețelei LAN. Acest număr nu poate fi mai mare de 254 minus adresa IP de început descrisă mai sus.

Secțiune	Descriere câmp
	<p>Termen atribuire client</p> <p>Termenul de atribuire a clientului reprezintă perioada de timp pentru care o adresă IP este validă. Atribuirile de adrese IP sunt reînnoite automat de către PC și alte dispozitive care utilizează DHCP pentru a obține adrese IP. Dacă o atribuire este lăsată să expire, adresa IP va reveni în mulțimea de adrese IP disponibile, care pot fi alocate de către serverul DHCP pe măsură ce dispozitive noi sunt adăugate la rețea. Termenul implicit este de 60 de minute, atunci când gateway-ul este online.</p> <p>DNS (Domanin Name Server) static LAN 1-3</p> <p>DNS este utilizat de către un PC sau alte dispozitive client pentru a descoperi adresele IP publice asociate cu un URL sau adresa sub formă de nume a unui site Web. Puteți specifica manual ce servere DNS urmează să fie utilizate de către dispozitivele din rețeaua dumneavoastră introducând adresele IP ale serverelor respective în aceste câmpuri. Altfel, gateway-ul va redirecționa automat informațiile serverului DNCS de la furnizorul dumneavoastră de servicii. Ca setare implicită, aceste câmpuri sunt necompletate.</p>
<p>Setări oră</p>	<p>Fus orar</p> <p>Selectați fusul orar pentru locația dumneavoastră. Dacă ora de la locația dumneavoastră se modifică în funcție de ora de vară, selectați Adaptare automată la ora de vară.</p>

Configurare > DDNS

Serviciul de nume de domenii dinamice (DDNS) furnizează gateway-ului rezidențial (care poate avea o adresă IP care se modifică) un nume de gazdă sau un URL ce poate fi rezolvat de aplicațiile din rețea prin intermediul unor interogări DNS standard. DDNS este util atunci când vă găzduiți propriul site Web, un server FTP sau un alt server în spatele dispozitivului. Înainte de a utiliza această caracteristică, trebuie să vă înregistrați pentru servicii DDNS.

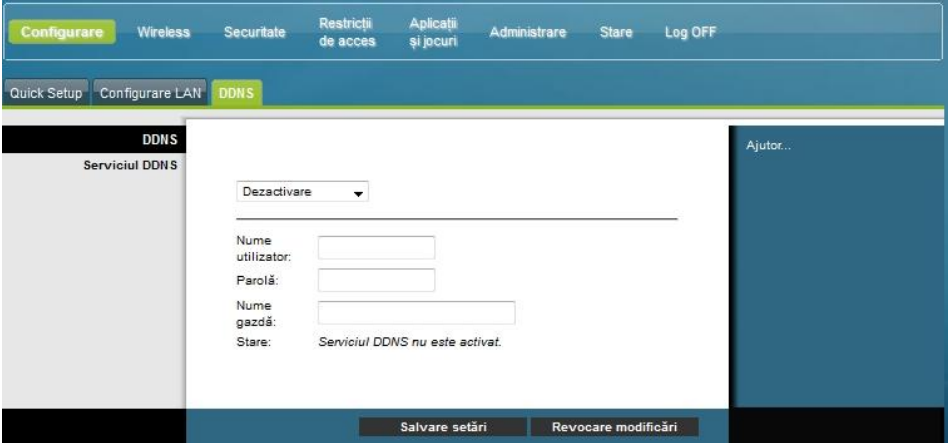
Selectați fila **DDNS** pentru a deschide pagina Configurare DDNS.

Cum configurez gateway-ul rezidențial DOCSIS?

Secțiune Descriere câmp

Serviciul DDNS Dezactivarea DDNS (setări implicite din fabrică)

Pentru a dezactiva DDNS, selectați **Dezactivare** din lista verticală și faceți clic pe **Salvare setări**.



The screenshot shows the DDNS configuration interface. At the top, there is a navigation bar with tabs: Configurare, Wireless, Securitate, Restricții de acces, Aplicații și jocuri, Administrare, Stare, and Log OFF. Below this, there are sub-tabs: Quick Setup, Configurare LAN, and DDNS. The main content area is titled 'DDNS Serviciul DDNS'. A dropdown menu is set to 'Dezactivare'. Below the dropdown are input fields for 'Nume utilizator:', 'Parolă:', and 'Nume gazdă:'. The 'Stare:' field shows 'Serviciul DDNS nu este activat.'. At the bottom, there are buttons for 'Salvare setări' and 'Revocare modificări'.

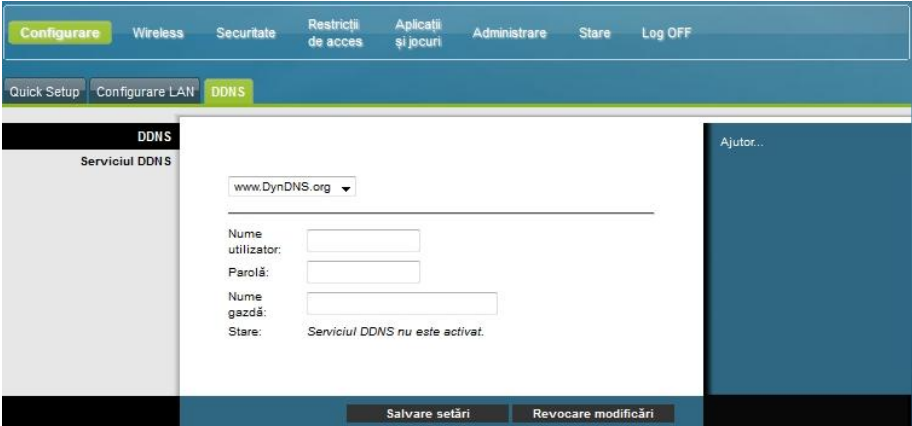
Activarea DDNS

Notă: Pentru a utiliza caracteristica DDNS, trebuie ca mai întâi să vă deschideți un cont și să stabiliți un URL cu www.DynDNS.org. Caracteristica DDNS nu va funcționa fără un cont valid.

Pentru a deschide un cont DDNS, deschideți browserul și introduceți www.DynDNS.org în bara de adresă. Urmați instrucțiunile de pe site-ul Web pentru a deschide un cont.

Pentru a activa DDNS, urmați acești pași.

- 1 Pe pagina DDNS, selectați **www.DynDNS.org** ca server DDNS.



The screenshot shows the DDNS configuration interface. The dropdown menu is now set to 'www.DynDNS.org'. The input fields for 'Nume utilizator:', 'Parolă:', and 'Nume gazdă:' are visible. The 'Stare:' field shows 'Serviciul DDNS nu este activat.'. The buttons 'Salvare setări' and 'Revocare modificări' are at the bottom.

- 2 Configurați câmpurile următoare:
 - Nume utilizator
 - Parolă
 - Nume gazdă

Secțiune	Descriere câmp
3	<p>Faceți clic pe Salvare setări. Dispozitivul va comunica serviciului DDNS adresa IP WAN (Internet) curentă, ori de câte ori această adresă se modifică.</p> <p>Important: Zona Stare a ferestrei va afișa starea conexiunii la serviciul DDNS.</p>

Configurarea setărilor wireless

Această secțiune descrie opțiunile disponibile pe pagina Wireless pe care le puteți utiliza pentru a configura parametrii WAP pentru a corespunde cerințelor și nevoilor dumneavoastră specifice.

Wireless > Setări de bază

Configurarea gateway-ului rezidențial pentru comunicații wireless vă oferă libertatea de a vă conecta la Internet din orice loc aflat în raza de acțiune a WAP fără a fi nevoit să utilizați conexiuni cu fir. Selectați fila **Setări de bază** pentru a deschide pagina Wireless - Setări de bază.

Pagina Setări de bază wireless vă permite să alegeți modul de lucru în rețea wireless și alte caracteristici de bază.

- Rețea wireless: Activare sau Dezactivare
- Configurație wireless: Manual sau Configurație protejată Wi-Fi (WPS)
- Mod rețea
- Frecvență radio
- Lățime canal
- Canal standard
- Nume rețea wireless (SSID)

Configurație protejată Wi-Fi (WPS)

Dacă selectați Configurație protejată Wi-Fi (WPS) drept configurație wireless, multe setări vor fi pre-configurate. WPS permite o configurare simplificată, care vă permite, la rândul său, să adăugați cu ușurință noi dispozitive cu capacități WPA la rețeaua dumneavoastră.

Important: La utilizarea modului WPS, WEP nu este acceptat. Dacă trebuie să utilizați criptarea WEP, WPS trebuie dezactivat, setând Configurația wireless la **Manual**.

Notă: WPS este setarea implicită.

Exemplu Configurație wireless - Configurație protejată Wi-Fi

The screenshot shows a web-based configuration interface for wireless settings. The main menu includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. The 'Wireless' section is active, with sub-tabs for 'Setări de bază', 'Securitate wireless', 'Filtru MAC', 'Setări avansate', 'Setări WDS', and 'QoS'. The 'Setări de bază' tab is selected, showing the 'Configurație protejată Wi-Fi' option. The configuration includes radio mode (Combinat), frequency (Activat 2,4 GHz), channel width (Canal standard - 20 MHz), and channel standard (Automat). A table lists the wireless network (SSID) as '63b£84', BSSID as '70:71:BC:84:9F:38', and the broadcast SSID checkbox is checked. Buttons for 'Salvare setări' and 'Revocare modificări' are at the bottom.

Descriere pagină Configurație wireless - Configurație protejată Wi-Fi

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura setările de bază ale Configurației protejate Wi-Fi pentru gateway-ul rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Setări de bază	<p>Activați sau Dezactivați rețeaua wireless</p> <p>Configurarea Configurației protejate Wi-Fi</p> <p>Caracteristica Configurație protejată Wi-Fi configurează automat o rețea wireless securizată prin criptare. Pentru a utiliza Configurație protejată Wi-Fi trebuie să aveți cel puțin încă un dispozitiv în rețea care să accepte Configurația protejată Wi-Fi. După ce ați configurat dispozitivele cu Configurație protejată Wi-Fi, puteți configura manual alte dispozitive.</p> <p>Configurarea butonului WPS (opțiunea 1)</p> <p>Apăsați butonul Configurație protejată Wi-Fi de pe pagina Setări wireless de bază sau butonul de pe panoul din spate al gateway-ului pentru a înregistra un client wireless cu gateway-ul. Apăsați butonul software Configurație protejată Wi-Fi de pe dispozitivul client, concomitent cu apăsarea butonului Configurație protejată Wi-Fi de pe gateway. Conexiunea va fi configurată automat.</p>

Secțiune	Descriere câmp
	<p>Configurarea WPS cu ajutorul numărului PIN al adaptorului Wi-Fi (opțiunea 2)</p> <p>Aceasta este cea mai sigură opțiune de a înregistra un client wireless cu gateway-ul. Aveți nevoie de numărul PIN de Configurație protejată Wi-Fi, pe care îl puteți găsi în utilitarul de Configurație protejată Wi-Fi al clientului. După ce introduceți numărul PIN de Configurație protejată Wi-Fi al clientului vă puteți conecta la gateway.</p> <p>Configurarea WPS utilizând numărul PIN al gateway-ului (opțiunea 3)</p> <p>Notați numărul PIN de Configurație protejată Wi-Fi al gateway-ului afișat pe pagina Configurație protejată Wi-Fi. Faceți clic pe butonul Înregistrare în Opțiunea 3 și apoi, utilizând orice utilitar de Configurație protejată Wi-Fi pentru client sau Microsoft Vista, introduceți numărul PIN de Configurație protejată Wi-Fi al gateway-ului în dispozitivul client pentru a finaliza înregistrarea.</p>

Exemplu pagină Configurație wireless manuală

The screenshot shows the 'Setări de bază' (Basic Settings) page for wireless configuration. The 'Rețea wireless' (Wireless Network) section is active, with 'Manual' selected for configuration. The 'Mod rețea' (Network Mode) is set to 'Combinat' (Mixed), 'Frecvență radio' (Radio Frequency) is 'Activat 2,4 GHz' (Activated 2.4 GHz), 'Lățime canal' (Channel Width) is 'Canal standard - 20 MHz' (Standard Channel - 20 MHz), and 'Canal standard' (Channel Standard) is 'Automat' (Automatic).

Nume rețea wireless (SSID)	BSSID	Difuzare SSID
63bfe4	70:71:BC:84:9F:38	<input checked="" type="checkbox"/>

Buttons at the bottom include 'Salvare setări' (Save Settings) and 'Revocare modificări' (Revoke Changes).

Descriere pagină Setări de bază wireless

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura manual setările de bază ale comunicațiilor wireless pentru gateway-ul rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Setări de bază	<p data-bbox="483 327 659 354">Rețea wireless</p> <p data-bbox="483 369 964 396">Activați sau Dezactivați rețeaua wireless</p> <p data-bbox="483 411 745 438">Configurație wireless</p> <p data-bbox="483 453 1360 512">Setarea implicită este WPS. Consultați <i>Configurație protejată Wi-Fi (WPS)</i> (la pagina 44) pentru mai multe informații despre utilizarea WPS.</p> <p data-bbox="483 527 1401 554">Selectați Manual pentru a configura manual rețeaua utilizând această opțiune.</p> <hr/> <p data-bbox="483 579 607 606">Mod rețea</p> <p data-bbox="483 621 1141 648">Alegeți una dintre aceste opțiuni pentru modul de rețea:</p> <p data-bbox="483 663 1232 690">Doar G, Combinat B/G, Combinat B/G/N (implicit din fabrică)</p> <p data-bbox="483 705 1321 764">Important: Dacă este selectată doar autentificarea TKIP, modul de rețea Combinat B/G/N nu este disponibil.</p> <p data-bbox="483 789 672 816">Frecvență radio</p> <p data-bbox="483 831 1292 858">Selectați Activat 2,4 GHz (implicit din fabrică) sau Dezactivat 5 GHz</p> <p data-bbox="483 873 1360 932">Notă: Este posibil ca banda de frecvențe radio de 5 GHz să nu fie acceptată pe unele modele.</p> <p data-bbox="483 957 639 984">Lățime canal</p> <p data-bbox="483 999 1183 1026">Alegeți Canal standard de 20 MHz sau Canal lat de 40 MHz</p> <p data-bbox="483 1052 667 1079">Canal standard</p> <p data-bbox="483 1094 1422 1201">Selectați unul dintre canalele din lista verticală pentru a corespunde setărilor rețelei dumneavoastră. Pentru a putea comunica, toate dispozitivele din rețeaua wireless trebuie să difuzeze pe același canal. Puteți selecta Automat (implicit din fabrică) pentru selectarea automată a canalului.</p>

Secțiune	Descriere câmp
	<p>Nume rețea wireless (SSID)</p> <p>SSID este numele rețelei dumneavoastră wireless. SSID este utilizat de către tehnologia wireless pentru a deosebi rețeaua dumneavoastră de alte rețele wireless din zonă. SSID poate avea maximum 32 de caractere. SSID implicit din fabrică este format, de obicei, din ultimele 6 caractere ale adresei CM MAC ce se regăsește pe eticheta de clasificare de pe partea de dedesubt a gateway-ului.</p> <p>Acest SSID reprezintă o identitate unică și nu trebuie modificat dacă nu doriți. Este posibil ca furnizorul dumneavoastră de servicii să vă ofere informații de configurare wireless care să necesite un SSID diferit.</p>
	<p>BSSID</p> <p>Afișează Identificatorul setului de servicii de bază (BSSID) al rețelei dumneavoastră wireless. BSSID este, de obicei, adresa MAC a punctului de acces wireless.</p> <p>Notă: Aceasta nu poate fi aceeași adresă MAC ca adresa CM MAC utilizată pentru a determina SSID implicit din fabrică.</p>
	<p>Difuzare SSID</p> <p>Când este bifată această casetă (implicit din fabrică), gateway-ul transmite sau își face cunoscută prezența față de alte dispozitive wireless. Dispozitivele client pot detecta automat punctul de acces atunci când această semnalizare este activată.</p> <p>Debifați această casetă dacă doriți să vă ascundeți rețeaua de clienți wireless. Dacă vă ascundeți rețeaua, va trebui să vă configurați fiecare client wireless manual.</p> <p>Important: Casetă de selectare Activat nu este utilizată în prezent și nu afectează funcționarea gateway-ului.</p>

Wireless > Securitate wireless

Prin selectarea unui mod de securitate wireless vă puteți proteja rețeaua. Dacă selectați **Dezactivare**, rețeaua dumneavoastră nu este securizată și orice dispozitiv wireless din raza ei se poate conecta la aceasta.

Pentru a ține intrușii la distanță de rețeaua dumneavoastră wireless, utilizați pagina Securitate wireless pentru a configura parametrii de securitate, inclusiv modul de securitate (nivelul de criptare), cheile de criptare și alte setări de securitate.

Selectați fila **Securitate wireless** pentru a deschide pagina Securitate wireless. Următorul tabel prezintă exemple de pagină Securitate wireless cu diverse moduri de securitate wireless selectate.

Descriere pagină Securitate wireless

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura securitatea wireless pentru gateway-ul rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
----------	----------------

Securitate wireless	Mod securitate wireless
---------------------	--------------------------------

	Alegeți una dintre aceste opțiuni pentru modul de securitate:
--	---

	WEP
--	------------

	Modul de securitate Wired Equivalent Privacy (WEP) este definit în cadrul standardului IEEE 802.11 original. Acest mod nu mai este recomandat, din cauza protecției slabe oferite.
--	--

	Utilizatorii sunt încurajați să migreze la WPA-Personal sau WPA2-Personal.
--	--

	Notă: Modul WPS nu acceptă WEP pe acest dispozitiv.
--	--

The screenshot shows the 'Securitate wireless' configuration page. The 'Mod securitate wireless' dropdown is set to 'WEP'. The 'Criptare' dropdown is set to '40 / 64 de biți (10 cifre hex)'. The 'Parolă wireless' field is empty, with an 'Afișare cheie' checkbox and a 'Generare' button. Below, there are four 'Cheie' fields (1-4) and a 'Cheie TX' dropdown, all containing the value '0101010101'. At the bottom, there are 'Salvare setări' and 'Revocare modificări' buttons.

Descrieri câmpuri

- **Criptare.** Selectați un nivel de criptare WEP, 40 / 64 de biți (10 cifre hexazecimale) sau 104 / 128 de biți (26 de cifre hexazecimale).
- **Parolă wireless.** Pentru a finaliza configurarea securității wireless trebuie să alegeți o parolă wireless pe care să o puteți memora ușor și care să fie greu de intuit pentru persoanele străine. În momentul conectării inițiale a unui dispozitiv wireless nou la rețea, va trebui să introduceți această parolă în secțiunea corespunzătoare de configurare a dispozitivului conectat. Pentru a îmbunătăți securitatea rețelei, nu divulgați această parolă utilizatorilor neautorizați. Introduceți o parolă formată din cel puțin 4 și cel mult 24 de caractere, alcătuită dintr-o combinație de litere și/sau cifre. Apoi, faceți clic pe **Generare** pentru a crea Fraza de acces.

Secțiune	Descriere câmp
	<ul style="list-style-type: none">■ Cheie 1-4. Dacă doriți să introduceți manual cheile WEP, completați câmpurile prevăzute. Fiecare cheie WEP poate consta din litere de la A la F și din cifre de la 0 la 9. Trebuie să aibă o lungime de 10 caractere pentru criptare pe 40/64 de biți sau de 26 de caractere pentru criptare pe 104/128 de biți.■ Cheie TX. Alegeți o Cheie de transmisie (TX) de la 1 la 4. Cheia TX este cheia care va fi utilizată pentru criptarea datelor dumneavoastră. Cu toate că pot fi create patru chei, doar o singură cheie este utilizată pentru criptarea datelor. Selectați una dintre cele patru chei pentru criptarea WEP. Utilizați cheia TX selectată pentru a vă configura clienții wireless.
	WPA
	Securitate pentru rețele personale - modurile WPA sau WPA2 Personal
	Accesul protejat Wi-Fi (WPA) reprezintă o tehnologie mai sigură decât WEP. WPA poate fi utilizat pentru rețele wireless de tip Întreprindere (aplicații pentru companii) și Personal (rețea de domiciliu). Vă recomandăm cu tărie să selectați WPA-Personal sau WPA2-Personal ca mod de securitate pentru rețeaua de domiciliu, în funcție de modul acceptat de adaptorul wireless de pe PC sau clienții wireless.
	WPA-Personal (denumit și WPA-PSK sau WPA cu cheie pre-partajată) asigură o rețea wireless mai securizată decât WEP. WPA-Personal introduce autentificarea TKIP a utilizatorului și chei de criptare mai puternice decât WEP.
	WPA2-Personal (denumit și WPA2-PSK sau WPA2 cu cheie pre-partajată) asigură cel mai sigur lucru în rețea wireless bazat pe standarde. WPA2-Personal încorporează AES (Advanced Encryption Standard) pentru transmisia de date.
	Notă: Nu toate adaptoarele wireless acceptă WPA2. WPA este acceptat de o gamă mai largă de dispozitive. Indiferent dacă utilizați WPA sau WPA2, asigurați-vă că utilizați o frază de acces „puternică”. O frază de acces puternică este un șir de caractere aleatorii, cu o lungime de cel puțin 21 de caractere.

Secțiune	Descriere câmp
----------	----------------

Selectați unul dintre următoarele trei moduri WPA sau WPA2 Personal:

- **WPA-Personal**
- **WPA2-Personal**
- **WPA sau WPA2-Personal**

The screenshot shows the 'Securitate wireless' configuration page. The 'Mod securitate wireless' dropdown menu is set to 'WPA-Personal'. Below it, the 'Criptare' dropdown is set to 'AES'. The 'Cheie pre-partajată' text input field contains the value '228210229', and the 'Afișare cheie' checkbox is checked. The 'Reînnoire cheie' field is set to '3600' seconds. At the bottom of the form, there are two buttons: 'Salvare setări' and 'Revocare modificări'.

Descrieri câmpuri

- **Criptare.** Setarea implicită este TKIP+AES.
- **Cheie pre-partajată.** Introduceți o cheie de 8 până la 63 de caractere.
- **Reînnoire cheie.** Introduceți o perioadă pentru Reînnoire cheie, care să comunice dispozitivului frecvența modificării cheilor de criptare. Valoarea implicită este de **3.600** de secunde.

Secțiune	Descriere câmp
----------	----------------

Securitate pentru rețele de tip Întreprindere - Moduri WPA-Enterprise

Această opțiune dispune de WPA utilizat în coordonare cu un server RADIUS pentru autentificarea clientului. (Această opțiune trebuie utilizată numai dacă la dispozitiv este conectat un server RADIUS.)

Selectați unul dintre următoarele trei moduri WPA sau WPA2 Enterprise:

- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA sau WPA2-Enterprise**

The screenshot shows a web-based configuration interface for wireless security. The main menu includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. The 'Wireless' section is active, with sub-tabs for 'Setări de bază', 'Securitate wireless', 'Filtru MAC', 'Setări avansate', 'Setări WDS', and 'QoS'. The 'Securitate wireless' tab is selected, showing a form with the following fields: 'Mod securitate wireless' (WPA sau WPA2-Enterprise), 'Criptare' (AES), 'Server RADIUS' (0.0.0.0), 'Port RADIUS' (1645), 'Cheie partajată' (empty), and 'Reînnoire cheie' (3600 secunde). There is an 'Afisare cheie' checkbox next to the shared key field. At the bottom, there are buttons for 'Salvare setări' and 'Revocare modificări'.

Descrieri câmpuri

- **Criptare.** Setarea implicită este TKIP+AES.
- **Server RADIUS.** Introduceți adresa IP a serverului RADIUS.
- **Port RADIUS.** Introduceți numărul portului utilizat de serverul RADIUS. Valoarea implicită este **1812**.
- **Cheie partajată.** Introduceți cheia utilizată de către dispozitiv și serverul RADIUS.
- **Reînnoire cheie.** Introduceți o perioadă pentru Reînnoire cheie, care să comunice dispozitivului frecvența modificării cheilor de criptare. Valoarea implicită este de **3.600** de secunde.

Wireless > Filtru MAC

Caracteristica Filtru MAC este utilizată pentru a permite sau pentru a bloca accesul la rețeaua dumneavoastră LAN în funcție de adresa MAC a dispozitivelor client wireless. Caracteristica Filtru MAC, cunoscută și ca listă de acces, poate fi utilizată pentru a ajuta la protejarea rețelei wireless împotriva accesului utilizatorilor neautorizați.

Selectați fila **Filtru MAC** pentru a deschide pagina Wireless - Filtru MAC.

The screenshot displays the 'Filtru MAC' configuration page. The top navigation bar includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. The 'Wireless' section is active, with sub-tabs for 'Setări de bază', 'Securitate wireless', 'Filtru MAC', 'Setări avansate', 'Setări WDS', and 'QoS'. The 'Filtru MAC' tab is selected.

On the left sidebar, there are links for 'Filtru MAC', 'Restricție de acces', and 'Listă filtru adrese MAC'. The main content area features:

- Radio buttons for **Activare** and **Dezactivare**, with **Dezactivare** selected.
- Radio buttons for **Blocare acces la rețeaua wireless pentru computerele de mai jos** and **Acordare acces la rețeaua wireless pentru computerele de mai jos**.
- A button labeled **Listă clienți wireless**.
- A grid of 32 MAC address input fields, labeled from MAC 01 to MAC 32. Each field contains the placeholder text '00:00:00:00:00:00'.

At the bottom of the page, there are two buttons: **Salvare setări** and **Revocare modificări**.

Descriere pagină Wireless - Filtru MAC

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura filtrarea adreselor MAC din rețeaua wireless pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Filtru MAC	Vă permite să Activați sau să Dezactivați Filtrarea MAC pentru gateway-ul rezidențial
Restricție de acces	Restricție de acces Puteți permite sau bloca accesul computerelor la rețeaua wireless. Selecția făcută aici afectează adresele listate pe această pagină. Alegeți una dintre următoarele opțiuni: <ul style="list-style-type: none">■ Blocați accesul computerelor listate mai jos la rețeaua wireless. Selectați această opțiune pentru a refuza accesul la Internet pentru adresele MAC ale dispozitivelor listate în tabel. Tuturor celorlalte adrese MAC li se va permite accesul la Internet.■ Permiteți accesul computerelor listate mai jos la rețeaua wireless. Selectați această opțiune pentru a permite accesul la Internet doar pentru adresele MAC ale dispozitivelor listate în tabel. Oricărui alte adrese MAC care nu sunt listate în tabel li se va refuza accesul la internet
Listă filtru adrese MAC	Listă filtru adrese MAC Lista filtru adrese MAC afișează utilizatorii al căror acces wireless doriți să îl controlați. Faceți clic pe Listă clienți wireless pentru a afișa o listă cu utilizatorii rețelei în funcție de adresa MAC. Din meniul vertical Pentru sortare puteți ordona tabelul în funcție de Adresă IP, Adresă MAC, Stare, Interfață sau Nume client. Pentru a vizualiza cele mai recente informații, faceți clic pe butonul Reîmprospătare.

Wireless > Setări avansate

Setările wireless avansate adaugă încă un nivel de securitate rețelei wireless pentru gateway-ul dumneavoastră rezidențial. Această pagină este utilizată pentru configurarea funcțiilor wireless avansate. Doar un administrator expert trebuie să ajusteze aceste setări. Setările incorecte pot reduce performanța wireless.

Selecționați fila **Setări avansate** pentru a deschide pagina Wireless - Setări avansate.

Utilizați această pagină pentru a configura următoarele opțiuni:

- Rată de transmisie
- Mod protecție CTS
- Interval semnalizare
- Interval DTM
- Prag fragmentare
- Prag RTS

The screenshot displays the 'Wireless avansat' configuration page. The top navigation bar includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. Below this, a secondary bar shows 'Setări de bază', 'Securitate wireless', 'Filtru MAC', 'Setări avansate' (highlighted), 'Setări WDS', and 'QoS'. The main content area is titled 'Wireless avansat' and contains the following settings:

- Rată de transmisie: Automat (Implicit: Auto)
- Mod protecție CTS: Dezactivare (Implicit: Dezactivare)
- Interval semnalizare: 100 (Implicit: 100 ms, Interval: 1-65535)
- Interval DTIM: 1 (Implicit: 1, Interval: 1-255)
- Prag fragmentare: 2346 (Implicit: 2346, Interval: 256-2346)
- Prag RTS: 2347 (Implicit: 2347, Interval: 0-2347)

At the bottom of the page, there are two buttons: 'Salvare setări' and 'Revocare modificări'.

Descriere pagină Setări wireless avansate

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura setările wireless avansate pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Wireless avansat	<p>Rată de transmisie</p> <p>Rata de transmisie de date trebuie configurată în funcție de viteza rețelei Wireless-N. Selectați dintr-un interval de viteze de transmisie sau selectați Automat pentru ca dispozitivul să utilizeze automat cea mai rapidă rată de transmisie și activați funcția Auto-rezervă. Funcția Auto-rezervă alege cea mai bună viteză posibilă pentru conexiunea dintre dispozitiv și un client wireless. Setarea implicită din fabrică este Automat.</p> <p>Alegeți una dintre următoarele opțiuni pentru rata de transmisie:</p> <ul style="list-style-type: none">■ Automat (implicit din fabrică)■ Utilizare rată moștenită■ 0: 6,5 sau 13,5 Mops■ 1: 13 sau 27 Mops■ 2: 19,5 sau 40,5 Mops■ 3: 26 sau 54 Mops■ 4: 39 sau 81 Mops■ 5: 52 sau 108 Mops■ 6: 58,5 sau 121,5 Mops■ 7: 65 sau 135 Mops■ 8: 13 sau 27 Mops■ 9: 26 sau 54 Mops■ 10: 39 sau 81 Mops■ 11: 52 sau 108 Mops■ 12: 78 sau 162 Mops■ 13: 104 sau 216 Mops■ 14: 117 sau 243 Mops■ 15: 130 sau 270 Mops <hr/> <p>Mod protecție CTS</p> <p>Modul protecție CTS (Clear-To-Send) îmbunătățește posibilitatea dispozitivului de a detecta toate transmisiile wireless, dar poate diminua semnificativ performanțele acestuia. Selectați Automat pentru a utiliza această caracteristică dacă este cazul, atunci când produsele Wireless-N/G nu pot transmite către dispozitiv într-un mediu cu trafic 802.11b ridicat. Selectați Dezactivare pentru a dezactiva permanent această funcție.</p> <hr/>

Secțiune	Descriere câmp
	<p>Interval semnalizare</p> <p>Valoarea intervalului de semnalizare indică intervalul de frecvență al semnalizării. Semnalizarea este un pachet difuzat de către dispozitiv pentru a sincroniza rețeaua wireless.</p> <p>(Implicit: 100 ms, Interval: 20-1.000)</p>
	<p>Interval DTIM</p> <p>Delivery Traffic Indication Message (DTIM) indică intervalul dintre transmisiile Difuzări/Difuzări multiple. Un câmp DTIM este un câmp de numărătoare inversă care informează clienții cu privire la următoarea fereastră pentru ascultarea mesajelor cu difuzare generală sau multiplă. După ce dispozitivul memorează mesajele cu difuzare generală sau multiplă pentru clienții asociați, acesta trimite următorul DTIM cu o frecvență egală cu valoarea intervalului DTIM. Clienții aud semnalele și se pregătesc pentru a recepționa mesajele cu difuzare generală sau multiplă.</p> <p>(Implicit: 1, Interval: 1-255)</p>
	<p>Prag fragmentare</p> <p>Valoarea pragului de fragmentare specifică dimensiunea maximă a unui pachet înainte ca datele să fie fragmentate în mai multe pachete. Dacă vă confrunțați cu o rată mare de eroare a pachetelor, puteți crește ușor pragul de fragmentare. Configurarea pragului de fragmentare la un nivel prea mic poate duce la performanțe slabe ale rețelei. Este recomandată doar o reducere ușoară a valorii implicite. În cele mai multe cazuri, acesta trebuie să rămână la valoarea implicită de 2.346.</p>
	<p>Prag RTS</p> <p>Pragul RTS stabilește care este dimensiunea pachetului peste care este invocat mecanismul gata de transmitere/liber pentru transmitere (RTS/CTS). Dacă vă confrunțați cu fluxuri de date inconsecvente, este recomandată doar o reducere ușoară a valorii implicite, și anume 2.346. Dacă un pachet din rețea este de dimensiuni mai mici decât pragul RTS prestabilit, mecanismul RTS/CTS nu va fi activat. Dispozitivul trimite unități RTS (Request to Send) către un anumit post receptor și negociază trimiterea unui cadru de date. După recepționarea RTS, postul wireless răspunde cu un cadru CTS (Clear to Send) pentru a confirma dreptul de a începe transmisia. Valoarea pragului RTS trebuie să rămână la valoarea sa implicită de 2.347.</p>

Wireless > Setări WDS

Pagina Setări sistem de distribuție wireless (WDS) vă permite să extindeți raza de acoperire a rețelei wireless prin implementarea de amplificatoare de semnal. Asigurați-vă că pentru toate dispozitivele activate prin WDS setările canalului sunt aceleași.

Selectați fila **Setări WDS** pentru a deschide pagina Wireless - Setări WDS. Utilizați această pagină pentru a configura setările WDS.

Descriere pagină Wireless - Setări WDS

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura setările de distribuție wireless pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
WDS	Adresă MAC WDS Afișează adresa MAC WDS (sau BSSID) a punctului de acces al gateway-ului
	Permite semnalului wireless să fie repetat de un amplificator Bifați această casetă pentru a permite unui client wireless să se conecteze la un amplificator și să direcționeze traficul dintre clientul wireless și un amplificator. Sunt permise maximum 3 amplificatoare.
	Adresă MAC punct de acces la distanță (MAC de la 1 la 3) Utilizați cele trei câmpuri (MAC 1, 2 și 3) pentru a introduce adresele MAC ale amplificatoarelor

Wireless > QoS

Calitatea serviciului (QoS) asigură un serviciu mai bun pentru tipuri de trafic în rețea cu prioritate crescută, ce pot presupune aplicații solicitante, în timp real, precum conferințe video. Setările QoS vă permit să specificați priorități pentru diferite tipuri de trafic. Traficul cu prioritate redusă va fi încetinit pentru a permite o rată de transfer mai bună sau întârzieri mai puține pentru traficul cu prioritate ridicată. Selectați fila **QoS** pentru a deschide pagina Wireless - QoS.

The screenshot shows a web interface for configuring wireless settings. The top navigation bar includes 'Configurare', 'Wireless' (highlighted), 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. Below this, a sub-navigation bar contains 'Setări de bază', 'Securitate wireless', 'Filtru MAC', 'Setări avansate', 'Setări WDS', and 'QoS' (highlighted). The main content area is titled 'Calitatea serviciilor (QoS)' and contains a 'Wireless' section with two settings: 'Asistență WMM' (set to 'Activare') and 'Niciun ACK' (set to 'Dezactivare'). A 'Ajutor...' link is visible on the right. At the bottom, there are 'Salvare setări' and 'Revocare modificări' buttons.

Setare	Valoare	Implicite
Asistență WMM:	<input checked="" type="radio"/> Activare	Dezactivare (Implicite: Activare)
Niciun ACK:	<input type="radio"/> Activare	<input checked="" type="radio"/> Dezactivare (Implicite: Dezactivare)

Descriere pagină Wireless - QoS

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura fiecare setare QoS. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

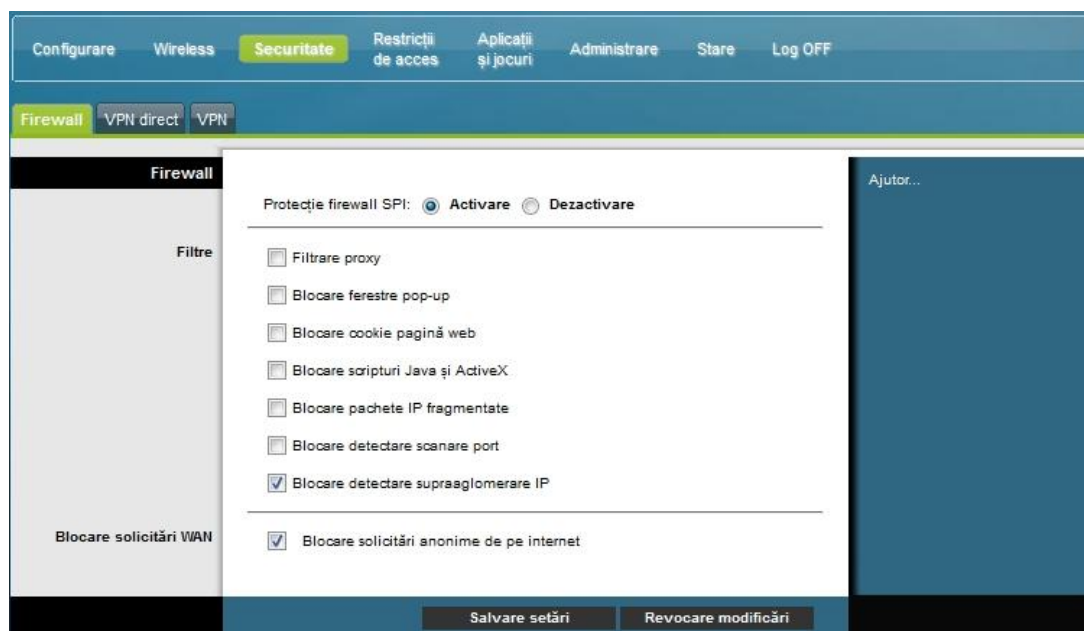
Secțiune	Descriere câmp
Calitatea serviciilor (QoS) Wireless	<p>Asistență WMM</p> <p>Dacă WMM (Multimedia Wi-Fi) este acceptat de către clienții wireless, activarea acestei caracteristici înseamnă că traficul de voce și multimedia va avea o prioritate mai mare față de restul traficului. Selectați opțiunea dorită:</p> <ul style="list-style-type: none">■ Activare (implicit din fabrică)■ Dezactivare <hr/> <p>Niciun ACK</p> <p>Vă permite să activați sau să dezactivați FĂRĂ ACK. Această caracteristică este recomandată pentru serviciile de date unde transmisia este importantă și pierderea de pachete este acceptabilă într-o anumită măsură. Dacă selectați Dezactivare, pentru fiecare pachet recepționat se va returna un pachet de confirmare. Acest lucru permite o transmisie mai sigură, însă încarcă traficul, ceea ce duce la reducerea performanțelor.</p> <p>Selectați opțiunea dorită:</p> <ul style="list-style-type: none">■ Activare■ Dezactivare (implicit din fabrică)

Configurare securitate

Securitate > Firewall

Tehnologia firewall avansată descurajează hackerii și protejează rețeaua de la domiciliu împotriva accesului neautorizat. Utilizați această pagină pentru a configura un firewall care să poată respinge prin filtrare diverse tipuri de trafic nedorit în rețeaua locală a gateway-ului.

Selectați fila **Firewall** pentru a deschide pagina Securitate - Firewall.



Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura firewall-ul pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Firewall	<p>Protecție firewall SPI</p> <p>Protecția firewall SPI blochează atacurile de tip refuz serviciu (DoS). Un atac DoS nu încearcă să fure date sau să avarieze computerul, ci supraîncarcă conexiunea la Internet, astfel încât să nu o puteți utiliza.</p> <p>Selectați opțiunea dorită:</p> <ul style="list-style-type: none"> ■ Activare (implicit din fabrică) ■ Dezactivare

Secțiune	Descriere câmp
Filtre	<p>Filtrare proxy</p> <p>Activează/dezactivează filtrarea proxy. Dacă utilizatorii locali au acces la servere proxy WAN, aceștia pot ignora filtrele de conținut și pot accesa site-uri Internet blocate de către dispozitiv. Dacă selectați funcția Filtrare proxy, aceasta va bloca accesul la orice server proxy WAN.</p> <p>Blocare ferestre pop-up</p> <p>Activează/dezactivează ferestrele pop-up. Unele aplicații uzuale utilizează ferestre pop-up ca parte a aplicației. Dezactivarea ferestrelor pop-up poate interfera cu unele dintre aceste aplicații.</p> <p>Blocare cookie pagină web</p> <p>Activează/dezactivează blocarea cookie-urilor. Această caracteristică filtrează livrarea nesolicitată de cookie-uri de pe Internet către dispozitive din rețeaua dumneavoastră locală. Cookie-urile sunt fișiere de computer care conțin informații personale sau date despre comportamentul de navigare pe Web.</p> <p>Blocare scripturi Java și ActiveX</p> <p>Activează/dezactivează appleturile Java și scripturile ActiveX. Această caracteristică ajută la protejarea dispozitivelor din rețeaua dumneavoastră privată împotriva appleturilor Java iritante sau rău-intenționate care sunt trimise, fără a fi solicitate, către dispozitive din rețeaua dumneavoastră privată de pe Internet. Aceste appleturi se execută automat în momentul în care sunt primite de un PC.</p> <p>Java este un limbaj de programare pentru site-uri Web. Dacă selectați caracteristica Filtrare appleturi Java, este posibil să nu aveți acces la site-uri Internet create cu ajutorul acestui limbaj de programare.</p> <p>Această caracteristică ajută, de asemenea, la protejarea dispozitivelor din rețeaua dumneavoastră privată împotriva controalelor ActiveX iritante sau rău-intenționate care sunt trimise, fără a fi solicitate, către dispozitive din rețeaua dumneavoastră privată de pe Internet. Aceste controale ActiveX se execută automat în momentul în care sunt primite de un PC.</p> <p>Blocare pachete IP fragmentate</p> <p>Activează/dezactivează filtrarea de pachete IP fragmentate. Această caracteristică ajută la protejarea rețelei dumneavoastră locale împotriva atacurilor de tip refuz serviciu lansate de pe Internet.</p> <p>Blocare detectare scanare port</p> <p>Activează/dezactivează răspunsul gateway-ului la scanări ale porturilor efectuate de pe Internet. Această caracteristică este concepută pentru a vă proteja rețeaua locală de hackerii de pe Internet care încearcă să obțină acces neautorizat la rețeaua dumneavoastră detectând porturile IP deschise de pe gateway-ul dumneavoastră.</p> <p>Blocare detectare supraaglomerare IP (bifat - implicit din fabrică)</p> <p>Blochează dispozitivele rău-intenționate care încearcă să supraaglomereze dispozitive sau rețele cu pachete de difuzare ilegale. Această practică mai este cunoscută și drept „furtună de difuzare”.</p>

Secțiune	Descriere câmp
Blocare solicitări WAN	Blocare solicitări anonime de pe internet (bifat – implicit din fabrică) Activați această caracteristică pentru a preveni acțiunile de tip „ping” asupra rețelei sau detectarea rețelei de către alți utilizatori de pe Internet. Caracteristica Blocare solicitări anonime de pe Internet ascunde, de asemenea, porturile rețelei. Ambele fac mai dificilă accesarea rețelei de către utilizatori externi.

Securitate > VPN direct

Utilizați această pagină pentru a configura suportul pentru Rețeaua virtuală privată (VPN). Activarea setărilor de pe această pagină permite tunelelor VPN care utilizează protocoalele IPsec sau PPTP să treacă prin firewall-ul gateway-ului. Selectați fila **VPN direct** pentru a deschide pagina Securitate - VPN direct.



Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura VPN direct pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
VPN direct	<p>IPSec direct</p> <p>Activează/dezactivează protocolul IPsec. IPSec reprezintă o suită de protocoale utilizate pentru a implementa un schimb securizat de pachete la nivelul IP. Dacă activați IPSec direct, aplicațiile care utilizează IPsec (securitate IP) pot trece direct prin firewall. Pentru a dezactiva IPSec direct, selectați Dezactivare.</p> <p>Selectați opțiunea dorită:</p> <ul style="list-style-type: none"> ■ Activare (implicit din fabrică) ■ Dezactivare
	<p>PPTP direct</p> <p>Activează/dezactivează Point-to-Point Tunneling Protocol (PPTP). PPTP permite Point-to-Point Protocol (PPP) să se conecteze prin tunel în cadrul unei rețele IP. Dacă activați PPTP direct, aplicațiile care utilizează Point-to-Point Tunneling Protocol (PPTP) pot trece direct prin firewall. Pentru a dezactiva PPTP direct, selectați Dezactivare.</p> <p>Selectați opțiunea dorită:</p> <ul style="list-style-type: none"> ■ Activare (implicit din fabrică) ■ Dezactivare

Securitate > VPN

O Rețea virtuală privată (VPN) reprezintă o conexiune între două puncte terminale aflate în rețele diferite care permite trimiterea în mod securizat a datelor private prin rețele publice sau alte rețele private. Acest lucru este posibil prin crearea unui „tunel VPN”. Un tunel VPN conectează cele două PC-uri sau rețele și permite transmiterea datelor prin Internet la fel ca într-o rețea privată. Tunelul VPN utilizează IPsec pentru a cripta datele trimise între cele două puncte terminale și încapsulează datele într-un cadru Ethernet/IP normal, permițând acestora să treacă în siguranță și fără probleme între rețele.

O VPN asigură o alternativă rentabilă și mai sigură față de utilizarea unei linii private, dedicate, închiriate pentru o rețea privată. Utilizând tehnicile standard din industrie pentru criptare și autentificare, o VPN IPsec creează o conexiune securizată care funcționează ca și cum ați fi conectat direct la rețeaua dumneavoastră locală.

De exemplu, o VPN permite utilizatorilor să stea acasă și să se conecteze la rețeaua companiei unde lucrează și să primească o adresă IP în rețeaua lor privată, ca și cum ar fi la birou, conectați la rețeaua LAN a companiei.

Selectați fila **VPN** pentru a deschide pagina Securitate - VPN.

Utilizați această pagină pentru a configura VPN pentru gateway-ul rezidențial.

The screenshot displays the Mikrotik WinBox interface for configuring a VPN tunnel. The top navigation bar includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. The 'Securitate' menu is highlighted, and the 'VPN' sub-menu is active. The main content area is titled 'Tunel VPN' and contains the following configuration options:

- Selectare intrare tunel:** A dropdown menu set to '1. (Unnamed)', with 'Creare', 'Stergere', and 'Rezumat' buttons.
- Tunel IPSec VPN:** Radio buttons for 'Activare' and 'Dezactivare', with 'Dezactivare' selected.
- Nume tunel:** An empty text input field.
- Grup securizat local:** Includes 'Subrețea' (Subnet) and 'IP' (0.0.0.0) and 'Mască' (255.255.255.0) fields.
- Grup securizat la distanță:** Includes 'Subrețea' (Subnet) and 'IP' (0.0.0.0) and 'Mască' (255.255.255.0) fields.
- Gateway securizat la distanță:** Includes 'Adresă IP' (IP Address) and 'IP' (0.0.0.0) fields.
- Gestionare chei (Key Management):** Includes 'Metodă schimb de chei' (Key Exchange Method) set to 'Auto (IKE)', 'Criptare' (Encryption) set to '3DES', 'Autentificare' (Authentication) set to 'MD5', 'PFS' (Perfect Forward Secrecy) set to 'Dezactivare', 'Cheie pre-partajată' (Pre-shared Key) masked with dots, and 'Durată de viață cheie' (Key Lifetime) set to '3600 secunde'.
- Stare (Status):** Displays 'NU este conectat' (Not connected).
- Buttons:** 'Conectare', 'Deconectare', 'Vizualizare jurnal', and 'Setări avansate' are located at the bottom of the configuration area.
- Footer Buttons:** 'Salvare setări' and 'Revocare modificări' are located at the very bottom of the page.

Descriere pagină Securitate - Tunel VPN

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura tunelul VPN pentru gateway-ul dumneavoastră. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Tunel VPN	Selectare intrare tunel Vă permite să afișați o listă cu tunelele VPN create Buton Creare Faceți clic pe acest buton pentru a crea o intrare nouă pentru tunel Buton Ștergere Faceți clic pe acest buton pentru a șterge toate setările pentru tunelul selectat Buton Rezumat Faceți clic pe acest buton pentru a afișa setările și starea tuturor tunelelor activate Tunel IPSec VPN Vă permite să activați sau să dezactivați protocolul IPSec pentru tunelul VPN Nume tunel Introduceți numele pentru acest tunel
Grup securizat local	Selectați utilizatorul (utilizatorii) din rețeaua locală care poate (pot) folosi acest tunel VPN. Poate fi o adresă IP unică sau o subrețea. Rețineți că grupul securizat local trebuie să corespundă cu grupul securizat la distanță al gateway-ului la distanță. IP Introduceți adresa IP a rețelei locale. Mască Dacă este selectată opțiunea Subrețea, introduceți masca pentru a stabili adresa IP din rețeaua locală
Grup securizat la distanță	Selectați utilizatorul (utilizatorii) LAN la distanță, aflat (afilați) după gateway-ul la distanță, care poate (pot) utiliza acest tunel VPN. Poate fi o adresă IP unică, o subrețea sau orice adrese. Dacă este aleasă setarea „Oricare”, gateway-ul se comportă ca un respondent și acceptă solicitări de la orice utilizator la distanță. Rețineți că grupul securizat la distanță trebuie să corespundă cu grupul securizat local al gateway-ului la distanță. IP Introduceți adresa IP a rețelei la distanță Mască Dacă este selectată opțiunea Subrețea, introduceți masca pentru a stabili adresele IP din rețeaua la distanță

Secțiune	Descriere câmp
Gateway securizat la distanță	<p>Selecționați opțiunea dorită, Adresă IP, Oricare sau FQDN. Dacă gateway-ul la distanță are o adresă IP dinamică, selecționați Oricare sau FQDN. Dacă este selectat Oricare, atunci gateway-ul va accepta solicitări de la orice adresă IP.</p> <p>FQDN</p> <p>Dacă este selectat FQDN, introduceți numele de domeniu al gateway-ului la distanță, astfel încât gateway-ul să poată localiza o adresă IP curentă utilizând DDNS</p> <p>IP</p> <p>Adresa IP din acest câmp trebuie să corespundă adresei IP publice (WAN sau Internet) a gateway-ului de la celălalt capăt al acestui tunel</p>
Gestionare chei	<p>Metodă schimb de chei</p> <p>Dispozitivul acceptă atât gestionarea manuală, cât și gestionarea automată a cheilor. Dacă este selectată gestionarea automată a cheilor, protocoalele Internet Key Exchange (IKE) sunt utilizate pentru a negocia materialul cheilor pentru asocierea de securitate (SA). Dacă este selectată gestionarea manuală a cheilor, nu este necesară negocierea cheilor. Pe scurt, gestionarea manuală a cheilor este utilizată în medii statice de dimensiuni reduse sau pentru operațiuni de depanare. Rețineți că ambele părți trebuie să utilizeze aceeași metodă de gestionare a cheilor.</p> <p>Selecționați una dintre următoarele opțiuni pentru metoda de schimbare a cheilor:</p> <ul style="list-style-type: none"> ■ Auto (IKE) <ul style="list-style-type: none"> – Criptare: Metoda Criptare stabilește lungimea cheii utilizate pentru a cripta/decripta pachete ESP. Rețineți că ambele părți trebuie să utilizeze aceeași metodă. – Autentificare: Metoda Autentificare autentifică pachetele Encapsulating Security Payload (ESP). Selecționați MD5 sau SHA. Rețineți că ambele părți (terminale VPN) trebuie să utilizeze aceeași metodă. <ul style="list-style-type: none"> ▪ MD5: un algoritm hash unidirecțional care produce o criptare pe 128 de biți ▪ SHA: un algoritm hash unidirecțional care produce o criptare pe 160 de biți – PFS: Dacă PFS este activat, etapa 2 a negocierii IKE va genera un nou material de chei pentru criptarea și autentificarea traficului IP. Rețineți că ambele părți trebuie să aibă PFS activat. – Cheie pre-partajată: IKE utilizează opțiunea Cheie pre-partajată pentru a autentifica perechea IKE la distanță. În acest câmp sunt acceptate atât caractere, cât și valori hexazecimale, de ex. „Eu_@123” sau „0x4d795f40313233”. Rețineți că ambele părți trebuie să utilizeze aceeași cheie pre-partajată. – Durată de viață cheie: Acest câmp specifică durata de viață a cheii generate prin metoda IKE. Dacă această durată expiră, se va renegocia automat o altă cheie. Durata de viață a cheii poate varia între 300 și 100.000.000 de secunde. Durata de viață implicită este 3.600 de secunde.

Secțiune	Descriere câmp
Gestionare chei (continuare)	<p>Manual</p> <ul style="list-style-type: none"> – Criptare: Metoda Criptare stabilește lungimea cheii utilizate pentru a cripta/decripta pachete ESP. Rețineți că ambele părți trebuie să utilizeze aceeași metodă. – Cheie de criptare: Acest câmp specifică o cheie utilizată pentru criptarea și decriptarea traficului IP. În acest câmp, sunt acceptate atât caractere, cât și valori hexazecimale. Rețineți că ambele părți trebuie să utilizeze aceeași cheie de criptare. – Autentificare: Metoda Autentificare autentifică pachetele Encapsulating Security Payload (ESP). Selectați MD5 sau SHA. Rețineți că ambele părți (terminale VPN) trebuie să utilizeze aceeași metodă. <ul style="list-style-type: none"> ▪ MD5: un algoritm hash unidirecțional care produce o criptare pe 128 de biți ▪ SHA: un algoritm hash unidirecțional care produce o criptare pe 160 de biți – Cheie de autentificare: Acest câmp specifică o cheie utilizată pentru autentificarea traficului IP. În acest câmp, sunt acceptate atât caractere, cât și valori hexazecimale. Rețineți că ambele părți trebuie să utilizeze aceeași cheie de autentificare. – SPI de intrare/SPI de ieșire: Indexul parametrilor de securitate (SPI) se află în antetul ESP. Acest lucru permite receptorului să selecteze SA corespunzătoare pentru procesarea pachetului. SPI este o valoare pe 32 de biți. Sunt acceptate atât caractere, cât și valori hexazecimale. De ex. „987654321” sau „0x3ade68b1”. Fiecare tunel trebuie să aibă SPI de intrare și SPI de ieșire unice. Două tuneluri nu pot partaja același SPI. Rețineți că SPI de intrare trebuie să corespundă cu SPI de ieșire al gateway-ului la distanță și invers.
Stare	Acest câmp afișează starea conectării pentru tunelul selectat. Starea poate fi Conectat sau Deconectat .

Secțiune	Descriere câmp
Butoane	<p data-bbox="396 321 521 352">Conectare</p> <p data-bbox="396 363 1425 457">Faceți clic pe acest buton pentru a stabili o conexiune pentru tunelul VPN curent. Dacă ați efectuat vreo modificare, faceți clic pe Salvare setări pentru a aplica mai întâi modificările.</p> <p data-bbox="396 468 548 499">Deconectare</p> <p data-bbox="396 510 1386 541">Faceți clic pe acest buton pentru a întrerupe o conexiune pentru tunelul VPN curent.</p> <p data-bbox="396 552 618 583">Vizualizare jurnal</p> <p data-bbox="396 594 1398 657">Faceți clic pe acest buton pentru a vizualiza jurnalul VPN, care afișează detalii pentru fiecare tunel stabilit.</p> <p data-bbox="396 667 581 699">Setări avansate</p> <p data-bbox="396 709 1377 835">Dacă metoda de schimb de chei este Automat (IKE), acest buton permite accesul la setări suplimentare pentru IKE. Faceți clic pe acest buton dacă gateway-ul nu poate stabili un tunel VPN către dispozitivul gateway-ului la distanță și asigurați-vă că Setările avansate corespund cu cele ale gateway-ului la distanță.</p> <ul style="list-style-type: none"> <li data-bbox="396 846 797 877">■ Etapă 1 - Mod de funcționare <ul style="list-style-type: none"> <li data-bbox="443 888 1159 919">Selectați metoda potrivită pentru terminalul VPN la distanță. <li data-bbox="443 930 1122 961">– Principal: modul Principal este mai lent, dar mai sigur <li data-bbox="443 972 1182 1003">– Agresiv: modul Agresiv este mai rapid, dar mai puțin sigur <li data-bbox="396 1014 643 1045">■ Identitate locală <ul style="list-style-type: none"> <li data-bbox="443 1056 1414 1119">Selectați opțiunea dorită pentru a corespunde cu setarea Identitate la distanță de la celălalt capăt al acestui tunel. <li data-bbox="443 1129 1179 1161">– Adresă IP locală: adresa dumneavoastră IP WAN (Internet) <li data-bbox="443 1171 992 1203">– Nume: numele domeniului dumneavoastră <li data-bbox="396 1213 699 1245">■ Identitate la distanță <ul style="list-style-type: none"> <li data-bbox="443 1255 1360 1318">Selectați opțiunea dorită pentru a corespunde cu setarea Identitate locală de la celălalt capăt al tunelului. <li data-bbox="443 1329 1357 1360">– Adresă IP locală: adresa IP WAN (Internet) a terminalului VPN la distanță <li data-bbox="443 1371 1187 1402">– Nume: numele de domeniu al terminalului VPN la distanță. <li data-bbox="396 1413 548 1444">■ Criptare <ul style="list-style-type: none"> <li data-bbox="443 1455 1425 1499">Acesta este algoritmul de criptare utilizat pentru SA IKE. Trebuie să corespundă cu setarea utilizată la celălalt capăt al tunelului.

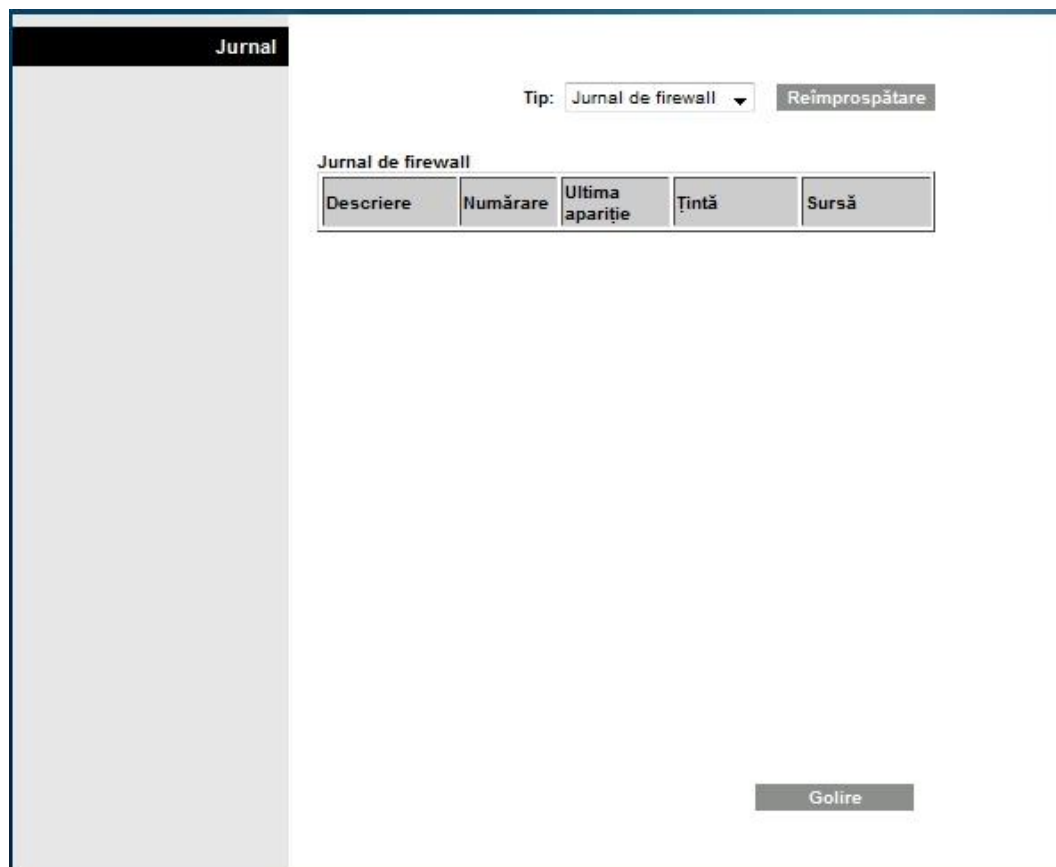
Vizualizare jurnal

Pagina Securitate - VPN - Vizualizare jurnal prezintă evenimentele capturate de firewall. Jurnalul afișează următoarele elemente:

- Descrierea evenimentului
- Numărul de evenimente petrecute
- Ultima apariție a unui eveniment
- Adresele țintă și sursă

Puteți vizualiza următoarele jurnale din această pagină:

- Jurnal de acces
- Jurnal de firewall
- Jurnal VPN
- Jurnal de control parental



Faceți clic pe **Golire** pentru a goli datele din jurnal.

Controlarea accesului la gateway

Restricții de acces > Filtrare adrese IP

Utilizați pagina Restricții de acces - Filtrare IP pentru a configura filtrele de adrese IP. Aceste filtre blochează accesul la Internet pentru o serie de adrese IP.

Notă: dacă nu sunteți familiarizat cu setările avansate detaliate în această secțiune, contactați furnizorul de servicii înainte de a încerca să modificați oricare dintre setările avansate implicite de filtrare IP ale gateway-ului rezidențial.

Selectați fila **Filtrare adrese IP** pentru a deschide pagina Restricții de acces - Filtrare adrese IP. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

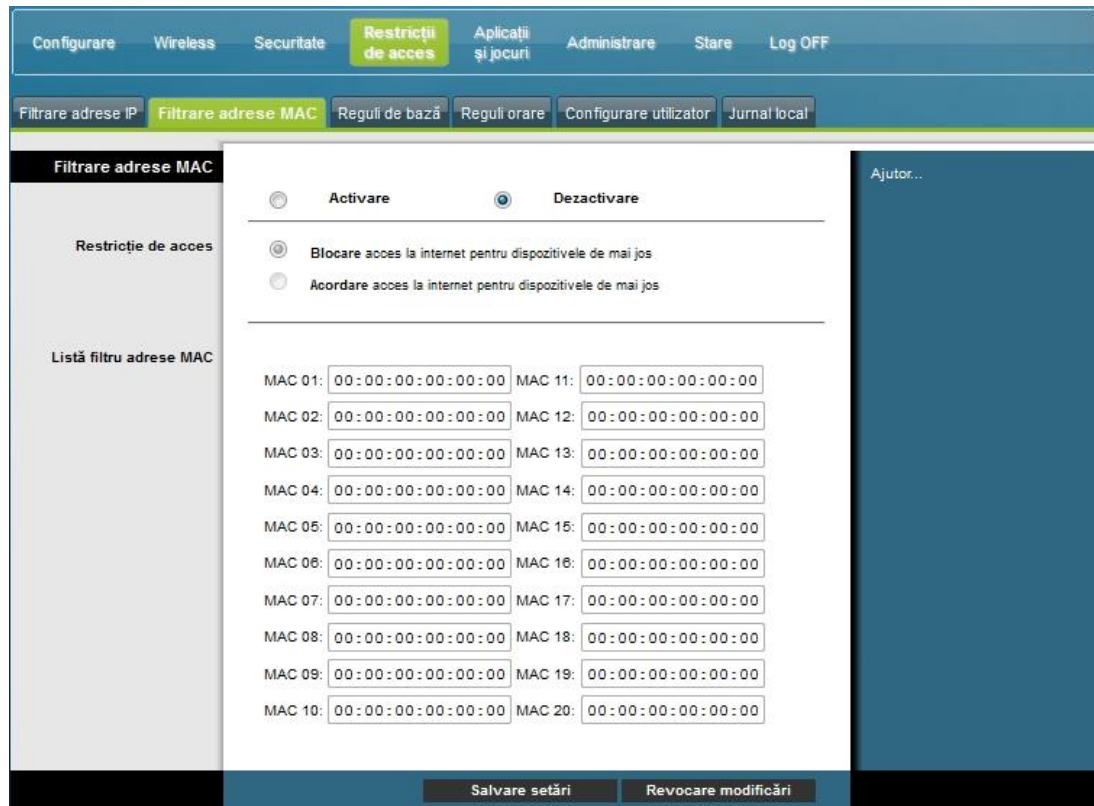
Adresă de început	Adresă de sfârșit	Activare
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>

Restricții de acces > Filtrare adrese MAC

Utilizați pagina Restricții de acces - Filtrare adrese MAC pentru a configura filtrele de adrese MAC. Cu ajutorul acestor filtre puteți permite sau bloca accesul la Internet pentru o serie de adrese MAC pe baza adresei MAC.

Notă: dacă nu sunteți familiarizat cu setările avansate detaliate în această secțiune, contactați furnizorul de servicii înainte de a încerca să modificați oricare dintre setările avansate implicite de filtrare IP ale gateway-ului rezidențial.

Selecțai fila **Filtrare adrese MAC** pentru a deschide pagina Restricții de acces - Filtrare adrese MAC.



Meniul vertical Blocare/Permitere vă permite să blocați sau să acordați acces la Internet adreselor MAC ale dispozitivelor pe care le enumerați în tabelul Filtre adrese MAC. Următorul tabel descrie funcția meniului vertical Blocare/Permitere. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Nume câmp	Descriere
Filtrare adrese MAC	<p>Blocare acces la internet pentru dispozitivele de mai jos Selectați Blocare acces la internet pentru dispozitivele de mai jos pentru a refuza accesul la Internet adreselor MAC ale dispozitivelor listate în tabel. Oricăror alte adrese MAC li se va permite accesul la internet.</p> <p>Acordare acces la internet pentru dispozitivele de mai jos Selectați Acordare acces la internet pentru dispozitivele de mai jos pentru a permite accesul la Internet doar adreselor MAC ale dispozitivelor listate în tabel. Oricăror alte adrese MAC care <i>nu</i> sunt listate în tabel li se va refuza accesul la internet</p>

Butoane cu funcții

Următoarele butoane cu funcții apar pe pagina Setări avansate - Filtrare adrese MAC.

Buton	Descriere
Aplicare	Salvează valorile pe care le introduceți în câmpuri, fără a închide pagina
Adăugare adresă MAC	Salvează adresa MAC introdusă în câmpul text corespunzător
Eliminare adresă MAC	Elimină adresa MAC selectată
Golire toate	Elimină toate adresele MAC definite

Restricții de acces > Reguli de bază

Restricțiile de acces vă permit să blocați sau să aprobați modalitățile specifice de utilizare sau de trafic pe Internet, cum ar fi accesul la Internet, aplicațiile specifice, site-urile Web și traficul de intrare în anumite zile sau intervale orare. Pagina Restricții de acces - Reguli de bază vă permite să configurați controale parentale pe gateway-ul rezidențial și să monitorizați persoanele care sunt autorizate să seteze controale parentale.

Controlarea accesului la gateway

Selecțai fila **Reguli de bază** pentru a deschide pagina Restricții de acces - Reguli de bază.

The screenshot shows the 'Reguli de bază' (Basic Rules) configuration page. The top navigation bar includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. Below this, a secondary bar contains 'Filtrare adrese IP', 'Filtrare adrese MAC', 'Reguli de bază', 'Reguli orare', 'Configurare utilizator', and 'Jurnal local'. The main content area is titled 'Configurare de bază control parental' and contains several sections:

- Activare control parental:** A checkbox for 'Activare control parental' with an 'Aplicare' button below it.
- Setări regulă:** A section for adding and managing rules, including an 'Adăugare regulă' button, a dropdown menu showing '1. Default', and an 'Eliminare regulă' button.
- Listă cuvinte cheie:** A section for adding and removing keywords, featuring a text input field, an 'Adăugare cuvânt cheie' button, and an 'Eliminare cuvânt cheie' button.
- Listă domenii blocate:** A section for adding and removing blocked domains, featuring a text input field, an 'Adăugare domeniu' button, and an 'Eliminare domeniu' button.
- Listă domenii permise:** A section for adding and removing permitted domains, featuring a text input field, an 'Adăugare domeniu permis' button, and an 'Eliminare domeniu permis' button.
- Înlocuire parolă:** A section for password replacement, including fields for 'Parolă', 'Introduceți din nou parola', and 'Durată acces' (set to 30), with an 'Aplicare' button.

An 'Ajutor...' link is visible on the right side of the page.

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura regulile de bază pentru restricțiile de acces pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Configurare de bază control parental	<p>Activare control parental</p> <p>Vă permite să activați sau să dezactivați controale parentale. Pentru a activa controale parentale, bifați caseta de selectare Activare control parental și faceți clic pe Aplicare. Pentru a dezactiva controale parentale, debifați caseta de selectare Activare control parental și faceți clic pe Aplicare.</p> <p>Adăugare regulă</p> <p>Adaugă și salvează o Regulă nouă la lista de reguli pentru conținut</p> <p>Eliminare regulă</p> <p>Elimină regula selectată din lista cu reguli pentru conținut</p>
Listă cuvinte cheie	<p>Listă cuvinte cheie</p> <p>Vă permite să creați o listă cu cuvinte cheie. Orice încercare de a accesa un URL care conține oricare dintre cuvintele cheie din această listă va fi blocată de către gateway</p> <p>Adăugare/Eliminare cuvânt cheie</p> <p>Vă permite să adăugați cuvinte cheie noi la listă sau să ștergeți cuvintele cheie selectate din listă</p>
Listă domenii blocate	<p>Listă domenii blocate</p> <p>Vă permite să creați o listă de domenii la care gateway-ul trebuie să blocheze accesul. Orice încercare de a accesa oricare dintre domeniile din această listă va fi blocată de către gateway</p> <p>Adăugare/Eliminare domeniu</p> <p>Vă permite să adăugați domenii noi la listă sau să ștergeți domeniile selectate din listă</p>
Listă domenii permise	<p>Listă domenii permise</p> <p>Vă permite să creați o listă cu domenii la care gateway-ul să permită accesul</p> <p>Adăugare/Eliminare domeniu permis</p> <p>Vă permite să adăugați domenii noi la listă sau să ștergeți domeniile selectate din listă</p>

Secțiune	Descriere câmp
Înlocuire parolă	<p>Parolă</p> <p>Vă permite să creați o parolă pentru înlocuirea temporară a restricțiilor de acces pentru utilizator la un site Internet blocat</p> <p>Introduceți din nou parola</p> <p>Reintroduceți aceeași parolă pentru confirmarea parolei de înlocuire din câmpul anterior</p> <p>Durată acces</p> <p>Vă permite să stabiliți o perioadă de timp, în minute, pentru care parola de înlocuire va permite accesul temporar la un site Internet restricționat</p> <p>Aplicare</p> <p>Salvează toate adăugirile, editările și modificările</p>

Pentru a utiliza blocarea cuvintelor cheie și a domeniilor

Blocarea cuvintelor cheie și a domeniilor vă permite să restricționați accesul la site-uri Internet prin blocarea accesului la acele site-uri pe baza unui cuvânt sau a unui șir text conținut de URL-urile utilizate pentru accesarea site-urilor Internet respective.

Blocarea domeniilor vă permite să restricționați accesul la site-uri Web pe baza numelui de domeniu al site-ului. Numele de domeniu reprezintă partea din URL care precede cunoscuta extensie .COM, .ORG sau .GOV.

Blocarea cuvintelor cheie vă permite să blocați accesul la site-uri Internet pe baza unui cuvânt cheie sau a unui șir text care se află oriunde în URL, nu doar în numele de domeniu.

Notă: Caracteristica de blocare a domeniilor blochează accesul la orice domeniu din Lista de domenii. Va bloca, de asemenea, domenii care conțin, în orice porțiune a lor, o potrivire exactă cu intrările din listă.

De exemplu, dacă introduceți **exemplu.com** ca domeniu, orice site care conține „exemplu.com” va fi blocat. În general, nu este recomandat să includeți „www.” într-un nume de domeniu, deoarece acest lucru limitează blocarea exclusiv la site-ul care se potrivește exact cu numele de domeniu. De exemplu, dacă introduceți **www.exemplu.com** în listă, doar site-ul care se potrivește exact acestui nume va fi blocat. Prin urmare, dacă nu includeți „www.”, toate site-urile din cadrul **exemplu.com**, precum și cele asociate acestuia, vor fi blocate.

Blocare acces la site-uri Web

Dacă doriți să blocați accesul la site-uri Web, utilizați **Lista domeniilor blocate** sau **Lista cuvintelor cheie**

Pentru a utiliza **Lista domeniilor blocate**, introduceți URL-urile sau numele de domenii ale site-urilor Web pe care doriți să le blocați.

Utilizați **Lista cuvintelor cheie** pentru a introduce cuvintele cheie pe care doriți să le blocați. Dacă vreunul dintre aceste cuvinte cheie apare în adresa URL a unui site Web, accesul la acel site va fi blocat. Rețineți că este verificată numai adresa URL, nu și conținutul fiecărei pagini Web.

Restricții de acces > Reguli orare

Utilizați pagina Restricții de acces - Reguli orare pentru a configura filtre de acces Web pentru a bloca întreg traficul Internet către și de la dispozitive din rețea specifice, în funcție de ziua din săptămână și de ora din zi pe care le selectați.

Selectați fila **Reguli orare** pentru a deschide pagina Restricții de acces - Reguli orare. Următoarea ilustrație este un exemplu de pagină Restricții de acces - Reguli orare.

Notă: Gateway-ul rezidențial utilizează ceasul de rețea gestionat de către furnizorul dumneavoastră de servicii de date. Ceasul trebuie să fie exact și să reprezinte ora din fusul dumneavoastră orar pentru ca această caracteristică să funcționeze corespunzător. Verificați dacă paginile Stare și Setare oră reflectă ora corectă. Dacă nu reflectă ora corectă, contactați furnizorul de servicii de date. Puteți, de asemenea, să ajustați dumneavoastră setările pentru a compensa diferența.

The screenshot displays the 'Reguli orare' (Time Rules) configuration page. The interface includes a navigation menu at the top with options like 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. Below the navigation, there are tabs for 'Filtrare adrese IP', 'Filtrare adrese MAC', 'Reguli de bază', 'Reguli orare', 'Configurare utilizator', and 'Jurnal local'. The main content area is titled 'Filtru ToD' and contains the following elements:

- An input field for adding a rule, with an 'Adăugare' (Add) button.
- A dropdown menu showing 'Nu a fost introdus niciun filtru.' (No filter has been introduced), an 'Activat' (Activated) checkbox, and an 'Eliminare' (Delete) button.
- A section for 'Zile de blocare' (Block days) with checkboxes for 'În fiecare zi' (Every day), 'Duminică' (Sunday), 'Luni' (Monday), 'Marți' (Tuesday), 'Miercuri' (Wednesday), 'Joi' (Thursday), 'Vineri' (Friday), and 'Sâmbătă' (Saturday).
- A section for 'Timp de blocare' (Block time) with a 'Toată ziua' (All day) checkbox.
- Time selection fields: 'Început:' (Start) and 'Sfârșit:' (End), each with dropdowns for hours (12), minutes (00), and AM/PM.
- Buttons at the bottom: 'Salvare setări' (Save settings) and 'Revocare modificări' (Revoke changes).

Descriere pagină Restricții de acces - Reguli orare

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura orare pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Filtru ToD	Adăugare Vă permite să adăugați un filtru sau o regulă orară nouă. Introduceți numele filtrului și faceți clic pe butonul Adăugare pentru a adăuga filtrul la listă. Regulile orare sunt utilizate pentru a restricționa accesul la Internet în funcție de zi și de oră. Eliminare Elimină filtrul selectat din lista cu filtre orare
Program	Zile de blocare Vă permite să controlați accesul în funcție de zilele săptămânii Timp de blocare Vă permite să controlați accesul în funcție de ora din zi

Restricții de acces > Configurare utilizator

Utilizați pagina Restricții de acces - Configurare utilizator pentru a configura conturi suplimentare și profiluri de utilizator pentru membrii familiei. Fiecărui profil îi pot fi atribuite niveluri individualizate de acces la Internet, după cum sunt definite de regulile de acces atribuite profilului utilizatorului respectiv.

Important: Aceste conturi suplimentare nu oferă acces administrativ la gateway.

Notă: Odată ce definiți și activați profiluri de utilizator, fiecare utilizator trebuie să se autentifice ori de câte ori dorește să acceseze Internetul. Utilizatorul se poate autentifica în momentul în care apare ecranul pop-up de autentificare în browserul Web. Utilizatorul trebuie să introducă numele de utilizator și parola corecte pentru a obține acces la Internet.

Selecționați fila **Configurare utilizator** pentru a deschide pagina Restricții de acces - Configurare utilizator.

Descriere pagină Restricții de acces - Configurare utilizator

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura setările de utilizator pentru gateway-ul dumneavoastră rezidențial. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Configurare utilizator	Adăugare utilizator Vă permite să adăugați un profil de utilizator nou. Introduceți numele utilizatorului și faceți clic pe butonul Adăugare utilizator pentru a adăuga utilizatorul la listă.
	Setări utilizator Vă permite să editați un profil de utilizator cu ajutorul meniului vertical pentru editarea unui profil de utilizator. Meniul vertical vă permite să apăsați profilul ce urmează a fi editat. Numele de utilizator și parolele sunt sensibile la majuscule și minuscule. Asigurați-vă că bifați caseta Activare pentru a activa profilul utilizatorului. Dacă un profil nu este activ, utilizatorul respectiv nu va avea acces la Internet. Pentru a elimina un profil de utilizator, utilizați meniul vertical pentru a selecta utilizatorul care să fie eliminat și faceți clic pe butonul Eliminare utilizator .

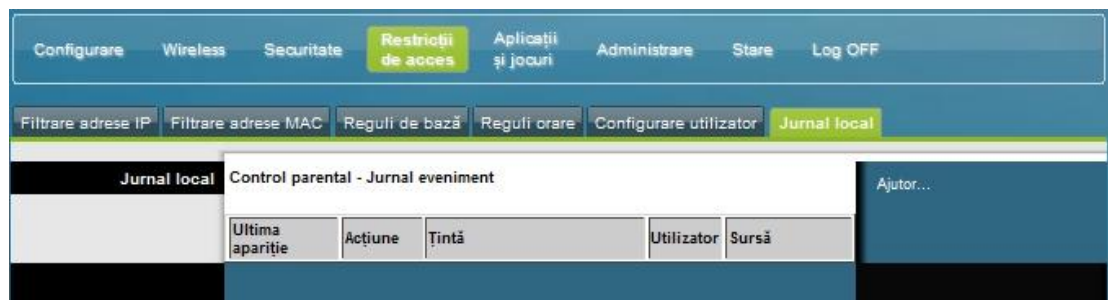
Secțiune	Descriere câmp
	<p>Parolă</p> <p>Introduceți în acest câmp parola utilizatorului selectat. Fiecare utilizator trebuie să introducă propriul nume de utilizator și propria parolă ori de câte ori utilizează Internetul. Numele de utilizator și parolele sunt sensibile la majuscule și minuscule.</p> <p>Notă: Gateway-ul rezidențial va permite fiecărui utilizator să acceseze Internetul, sub restricția regulilor selectate pe această pagină pentru utilizatorul respectiv.</p> <p>Introduceți din nou parola</p> <p>Reintroduceți aceeași parolă pentru confirmarea parolei din câmpul anterior</p> <p>Utilizator de încredere</p> <p>Bifați această casetă dacă utilizatorul selectat în momentul respectiv este desemnat ca fiind utilizator de încredere. Utilizatorii de încredere nu fac obiectul regulilor de acces la Internet.</p> <p>Regulă cu privire la conținut</p> <p>Selectați Regula cu privire la conținut pentru profilul utilizatorului curent. Regulile cu privire la conținut trebuie, mai întâi, definite, accesând pagina Configurare reguli. Puteți accesa pagina Configurare reguli făcând clic pe fila „Reguli de bază” din această pagină.</p> <p>Regulă de acces cu privire la oră</p> <p>Selectați Regula de acces cu privire la oră pentru profilul utilizatorului curent. Regulile de acces cu privire la oră trebuie, mai întâi, definite, accesând pagina Reguli orare. Puteți accesa pagina Reguli orare făcând clic pe fila „Reguli orare” din această pagină.</p> <p>Durăta sesiune</p> <p>1.440 de minute [Implicit din fabrică, atunci când este creat un utilizator. Altfel, este 0 (zero)].</p> <p>Introduceți durata în minute pentru care utilizatorul va beneficia de acces la Internet, începând cu ora la care se autentifică folosind numele de utilizator și parola.</p> <p>Notă: Setați durata sesiunii la 0 (zero) pentru a preveni expirarea sesiunii.</p> <p>Timp de inactivitate</p> <p>60 de minute [Implicit din fabrică, atunci când este creat un utilizator. Altfel, este 0 (zero)].</p> <p>Introduceți durata din timpul unei sesiuni a unui utilizator în care nu există activitate pe Internet și care să indice că utilizatorul nu mai este online. Dacă este declanșat contorul de inactivitate, sesiunea utilizatorului se va închide automat. Pentru a redobândi accesul la Internet, utilizatorul trebuie să se logheze din nou cu numele de utilizator și cu parola.</p> <p>Notă: Setați Valoarea timpului de inactivitate la 0 (zero) pentru a preveni expirarea sesiunii.</p>

Restricții de acces > Jurnal local

Această pagină vă permite să urmăriți, în funcție de utilizator, orice încercare făcută de utilizatorul respectiv de a accesa site-uri Internet restricționate. Tot din această pagină puteți vizualiza evenimentele capturate de caracteristica de raportare a evenimentelor de control parental.

Selectați fila **Jurnal local** pentru a deschide pagina Restricții de acces - Jurnal local.

Următoarea ilustrație este un exemplu de pagină Restricții de acces - Jurnal local.



Secțiune	Descriere câmp
Jurnal local	Ultima apariție
Control parental - Jurnal eveniment	Afișează ora celei mai recente încercări de a accesa un site Internet restricționat
	Acțiune
	Afișează acțiunea întreprinsă de sistem
	Țintă
	Afișează URL-ul site-ului restricționat
	Utilizator
	Afișează utilizatorul care a încercat să acceseze un site restricționat
	Sursă
	Afișează adresa IP a PC-ului care a fost utilizat în încercarea de a accesa un site Web restricționat

Configurarea aplicațiilor și a jocurilor

Prezentare generală

Majoritatea celor mai cunoscute aplicații Internet sunt acceptate de Gateway-uri la nivel de aplicație (ALG). ALG ajustează automat firewall-ul gateway-ului pentru a permite trecerea datelor fără a efectua nicio setare individualizată. Vă recomandăm să testați aplicația înainte de a efectua modificări în această secțiune.

Aplicații și jocuri > Filtrare porturi

Utilizați această fereastră pentru a configura filtrele pentru porturile protocolului de control al transmisiei (TCP) și al protocolului pentru diagrama informațiilor utilizatorului (UDP). Aceste filtre împiedică accesul la internet pentru anumite porturi TCP/UDP. Puteți bloca, de asemenea, traficul de ieșire TCP/UDP de pe PC-uri către WAN, pentru anumite numere de porturi IP. Acest filtru nu este bazat pe adrese IP sau adrese MAC. Sistemul blochează intervalele de porturi specificate pentru toate PC-urile.

Selectați fila **Filtrare porturi** pentru a deschide pagina Aplicații și jocuri - Filtrare porturi.

The screenshot displays the 'Filtrare porturi' configuration page. At the top, there is a navigation bar with tabs: Configurare, Wireless, Securitate, Restricții de acces, **Aplicații și jocuri**, Administrare, Stare, and Log OFF. Below this, there are sub-tabs: **Filtrare porturi**, Redirecționare interval de porturi, Declanșare interval de porturi, and DMZ. The main content area is titled 'Filtrare porturi' and contains a table with the following structure:

Port de început	Port de sfârșit	Protocol	Activare
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>
0	0	Ambele	<input type="checkbox"/>

At the bottom of the page, there are two buttons: 'Salvare setări' (Save settings) and 'Revocare modificări' (Revoke changes). On the right side, there is a link for 'Ajutor...' (Help...).

Descriere pagină Aplicații și jocuri - Filtrare porturi

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura caracteristicile de filtrare a porturilor pentru aplicații și jocuri utilizate pe gateway-ul dumneavoastră rezidențial. Faceți clic pe caseta de selectare **Activare** pentru a activa redirectionarea de porturi pentru aplicația respectivă. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Filtrare porturi	Port de început: Acesta este începutul intervalului de porturi. Introduceți începutul intervalului de numere de porturi (porturi externe) utilizate de server sau de aplicația pe Internet. Dacă este necesar, pentru mai multe informații, consultați documentația software a aplicației pe Internet.
	Port de sfârșit: Acesta este sfârșitul intervalului de porturi. Introduceți sfârșitul intervalului de numere de porturi (porturi externe) utilizate de server sau de aplicația pe Internet. Dacă este necesar, pentru mai multe informații, consultați documentația software a aplicației pe Internet.
	Protocol Selectați unul dintre următoarele protocoale: <ul style="list-style-type: none"> ■ TCP ■ UDP ■ Ambele
	Activare: Bifați această casă pentru a activa filtrarea pe porturile specificate.

Aplicații și jocuri > Redirecționare interval de porturi

Important: În mod normal, gateway-ul implementează o caracteristică denumită Translatarea porturilor. Translatarea porturilor monitorizează care sunt porturile utilizate efectiv de către PC-uri sau de către alte dispozitive din rețeaua dumneavoastră LAN. Această monitorizare asigură un nivel suplimentar de securitate, în plus față de ce oferă firewall-ul. Totuși, există unele aplicații care necesită ca gateway-ul să utilizeze anumite porturi pentru a se conecta prin Internet.

Utilizați Redirecționare interval de porturi pentru a redirecționa porturi de la rețeaua publică de Internet către adrese IP specifice din rețeaua dumneavoastră locală. Selectați fila **Redirecționare interval de porturi** pentru a deschide pagina Aplicații și jocuri - Redirecționare interval de porturi.

Descriere pagină Aplicații și jocuri - Redirecționare interval de porturi

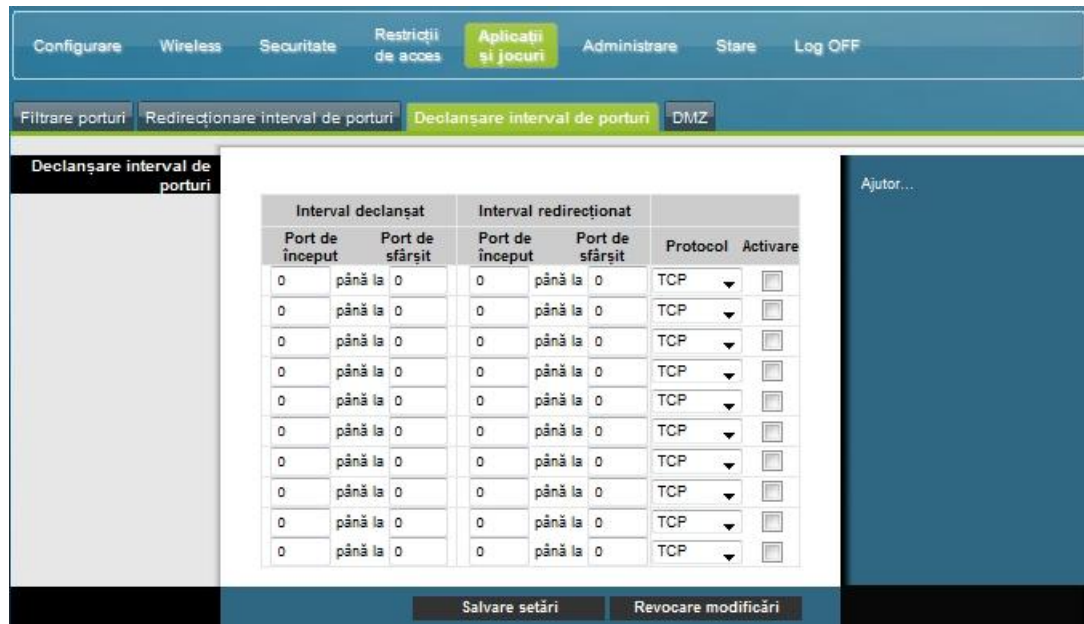
Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura redirecționarea intervalului de porturi pentru gateway-ul rezidențial. Selectați Activare pentru ambele. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Redirecționare interval de porturi	Început Pentru Portul de început, selectați un port din intervalul recomandat 49152 - 65535. Rețineți că porturile utilizate sunt specifice programului, așa că verificați care sunt cele a căror redirecționare o necesită programul.
	Sfârșit Pentru Portul de sfârșit, selectați un port din intervalul recomandat 49152 - 65535. Rețineți că porturile utilizate sunt specifice programului, așa că verificați care sunt cele a căror redirecționare o necesită programul.
	Protocol Selectați unul dintre următoarele protocoale: <ul style="list-style-type: none"> ■ TCP ■ UDP ■ Ambele
	Adresă IP Introduceți adresa IP a computerului căruia urmează să îi fie aplicată.
	Activare Bifați această casetă pentru a activa redirecționarea porturilor pentru porturile și adresele IP specificate.

Aplicații și jocuri > Declanșare interval de porturi

Declanșarea intervalului de porturi reprezintă un mod de a redirecționa porturi în mod dinamic către un PC din rețeaua LAN care are nevoie de acestea la un moment dat. Acel moment este atunci când PC-ul execută o anumită aplicație care efectuează un eveniment care declanșează ruterul. Acest eveniment trebuie să fie un acces de ieșire al unui interval particular de porturi.

Selectați fila **Declanșare interval de porturi** pentru a deschide pagina Aplicații și jocuri - Declanșare interval de porturi.



Descriere pagină Aplicații și jocuri - Declanșare interval de porturi

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura declanșarea intervalului de porturi pentru gateway-ul rezidențial. Selectați Activare pentru ambele. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
----------	----------------

Declanșare interval de porturi	
--------------------------------	--

Interval declanșat	<p>Port de început</p> <p>Pentru Portul de început, selectați un port din intervalul recomandat 49152 - 65535. Rețineți că porturile utilizate sunt specifice programului, așa că verificați care sunt cele a căror redirecționare o necesită programul.</p> <hr/> <p>Port de sfârșit</p> <p>Pentru Portul de sfârșit, selectați un port din intervalul recomandat 49152 - 65535. Rețineți că porturile utilizate sunt specifice programului, așa că verificați care sunt cele a căror redirecționare o necesită programul.</p>
---------------------------	---

Interval redirectionat	<p>Port de început</p> <p>Pentru Portul de început, selectați un port din intervalul recomandat 49152 - 65535. Rețineți că porturile utilizate sunt specifice programului, așa că verificați care sunt cele a căror redirecționare o necesită programul.</p>
-------------------------------	---

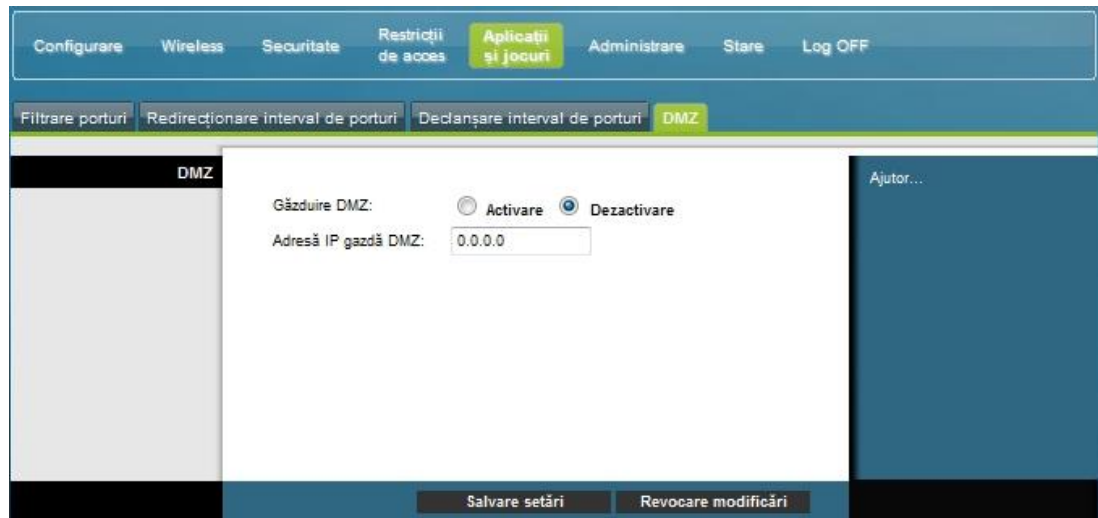
Secțiune	Descriere câmp
	<p>Port de sfârșit</p> <p>Pentru Portul de sfârșit, selectați un port din intervalul recomandat 49152 - 65535. Rețineți că porturile utilizate sunt specifice programului, așa că verificați care sunt cele a căror redirectionare o necesită programul.</p>
	<p>Protocol</p> <p>Selectați unul dintre următoarele protocoale:</p> <ul style="list-style-type: none"> ■ TCP ■ UDP ■ Ambele
	<p>Activare</p> <p>Faceți clic pe caseta de selectare Activare, pentru a activa declanșarea intervalului de porturi pentru aplicația respectivă.</p>

Aplicații și jocuri > DMZ

Utilizați această pagină pentru a configura o adresă IP ale cărei porturi sunt expuse direct la rețeaua publică de Internet sau la rețeaua de arie largă (WAN). Găzduirea în Zona demilitarizată (DMZ) este denumită, de obicei, „gazdă expusă” și vă permite să specificați un destinatar al traficului WAN pe care Translatarea adreselor de rețea (NAT) nu îl poate transla către un PC local cunoscut.

O DMZ este utilizată, de obicei, de către o companie care dorește să găzduiască propriul server de Internet. DMZ permite plasarea unei adrese IP pe partea de Internet a firewall-ului gateway-ului, în timp ce toate celelalte rămân protejate în spatele firewall-ului.

DMZ permite unui dispozitiv să fie direct accesibil traficului de pe Internet, precum un server Web (HTTP), un server FTP, un server SMTP (e-mail) și un server al sistemului de nume de domenii (DNS). Selectați fila **DMZ** pentru a deschide pagina **Aplicații și jocuri - DMZ**.



Descriere pagină Aplicații și jocuri - DMZ

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura declanșarea intervalului de porturi pentru gateway-ul rezidențial. Selectați **Activare** pentru fiecare adresă IP de gazdă DMZ. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
DMZ	<p>Găzduire DMZ</p> <p>Selectați opțiunea dorită:</p> <ul style="list-style-type: none">■ Activare■ Dezactivare (implicit din fabrică)
	<p>Adresă IP gazdă DMZ</p> <p>DMZ permite unei adrese IP să fie neprotejată, în timp ce toate celelalte rămân protejate. Introduceți în acest câmp adresa IP a computerului pe care doriți să îl expuneți la Internet.</p>

Gestionarea gateway-ului

Administrare > Gestionare

Pagina Administrare - Gestionare permite administratorului rețelei să gestioneze anumite funcții ale gateway-ului pentru acces și securitate. Selectați fila **Gestionare** pentru a deschide pagina Administrare - Gestionare.

Important: Următoarea pagină este afișată atunci când **DHCP** (implicit din fabrică) se află în modul Conexiune. Pagina afișată atunci când este selectat **IP static** este prezentată și descrisă mai târziu în această secțiune.

The screenshot displays the 'Gestionare' (Management) page for a gateway. The interface is organized into a top navigation bar, a sub-menu, and a main configuration area. The main area is divided into sections for WAN setup, gateway access, and protocol settings. The 'Tip conexiune internet' section shows 'Mod de lucru' set to 'Mod ruter', 'Mod conexiune' set to 'DHCP', and 'Dimensiune MTU' set to 0. The 'Acces gateway' section includes 'Acces local' and 'Acces de la distanță' options, with fields for user name and password, and a security warning. The 'Gestionare la distanță' section has radio buttons for 'Activare' (selected) and 'Dezactivare', and a 'Port de gestionare' field set to 8080. The 'UPnP' section has radio buttons for 'UPnP' (Dezactivare selected) and 'Activare'. The 'IGMP' section has radio buttons for 'Proxy IGMP' (Activare selected) and 'Dezactivare'. At the bottom, there are buttons for 'Salvare setări' and 'Revocare modificări'.

Descriere pagină Administrare - Gestionare

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura gestionarea administrativă pentru gateway-ul rezidențial atunci când este selectat modul de conexiune DHCP sau IP static. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Câmp	Descriere
Gateway Setup (WAN) Tip conexiune internet Tip conexiune internet	Mod conexiune Această setare vă permite să stabiliți modul în care obține WAN (sau interfața dintre gateway și Internet) adresa sa IP. DHCP (implicit din fabrică) Permite gateway-ului să obțină automat o adresă IP publică
Acces gateway Acces local Acces de la distanță	Mod de lucru: Mod ruter Mod conexiune: DHCP Dimensiune MTU: 0 Nume utilizator curent: Modificare nume de utilizator la: Modificare parolă la: Introduceți din nou parolă nouă: AVERTISMENT DE SECURITATE - parola este configurată la valoarea implicită din fabrică. Ca o măsură de securitate, se recomandă schimbarea parolei. Gestionare la distanță: <input checked="" type="radio"/> Activare <input type="radio"/> Dezactivare Port de gestionare: 8080
UPnP	UPnP: <input type="radio"/> Activare <input checked="" type="radio"/> Dezactivare
IGMP	Proxy IGMP: <input checked="" type="radio"/> Activare <input type="radio"/> Dezactivare

Câmp**Descriere****IP static**

Vă permite să specificați adresa IP WAN și informațiile corespunzătoare despre server ca valori statice sau fixe care vor fi utilizate ori de câte ori gateway-ul este online

Adresă IP Internet

Introduceți adresa IP a gateway-ului (așa cum se vede de pe Internet)

Mască subrețea

Introduceți masca de subrețea a gateway-ului (așa cum se vede de pe Internet, inclusiv furnizorul dumneavoastră de servicii)

Gateway implicit

Introduceți gateway-ul implicit al serverului furnizorului de servicii

DNS principal

Introduceți adresa(e) serverului primar de nume de domenii, furnizată(e) de către furnizorul dumneavoastră de servicii. Acesta este obligatoriu.

Câmp	Descriere
MTU	<p>DNS secundar</p> <p>Introduceți adresa(ele) serverului secundar de nume de domenii, furnizată(e) de către furnizorul dumneavoastră de servicii. Acesta este opțional.</p>
Acces gateway Acces local	<p>Dimensiune MTU</p> <p>MTU reprezintă unitatea maximă de transmisie. Dimensiunea MTU specifică cea mai mare dimensiune a unui pachet permisă pentru transmiterea prin Internet. . Valoarea implicită din fabrică = 0 (1.500 octeți)</p> <p>Nume utilizator curent</p> <p>Identifică utilizatorul autentificat în momentul respectiv</p> <p>Modificare nume de utilizator la</p> <p>Acest câmp vă permite să vă modificați numele de utilizator. Dacă doriți să vă modificați numele de utilizator, introduceți noul nume de utilizator în acest câmp și faceți clic pe Salvare setări pentru a aplica modificarea.</p> <p>Notă: Numele de utilizator implicit din fabrică este un câmp necompletat.</p> <p>Modificare parolă la</p> <p>Acest câmp vă permite să vă modificați parola. Dacă doriți să vă modificați parola, introduceți noua parolă în acest câmp. Apoi, reintroduceți noua parolă în câmpul Reintroducere parolă nouă și faceți clic pe Salvare setări pentru a aplica modificarea.</p> <p>Notă: Parola implicită din fabrică este un câmp necompletat.</p> <p>Introduceți din nou parolă nouă</p> <p>Vă permite să reintroduceți parola nouă. Trebuie să introduceți aceeași parolă ca cea introdusă în câmpul anterior Modificare parolă la. După ce reintroduceți noua parolă, faceți clic pe Salvare setări pentru a aplica modificarea.</p>

Câmp	Descriere
Acces de la distanță	<p>Gestionare la distanță</p> <p>Vă permite să activați și să dezactivați gestionarea la distanță. Această caracteristică vă permite să accesați și să gestionați setările gateway-ului de pe Internet, atunci când nu sunteți acasă. Pentru a permite accesul la distanță, selectați Activare. Altfel, păstrați setarea implicită, Dezactivare. Protocolul HTTP este necesar pentru gestionarea la distanță. Pentru a accesa dispozitivul la distanță, introduceți <code>https://xxx.xxx.xxx.xxx:8080</code> (x-urile reprezintă adresa IP Internet publică a dispozitivului, iar 8080 reprezintă portul specificat) în câmpul Adresă al browserului Web.</p> <p>Port gestionare</p> <p>Introduceți numărul portului care va fi deschis pentru acces extern. Setarea implicită din fabrică este 8080. Acest port trebuie utilizat atunci când stabiliți o conexiune la distanță.</p>
UPnP	<p>UPnP</p> <p>UPnP (Universal Plug and Play) permite Windows XP și Vista să configureze automat gateway-ul pentru diferite aplicații pe Internet, cum ar fi jocurile sau videoconferințele. Dacă doriți să utilizați UPnP, păstrați setarea implicită, Activare. Altfel, selectați Dezactivare.</p>
IGMP	<p>Proxy IGMP</p> <p>Protocolul Internet Group Multicast (IGMP) este utilizat pentru a stabili calitatea de membru într-un grup de difuzare multiplă și este utilizat, în mod obișnuit, pentru aplicații cu redare în flux prin difuzare multiplă. De exemplu, este posibil să aveți Internet Protocol Television (IPTV) cu mai multe set-top box-uri în aceeași rețea locală. Aceste set-top box-uri au fluxuri video diferite care se execută simultan, așa că ar trebui să utilizați caracteristica IGMP a ruterului.</p> <p>Redirecționarea IGMP (cu proxy) este un sistem care îmbunătățește difuzarea multiplă pentru clienți din rețeaua LAN. În cazul în care clienții acceptă această opțiune, păstrați setarea implicită, Activare. Altfel, selectați Dezactivare.</p>

Administrare > Raportare

Administrare - Raportare vă permite să trimiteți prin e-mail diverse activități ale sistemului către adresa dumneavoastră de e-mail.

Selecționați fila **Raportare** pentru a deschide pagina Administrare - Raportare.

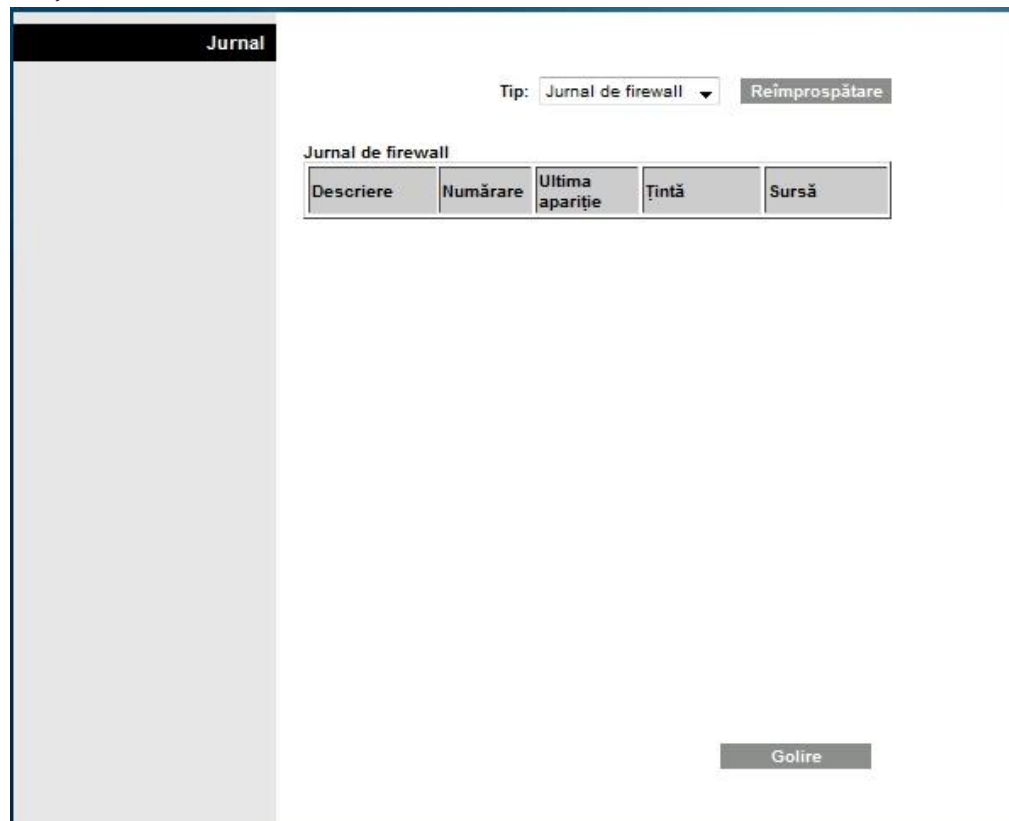
Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura caracteristica de raportare pe gateway. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Raportare	<p>Avertizări e-mail</p> <p>Dacă este activat, va fi trimis un e-mail imediat ce sunt detectate evenimente ce trebuie raportate. Pentru a utiliza această caracteristică, furnizați informațiile necesare despre adresa de e-mail.</p>
	<p>Server de e-mail SMTP</p> <p>Introduceți adresa (nume domeniu) sau adresa IP a serverului Simple Mail Transport Protocol (SMTP) pe care îl utilizați pentru trimiterea e-mailurilor.</p>
	<p>Adresă de e-mail pentru jurnale de avertizări</p> <p>Introduceți adresa de e-mail care trebuie să primească jurnalele.</p>

Vizualizare jurnal

Pentru a vizualiza jurnalele, efectuați pașii următori.

- 1 Faceți clic pe **Vizualizare jurnal**. Se deschide o fereastră nouă cu pagina datelor din jurnal.



- 2 Pentru a vizualiza un anumit jurnal, selectați una dintre următoarele opțiuni din meniul vertical Tip:
 - Toate
 - Jurnal de acces
 - Jurnal de firewall
 - Jurnal VPN
- 3 După ce sunt afișate datele jurnalului, utilizați una dintre următoarele opțiuni:
 - Faceți clic pe butonul **Reîmprospătare** pentru a actualiza jurnalul.
 - Faceți clic pe butonul **Golire** pentru a goli informațiile din jurnalul curent.
 - Faceți clic pe butonul **Pagina anterioară** pentru a reveni la informațiile afișate anterior.
 - Faceți clic pe butonul **Pagina următoare** pentru a vedea secțiunea următoare a jurnalului, dacă este disponibilă.

Administrare > Diagnosticare

Administrare - Diagnosticare vă permite să verificați starea conexiunii la Internet utilizând un test de tip Ping.

Selectați fila **Diagnosticare** pentru a deschide pagina Administrare - Diagnosticare.

Utilizați descrierile și instrucțiunile din tabelul următor pentru a configura caracteristica de diagnosticare pe gateway. După ce efectuați selecțiile, faceți clic pe **Salvare setări** pentru a aplica modificările sau pe **Revocare modificări** pentru a le revoca.

Secțiune	Descriere câmp
Test ping	
Parametri test ping	
	IP țintă ping Adresa IP către care doriți să dați comanda ping
	Dimensiune ping Dimensiunea pachetului pe care doriți să-l utilizați
	Număr de pinguri Numărul de repetări ale comenzii ping către dispozitivul țintă
	Interval ping Perioada de timp (milisecunde) dintre pinguri
	Expirare ping Perioada de timp (milisecunde) dorită până la expirare. Dacă nu se primește niciun răspuns în timpul acestei perioade de ping, testul ping va fi considerat un eșec

Secțiune	Descriere câmp
	<p>Start test</p> <p>Pentru a iniția un test, efectuați pașii de mai jos.</p> <ol style="list-style-type: none"> 1 Faceți clic pe Start test pentru a iniția testul. Se deschide o pagină nouă, care afișează un rezumat al rezultatelor testului. 2 Faceți clic pe Salvare setări pentru a salva rezultatele sau faceți clic pe Revocare modificări pentru a revoca testul.

Administrare > Copie de rezervă și restabilire

Administrare - Copie de siguranță și restabilire vă permite să efectuați o copie de rezervă a configurației gateway-ului și să o stocați pe computer. Puteți utiliza acest fișier pentru a restabili o configurație salvată anterior pentru gateway.

Selectați fila **Copie de rezervă și restabilire** pentru a deschide pagina Administrare - Copie de rezervă și restabilire.



ATENȚIE:

Restabilirea unui fișier de configurație va distruge (suprascrie) toate setările existente.



Secțiune	Descriere câmp
Configurație copie de siguranță	Utilizați Configurație copie de siguranță pentru a salva o copie a configurației curente și pentru a stoca fișierul pe computer. Faceți clic pe Copie de siguranță pentru a începe descărcarea.
Restabilire configurație	Utilizați caracteristica Restabilire configurație pentru a restabili un fișier de configurație salvat anterior. Faceți clic pe Browse

Secțiune	Descriere câmp
	(Răsfoire) pentru a selecta fișierul de configurație și apoi faceți clic pe Restabilire pentru a încărca fișierul de configurație pe dispozitiv.

Administrare > Repornire dispozitiv

Pagina Administrare - Setări implicite din fabrică vă permite să restaurați configurația la setările implicite din fabrică. Selectați fila **Repornire dispozitiv** pentru a deschide pagina Administrare - Repornire dispozitiv.



ATENȚIE:

Dacă restabiliți setările implicite din fabrică, gateway-ul va pierde toate setările pe care le-ați introdus. Înainte de a reinițializa gateway-ul la setările implicite din fabrică, notați-vă toate setările personalizate. După restabilirea valorilor implicite, va trebui să reintroduceți toate setările de configurare.

Restabilire setări implicite din fabrică

Pentru a restabili setările implicite din fabrică, faceți clic pe **Restabilire setări implicite din fabrică** pentru a reinițializa toate setările de configurare la valorile implicite. Toate setările salvate se vor pierde în momentul restabilirii setărilor implicite.

Monitorizarea stării gateway-ului

Această secțiune descrie opțiunile disponibile în fila Stare și pe care le puteți utiliza pentru a monitoriza starea gateway-ului rezidențial și pentru a diagnostica dispozitivul și rețeaua.

Stare > Gateway

Pagina Stare - Gateway afișează informații despre gateway și setările sale curente. Informațiile de pe ecran variază în funcție de tipul conexiunii la Internet pe care o folosiți.

Selectați fila **Gateway** pentru a deschide ecranul Stare - Gateway. Faceți clic pe **Reîmprospătare** pentru a actualiza datele afișate pe ecran.

Informații gateway	
Versiune firmware:	EPC3925-E SIP-12-v302r125532-110628c_upc-TEST
Adresă MAC:	00:25:2e:63:bf:84
Ora locală:	Lu Aug 15 11:23:55 2011

Conexiune internet	
Adresă IP internet:	10.33.16.31
Mască subrețea:	255.255.224.0
Gateway implicit:	10.33.0.1
DNS 1:	192.168.19.1
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0

Monitorizarea stării gateway-ului

Utilizați descrierile din tabelul următor pentru a examina starea gateway-ului și a conexiunii la Internet.

Secțiune	Descriere câmp
Informații gateway	<p>Versiune firmware Numărul de versiune firmware.</p> <p>Adresă MAC (adresă CM MAC) O adresă alfanumerică unică pentru interfața coaxială a modemului cu cablu, care este utilizată pentru conectarea la sistemul terminal al modemului cu cablu (CMTS) la capătul de încărcare. O adresă de control al accesului la media (MAC) este o adresă hardware ce identifică în mod unic fiecare nod al unei rețele.</p> <p>Ora locală Este afișată ora, conform fusului orar selectat în pagina Configurare de bază.</p>
Conexiune Internet	<p>Adresă IP Afișează adresa IP a interfeței WAN. Această adresă este atribuită gateway-ului în momentul în care intră online.</p> <p>Mască subrețea Afișează masca de subrețea pentru portul WAN. Această adresă este atribuită automat portului WAN de către furnizorul dumneavoastră de servicii Internet, cu excepția cazului în care este configurată o adresă IP statică.</p> <p>Gateway implicit Adresa IP a gateway-ului implicit al furnizorului de servicii Internet.</p> <p>DNS1-3 Adresele IP DNS utilizate în momentul respectiv de către gateway.</p> <p>WINS Adresa IP WINS utilizată în momentul respectiv de către gateway.</p>

Stare > Rețea locală

Pagina Stare - Rețea locală afișează informații despre starea rețelei locale.

Selectați fila **Rețea locală** pentru a deschide pagina Stare - Rețea locală. Faceți clic pe **Reîmprospătare** pentru a actualiza datele de pe pagină.



Utilizați tabelul următor pentru a examina starea gateway-ului și a conexiunii la Internet.

Secțiune	Descriere câmp
Rețea locală	Adresă MAC O adresă alfanumerică unică pentru rețeaua LAN privată, de la domiciliu. O adresă MAC este o adresă hardware ce identifică în mod unic fiecare nod al unei rețele.
	Adresă IP internet Afișează adresa IP pentru subrețeaua LAN
	Mască subrețea Afișează masca de subrețea pentru rețeaua LAN
	Server DHCP Afișează starea serverului DHCP local (Activat sau Dezactivat)
	Început adrese IP Afișează începutul intervalului de adrese IP utilizat de serverul DHCP din gateway-ul dumneavoastră
	Sfârșit adrese IP Afișează sfârșitul intervalului de adrese IP utilizate de serverul DHCP

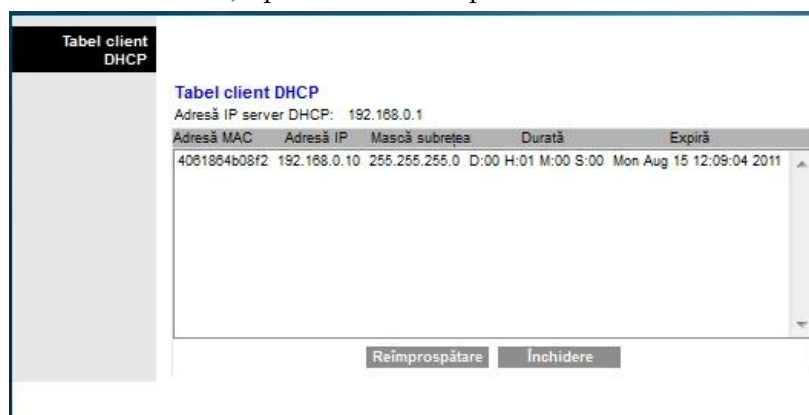
Secțiune

Descriere câmp

Tabel client DHCP

Faceți clic pe **Tabel client DHCP** pentru a prezenta dispozitivele atașate la rețeaua LAN și care au primit adrese IP de la serverul DHCP din gateway. Pe pagina Tabel client DHCP veți vedea o listă cu clienții DHCP (computere și alte dispozitive din rețea), care va conține următoarele informații: nume gazdă client, adrese IP, adrese MAC și durata până la expirarea adreselor IP alocate. Pentru a regăsi cele mai recente informații, faceți clic pe **Reîmprospătare**. Pentru a părăsi această pagină și pentru a reveni la pagina Rețea locală, faceți clic pe **Închidere**.

Următoarea ilustrație prezintă un exemplu de Tabel client DHCP.



Tabel ARP/RARP

Faceți clic pe **Tabel ARP/RARP** pentru a vedea o listă completă cu toate dispozitivele conectate la rețeaua dumneavoastră. Pentru a regăsi cele mai recente informații, faceți clic pe **Reîmprospătare**. Pentru a părăsi această pagină și pentru a reveni la pagina Rețea locală, faceți clic pe **Închidere**.

Următoarea ilustrație prezintă un exemplu de Tabel ARP/RARP.



Stare > Wireless

Pagina Stare - Rețea wireless afișează informații de bază despre rețeaua wireless a gateway-ului.

Selectați fila **Wireless** pentru a deschide pagina Stare - Wireless. Faceți clic pe **Reîmprospătare** pentru a actualiza datele de pe pagină.



The screenshot shows the 'Stare > Wireless' page of a gateway. The top navigation bar includes 'Configurare', 'Wireless', 'Securitate', 'Restricții de acces', 'Aplicații și jocuri', 'Administrare', 'Stare', and 'Log OFF'. Below this, there are tabs for 'Gateway', 'Rețea locală', 'Wireless', 'Voce', and 'WAN DOCSIS'. The 'Wireless' tab is active. The main content area is titled 'Rețea wireless' and displays the following information:

Adresă MAC:	63bf84 (70:71:BC:84:9F:38)
Mod:	802.11n 2,4 GHz
Nume rețea (SSID):	"63bf84"
Frecvență radio:	Canal standard - 20 MHz
Canal standard:	1
Securitate:	AES
Difuzare SSID:	Deschis

On the right side of the page, there is a link for 'Ajutor...'. At the bottom right, there is a 'Reîmprospătare' button.

Descriere pagină Stare - Wireless

Utilizați tabelul următor pentru a examina starea rețelei dumneavoastră wireless.

Secțiune	Descriere câmp
Rețea wireless	Adresă MAC Afișează adresa MAC a punctului de acces wireless local al gateway-ului
	Frecvență radio Afișează una dintre următoarele benzi de frecvențe radio aflate în uz în momentul respectiv: <ul style="list-style-type: none">■ 2,4 GHz■ 5 GHz■ 2,4 și 5 GHz
	Notă: Nu toate produsele acceptă banda de frecvențe radio de 5 GHz.
	Nume rețea (SSID) Afișează numele sau identificatorul setului de servicii (SSID) al punctului de acces wireless
	Lățime canal Afișează setarea lățimii de bandă a canalului selectată în pagina Setări wireless de bază
	Canal lat Afișează setarea Canal lat selectată în pagina Setări wireless de bază
	Canal standard Afișează setarea Canal standard selectată în pagina Setări wireless de bază
	Securitate Afișează metoda de securitate utilizată de rețeaua wireless
	Difuzare SSID Afișează starea caracteristicii Difuzare SSID a gateway-ului

Stare > WAN DOCSIS

Stare WAN DOCSIS afișează informații despre sistemul modemului cu cablu.

Selectați fila **WAN DOCSIS** pentru a deschide pagina Stare - WAN DOCSIS.

The screenshot displays the WAN DOCSIS status page. At the top, there is a navigation bar with tabs for Gateway, Rețea locală, Wireless, Voce, and WAN DOCSIS (selected). Below the navigation bar, the page is divided into several sections:

- Despre:** A table listing modem details:

Model:	Cisco EPC3925
Distribuitor:	Cisco
Versiune hardware:	1.0
Număr de serie:	228210229
Adresă MAC:	00:25:2e:63:bf:84
Versiune Bootloader:	2.3.0_R1
Versiune curentă software:	EPC3925-ESIP-12-v302r125532-110628c_upc-TEST
Nume firmware:	epc3925-ESIP-12-v302r125532-110628c_upc-TEST.bi
Oră generare firmware:	Jun 28 09:17:03 2011
Stare modem de cablu:	Operațional
Rețea wireless	Enable
- Stare modem de cablu:** A table showing DOCSIS status:

Scanare descărcare DOCSIS:	Finalizat
Interval DOCSIS:	Finalizat
DHCP DOCSIS:	Finalizat
TFTP DOCSIS:	Finalizat
Înreg. date DOCSIS finalizată:	Finalizat
Confidențialitate DOCSIS:	Activat
- Canale de descărcare:** A table showing signal levels for 8 channels:

Canal	Nivel alimentare:	Raport semnal - zgomot:
Canal 1:	11.4 dBmV	45.1 dB
Canal 2:	10.8 dBmV	45.5 dB
Canal 3:	11.5 dBmV	45.5 dB
Canal 4:	10.4 dBmV	44.2 dB
Canal 5:	11.3 dBmV	44.5 dB
Canal 6:	10.5 dBmV	44.2 dB
Canal 7:	11.0 dBmV	44.7 dB
Canal 8:	10.0 dBmV	44.5 dB
- Canale de încărcare:** A table showing power levels for 4 channels:

Canal	Nivel alimentare:
Canal 1:	28.7 dBmV
Canal 2:	0.0 dBmV
Canal 3:	0.0 dBmV
Canal 4:	0.0 dBmV

At the bottom of the page, there is a button labeled "Reîmprospătare".

Descriere pagină WAN DOCSIS

Utilizați descrierile din tabelul următor pentru a examina starea rețelei dumneavoastră WAN DOCSIS.

Secțiune	Descriere câmp
Despre	Model Afișează numele gateway-ului rezidențial
	Distribuitor Afișează producătorul gateway-ului rezidențial
	Versiune hardware Afișează versiunea circuitului imprimat
	Număr de serie Afișează numărul de serie unic al gateway-ului rezidențial
	Adresă MAC (adresă CM MAC) Afișează adresa CM MAC. Adresa CM MAC este o adresă alfanumerică unică pentru interfața coaxială a modemului cu cablu, care este utilizată pentru conectarea la CMTS la capătul de încărcare. O adresă MAC este o adresă hardware ce identifică în mod unic fiecare nod al unei rețele.
	Versiune Bootloader Afișează versiunea codului de revizuire a sistemului de încărcare
	Versiune curentă software Afișează versiunea revizuirii firmware
	Nume firmware Afișează numele firmware
	Oră generare firmware Afișează data și ora generării firmware-ului
	Stare modem de cablu Afișează una dintre stările curente posibile ale gateway-ului
Canale de descărcare	Canalele 1-8 Afișează nivelul de putere și raportul semnal-zgomot pentru canalele de descărcare active
Canale de încărcare	Canalele 1-4 Afișează nivelul de putere pentru canalele de încărcare active

Întrebări frecvente

Î. Cum configurez protocolul TCP/IP?

R. Pentru a configura protocolul TCP/IP, trebuie să aveți instalată în sistem o placă de rețea (NIC) Ethernet cu protocol de comunicații TCP/IP. TCP/IP este un protocol de comunicații utilizat pentru accesarea Internetului. Această secțiune conține instrucțiuni pentru configurarea TCP/IP pe dispozitivele dumneavoastră de Internet, pentru a funcționa cu gateway-ul rezidențial în medii Microsoft Windows sau Macintosh.

Protocolul TCP/IP într-un mediu Microsoft Windows este diferit pentru fiecare sistem de operare. Urmăți instrucțiunile din această secțiune corespunzătoare pentru sistemul dumneavoastră de operare.

Configurarea TCP/IP pe sisteme Windows 2000

- 1 Faceți clic pe **Start**, selectați **Setări** și alegeți **Conexiuni de rețea și pe linie comutată**.
- 2 Faceți dublu clic pe pictograma **Conexiune de rețea locală** din fereastra Conexiuni de rețea și pe linie comutată.
- 3 Faceți clic pe **Proprietăți** în fereastra Stare conexiune de rețea locală.
- 4 Faceți clic pe **Protocol Internet (TCP/IP)** în fereastra Proprietăți conexiune de rețea locală și apoi faceți clic pe **Proprietăți**.
- 5 Selectați **Se obține automat o adresă IP** și **Se obține automat adresa de server DNS** în fereastra Proprietăți Protocol Internet (TCP/IP) și apoi faceți clic pe **OK**.
- 6 Faceți clic pe **Da** pentru a reporni computerul în momentul în care se deschide fereastra Rețea locală. Computerul repornește. Protocolul TCP/IP este acum configurat pe PC, iar dispozitivele Ethernet sunt gata de utilizare.
- 7 Încercați să accesați Internetul. Dacă nu puteți accesa Internetul, contactați furnizorul de servicii pentru asistență suplimentară.

Configurarea TCP/IP pe sisteme Windows XP

- 1 Faceți clic pe **Start** și, în funcția de configurarea meniului Start, alegeți una dintre următoarele opțiuni:
 - Dacă utilizați meniul de Start implicit Windows XP, selectați **Conectare la**, alegeți **Se afișează toate conexiunile** și apoi treceți la pasul 2.
 - Dacă utilizați meniul de Start clasic Windows XP, selectați **Setări**, alegeți **Conexiuni în rețea**, faceți clic pe **Conexiune de rețea locală** și apoi treceți la pasul 3.
- 2 Faceți dublu clic pe pictograma **Conexiune de rețea locală** din secțiunea LAN sau Internet de mare viteză a ferestrei Conexiuni în rețea.
- 3 Faceți clic pe **Proprietăți** în fereastra Stare conexiune de rețea locală.

- 4 Faceți clic pe **Protocol Internet (TCP/IP)** și apoi faceți clic pe **Proprietăți** în fereastra Proprietăți conexiune de rețea locală.
- 5 Selectați **Se obține automat o adresă IP** și **Se obține automat adresa de server DNS** în fereastra Proprietăți Protocol Internet (TCP/IP) și apoi faceți clic pe **OK**.
- 6 Faceți clic pe **Da** pentru a reporni computerul în momentul în care se deschide fereastra Rețea locală. Computerul repornește. Protocolul TCP/IP este acum configurat pe PC, iar dispozitivele Ethernet sunt gata de utilizare.
- 7 Încercați să accesați Internetul. Dacă nu puteți accesa Internetul, contactați furnizorul de servicii pentru asistență suplimentară.

Configurarea TCP/IP pe sisteme Macintosh

- 1 Faceți clic pe pictograma **Apple** din colțul din dreapta sus al Finder (Program de găsim). Defilați în jos la **Control Panels** (Panouri de control) și apoi faceți clic pe **TCP/IP**.
- 2 Faceți clic pe **Edit** (Editare) din Finder (Program de găsim) în partea de sus a paginii. Defilați până în partea de jos a meniului și apoi faceți clic pe **User Mode** (Mod utilizator).
- 3 Faceți clic pe **Advanced** (Avansat) în fereastra User Mode (Mod utilizator) și apoi faceți clic pe **OK**.
- 4 Faceți clic pe săgețile de selectare sus/jos amplasate la dreapta secțiunii Connect Via (Conectare prin) a ferestrei TCP/IP și apoi faceți clic pe **Using DHCP Server** (Utilizare server DHCP).
- 5 Faceți clic pe **Options** (Opțiuni) în fereastra TCP/IP și apoi faceți clic pe **Active** (Activ) în fereastra TCP/IP Options (Opțiuni TCP/IP).
Notă: Asigurați-vă că **opțiunea Load only when needed** (Se încarcă doar când este necesar) este *debifată*.
- 6 Verificați dacă opțiunea **Use 802.3** (Se utilizează 802.3) din colțul din dreapta sus al ferestrei TCP/IP este debifată. Dacă această opțiune este bifată, debifați-o și apoi faceți clic pe **Info** (Informații) din colțul din stânga jos.
- 7 Există vreo adresă hardware listată în această fereastră?
 - Dacă **da**, faceți clic pe **OK**. Pentru a închide fereastra TCP/IP Control Panel (Panou de control), faceți clic pe **File** (Fișier) și apoi defilați în jos pentru a face clic pe **Close** (Închidere). Ați finalizat această procedură.
 - Dacă **nu**, trebuie să opriți sistemul Macintosh.
- 8 În timp ce acesta este oprit, apăsați simultan și mențineți apăsată tastele **Command (Apple)** (Comandă), **Option** (Opțiune), **P** și **R** de pe tastatură. Menținând aceste taste apăsată, porniți sistemul Macintosh, însă nu eliberați tastele până nu auziți sunetul Apple cel puțin de trei ori, atunci eliberați tastele și lăsați computerul să repornească.
- 9 După ce computerul a încărcat complet sistemul de operare, repetați pașii de la 1 la 7 pentru a vă asigura că toate setările TCP/IP sunt corecte. În cazul în care computerul tot nu are o adresă hardware, contactați distribuitorul Apple autorizat sau centrul de asistență tehnică Apple pentru asistență suplimentară.

Î. Cum reînnoiesc adresa IP pe PC-ul meu?

R. Dacă PC-ul nu poate accesa Internetul după ce gateway-ul rezidențial este online, este posibil ca PC-ul să nu își fi reînnoit adresa IP. Urmați instrucțiunile din această secțiune corespunzătoare pentru sistemul dumneavoastră de operare pentru a reînnoi adresa IP a PC-ului.

Reînnoirea adresei IP pe sisteme Windows 95, 98, 98SE și ME

- 1 Faceți clic pe **Start** și apoi pe **Executare** pentru a deschide fereastra Executare.
- 2 Tastați **winipcfg** în câmpul Deschidere și faceți clic pe **OK** pentru a executa comanda winipcfg. Se deschide fereastra Configurație IP.
- 3 Faceți clic pe săgeata jos din partea dreaptă a câmpului de sus și selectați adaptorul Ethernet instalat pe PC. Fereastra Configurație IP afișează informațiile despre adaptorul Ethernet.
- 4 Faceți clic pe **Eliberare** și apoi pe **Reînnoire**. Fereastra Configurație IP afișează o adresă IP nouă.
- 5 Faceți clic pe **OK** pentru a închide fereastra Configurație IP și ați finalizat această procedură.

Notă: Dacă nu puteți accesa Internetul, contactați furnizorul de servicii pentru asistență suplimentară.

Reînnoirea adresei IP pe sisteme Windows NT, 2000 sau XP

- 1 Faceți clic pe **Start** și apoi pe **Executare**. Se deschide fereastra Executare.
- 2 Tastați **cmd** în câmpul Deschidere și faceți clic pe **OK**. Se deschide o fereastră cu o linie de comandă.
- 3 Tastați **ipconfig/release** pe linia C:/ și apăsați **Enter**. Sistemul eliberează adresa IP.
- 4 Tastați **ipconfig/renew** pe linia C:/ și apăsați **Enter**. Sistemul afișează o adresă IP nouă.
- 5 Faceți clic pe **X** din colțul din dreapta sus al ferestrei pentru a închide fereastra cu linia de comandă. Ați finalizat această procedură.

Notă: Dacă nu puteți accesa Internetul, contactați furnizorul de servicii pentru asistență suplimentară.

Î. Ce se întâmplă dacă nu mă abonez la serviciul de televiziune prin cablu?

R. Dacă în zona în care vă aflați există un serviciu de televiziune prin cablu, serviciul de date poate fi disponibil cu sau fără abonarea la serviciul de televiziune prin cablu. Contactați furnizorul de servicii local pentru informații complete despre serviciile prin cablu, inclusiv acces la Internet de mare viteză.

Î. Cum pot solicita instalarea?

R. Apelați furnizorul de servicii pentru a solicita informații despre instalarea asigurată de specialiști. O instalare efectuată de specialiști asigură o conexiune prin cablu corespunzătoare între modem și PC, precum și configurarea adecvată a tuturor setărilor hardware și software. Contactați furnizorul de servicii pentru mai multe informații despre instalare.

Î. Cum se conectează gateway-ul rezidențial la computerul meu?

R. Gateway-ul rezidențial se conectează la PC utilizând o conexiune wireless sau portul Ethernet 10/100/1000BASE-T de pe PC. Dacă doriți să utilizați o interfață Ethernet, puteți găsi plăci Ethernet la distribuitorul local de PC-uri sau de echipamente de birou sau la furnizorul dumneavoastră de servicii. Pentru cea mai bună performanță prin intermediul unei conexiuni Ethernet, PC-ul trebuie să fie echipat cu o placă Ethernet Gigabit.

Î. După ce gateway-ul rezidențial este conectat, cum accesez Internetul?

R. Furnizorul de servicii local devine furnizorul de servicii Internet (ISP). Acesta oferă o gamă largă de servicii, inclusiv e-mail, chat, știri și servicii de informații. Furnizorul dumneavoastră de servicii vă va furniza software-ul necesar.

Î. Mă pot uita la televizor și să navighez pe Internet în același timp?

R. Cu siguranță! Dacă vă abonați la un serviciu de televiziune prin cablu, vă puteți uita la televizor și puteți utiliza gateway-ul rezidențial în același timp, conectând televizorul și gateway-ul rezidențial la rețeaua prin cablu, utilizând un divizor de semnal prin cablu opțional.

Aspecte de depanare obișnuite

Nu înțeleg indicatorii de stare de pe panoul frontal

Consultați *Funcții ale indicatorilor de stare cu LED de pe panoul frontal* (la pagina 113) pentru mai multe informații detaliate despre funcțiile și funcționarea indicatorilor de stare cu LED de pe panoul frontal.

Gateway-ul rezidențial nu înregistrează o conexiune Ethernet

- Asigurați-vă că există o placă Ethernet în computer și că software-ul de driver Ethernet este instalat corespunzător. Dacă achiziționați și instalați o placă Ethernet, urmați cu atenție instrucțiunile de instalare.
- Verificați starea indicatorilor luminoși de stare de pe panoul frontal.

Gateway-ul rezidențial nu înregistrează o conexiune Ethernet după conectarea la un hub

În cazul în care conectați mai multe PC-uri la gateway-ul rezidențial, trebuie să conectați mai întâi modemul la portul uplink al hubului, utilizând cablul de legătură corect. LED-ul LINK al hubului va ilumina încontinuu.

Gateway-ul rezidențial nu înregistrează o conexiune prin cablu

- Modemul funcționează cu un cablu coaxial RF standard de 75 ohmi. Dacă utilizați un cablu diferit, gateway-ul rezidențial nu va funcționa corect. Contactați furnizorul de servicii prin cablu pentru a stabili dacă utilizați cablul corect.
- Este posibil ca placa de rețea sau interfața USB să fie defectă. Consultați informațiile despre depanare din documentația plăcii de rețea sau a interfeței USB.

Sfaturi pentru performanță îmbunătățită

Verificare și corectare

Dacă gateway-ul rezidențial nu funcționează conform așteptărilor, următoarele sfaturi pot fi de ajutor. Dacă aveți nevoie de asistență suplimentară, contactați furnizorul de servicii.

- Verificați dacă fișa de alimentare CA a gateway-ului rezidențial este introdusă corect într-o priză electrică.
- Verificați dacă gateway-ul rezidențial nu are cablul de alimentare CA conectat la o priză care să fie controlată de la un comutator de perete. Dacă un comutator de perete controlează priza electrică, asigurați-vă că acesta este în poziția **PORNIT**.
- Verificați dacă indicatorul de stare cu LED **ONLINE** de pe panoul frontal al gateway-ului rezidențial este aprins.
- Verificați dacă serviciul prin cablu este activ și dacă acceptă servicii bidirecționale.
- Verificați dacă toate cablurile sunt conectate corect și dacă utilizați cablurile corecte.
- Verificați dacă protocolul TCP/IP este instalat și configurat corect, în cazul în care utilizați conexiunea Ethernet.
- Verificați dacă ați apelat furnizorul de servicii și i-ați comunicat numărul de serie și adresa MAC ale gateway-ului rezidențial.
- Dacă utilizați un divizor de semnal prin cablu, pentru a putea conecta gateway-ul rezidențial la alte dispozitive, îndepărtați divizorul și reconectați cablurile, astfel încât gateway-ul rezidențial să fie conectat direct la intrarea pentru cablu. Dacă gateway-ul rezidențial funcționează acum corect, este posibil ca divizorul de semnal prin cablu să fie defect sau să fie nevoie să îl înlocuiți.
- Pentru cea mai bună performanță prin intermediul unei conexiuni Ethernet, PC-ul trebuie să fie echipat cu o placă Ethernet Gigabit.

Funcții ale indicatorilor de stare cu LED de pe panoul frontal

Alimentare inițială, calibrare și înregistrare (alimentare CA)

Următorul grafic ilustrează secvența de pași și felul în care arată indicatorii de stare cu LED de pe panoul frontal al gateway-ului rezidențial în timpul alimentării, calibrării și înregistrării în rețea, atunci când gateway-ul rezidențial este alimentat cu CA. Utilizați acest grafic pentru a depana procesele de alimentare, calibrare și înregistrare ale gateway-ului rezidențial.

Notă: După ce gateway-ul rezidențial finalizează Pasul 11 (Înregistrare telefon finalizată), modemul trece imediat la Funcționarea normală. Consultați *Funcționare normală (alimentare CA)* (la pagina 115).

Indicatori de stare cu LED de pe panoul frontal în timpul alimentării inițiale, calibrării și înregistrării							
Partea 1, Înregistrare date de mare viteză							
Pas:		1	2	3	4	5	6
Indicator panou frontal		Test automat	Scanare descărcare	Blocare semnal descărcare	Stabilire intervale	Solicitare adresă IP	Solicitare fișier pentru furnizare de date de mare viteză
1	POWER	Aprins	Aprins	Aprins	Aprins	Aprins	Aprins
2	DS	Aprins	Clipește	Aprins	Aprins	Aprins	Aprins
3	US	Aprins	Stins	Stins	Clipește	Aprins	Aprins
4	ONLINE	Aprins	Stins	Stins	Stins	Stins	Clipește
5	ETHERNET 1-4	Aprins	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
6	USB	Aprins	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
7	WIRELESS LINK	Stins	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
8	WIRELESS SETUP	Stins	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
9	TEL 1	Aprins	Stins	Stins	Stins	Stins	Stins
10	TEL 2	Aprins	Stins	Stins	Stins	Stins	Stins

Funcții ale indicatorilor de stare cu LED de pe panoul frontal

Indicatori de stare cu LED de pe panoul frontal în timpul alimentării inițiale, calibrării și înregistrării						
Partea 2, Înregistrare telefon						
Pas		7	8	9	10	11
	Indicator panou frontal	Înregistrare rețea de date finalizată	Solicitare adresă IP telefon	Solicitare fișier furnizare telefon	Repornire serviciu de voce	Înregistrare telefon finalizată
1	POWER	Aprins	Aprins	Aprins	Aprins	Aprins
2	DS	Aprins	Aprins	Aprins	Aprins	Aprins
3	US	Aprins	Aprins	Aprins	Aprins	Aprins
4	ONLINE	Aprins	Aprins	Aprins	Aprins	Aprins
5	ETHERNET 1 - 4	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
6	USB	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
7	WIRELESS LINK	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește	Aprins sau clipește
8	WIRELESS SETUP	Stins	Stins	Stins	Aprins sau clipește	Aprins sau clipește
9	TEL 1	Stins	Clipește	Stins	Clipește	Aprins
10	TEL 2	Stins	Stins	Clipește	Clipește	Aprins

Funcționare normală (alimentare CA)

Graficul următor ilustrează felul în care arată indicatorii de stare cu LED de pe panoul frontal al gateway-ului rezidențial în timpul funcționării normale, atunci când gateway-ul este alimentat cu CA.

Indicatori de stare cu LED de pe panoul frontal în condiții normale		
Indicator panou frontal	Funcționare normală	
1	POWER	Aprins
2	DS	Aprins
3	US	Aprins
4	ONLINE	Aprins
5	ETHERNET 1 - 4	<ul style="list-style-type: none"> ■ Aprins - Când un singur dispozitiv este conectat la portul Ethernet și modemul nu trimite și nu primește date ■ Clipește - Când un singur dispozitiv Ethernet este conectat și sunt transferate date între echipamentul de la sediul clientului (CPE) și gateway-ul wireless de la domiciliu ■ Stins - Când la porturile Ethernet nu este conectat niciun dispozitiv
6	USB	<ul style="list-style-type: none"> ■ Aprins - Când un singur dispozitiv este conectat la portul USB și modemul nu trimite și nu primește date ■ Clipește - Când un singur dispozitiv USB este conectat și sunt transferate date între echipamentul de la sediul clientului (CPE) și gateway-ul wireless de la domiciliu ■ Stins - Când la porturile USB nu este conectat niciun dispozitiv
7	WIRELESS LINK	<ul style="list-style-type: none"> ■ Aprins - Când punctul de acces wireless este activat și funcțional ■ Clipește - Când sunt transferate date între CPE și gateway-ul wireless de la domiciliu ■ Stins - Când punctul de acces wireless este dezactivat de către utilizator
8	WIRELESS SETUP	<ul style="list-style-type: none"> ■ Stins - Când configurarea wireless nu este activă ■ Clipește - Când configurarea wireless este activă pentru a adăuga noi clienți wireless la rețeaua wireless
9	TEL 1	<ul style="list-style-type: none"> ■ Aprins - Când serviciul de telefonie este activat ■ Clipește - Când linia 1 este în uz
10	TEL 2	<ul style="list-style-type: none"> ■ Aprins - Când serviciul de telefonie este activat ■ Clipește - Când linia 2 este în uz

Condiții speciale

Următorul grafic descrie felul în care arată indicatorii de stare cu LED de pe panoul frontal al modemului cu cablu în timpul condițiilor speciale, pentru a vă arăta când vă este refuzat accesul la rețea.

Indicatori de stare cu LED de pe panoul frontal în condiții speciale		
Indicator panou frontal		Acces la rețea refuzat
1	POWER	Clipește încet O dată pe secundă
2	DS	Clipește încet O dată pe secundă
3	US	Clipește încet O dată pe secundă
4	ONLINE	Clipește încet O dată pe secundă
5	ETHERNET 1 - 4	Clipește încet O dată pe secundă
6	USB	Clipește încet O dată pe secundă
7	WIRELESS LINK	Clipește încet O dată pe secundă
8	WIRELESS SETUP	Clipește încet O dată pe secundă
9	TEL 1	Stins
10	TEL 2	Stins

Note

Mărci comerciale

Cisco și sigla Cisco sunt mărci comerciale sau mărci înregistrate ale Cisco și/sau afiliaților săi în S.U.A. și în alte țări. O listă cu mărcile comerciale ale Cisco poate fi găsită la www.cisco.com/go/trademarks.

DOCSIS este marcă comercială înregistrată a Cable Television Laboratories, Inc. EuroDOCSIS, EuroPacketCable și PacketCable sunt mărci comerciale ale Cable Television Laboratories, Inc.

Alte mărci comerciale terțe menționate reprezintă proprietatea deținătorilor lor de drept. Utilizarea cuvântului „partener” nu implică neapărat o relație de parteneriat între Cisco și orice altă companie. ^(1009R)

Declinare de responsabilitate

Cisco Systems, Inc. nu își asumă nicio responsabilitate pentru erorile sau omisiunile ce pot apărea în acest ghid. Ne rezervăm dreptul de a modifica acest ghid în orice moment, fără notificare.

Notificare de drepturi de autor pentru documentație

Informațiile din acest document pot fi modificate fără notificare. Nicio parte a acestui document nu poate fi reprodusă, în nicio formă, fără permisiunea expresă, în scris, din partea Cisco Systems, Inc.

Utilizarea de software și firmware

Software-ul descris în acest document este protejat prin legea drepturilor de autor și vă este pus la dispoziție în baza unui acord de licență. Puteți utiliza sau copia acest software doar în conformitate cu termenii acordului de licență.

Firmware-ul din acest echipament este protejat prin legea drepturilor de autor. Puteți utiliza firmware-ul doar în echipamentul în care este furnizat. Este interzisă orice reproducere sau distribuire a acestui firmware sau a oricărei părți a acestuia, fără consimțământul nostru expres, în scris.

Pentru informații

Pentru informații

Dacă aveți întrebări

Dacă aveți întrebări de natură tehnică, apăsați la Serviciile Cisco pentru asistență. Urmăriți opțiunile de meniu pentru a vorbi cu un inginer de service.



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

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

Acest document include diverse mărci comerciale ale Cisco Systems, Inc. Consultați secțiunea Note a acestui document pentru o listă cu mărcile comerciale ale Cisco Systems, Inc. utilizate în acest document.

Disponibilitatea produselor și a serviciilor se pot modifica fără notificare.

© 2011 Cisco și/sau afiliații săi. Toate drepturile rezervate
Septembrie 2011

Număr componentă 4041328 Rev A