

Manual de instruções do HGA12R-02

Índice

Login na Interface Web de gerenciamento do gateway	2
Visão geral	4
Status da rede	5
Status do modem conectado por cabo	6
Rede IP Local	7
WiFi	8
Edição da configuração básica do modo de rádio	10
Ajustes de configuração de WPS	16
WAN	18
Ajustes de Firewall	20
Versão do software do gateway	23
Informação de hardware do sistema	24
Informações de hardware sem fio	25
Computadores	26
Menu de controle parental	27
Sites gerenciados	28
Configuração de sites bloqueados	29
Configuração de palavras-chave bloqueadas	31
Configuração de computadores confiáveis	33
Managed Services	35
Configuração de serviços bloqueados	36
Configuração de computadores confiáveis	39
Dispositivos gerenciados	41
Permissão de dispositivos	42
Bloqueio de serviços	45
Menu Advanced	48
Encaminhamento de porta	49
Inclusão de serviço de encaminhamento de porta	50
Disparo de porta	52
Inclusão de disparo de porta	53
Gerenciamento remoto	55
DMZ	56
QoS	57
Descoberta de dispositivo	59
VPN	61
Menu Troubleshooting	62
Ferramentas de diagnóstico de rede	63
Teste da conectividade com um endereço de destino	64
Restaurar/Reiniciar	65
Alterar senha	66

Login na Interface Web de gerenciamento do gateway

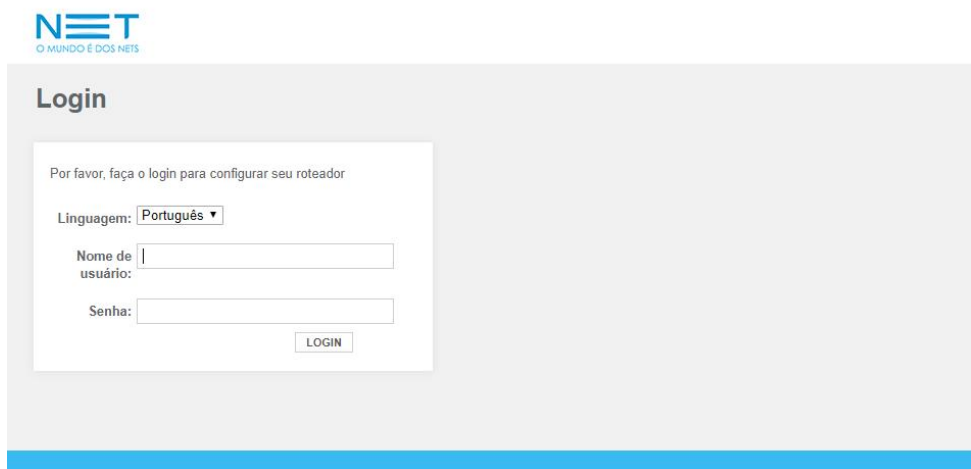
Para acessar as definições de configuração do gateway, abra um navegador da web no computador e faça login na interface de administração do gateway.

Para acessar as configurações do administrador do Gateway, use o procedimento a seguir.

1. Abra um navegador da Web.

Observação: O computador não precisa estar on-line para configurar o gateway.

2. Na barra de endereço do navegador, digite **http://192.168.0.1** e pressione a tecla **Enter**. Então a página de login aparecerá da seguinte forma:



3. Na página de login, selecione seu idioma. Em seguida, a interface do usuário será exibida no idioma selecionado após o login.

4. Nos campos **Nome de usuário** e **Senha**, insira o nome de usuário e a senha padrão fornecidos.

Observação: O nome de usuário e a senha padrão estão localizados na parte inferior do produto.

MODEL: HGA12R-02	DOCSIS3.0	SW X.X	HUMAX
INPUT: 12V  , 2.0A	FABR: MM/YYYY		
			
S/N: 13321600001			
			
CM MAC: C0D962FFDCF6			
			
EMTA MAC: C0D962FFDCF9			
IP: 192.168.0.1	SSID 2G: NET_2GFFDCF6		
Usuários: NET_FFDCF6	SSID 5G: NET_5GFFDCF6		
Senha: C0D962FFDCF6	Senha: 62FFDCF6		
Produzido por : HUMAX DO BRASIL INDÚSTRIA ELETRÔNICA LTDA. Rua Matrinxã, 687 - Edifício 2, Parte 2 - Distrito Industrial Manaus - AM - Brasil CEP 69075-150 CNPJ: 13.645.479/0001-65 Indústria Brasileira			 1168-16-4704  (01)07898934016180

-
5. Clique em **LOGIN** para acessar o gateway. A interface de gerenciamento da Web é iniciada e a Etapa 1 do Assistente de rede doméstica é exibida.

Observação: Depois de efetuar login na interface de gerenciamento da Web, recomendamos alterar o nome de usuário e a senha padrão em **Gateway > Wizard**.

Visão geral

Gateway > At a Glance

A página At a Glance mostra informações sobre a rede e dispositivos conectados. Esta página está organizada em quatro áreas:

- **Home Network** mostra o status da conexão de Ethernet, dispositivos sem fio e nível de segurança do firewall.
- **Connected Devices** mostra o endereço MAC dos dispositivos conectados ao Gateway. Clique em **VIEW CONNECTED DEVICES** para abrir a página Computers para visualizar dispositivos que o Gateway detecta automaticamente usando o DHCP.
- **Software Versions** mostra as versões dos softwares eMTA, DOCSIS e PacketCable.
- **Recent Network Updates** mostra alertas e avisos emitidos pelo Gateway. Uma lista suspensa permite filtrar as informações para exibir as atualizações de hoje, ontem, semana passada, mês passado e últimos 90 dias.

The screenshot displays the 'Sistema > Status' page of a NET Gateway. The page is organized into several sections:

- System Status:** A summary box at the top stating 'Ver informações sobre a sua rede e dispositivos conectados.' with a 'mais' link.
- Rede Local (Local Network):** Shows 'Ethernet' and 'Wi-Fi / 0 Dispositivos conectados' with green checkmarks. Below this, it indicates 'Nível de segurança do Firewall: Segurança baixa' (Low Firewall Security Level).
- Dispositivos conectados (Connected Devices):** Lists 'hbr_eng_02' (with a red X) and 'laptop-5iq1pjo2' (with a green checkmark). A button labeled 'VISUALIZAR DISPOSITIVOS CONECTADOS' is present.
- Versões de Software (Software Versions):** Displays 'Versão de Software (eMTA & DOCSIS): BRGCAA 1.1.53-test' and 'Packet Cable: PacketCable 1.5'.
- Atualizações recentes Rede (Recent Network Updates):** Features a dropdown menu set to 'Hoje' (Today). It shows 'Alertas: (0)' and 'Avisos: (5)'. Two login success messages are visible: '<11>Jun 12 10:12:01 : #LOGIN# User humaxadmin login success!' and '<11>Jun 12 10:13:57 : #LOGIN# User humaxadmin login success!'.

The top right corner includes navigation links for 'Sair' and 'Alterar senha', and status indicators for 'Internet' (red X), 'Wi-Fi' (green checkmark), and 'Segurança baixa' (red X).

Status da rede

Gateway > Connection > Network Status

A página Status exibe informações sobre o status da conexão do Gateway. Esta página está organizada em quatro áreas:

- **Local IP Network** mostra o status da rede local, a velocidade da conexão, o endereço IPv4, a máscara de sub-rede, o status do servidor DHCP, o número de clientes conectados e o tempo de concessão do DHCP.
- **WiFi Network 2.4G** mostra o status, os protocolos e o tipo de segurança da rede sem fio 2.4G. O botão A VIEW permite visualizar informações da porta LAN Wi-Fi.
- **WAN IP Network** mostra o status da conexão com a Internet, o endereço IP da WAN, o status do cliente DHCP e o tempo de expiração do DHCP. O botão VIEW permite visualizar informações sobre a conexão de rede de longa distância.
- **WiFi Network 5G** mostra o status, os protocolos e o tipo de segurança da rede sem fio 5G. O botão VIEW permite visualizar informações da porta LAN Wi-Fi.

NET
O MUNDO É DOS NETS

Sair • Alterar senha

Internet Wi-Fi Segurança baixa

Sistema > Conexão > Status da rede

Exibir informações sobre o status da conexão Gateway. [Mais](#)

Rede de IP Local	Rede Wi-Fi 2.4GHz
Rede Local: Conectado	Rede Wi-Fi: Ativo
Endereço IP (IPv4): 192.168.0.1	Protocolos: 802.11 b/g/n Suportados:
Máscara de SubRede: 255.255.255.0	Segurança: WPA2-PERSONAL-AES
Servidor DHCP: correto	Número de clientes conectados: 0
Número de clientes conectados: 1	
Tempo de Concessão do DHCP: 1days	

Rede IP WAN	Rede Wi-Fi 5GHz
Internet: Inativo	Rede Wi-Fi: Ativo
Tempo de Funcionamento do Sistema: 0h:41m:46s	Protocolos: 802.11 a/n/ac Suportados:
Endereço IP WAN: 0.0.0.0	Segurança: WPA2-PERSONAL-AES
Endereço DNS: 0	Número de clientes conectados: 0
Endereço Ipv6 WAN:	
Prefixo:	
Cliente DHCP: Habilitado	
DHCP Tempo limite: 0	
CM MAC: 40:3D:EC:FA:D5:9C	
eMTA MAC: 40:3D:EC:FA:D5:A0	
WAN MAC: 40:3D:EC:FA:D5:9F	

Status do modem conectado por cabo

Gateway > Connection > CM Status

A página CM Status exibe as informações do modem conectado por cabo sobre o produto e os valores de ligação de canal downstream e upstream.

NET
O MUNDO É DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Sistema > Conexão > Status do CM

Ver informações técnicas relacionadas à sua conexão CM. [mais](#)

Cable Modem

Estado do CM:	Forwarding_disabled
Versão de HW:	1.0
Fabricante:	HUMAX Co., Ltd.
Versão do BOOT:	PSPU-Boot 2.0.0.38
Versão de SW:	BRGCAA 1.1.53-test
Modelo:	HGA12R-02
Tipo do Produto:	Access Point
Flash Part:	1
Nome do arquivo de SW:	BRGCAA-1.1.53-test.20180611192216.bin
Serial Number:	7 618013171899

Downstream Valor da Junção de Canais

ID do Canal	1	2	3	4	5	6	7	8
Frequência	615.00 MHz	621.00 MHz	627.00 MHz	633.00 MHz	639.00 MHz	645.00 MHz	651.00 MHz	657.00 MHz
SNR	40.366dB	40.366dB	40.366dB	40.946dB	40.366dB	40.366dB	38.605dB	38.983dB
Sinal	12.40 dBmV	12.40 dBmV	12.60 dBmV	12.10 dBmV	11.80 dBmV	11.20 dBmV	11.20 dBmV	10.70 dBmV
Modulação	QAM256	QAM256	QAM256	QAM256	QAM256	QAM256	QAM256	QAM256

ID do Canal	9	10	11	12	13	14	15	16
Frequência	663.00 MHz	669.00 MHz	675.00 MHz	681.00 MHz	687.00 MHz	693.00 MHz	699.00 MHz	705.00 MHz
SNR	40.366dB	40.366dB	40.366dB	40.366dB	40.366dB	40.946dB	40.366dB	40.946dB
Sinal	11.20 dBmV	12.00 dBmV	12.60 dBmV	12.20 dBmV	13.00 dBmV	13.60 dBmV	12.80 dBmV	11.90 dBmV
Modulação	QAM256	QAM256	QAM256	QAM256	QAM256	QAM256	QAM256	QAM256

Upstream Valor da Junção de Canais

ID do Canal	7	8	6	5
Frequência	38.40 MHz	40.10 MHz	33.10 MHz	29.00 MHz
Taxa de Símbolo	2560kSym/sec	2560kSym/sec	2560kSym/sec	2560kSym/sec
Potência do sinal:	50.00dBmV	50.50dBmV	49.00dBmV	49.00dBmV
Largura do Canal	3.20 MHz	3.20 MHz	3.20 MHz	3.20 MHz
Tamanho do Slot	4	4	4	4
Início do Intervalo de Backoff	2	2	2	2
Fim do Intervalo de Backoff	7	7	7	7
Modulação	64QAM	64QAM	64QAM	64QAM

Rede IP Local

Gateway > Connection > Local IP Network

A página Local IP Network exibe as informações sobre a configuração IP local. Preencha os campos para configurar sua rede IP local.

The screenshot shows the NET router configuration interface. At the top left is the NET logo with the tagline "O MUNDO É DOS NETS". At the top right, there are links for "Sair" and "Alterar senha", and status indicators for "Internet" (red X), "Wi-Fi" (green check), and "Segurança baixa" (red X).

The main navigation menu on the left includes: Sistema, Status, Conexão, Status da Rede, Status do CM, Rede de IP Local (highlighted), Wi-Fi, WAN, Firewall, Software, Hardware, Dispositivos conectados, Controle de Pais, Avançado, Solução de problemas, and MSO.

The main content area is titled "Sistema > Conexão > Rede de IP Local". It contains a "Configuração do IP da rede local" section with a "mais" link. Below this is the "IPv4" configuration section, which includes:

- Endereço do Sistema: 192 . 168 . 0 . 1
- Máscara de SubRede: 255.255.255.0
- DHCP Endereço inicial: 192 . 168 . 0 . 2
- DHCP Endereço final: 192 . 168 . 0 . 200
- Tempo de Concessão do DHCP: 1 Dias

Below the IPv4 section are two buttons: "SALVAR CONFIGURAÇÕES" and "RESTAURAR CONFIGURAÇÕES PADRÕES".

At the bottom is the "IPv6" section, which is currently empty, showing a table with headers: "Nome de Interface", "Endereço IP", "Comprimento do Prefixo", and "Status".

WiFi

Gateway > Connection > WiFi

A página WiFi mostra informações avançadas sobre as conexões Wi-Fi do Gateway. Esta página está organizada nas seguintes áreas:

- **Radio Mode** mostra o modo, o status e os protocolos configurados para os rádios sem fio de 2,4 GHz e 5 GHz do Gateway.
 - O botão **EDIT** permite definir os ajustes básicos da rede Wi-Fi do Gateway. Consultar “Edição da configuração básica do modo de rádio”.
- **Private WiFi Network 2.4G** mostra o nome da rede Wi-Fi 2.4G à qual o Gateway está conectado, juntamente com o status e o modo de segurança da conexão de rede Wi-Fi do Gateway.
 - O botão **EDIT** permite definir as configurações particulares da rede Wi-Fi 2.4G e os ajustes de filtro MAC.
- **Private WiFi Network 5G** mostra o nome da rede Wi-Fi 5G à qual o Gateway está conectado, juntamente com o status e o modo de segurança da conexão de rede Wi-Fi do Gateway.
 - O botão **EDIT** permite definir as configurações particulares da rede Wi-Fi 5G e as configurações do filtro MAC.

Os botões **ADD WIFI 2.4G PROTECTED SETUP (WPS) CLIENT** e **ADD WIFI 5G PROTECTED SETUP (WPS) CLIENT** na parte inferior da página permitem ativar ou desativar o WPS para essas redes, adicionar clientes sem fio e desfazer bloqueios do WPS 2. Consultar “Ajustes de configuração de WPS”.

A opção **RESTORE DEFAULT SETTINGS** na parte inferior da página faz que o Gateway retorne às configurações padrão de fábrica.

- Sistema
- Conexão
 - Status da Rede
 - Status do CM
 - Rede de IP Local
 - Wi-Fi**
 - WAN
 - Firewall
 - Software
- Hardware
- Dispositivos conectados
- Controle de Pais
- Avançado
- Solução de problemas
- MSO

Sistema > Conexão > Wi-Fi

Ver informações técnicas sobre sua conexão Wi-Fi. Clique Adicionar WP S para adicionar clientes WiFi a sua rede.

Modo da antena

modo	Status	Protocolos		
Modo 2.4GHz	Habilitado	802.11 b/g/n	EDITAR	EDITAR MSO
Modo 5GHz	Habilitado	802.11 a/n/ac	EDITAR	EDITAR MSO

Rede Wi-Fi 2.4GHz

Nome	Status	Modo de Segurança	
NET_2GFAD59C	Habilitado	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_1	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_2	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_3	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_4	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_5	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_6	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_2GFAD59C_7	Desativar	WPA2-PERSONAL-AES	EDITAR

Rede Wi-Fi 5GHz

Nome	Status	Modo de Segurança	
NET_5GFAD59C	Habilitado	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_1	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_2	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_3	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_4	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_5	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_6	Desativar	WPA2-PERSONAL-AES	EDITAR
NET_5GFAD59C_7	Desativar	WPA2-PERSONAL-AES	EDITAR

[ADICIONAR CLIENTE DE CONFIGURAÇÃO PROTEGIDA DE WI-FI 2.4G\(WP S\)](#) [ADICIONAR CLIENTE DE CONFIGURAÇÃO PROTEGIDA DE WI-FI 5G\(WP S\)](#)

[RESTAURAR CONFIGURAÇÃO PADRÃO DE WI-FI](#)

[RESTAURAR WI-FI](#)

Edição da configuração básica do modo de rádio

A área do **modo de rádio** da página WiFi fornece um botão **EDIT** para editar os ajustes básicos dos rádios sem fio de 2,4 GHz e 5 GHz do Gateway.

O procedimento a seguir descreve como alterar as configurações básicas do modo de rádio para os rádios sem fio do Gateway. Há botões **EDIT** separados para os rádios de 2,4 GHz e 5 GHz do Gateway.

1. Em **Radio Mode**, clique no botão **EDIT** ao lado do rádio relevante:

– Para configurações de rádio Wi-Fi de 2,4 GHz, aparece uma página semelhante a página à esquerda.

– Para configurações de rádio Wi-Fi de 5 GHz, aparece uma página semelhante à página direita.

2. Preencha as opções da página.

3. Clique em **SAVE SETTINGS**.

Editar opções de configuração de rede WiFi privada

Opções	Descrição
Band Status	Ativa ou desativa o rádio de 2,4 GHz ou 5 GHz do Gateway. <ul style="list-style-type: none">• Se você clicou no botão EDIT de 2.4G, ativa ou desativa o rádio de 2,4 GHz do Gateway.• Se você clicou no botão EDIT de 5G, ativa ou desativa o rádio de 5 GHz do Gateway.
Mode Mode 2.4G	Utilize este campo para selecionar o modo sem fio do Gateway: Se você clicou no botão EDIT de 2.4G, as opções são: <ul style="list-style-type: none">• 802.11 b = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11b.• 802.11 g = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11g.• 802.11 n = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11n.• 802.11 b/g = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11b e dispositivos 802.11g.• 802.11 g/n = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11g e dispositivos 802.11n.• 802.11 b/g/n = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11b, 802.11g e dispositivos 802.11n.
Mode 5G	Se você clicou no botão EDIT de 5G, as opções são: <ul style="list-style-type: none">• 802.11 a = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11a.• 802.11 a/n = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11a e dispositivos 802.11n.• 802.11 ac = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11ac• 802.11 n/ac = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11n e dispositivos 802.11ac.• 802.11 a/n/ac = selecione esta configuração se a rede sem fio possuir apenas dispositivos IEEE 802.11a, 802.11n e dispositivos 802.11ac.
Channel Selection	Selecione como o gateway selecionará um canal para comunicação pela rede sem fio. As opções são: <ul style="list-style-type: none">• Automatic = o Gateway seleciona o canal automaticamente.• Manual = o Gateway usa o canal especificado na opção Channel.
Channel	Se a Channel Selection estiver definido como Manual, selecione um canal no qual o rádio deve operar. Esta opção não aparece quando a seleção de canais está

	definida como Automática.
Botão SAVE SETTINGS	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.

Opções	Descrição
Configuração de rede WiFi privada	
Enable/Disable Private WiFi	Ativa ou desativa a operação de banda de 2,4/5 GHz do Wi-Fi privado do Gateway.
Network Name (SSID)	Digite um nome para a rede sem fio. O nome do Wi-Fi tornará mais fácil que usuários de outros dispositivos saibam a que rede estão se conectando.
Security Mode	<p>Para evitar que outros computadores na área usem sua conexão com a Internet, proteja sua rede sem fio selecionando um método de criptografia desta lista suspensa. Existem várias opções disponíveis, entre elas as seguintes. (Risky aparece ao lado de opções que fornecem pouca ou nenhuma proteção.)</p> <p>OPEN = as transmissões sem fio não estão protegidas.</p> <p>WEP = criptografia básica e, portanto, menos segura (ou seja, pode ser facilmente quebrada, mas é compatível com uma ampla gama de dispositivos, incluindo hardware mais antigo). As opções WEP 64- e 128-bit estão disponíveis.</p> <p>WPA-PERSONAL-T KIP (TKIP) = um padrão de Wi-Fi que é mais forte que a criptografia WEP. Esta seleção usa a criptografia TKIP (Temporal Key Integrity Protocol) para fornecer proteção contra hackers. Se desejar o WPA, cada dispositivo da sua rede sem fio deverá usar o mesmo método WPA e senha de rede, ou a rede não funcionará corretamente.</p> <p>WPA2-PERSONAL = há várias versões disponíveis. Alguns usam criptografia TKIP, enquanto outros usam o AES (Advanced Encryption System), que utiliza uma criptografia simétrica de dados em bloco de 128 bits. WPA2 Personal é mais forte que a criptografia WPA. Cada dispositivo da sua rede sem fio deverá usar o mesmo método WPA e senha de rede, ou a rede não funcionará corretamente.</p> <p>WPA-ENTERPRISE = esta opção usa WPA e deve ser usada com um servidor RADIUS conectado ao gateway. Cada dispositivo da sua rede sem fio deverá usar o mesmo método WPA e senha de rede, ou a rede não funcionará corretamente. Esta configuração exige que um servidor RADIUS seja conectado ao gateway.</p> <p>WPA2-ENTERPRISE = essa opção usa o WPA2 e deve ser usada com um servidor RADIUS conectado ao Gateway. WPA2-ENTERPRISE é compatível com dois métodos de criptografia, TKIP e AES, com chaves de criptografia dinâmicas. Selecione o tipo de algoritmo, AES ou TKIP. Cada dispositivo da sua rede sem fio deverá usar o mesmo método WPA e senha de rede, ou a rede não funcionará corretamente. Esta configuração exige que um servidor RADIUS seja conectado ao gateway.</p> <p>WPA-WPA2-ENTERPRISE = permite que seus dispositivos se conectem usando a opção de segurança compatível mais forte, WPA ou WPA2. Cada dispositivo da sua rede sem fio deverá usar o mesmo método WPA e senha de rede, ou a rede não funcionará corretamente. Esta configuração exige que um servidor RADIUS seja conectado ao gateway.</p>
Network Password	<p>Se selecionar um dos ajustes de criptografia WEP, WPA ou WPA2, insira a senha que diferencia maiúsculas de minúsculas usada para criptografia e descryptografia. Por segurança, cada caractere de senha digitado é mascarado com um ponto (*). Se especificar uma senha hexadecimal, use as letras de A a F e os números de 0 a 9.</p> <p>WEP 64 requer uma senha com 5 caracteres ASCII ou 10 caracteres hexadecimais.</p> <p>WEP 128: requer uma senha com 13 caracteres ASCII ou 16 caracteres hexadecimais.</p> <p>Os demais métodos de criptografia requerem uma senha com 8 caracteres ASCII ou 64 caracteres hexadecimais.</p>

WEP 802.1x	Se Security Mode estiver definido como uma das opções WEP, use esta opção para ativar ou desativar o WEP 802.1x. WEP 802.1x é um protocolo de segurança robusto que usa o controle de porta com chaves de criptografia dinamicamente alteradas, atualizadas automaticamente pela rede. WEP 802.11x usa um servidor RADIUS (Remote Authentication Dial-in Service) para fins de autenticação. Este servidor deve estar fisicamente conectado ao Gateway. Se habilitar essa opção, defina as próximas três opções do RADIUS.
Radius Server IP	Se o WEP 802.1x estiver ativado, digite o endereço IP do servidor RADIUS.
Port	Se o WEP 802.1x estiver ativado, digite o número da porta do servidor RADIUS.
Radius Password	Se o WEP 802.1x estiver ativado, digite a senha do servidor RADIUS.
Broadcast Network Name (SSID)	Marque para ativar a transmissão do SSID. Quando os dispositivos sem fio pesquisam redes sem fio com as quais se associam, eles detectam a transmissão SSID pelo Gateway. Se ativado, o SSID da rede sem fio do Gateway será transmitido sem fio.

Opções	Descrição
WMM Enable	<p>Wi-Fi Multimedia (WMM) WMM usa um protocolo chamado EDCA (Enhanced Distributed Channel Access) para priorizar o tráfego na rede sem fio. A habilitação dessa configuração ajuda nos aplicativos de streaming, como áudio, vídeo e voz sobre conexões sem fio, se o dispositivo sem fio de destino também oferecer suporte ao WMM. Por exemplo:</p> <ul style="list-style-type: none"> • Em conversas por Voice Over IP (VoIP), é menos provável ouvir atrasos. • Assistindo a vídeos, é mais provável obter uma ação sem ruído. <p>Isso atrasa outros tráfegos de rede de natureza menos crítica, como o download de arquivos grandes, em que um pequeno atraso é aceitável.</p>
WMM Power Save	<p>Ativa ou desativa a economia de energia do WMM. O WMM Power Save oferece economia de energia avançada e é otimizado para aplicativos sensíveis à latência, como aplicativos de telefonia VOIP via Internet e aplicativos que transmitem tráfego de áudio e vídeo. WMM Power Save usa menos quadros para transmitir a mesma quantidade de dados em um tempo menor e estende o tempo em que os dispositivos podem permanecer em um estado de baixa energia.</p>
Botão SAVE SETTINGS	<p>Depois de definir os ajustes da Rede WiFi Privada nesta página, clique neste botão para salvar os ajustes.</p>
Ajuste de filtro Mac	
Mac Filtering Mode	<p>O modo de filtragem de endereço do controle de acesso à mídia (MAC) controla o acesso à rede com base no endereço MAC do adaptador de rede. Um endereço MAC é um ID exclusivo atribuído pelo fabricante do adaptador de rede. Este recurso pode ser configurado para permitir tudo, permitir ou negar acesso à rede/Internet a dispositivos com base em seu endereço MAC. O endereço MAC pode ser memorizado automaticamente pelo Gateway ou especificado manualmente usando as opções em Index MAC Address.</p> <p>Use esta lista suspensa para selecionar o método utilizado pelas estações do cliente para se conectar ao Gateway. As opções são:</p> <p>Allow-All = permite que todas as estações sem fio se conectem (autentiquem-se) na rede Wi-Fi.</p> <p>Allow = permite que apenas o endereço MAC memorizado automaticamente ou inserido manualmente especificado em Index MAC Address conecte-se à rede Wi-Fi.</p> <p>Deny = Impede que o endereço MAC memorizado automaticamente ou inserido manualmente especificado em Index MAC Address conecte-se à rede Wi-Fi.</p>
Index MAC Address	<p>Especifique como a lista de filtros MAC é preenchida. As opções são:</p> <p>Auto-Learned Wireless Devices = o Gateway memoriza os endereços MAC dos dispositivos cuja presença ele memorizou automaticamente.</p> <p>Manually Added Wireless Devices = insira o endereço MAC do dispositivo.</p>
Botão SAVE FILTER SETTING	<p>Depois de configurar os Ajustes de filtro Mac nesta página, clique neste botão para salvar os ajustes.</p>

Ajustes de configuração de WPS

A página WIFI fornece dois botões para definir os ajustes de WPS:

- **ADD WIFI 2.4G PROTECTED SETUP (WPS) CLIENT** permite definir os ajustes WPS para o rádio sem fio de 2,4 GHz do Gateway.
- **ADD WIFI 5G PROTECTED SETUP (WPS) CLIENT** permite definir os ajustes WPS para o rádio sem fio de 5 GHz do Gateway.

Os ajustes de WPS para os rádios sem fio de 2,4 GHz e 5 GHz são os mesmas.

Também é possível exibir essas páginas clicando em **ADD WIFI PROTECTED SETUP (WPS 2.4G) CLIENT** ou **ADD WIFI PROTECTED SETUP (WPS 5G) CLIENT** em Connected Devices > Computers page.

Observação: Ative o WPS antes que um dispositivo sem fio possa se conectar ao Gateway usando o WPS. Para configurar os ajustes de WPS:

1. Clique no botão **ADD WIFI PROTECTED SETUP (WPS) CLIENT** relativo ao rádio sem fio que deseja configurar:

– Para configurações de rádio Wi-Fi de 2,4 GHz, aparece uma página semelhante a página à esquerda.

– Para configurações de rádio Wi-Fi de 5 GHz, aparece uma página semelhante à página direita.

2. Preencha as opções da página WPS.

Opções da página WPS

Opções	Descrição
Ativar/Desativar WPS	
WPS	Ativa ou desativa o WPS. Se você clicar em Enabled, preencha os campos restantes na página.
Security	Um campo somente leitura que mostra os ajustes de segurança do Gateway.
Encryption	Um campo somente leitura que mostra os ajustes de criptografia do Gateway.
AP PIN	Um campo somente leitura que mostra o número de identificação pessoal do ponto de acesso.
Configured Status	Um campo somente leitura que mostra o status de configuração do Gateway. Clicar em RESET TO UNCONFIGURED redefine os ajustes WPS à sua configuração padrão.
Adicionar cliente sem fio (WPS)	
Opções de conexão	Selecione o método usado para estabelecer a conexão WPS (Wi-Fi Protected Setup) entre dispositivos sem fio e o gateway. As opções são: Push Button = selecione essa opção para usar o botão WPS no painel frontal do Gateway e o dispositivo sem fio para fazer a conexão. Pin Number = um PIN é um número único que pode ser usado para adicionar um cliente a uma rede existente ou para criar uma nova rede. Selecione esta opção para inserir um PIN de 8 dígitos para configurar o WPS. Depois, insira o mesmo PIN de oito dígitos no campo Wireless Client's PIN e no cliente sem fio para

	estabelecer a conexão sem fio.
Wireless Client's PIN	Se Connection Options estiver definido como Pin Number, insira o PIN utilizado com o cliente sem fio para estabelecer a conexão sem fio. Essa opção não aparece se Connection Options estiver definido como Push Button.
Botão PAIR	Se Connection Options estiver definido como Push Button, clique neste botão e pressione o botão WPS no cliente sem fio para criar a conexão sem fio. A conexão sem fio é feita em dois minutos. Você também pode pressionar o botão WPS no painel frontal deste Gateway para iniciar o WPS em vez de clicar no botão PAIR.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.
WPS Lock Status	
lock_status	Um campo somente leitura que mostra o status de bloqueio do Gateway. O WPS é um método para configurar um novo Gateway sem fio usando um botão ou PIN. O WPS possui uma vulnerabilidade que torna o PIN suscetível a tentativas de força bruta. O Gateway protege-se após várias tentativas de autenticação por PIN mal sucedidas, entrando em estado de bloqueio. Durante o estado de bloqueio, nenhuma das tentativas de WPS usando o PIN do Gateway funcionará. Enquanto o Gateway estiver em estado de bloqueio, os usuários ainda poderão usar o método do botão WPS para se conectar à rede sem fio. Clicar em UNLOCK faz o gateway retornar ao estado de bloqueio.

WAN

Connection > WAN

A página WAN mostra informações sobre a rede de longa distância (Wide Area Network), o modem a cabo e os valores de ligação downstream e upstream. Essas informações são úteis ao entrar em contato com o atendimento ao cliente ou ao solucionar problemas técnicos.

Observação: Esta página também está disponível na página Status clicando em **VIEW** na área **WAN IP Network**.

The screenshot shows the NET router configuration interface. The top left features the NET logo with the tagline 'O MUNDO E DOS NETS'. The top right has links for 'Sair' and 'Alterar senha', along with status indicators for 'Internet' (red X), 'Wi-Fi' (green check), and 'Segurança baixa' (red X). The main navigation menu on the left includes 'Sistema', 'Conexão', 'Status da Rede', 'Status do CM', 'Rede de IP Local', 'Wi-Fi', 'WAN', 'Firewall', 'Software', 'Hardware', 'Dispositivos conectados', 'Controle de Pais', 'Avançado', 'Solução de problemas', and 'MSO'. The current page is titled 'Sistema > Conexão > WAN'. Below the title, there is a link to 'Ver informações técnicas relacionadas à sua conexão CM.' and a 'mais' link. The 'Switch Mode' section shows 'Modo IP WAN' with 'Bridge' and 'Roteador' buttons. The 'Endereço IP WAN' section has a 'Configurar Endereço IP WAN' toggle (currently 'Habilitado') and input fields for 'Endereço IP WAN' (0.0.0.0), 'Máscara de Subrede IP WAN' (255.255.254.0), and 'Endereço do Gateway IP WAN' (189.102.206.1). The 'Endereço DNS' section has a 'Configurar Endereço DNS' toggle (currently 'Habilitado') and input fields for 'DNS primário' (0.0.0.0) and 'DNS secundário' (0.0.0.0). At the bottom, there are 'SALVAR CONFIGURAÇÕES' and 'CANCELAR' buttons.

WAN	
Opções	Descrição
Internet	Um campo somente leitura que mostra o status da conexão com a Internet.
System Uptime	Um campo somente leitura que mostra o tempo de atividade do sistema desde a inicialização.
WAN IP Address	Um campo somente leitura que mostra o endereço WAN IP v4 obtido do provedor de serviços.
WAN IPv6 Address	Um campo somente leitura que mostra o endereço WAN IP v6 obtido do provedor de serviços.
Prefix	Um campo somente leitura que mostra o tamanho do prefixo IPv6.
DHCP Client	Um campo somente leitura que mostra se a função DHCP Client está ativada ou desativada.
DHCP Expiry Time	Um campo somente leitura que mostra o tempo expirado atualmente à esquerda do cliente DHCP. Quando o tempo expirar, a configuração pode parar de funcionar.
CM MAC	Um campo somente leitura que mostra o endereço MAC do CM.
WAN MAC	Um campo somente leitura que mostra o endereço MAC da interface WAN do Gateway.
Modem a cabo	
Campos somente leitura que mostram informações técnicas relacionadas ao seu modem a cabo, como a versão do hardware, o fornecedor e as versões de boot e core.	
Ligação downstream de canal	
A ligação downstream de canal permite que o Gateway receba tráfego downstream em múltiplos canais downstream. Esses campos somente leitura mostram os valores de ligação downstream de canal, como ID do canal, frequência, relação sinal-ruído, potência e modulação.	
Ligação upstream de canal	
A ligação upstream de canal é uma forma de aumentar a largura de banda upstream transmitindo dados em múltiplos canais upstream em simultâneo. Esses campos somente leitura mostram os valores de ligação upstream de canal, como ID do canal, frequência, nível de potência, início e fim de backoff de intervalo e modulação.	

Ajustes de Firewall

Gateway > Firewall

O Gateway inclui um firewall interno cujo nível de segurança pode ser selecionado usando a página Firewall Settings. Os níveis de segurança variam de mínimo (baixa segurança) a máximo (alta segurança).



Página de ajustes de Firewall

Para selecionar um nível de segurança, clique no botão de opção ao lado do nível e em **SAVE SETTINGS**. Para ver a proteção associada a um nível de segurança, clique no nome do nível de segurança para expandir o nível de segurança.

• **Segurança máxima (Alta)**

Allow (LAN-to-WAN):

- HTTP and HTTPS (TCP port 80, 443)
- FTP (TCP port 21)
- DNS (TCP/UDP port 53)
- NTP (TCP ports 119, 123)
- email (TCP ports 25, 110, 143, 465, 587, 993, 995)
- VPN(GRE, UDP 500, TCP 1723)
- iTunes (TCP port 3689)

Clicar no nível de segurança sublinhado...

...exibe essa lista expandida de itens permitidos ou bloqueados.

Exemplo de expansão da segurança máxima

Ao clicar nas palavras da opção **Custom Security** (não no botão de opções ao lado das palavras), as opções serão exibidas. É possível então escolher as opções desejadas para personalizar os ajustes de segurança para atender às suas necessidades. Depois de verificar as opções desejadas, clique no botão de opções para selecionar a segurança personalizada.

• **Segurança Personalizada**

Blocked (LAN-to-WAN):

- Desativar firewall
- Block http (TCP ports 80, 443)
- Bloquear ICMP
- Bloquear Multicast
- Bloquear aplicações Peer-to-peer
- Bloquear IDENT (port 113)

Exemplo de expansão da segurança personalizada

Opções da página de ajustes de Firewall

Opções	Descrição
Maximum Security (High)	Máxima segurança é o nível mais alto de segurança do firewall. Este nível bloqueia todos os aplicativos, incluindo aplicativos de voz (como Gtalk e Skype) e aplicativos P2P, mas permite serviços de navegação na Internet, e-mail, VPN, DNS e iTunes.
Typical Security (Medium)	A segurança típica é o nível médio de segurança do firewall. Este nível bloqueia aplicativos P2P e emite ping para o Gateway, e ao mesmo tempo permite todos os outros tráfegos.
Minimum Security (Low)	A segurança mínima é o nível mais baixo de segurança do firewall. Não bloqueia aplicativos e tráfego. Selecione este nível se não estiver familiarizado com as configurações do firewall.
Custom Security	Esse nível de segurança é pré-configurado para bloquear todo o acesso à rede local da Internet, exceto "computadores confiáveis" definidos na página Managed Sites e na página Managed Services. Somente serviços comumente utilizados, como navegação na Web e e-mail, são permitidos. Se selecionar esta opção, uma lista de caixas de seleção permitirá desativar todo o firewall ou bloquear determinado tráfego.
Botão SAVE SETTINGS	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão RESTORE DEFAULT SETTINGS	Clique neste botão para fazer que o Gateway retorne aos seus ajustes padrão. Não é exibida nenhuma mensagem de alerta antes de o Gateway retornar aos seus ajustes padrão. Se clicar nesse botão, o Gateway deixará a interface de gerenciamento da Web e será necessário efetuar login na interface novamente.

Versão do software do gateway

Gateway > Software

A página de versão do software do gateway apresenta:

- Versão de software de eMTA e DOCSIS
- Nome do modem packetcable



The screenshot shows the NET gateway management interface. At the top left is the NET logo with the tagline 'O MUNDO É DOS NETS'. At the top right, there are status indicators for Internet (red X), Wi-Fi (green checkmark), and Segurança baixa (red X). Below the logo is a navigation menu with options: Sistema (selected), Status, Conexão, Firewall, Software, Hardware, Dispositivos conectados, Controle de Pais, Avançado, Solução de problemas, and MSO. The main content area is titled 'Sistema > Software' and contains a sub-header 'Sistema Versão de Software'. Below this, there is a box with the text 'Versão de Software (eMTA & DOCSIS):' and 'BRGCAA 1.1.53-test'. Below that, another box shows 'Packet Cable: PacketCable 1.5'. At the top right of the main content area, there are links for 'Sair' and 'Alterar senha', and a 'mais' link next to the sub-header.

Página de versão do software do gateway

Informação de hardware do sistema

Gateway > Hardware > System Hardware

A página System Hardware Info mostra as seguintes informações sobre o hardware do Gateway:

- Modelo, identificador de hardware e número de série
- Velocidade do processador
- Memória Dinâmica de Acesso Aleatório (DRAM) e flash

The screenshot shows the NET gateway's system hardware information page. The page title is "Sistema > Hardware > Hardware do sistema". The left sidebar contains a navigation menu with the following items: Sistema (selected), Conexão, Firewall, Software, Hardware (expanded), Hardware do sistema (selected), Wi-Fi, Dispositivos conectados, Controle de Pais, Avançado, Solução de problemas, and MSO. The main content area displays the following information:

- Modelo: HGA12R-02
- Identificador HW: 1.0
- Serial Number: 7 618013171869
- Velocidade do Processador Arm:
- Velocidade do Processador Atom: 1: 1200.00 ; 2: 1200.00 [DogoMIPS]
- DRAM: 512 MB
- Flash: 256 MB

At the top right of the page, there are status indicators for Internet (red X), Wi-Fi (green checkmark), and Segurança baixa (red X). There are also links for "Sair" and "Alterar senha".

Página de informações de hardware do sistema

Informações de hardware sem fio

Gateway > Hardware > Wireless

O Gateway suporta conexões sem fio Wi-Fi simultâneas de 2,4 GHz e 5 GHz. A página de informações de hardware sem fio mostra o status do link Wi-Fi e o endereço MAC das portas LAN Wi-Fi de 2,4 GHz e 5 GHz do Gateway.

Se um cliente sem fio estiver conectado às portas LAN Wi-Fi do Gateway, o **Status do link WiFi** estará **Ativo** para essa porta; caso contrário, o **status do link WiFi** estará **inativo**.

Observação: Esta página também está disponível na página Status ao clicar em **VIEW** na área **WiFi Network 2.4G** ou **WiFi Network 5G**.

The screenshot shows the NET Gateway web interface. At the top left is the NET logo with the tagline 'O MUNDO É DOS NETS'. At the top right, there are links for 'Sair' and 'Alterar senha', and status indicators for 'Internet' (red X), 'Wi-Fi' (green checkmark), and 'Segurança baixa' (red X). The main navigation menu on the left includes 'Sistema', 'Conexão', 'Firewall', 'Software', 'Hardware', 'Dispositivos conectados', 'Controle de Pais', 'Avançado', 'Solução de problemas', and 'MSO'. The 'Hardware' section is expanded to show 'Hardware do sistema' and 'Wi-Fi'. The main content area is titled 'Sistema > Hardware > Wi-Fi' and contains a message: 'Seu Gateway oferece simultâneos 2,4 GHz e 5 GHz Wi-Fi para se conectar à rede Wi-Fi.' Below this are two panels for 'Porta LAN Wi-Fi (2.4 GHz)' and 'Porta LAN Wi-Fi (5 GHz)'. Both panels show 'Status do link Wi-Fi Inativo' and 'Endereço MAC: 40:3D:EC:FA:D5:A9'.

Página de informações de hardware sem fio

Computadores

Connected Devices > Computers

O Gateway usa o DHCP para descobrir automaticamente os computadores conectados a ele e exibe essas informações na página Computers. Esta página contém duas áreas:

- **Online Computers** mostra computadores conectados atualmente on-line.
- **Offline Computers** mostra dispositivos que foram conectados à sua rede, mas não estão conectados no momento.

Na parte inferior da página, os botões **ADD WIFI PROTECTED SETUP (WPS 2.4G) CLIENT** e **ADD WIFI PROTECTED SETUP (WPS 5G) CLIENT** permite ativar ou desativar o WPS, adicionar clientes sem fio e liberar bloqueios do WPS. Para maiores informações, consulte “Ajustes de WPS”.

Observação: Ative o WPS antes que um dispositivo sem fio possa se conectar ao Gateway usando o WPS.



The screenshot shows the NET Gateway web interface. At the top left is the NET logo with the tagline "O MUNDO É DOS NETS". At the top right, there are status indicators for Internet (red X), Wi-Fi (green checkmark), and Segurança baixa (red X). Below the logo is a navigation menu with options: Sistema, Dispositivos conectados (selected), Dispositivos, Controle de Pais, Avançado, Solução de problemas, and MSO. The main content area is titled "Dispositivos conectados > Dispositivos" and contains a sub-header "Ver os computadores conectados à rede local do Gateway." with a "mais" link. There are two tables: "Dispositivos Online" and "Dispositivos desligados".

Nome do Dispositivo	Endereço IP	DHCP/IP estático	Conexão	Endereço MAC
laptop-5iq 1pjo2	192.168.0.97	dhcp	ethernet	64:1C:67:86:56:AF

Nome do Dispositivo	Endereço IP	DHCP/IP estático	Conexão	Endereço MAC
hbr_eng_02	192.168.0.14	dhcp	ethernet	64:1C:67:6C:66:05

At the bottom of the interface, there are two buttons: "ADICIONAR CLIENTE DE CONFIGURAÇÃO PROTEGIDA DE WI-FI 2.4G(WPS)" and "ADICIONAR CLIENTE DE CONFIGURAÇÃO PROTEGIDA DE WI-FI 5G(WPS)".

Página de computadores

Menu de controle parental

Controlar a navegação na Web pode impedir que crianças e funcionários acessem conteúdo perigoso na Internet, ou tenham que julgar quais relacionamentos seriam adequados em salas de bate-papo. O fato é que sites, usuários de sala de bate-papo e programas baixados podem não oferecer o melhor para você, sua família ou seus funcionários. Os inescrupulosos podem tentar manipular as pessoas de quem você gosta ou tentar ganhar confiança, o que pode oferecer um acesso inaceitável à sua família, seus colegas de trabalho, seu computador ou informações pessoais.

O menu Parental Control contém as seguintes páginas para controlar o acesso à Internet:

- **Managed Sites** - restringe o acesso a determinados sites e palavras-chave e define computadores confiáveis que podem acessar esses sites e palavras-chave.
- **Managed Services** - restringe o acesso a serviços e define computadores confiáveis que podem acessar esses serviços.
- **Managed Devices** - configura a lista de dispositivos para permitir ou bloquear a conexão com a rede.
- **Reports** – gera, imprime e faz download de relatórios.

Sites gerenciados

Parental Control > Managed Sites

A página Managed Sites permite configurar:

- Sites bloqueados
- Senhas bloqueadas
- Computadores confiáveis que podem acessar sites e palavras-chave bloqueados

The screenshot displays the NET parental control interface. At the top left is the NET logo with the tagline 'O MUNDO É DOS NETS'. On the top right, there are links for 'Sair' and 'Alterar senha', and status indicators for 'Internet', 'Wi-Fi', and 'Segurança baixa'. A left sidebar contains a navigation menu with categories: Sistema, Dispositivos conectados, Controle de Pais (selected), Avançado, Solução de problemas, and MSO. Under 'Controle de Pais', there are sub-items: Gerenciamento de Sites (selected), Gerenciamento de Serviços, and Gerenciamento de Dispositivos. The main content area is titled 'Controle de Pais > Gerenciamento de Sites'. It includes a description: 'Restringir o acesso a sites específicos para a identificação computadores / dispositivos nesta rede.' Below this, there are three main sections: 1. 'Gerenciamento de Sites para Controle de Pais Managed Sites' with a 'Habilitar Filtro' toggle set to 'Desativado'. 2. 'Sites bloqueados' with a '+ ADICIONAR' button and a table with columns 'URL' and 'Quando'. 3. 'Palavra-chave bloqueada' with a '+ ADICIONAR' button and a table with columns 'Palavra-chave' and 'Quando'. 4. 'Dispositivos confiáveis' with a '+ ADICIONAR' button and a table with columns 'Nome do dispositivo', 'MAC', and 'Confiável'. The table for 'Dispositivos confiáveis' contains two entries: 1. 'hbr_eng_02' with MAC '64:1C:67:6C:66:05' and 'Confiável' buttons 'Não' and 'Sim'. 2. 'laptop-5iq1pjo2' with MAC '64:1C:67:86:56:AF' and 'Confiável' buttons 'Não' and 'Sim'.

Página de sites gerenciados

Configuração de sites bloqueados

Usando a página Managed Sites, é possível bloquear o acesso a determinados sites de computadores locais. Para definir sites bloqueados na página Managed Sites:

1. Na tabela **Blocked Sites**, clique no botão **+ADD**. A página Add Blocked Sites é exibida.
2. Preencha os campos da página Add Blocked Sites.
3. Clique em **SAVE**. O URL bloqueado e o horário de início e término do bloqueio do URL aparecem na tabela Blocked Sites da página Managed Sites.
4. Ao lado de **Enable Filter** na página Managed Sites, clique em **Enabled** para ativar os filtros de controle parental configurados nesta página. (Para desativar os filtros de controle parental configurados nesta página, clique em **Disabled**.)
5. Para editar um site bloqueado, clique no botão **EDIT** ao lado do site bloqueado que deseja modificar, edite os ajustes e clique em **SAVE**.
6. Para excluir um site bloqueado, clique no **X** ao lado do site. Quando uma mensagem de alerta for exibida, clique em **OK** para excluir o site bloqueado ou **CANCEL** para mantê-lo.

NET
O MUNDO E DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Controle de Pais > Gerenciamento de Sites

Restringir o acesso a sites específicos para a identificação computadores / dispositivos nesta rede. [mais](#)

Gerenciamento de Sites para Controle de Pais Managed Sites

Habilitar Filtro: **Habilitado** Desativado

Sites bloqueados

+ ADICIONAR

URL	Quando
-----	--------

Palavra-chave bloqueada

+ ADICIONAR

Palavra-chave	Quando
---------------	--------

Dispositivos confiáveis

+ ADICIONAR

	Nome do dispositivo	MAC	Confiável
1	hbr_eng_02	64:1C:67:6C:66:05	Não Sim
2	laptop-5iq1pjo2	64:1C:67:86:56:AF	Não Sim

Página Add Blocked Sites

Opções da página Add Blocked Sites

Opções	Descrição
URL	Digite o URL do site que deseja bloquear.
Always Block?	Selecione se deseja que o Gateway sempre bloqueie esse URL. As opções são: <ul style="list-style-type: none">• No = o Gateway nem sempre bloqueia esse URL. Use Set Block Time e Set Blocked Days para dizer ao Gateway quando iniciar e interromper o bloqueio deste URL.• Yes = o Gateway sempre bloqueia esse URL até que se interrompa o bloqueio.
Set Block Time	Se definir Always Block como No, selecione a hora em que o Gateway bloqueará esse URL. <ul style="list-style-type: none">• Start from = selecione a hora de início do bloqueio do URL pelo Gateway.• End on = selecione a hora de término do bloqueio do URL pelo Gateway.
Set Blocked Days	Se definir Always Block como No, selecione os dias em que o Gateway bloqueará esse URL. Links e caixas de seleção estão disponíveis para selecionar todos os dias nenhum dia ou dias individuais da semana. <ul style="list-style-type: none">• Select All = Clique neste link para selecionar todos os sete dias.• Select None = Clique neste link para desmarcar os sete dias.• Monday - Sunday = marque as caixas de seleção que correspondem aos dias em que deseja que o Gateway bloqueie esse URL.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Configuração de palavras-chave bloqueadas

Usando a página Managed Sites, é possível bloquear o acesso a determinadas palavras-chave de computadores locais. Para definir palavras-chave bloqueadas na página Managed Sites:

1. Na tabela **Blocked Keywords**, clique no botão **+ADD**. A página **Add Blocked Keywords** é exibida.
2. Preencha os campos da página **Add Blocked Keywords**.
3. Clique em **SAVE**. A palavra-chave bloqueada e o horário de início e término do bloqueio da palavra-chave aparecem na tabela Blocked Sites da página Managed Sites.
4. Ao lado de **Enable Filter** na página Managed Sites, clique em **Enabled** para ativar os filtros de controle parental configurados nesta página. (Para desativar os filtros de controle parental configurados nesta página, clique em **Disabled**.)
5. Para editar uma palavra-chave bloqueada, clique no botão **EDIT** ao lado da palavra-chave bloqueada que deseja modificar, edite os ajustes e clique em **SAVE**.
6. Para excluir uma palavra-chave bloqueada, clique no **X** ao lado da palavra-chave. Quando uma mensagem de alerta aparecer, clique em **OK** para excluir a palavra-chave bloqueada ou **CANCEL** para mantê-la.



The screenshot displays the NET parental control interface. The top left features the NET logo with the tagline 'O MUNDO É DOS NETS'. The top right shows user options: 'Sair' and 'Alterar senha', along with status indicators for 'Internet', 'Wi-Fi', and 'Segurança baixa'. The main navigation menu on the left includes 'Sistema', 'Dispositivos conectados', 'Controle de Pais', 'Avançado', and 'Solução de problemas'. The 'Controle de Pais' section is expanded, showing 'Gerenciamento de Sites' as the active sub-section. The main content area is titled 'Controle de Pais > Gerenciamento de Sites > Adicionar bloqueio de palavras-chave'. A modal window titled 'Adicionada palavra-chave a ser bloqueada' is open, containing the following fields and options: 'Palavra-chave:' (text input), 'Bloquear sempre?' (radio buttons for 'Não' and 'Sim'), 'Definir Tempo de Bloqueio' (start and end time pickers), and 'Set Blocked Days' (checkboxes for days of the week, all of which are checked). At the bottom of the modal are 'SALVAR' and 'CANCELAR' buttons.

Página Add Blocked Keywords

Opções da página Add Blocked Keywords

Opções	Descrição
Keyword	Digite a palavra-chave que deseja bloquear.
Always Block?	Selecione se deseja que o Gateway sempre bloqueie essa palavra-chave. As opções são: <ul style="list-style-type: none">• No = o Gateway nem sempre bloqueia essa palavra-chave. Use Set Block Time e Set Blocked Days para dizer ao Gateway quando iniciar e interromper o bloqueio desta palavra-chave.• Yes = o Gateway sempre bloqueia essa palavra-chave até que se interrompa o bloqueio.
Set Block Time	Se definir Always Block como No, selecione a hora em que o Gateway bloqueará essa palavra-chave. <ul style="list-style-type: none">• Start from = selecione a hora de início do bloqueio da palavra-chave pelo Gateway.• End on = selecione a hora de término do bloqueio do URL pela palavra-chave.
Set Blocked Days	Se definir Always Block como No, selecione os dias em que o Gateway bloqueará essa palavra-chave. Links e caixas de seleção estão disponíveis para selecionar todos os dias nenhum dia ou dias individuais da semana. <ul style="list-style-type: none">• Select All = Clique neste link para selecionar todos os sete dias.• Select None = Clique neste link para desmarcar os sete dias.• Monday - Sunday = marque as caixas de seleção que correspondem aos dias em que deseja que o Gateway bloqueie essa palavra-chave.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Configuração de computadores confiáveis

Na página Managed Sites, é possível definir computadores confiáveis com permissão para acessar sites e palavras-chave bloqueados.

Para configurar computadores confiáveis na página Managed Sites:

1. Na área **Trusted Computers**, clique no botão **+ADD**. A página Add Trust Computer é exibida.
2. Preencha os campos da página Add Trust Computer.
3. Clique em **SAVE**. O nome do computador confiável e seu endereço MAC são exibidos na tabela Trusted Computers da página Managed Sites.
4. Ao lado de **Enable Filter** na página Managed Sites, clique em **Enabled** para ativar os filtros de controle parental configurados nesta página. (Para desativar os filtros de controle parental configurados nesta página, clique em **Disabled**.)
5. Depois que um computador confiável for definido, use os botões **No** ou **Yes** ao lado do computador confiável na página Managed Sites para alternar entre confiáveis e não confiáveis.

NET
O MUNDO É DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Controle de Pais > Gerenciamento de Sites > Adicionar Dispositivo confiável

Adicionar Dispositivo do Usuário de Confiança

Nome do dispositivo:

MAC do computador:

SALVAR

Página Add Trust Computer

Opções da página Add Trust Computer

Opções	Descrição
Computer Name	Digite um nome para o computador que deseja designar como computador confiável. O nome deve ser único e permitir que se diferencie esse computador confiável de outros que se possam definir.
Computer MAC	Digite o endereço MAC do computador que deseja designar como o computador confiável.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.

Managed Services

Parental Control > Managed Services

A página Managed Services permite configurar:

- Serviços bloqueados
- Computadores confiáveis que podem acessar serviços bloqueados

The screenshot displays the 'Controle de Pais > Gerenciar Serviços' interface. At the top, there's a status bar with 'Internet' (disabled), 'Wi-Fi' (enabled), and 'Segurança baixa'. The sidebar on the left lists navigation options: Sistema, Dispositivos conectados, Controle de Pais (selected), Gerenciamento de Sites, Gerenciamento de Serviços, Gerenciamento de Dispositivos, Avançado, Solução de problemas, and MSO. The main content area features a search bar, a 'Gerenciar Serviços para Controle de Pais' section with 'Habilitar Serviços' set to 'Desativado', a 'Serviços bloqueados' table with columns for 'Serviços', 'Protocolo', 'Porta de início', 'Porta Final', and 'Quando', and a 'Dispositivos confiáveis' table with columns for 'Nome do dispositivo', 'MAC', and 'Confiável'. The trusted devices table contains two entries: 'hbr_eng_02' and 'laptop-5iq1pjo2', both with 'Não' selected in the 'Confiável' column.

Serviços	Protocolo	Porta de início	Porta Final	Quando
----------	-----------	-----------------	-------------	--------

Nome do dispositivo	MAC	Confiável
0 hbr_eng_02	64:1C:67:6C:66:05	<input checked="" type="radio"/> Não <input type="radio"/> Sim
1 laptop-5iq1pjo2	64:1C:67:86:56:AF	<input checked="" type="radio"/> Não <input type="radio"/> Sim

Página Managed Services

Configuração de serviços bloqueados

Usando a página Managed Services, é possível bloquear o acesso a determinados serviços de computadores locais. Para definir serviços bloqueados na página Managed Services:

1. Na área **Blocked Services**, clique no botão **+ADD**. A página Add Blocked Service é exibida.
2. Preencha os campos da página Add Blocked Service.
3. Clique em **SAVE**. O serviço bloqueado aparece na tabela Blocked Services na página Managed Services, junto com o protocolo associado, iniciando e interrompendo as portas e bloqueando o dia e a hora.
4. Ao lado de **Enable Services** na página Managed Services, clique em **Enabled** para ativar os filtros de controle parental configurados nesta página. (Para desativar os filtros de controle parental configurados nesta página, clique em **Disabled**.)
5. Para editar um serviço bloqueado, clique no botão **EDIT** ao lado do serviço bloqueado que deseja modificar, edite os ajustes e clique em **SAVE**.
6. Para excluir um serviço bloqueado, clique no **X** ao lado do serviço. Quando uma mensagem de alerta aparecer, clique em **OK** para excluir o serviço bloqueado ou **CANCEL** para mantê-la.

- › Sistema
- › Dispositivos conectados
- ▼ **Controle de Pais**
 - Gerenciamento de Sites
 - [Gerenciamento de Serviços](#)
 - Gerenciamento de Dispositivos
- › Avançado
- › Solução de problemas
- › MSO

Controle de Pais > Gerenciar Serviços > Adicionar bloqueio de serviço

Serviço bloqueado

Usuário de Serviço Definido:

Protocolo:

Porta de início:

Porta Final:

Bloquear sempre?

Definir Tempo de Bloqueio

Iniciar de:

Termina em:

Set Blocked Days [Selecionar todos](#) | [Selecionar nenhum](#)

- Segunda-feira
- Terça-feira
- Quarta-feira
- quinta-feira
- Sexta-Feira
- Sábado
- Domingo

Página Add Blocked Service

Opções da página Add Blocked Service

Opções	Descrição
User Defined Service	Digite o serviço que deseja bloquear.
Protocol	O tipo de protocolo associado ao serviço a ser bloqueado. As opções são: <ul style="list-style-type: none">• TCP• UDP• TCP/UDP
Start Port	Número da porta em que se iniciará o bloqueio. Se necessário, entre em contato com o fornecedor do aplicativo para obter essas informações.
End Port	Número da porta em que se encerrará o bloqueio. Se necessário, entre em contato com o fornecedor do aplicativo para obter essas informações.
Always Block?	Selecione se deseja que o Gateway sempre bloqueie esse serviço. As opções são: <ul style="list-style-type: none">• No = o Gateway nem sempre bloqueia esse serviço. Use Set Block Time e Set Blocked Days para dizer ao Gateway quando iniciar e interromper o bloqueio deste serviço.• Yes = o Gateway sempre bloqueia esse serviço até que se interrompa o bloqueio.
Set Block Time	Se houver selecionado No em Always Block?, selecione a hora em que o Gateway bloqueará este serviço. <ul style="list-style-type: none">• Start from = selecione a hora de início do bloqueio do serviço pelo Gateway.• End on = selecione a hora de término do bloqueio do serviço pelo Gateway.
Set Blocked Days	Se houver selecionado No em Always Block?, selecione os dias em que o Gateway bloqueará este serviço. Links e caixas de seleção estão disponíveis para selecionar todos os dias nenhum dia ou dias individuais da semana. <ul style="list-style-type: none">• Select All = Clique neste link para selecionar todos os sete dias.• Select None = Clique neste link para desmarcar os sete dias.• Monday - Sunday = marque as caixas de seleção que correspondem aos dias em que deseja que o Gateway bloqueie esse serviço.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Configuração de computadores confiáveis

Na página Managed Services, é possível definir computadores confiáveis com permissão para acessar serviços e aplicativos bloqueados.

Para definir computadores confiáveis na página Managed Services:

1. Na área **Trusted Computers**, clique no botão **+ADD**. A página Add Trust Computer é exibida.
2. Preencha os campos da página Add Trust Computer.
3. Clique em **SAVE**. O nome do computador confiável e seu endereço MAC são exibidos na tabela Trusted Computers da página Managed Services.
4. Ao lado de **Enable Services** na página Managed Services, clique em **Enabled** para ativar os filtros de controle parental configurados nesta página. (Para desativar os filtros de controle parental configurados nesta página, clique em **Disabled**.)
5. Depois que um computador confiável for definido, use os botões **No** ou **Yes** ao lado do computador confiável na página Managed Services para alternar entre confiáveis e não confiáveis.



A imagem mostra a interface de usuário de um sistema de gerenciamento de rede. No topo, há o logotipo da NET e o slogan "O MUNDO É DOS NETS". À direita, há links para "Sair" e "Alterar senha", além de indicadores de status para "Internet", "Wi-Fi" e "Segurança baixa". O menu lateral à esquerda contém opções como "Sistema", "Dispositivos conectados", "Controle de Pais", "Avançado" e "Solução de problemas". O conteúdo principal exibe o caminho "Controle de Pais > Gerenciar Serviços > Adicionar Dispositivo confiável". Abaixo, há um formulário intitulado "Adicionar Dispositivo do Usuário de Confiança" com campos para "Nome do dispositivo:" e "MAC do computador:", e um botão "SALVAR".

Página Add Trust Computer

Opções da página Add Trust Computer

Opções	Descrição
Device Name	Digite um nome para o computador que deseja designar como computador confiável. O nome deve ser único e permitir que se diferencie esse computador confiável de outros que se possam definir.
Computer MAC	Digite o endereço MAC do computador que deseja designar como o computador confiável.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.

Dispositivos gerenciados

Parental Control > Managed Devices

A página Managed Devices permite criar uma lista de dispositivos que são:

- Dispositivos com permissão para conectar-se à Internet
- Dispositivos sem permissão para conectar-se à Internet



The screenshot shows the NET parental control interface. At the top left is the NET logo with the tagline 'O MUNDO É DOS NETS'. On the top right, there are status indicators for Internet (green checkmark), Wi-Fi (green checkmark), and Segurança baixa (red X). Below the logo is a navigation menu with options: Sistema, Dispositivos conectados, Controle de País (selected), Gerenciamento de Sites, Gerenciamento de Serviços, Gerenciamento de Dispositivos (highlighted in blue), Avançado, and Solução de problemas. The main content area is titled 'Controle de País > Gerenciar Dispositivos'. It contains a text box explaining that it shows a list of devices allowed or blocked from connecting to the network. Below this is a 'Gerenciamento de Dispositivos' section with two toggle switches: 'Habilitar Gerenciador de dispositivos' (set to 'Habilitado') and 'Tipo de Acesso' (set to 'Permitir'). At the bottom, there is a 'Dispositivos bloqueados' section with a '+ ADICIONAR DISPOSITIVOS BLOQUEADOS' button and a table with columns for 'Nome do dispositivo', 'Endereço MAC', and 'Quando'.

Página Managed Devices

Permissão de dispositivos

Na página Managed Devices, é possível criar uma lista de dispositivos que podem se conectar à Internet de acordo com as regras definidas pelo administrador.

Para adicionar dispositivos permitidos na página Managed Devices:

1. Em **Managed Devices**, verifique se **Access Type** está definido como *Block All*. Se estiver definido como **Allow All**, clique em **Block All**.

Observação: Se houver configurado dispositivos bloqueados, alterar os tipos de acesso ao clicar em Block All exibirá uma mensagem informando que a alteração dos tipos de acesso removerá a lista de dispositivos original. Clique em OK para continuar e excluir a lista de dispositivos original ou clique em Cancel para cancelar a operação e manter a lista de dispositivos original.

2. Em **Allowed Devices**, clique em **+ADD ALLOWED DEVICE**. A página Add Allowed Device é exibida.

3. Preencha os campos da página Add Allowed Device.

4. Clique em **SAVE**. O nome do computador do dispositivo permitido, seu endereço MAC e a data e hora da permissão aparecem na tabela Allowed Devices, na página Managed Devices.

5. Em **Managed Devices**, ao lado de **Enable Managed Devices**, na página Managed Sites, clique em **Enabled** para ativar os dispositivos gerenciados configurados nesta página. (Para desativar os serviços gerenciados configurados nesta página, clique em **Disable**.)

6. Depois que um dispositivo permitido for adicionado, será possível editá-lo clicando em **EDIT** ao lado do dispositivo, alterar os ajustes e clicar em **SAVE**.

7. Para excluir um dispositivo permitido, clique no **X** ao lado dele. Quando uma mensagem de alertar perguntar se deseja excluir o dispositivo, clique em **OK** para excluir o dispositivo ou em **CANCEL** para mantê-lo.

- Sistema
- Dispositivos conectados
- Controle de Pais**
 - Gerenciamento de Sites
 - Gerenciamento de Serviços
 - Gerenciamento de Dispositivos
- Avançado
- Solução de problemas
- MSO

Controle de Pais > Gerenciar Dispositivos > Adicionar dispositivos bloqueados

Adicionar bloqueio de acesso

Set Blocked Device

Nome do dispositivo	Endereço MAC
<input type="radio"/> hbr_eng_02	64:1C:67:6C:66:05
<input type="radio"/> laptop-5iq1pjo2	64:1C:67:86:56:AF

Custom Device:

Bloquear sempre?

Definir Tempo de Bloqueio

Iniciar de:

Termina em:

Definir Dias Bloqueados [Selecionar todos](#) | [Selecionar nenhum](#)

- Segunda-feira
- Terça-feira
- Quarta-feira
- quinta-feira
- Sexta-Feira
- Sábado
- Domingo

Página Add Allowed Device

Opções da página Add Allowed Device

Opções	Descrição
Set Allowed Device	Selecione um dispositivo que deseja permitir. Pode ser um dispositivo cujo nome de computador e endereço MAC já estejam exibidos nesta página ou um dispositivo personalizado cujo nome de computador e endereço MAC você insira em Custom Device.
Always Allow?	Selecione se deseja que o Gateway sempre permita este dispositivo. As opções são: <ul style="list-style-type: none">• No = o Gateway nem sempre permite este dispositivo. Use Set Allow Time e Set Allowed Days para dizer ao Gateway quando permitir este dispositivo.• Yes = o Gateway sempre permite este serviço até que se remova a permissão.
Set Allow Time	Se Always Allow? estiver definido como No, selecione a hora em que o Gateway deve permitir o dispositivo. • Start from = selecione a hora de início da permissão do dispositivo pelo Gateway. • End on = selecione a hora de término da permissão do dispositivo oferecida pelo Gateway.
Set Allow Days	Se Always Allow? estiver definido como No, selecione os dias em que o Gateway deve permitir o dispositivo. Links e caixas de seleção estão disponíveis para selecionar todos os dias nenhum dia ou dias individuais da semana. <ul style="list-style-type: none">• Select All = Clique neste link para selecionar todos os sete dias.• Select None = Clique neste link para desmarcar os sete dias.• Monday - Sunday = marque as caixas de seleção que correspondem aos dias em que deseja que o Gateway permita este dispositivo.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Bloqueio de serviços

Na página Managed Devices, é possível criar uma lista de dispositivos com bloqueio de acesso à Internet de acordo com as regras definidas pelo administrador.

Para adicionar dispositivos bloqueados na página Managed Devices:

1. Em **Managed Devices**, verifique se **Access Type** está definido como **Allow All**. Se estiver definido como **Block All**, clique em **Allow All**.

Observação: Se houver configurado dispositivos permitidos, alterar os tipos de acesso ao clicar em Allow All exibirá uma mensagem informando que a alteração dos tipos de acesso removerá a lista de dispositivos original. Clique em OK para continuar e excluir a lista de dispositivos original ou clique em Cancel para cancelar a operação e manter a lista de dispositivos original.

2. Em **Blocked Devices**, clique em **+ADD BLOCKED DEVICE**. A página Add Blocked Device é exibida.

3. Preencha os campos da página Add Blocked Device.

4. Clique em **SAVE**. O nome do computador do dispositivo bloqueado, seu endereço MAC e a data e hora do bloqueio aparecem na tabela Blocked Devices, na página Managed Devices.

5. Em **Managed Devices**, ao lado de **Enable Managed Devices**, na página Managed Sites, clique em **Enabled** para ativar os dispositivos gerenciados configurados nesta página. (Para desativar os serviços gerenciados configurados nesta página, clique em **Disable**.)

6. Depois que um dispositivo bloqueado for adicionado, será possível editá-lo clicando no botão **EDIT** ao lado do dispositivo, alterar os ajustes e clicar em **SAVE**.

7. Para excluir um dispositivo bloqueado, clique no **X** ao lado dele. Quando uma mensagem de alertar perguntar se deseja excluir o dispositivo, clique em **OK** para excluir o dispositivo ou em **CANCEL** para mantê-lo.

- Sistema
- Dispositivos conectados
- Controle de Pais**
 - Gerenciamento de Sites
 - Gerenciamento de Serviços
 - Gerenciamento de Dispositivos
- Avançado
- Solução de problemas
- MSO

Controle de Pais > Gerenciar Dispositivos > Adicionar dispositivos bloqueados

Adicionar bloqueio de acesso

Set Blocked Device

Nome do dispositivo	Endereço MAC
<input type="radio"/> hbr_eng_02	64:1C:67:6C:66:05
<input type="radio"/> laptop-5iq1pjo2	64:1C:67:86:56:AF

Custom Device:

Bloquear sempre?

Definir Tempo de Bloqueio

Iniciar de: 0 | 00 | AM

Termina em: 11 | 59 | PM

Definir Dias Bloqueados [Selecionar todos](#) | [Selecionar nenhum](#)

- Segunda-feira
- Terça-feira
- Quarta-feira
- quinta-feira
- Sexta-Feira
- Sábado
- Domingo

Página Add Blocked Device

Opções da página Add Blocked Device

Opções	Descrição
Set Blocked Device	Selecione um dispositivo que deseja bloquear. Pode ser um dispositivo cujo nome de computador e endereço MAC já estejam exibidos na caixa de diálogo ou um dispositivo personalizado cujo nome de computador e endereço MAC você insira em Custom Device.
Always Block?	Selecione se deseja que o Gateway sempre bloqueie este dispositivo. As opções são: <ul style="list-style-type: none">• No = o Gateway nem sempre bloqueia este dispositivo. Use Set Allow Time e Set Allowed Days para dizer ao Gateway quando bloquear este dispositivo.• Yes = o Gateway sempre bloqueia esse dispositivo até que se remova o bloqueio.
Set Block Time	Se definir Always Block como No, selecione a hora em que o Gateway bloqueará este dispositivo. <ul style="list-style-type: none">• Start from = selecione a hora de início do bloqueio do dispositivo pelo Gateway.• End on = selecione a hora de término do bloqueio do dispositivo pelo Gateway.
Set Block Days	Se definir Always Block como No, selecione os dias em que o Gateway bloqueará este dispositivo. Links e caixas de seleção estão disponíveis para selecionar todos os dias nenhum dia ou dias individuais da semana. <ul style="list-style-type: none">• Select All = Clique neste link para selecionar todos os sete dias.• Select None = Clique neste link para desmarcar os sete dias.• Monday - Sunday = marque as caixas de seleção que correspondem aos dias em que deseja que o Gateway bloqueie este dispositivo.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Menu Advanced

O menu Advanced contém páginas para executar os seguintes procedimentos avançados de configuração:

- Port Forwarding - ativa ou desativa o encaminhamento de porta
- Port Triggering - ativa ou desativa o disparo de porta
- Remote Management – ativa ou desativa o gerenciamento remoto
- DMZ - configura um computador para acesso à Internet bidirecional irrestrito, definindo-o como um host DMZ virtual.
- QoS - configura os ajustes de QoS do gateway
- Device Discovery - configura o Gateway para detectar automaticamente dispositivos compatíveis com Plug and Play Universal (UPnP) na rede.
- VPN – configura túnel VPN e túnel IPSec

Encaminhamento de porta

Advanced > Port Forwarding

O encaminhamento de porta é um método para tornar um computador na rede acessível a computadores na Internet, mesmo que se esteja por trás do Gateway. A página Port Forwarding permite configurar serviços de encaminhamento de porta que permitem que usuários da Internet acessem serviços predefinidos, como HTTP (80), FTP (20/21) e AIM/ICQ (5190), bem como serviços personalizados (outros). Executa-se o encaminhamento de porta redirecionando o endereço IP da WAN e a porta de serviço para um endereço IP e uma porta de serviço locais.

Todo programa no computador que utilize a internet é programado para enviar os pacotes através de portas específicas. Portas são caminhos virtuais pelos quais a informação na Internet viaja. Uma boa analogia é pensar em portas como extensões em um sistema telefônico. Às vezes as portas são selecionadas arbitrariamente pelos programadores do software, mas outras vezes os programadores usam uma porta padrão, dependendo da funcionalidade do software. Exemplos de usos padrão do setor para portas comuns:

- Páginas HTML: porta 80
- Transferência de arquivos por FTP: porta 21
- E-mail POP3: porta 110
- MSN Messenger: porta 6901 e portas 6891-6900

NET
O MUNDO É DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Avançado > Encaminhamento de Porta

Gerenciar o acesso externo a determinadas portas em sua rede doméstica. [mais](#)

Encaminhamento de porta

Habilitar Encaminhamento de Porta: Habilitado Desativado

Nome	Tipo	IP Interno	IP Remoto	Porta Pub	Porta P	Ativar Intervalo
------	------	------------	-----------	-----------	---------	------------------

ADICIONAR SERVIÇOS

Página Port Forwarding

Inclusão de serviço de encaminhamento de porta

Para incluir um serviço de encaminhamento de porta na página Port Forwarding:

1. Ao lado de **Enable Port Forwarding**, clique em **Enabled**.
2. Clique no botão **ADD SERVICES**. A página Add Service é exibida.
3. Preencha os campos da página Add Service.
4. Clique em **ADD**. O serviço de encaminhamento de porta aparece na tabela Port Forwarding na página Port Forwarding.
5. Para editar um serviço bloqueado, clique no botão **EDIT** ao lado do serviço que deseja modificar, edite os ajustes e clique em **ADD**.
6. Para excluir uma regra de encaminhamento de porta, clique no **X** ao lado da regra. Quando uma mensagem de alerta aparecer, clique em **OK** para excluir a regra de encaminhamento de porta ou **CANCEL** para mantê-la.

NET
O MUNDO É DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Sistema
Dispositivos conectados
Controle de Pais
Avançado
Encaminhamento de porta
Ativação de Porta
Gerenciamento Remoto
DMZ
QoS
Descoberta de dispositivos
VPN
Solução de problemas
MSO

Avançado > Encaminhamento de Porta > Add Encaminhamento de Porta

Gerenciar o acesso externo a determinadas portas em sua rede doméstica. [mais](#)

Adicionar Encaminhamento de Porta

Serviços comuns: AIM

Tipo de Serviço: TCP / UDP

Porta de início: 5190

Porta Final: 5190

Porta Interna:

Habilitar Port Range: Habilitado Desativado

Endereço de IP interno: . . .

Endereços de IP remoto: Any

ADD CANCELAR

Página Add Service

Opções da página Add Service

Opções	Descrição
Common Services	Selecione o serviço para o qual está definindo a regra de encaminhamento de porta. As opções são: <ul style="list-style-type: none">• AIM• FTP• IRC• HTTP• Other = insira o nome do serviço no campo Other Service.
Other Service	Se definir Common Services como Other, insira o nome do serviço que deseja adicionar.
Service Type	Selecione o protocolo associado ao serviço. As opções são: <ul style="list-style-type: none">• TCP/UDP• TCP• UDP
Starting Port	Digite a porta inicial de operação do serviço.
Ending Port	Digite a porta final de operação do serviço.
Internal Port	Digite o número da porta do PC da LAN ou do servidor para onde as solicitações serão encaminhadas.
Enable Port Range	
Internal IP Address	Digite o endereço de IP do PC da LAN ou do servidor para onde as solicitações serão encaminhadas.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Disparo de porta

Advanced > Port Triggering

A página Port Triggering permite gerenciar o acesso externo a portas específicas em sua rede doméstica usando o disparo automático.

Quando o disparo de porta está ativado, o Gateway monitora o tráfego de saída. Se o Gateway detectar tráfego na porta de saída especificada, ele memorizará o endereço IP do computador que enviou os dados, disparará a porta de entrada e encaminhará o tráfego de entrada para o computador disparador.

Para usar o disparo de porta, especifique qual tipo de serviço e número de porta deseja acompanhar, junto com outros parâmetros relacionados. Isso permite que o Gateway transmita os aplicativos especiais para as portas apropriadas especificadas.

NET
O MUNDO E DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Avançado > Ativação de Porta

Gerenciar o acesso externo a determinadas portas em sua rede doméstica. [mais](#)

Ativação de Porta

Habilitar Ativação de Porta: Habilitado Desativado

Nome do Serviço	Tipo de Serviço	Usuário do Serviço	Porta Inicial de Ativação	Porta Final de Ativação	Porta Inicial Ativada	Porta Final Ativada:
ADICIONAR SERVIÇOS						

Página Port Triggering

Inclusão de disparo de porta

Para definir um disparador de porta na página Port Triggering:

1. Ao lado de **Enable Port Triggering**, clique em **Enabled**.
2. Clique no botão **ADD SERVICES**. A página Add Port Triggering é exibida.
3. Preencha os campos da página Add Port Triggering.
4. Clique em **ADD**. O disparo de porta aparece na tabela Port Triggering na página Port Triggering.
5. Para editar o disparo de porta, clique no botão **EDIT** ao lado do disparo de porta que deseja modificar, edite os ajustes e clique em **ADD**.
6. Para excluir o disparo de porta, clique no **X** ao lado do disparo. Quando uma mensagem de alerta for exibida, clique em **OK** para excluir a regra de disparo de porta ou **CANCEL** para mantê-la.

NET
O MUNDO É DOS NETS

Sair · Alterar senha
Internet Wi-Fi Segurança baixa

Avançado > Ativação de Porta > Add Ativação de Porta

Adicionar regra para Port Trigger [mais](#)

Adicionar Ativação de Porta

Nome do Serviço:

Usuário do Serviço:

Tipo de Serviço:

Porta Inicial de Ativação:

Porta Final de Ativação:

Porta Inicial Ativada:

Porta Final Ativada:

Página Add Port Triggering

Opções da página Add Port Triggering

Opções	Descrição
Service Name	Digite um nome para identificar o acionador. O nome deve ser único e permitir que se diferencie esse serviço de outros que se possam definir.
Service User	Selecione um usuário de serviço na lista de usuários. As opções são: <ul style="list-style-type: none">• All Users• Single User = insira o endereço IP do usuário no campo IP Address.
IP Address	Se definir Service User como Single User, insira o endereço IP do usuário.
Service Type	Selecione o tipo de protocolo que deseja usar com o disparador. As opções são: <ul style="list-style-type: none">• TCP/UDP• TCP• UDP Por exemplo, para rastrear o protocolo H.323, o tipo de protocolo deve ser TCP.
Triggering Starting Point	Digite uma porta inicial a ser usada como disparadora para o aplicativo especial. Por exemplo, para rastrear o protocolo H.323, a porta inicial deve ser 1720.
Triggering Ending Point	Digite uma porta final a ser usada como disparadora para o aplicativo especial. Por exemplo, para rastrear o protocolo H.323, a porta final deve ser 1720.
Triggered Starting Port	Digite a porta inicial a ser encaminhada.
Triggered Ending Port	Digite a porta final a ser encaminhada.
Botão ADD	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.

Gerenciamento remoto

Advanced > Remote Management

A página Remote Management permite que o Gateway seja configurado a partir da WAN, acessando o endereço IP da WAN na porta 8080 do Gateway de qualquer lugar na Internet (por exemplo, na janela de URL do navegador, digite `http://WanIPAddress:8080/` para acessar remotamente o roteador).

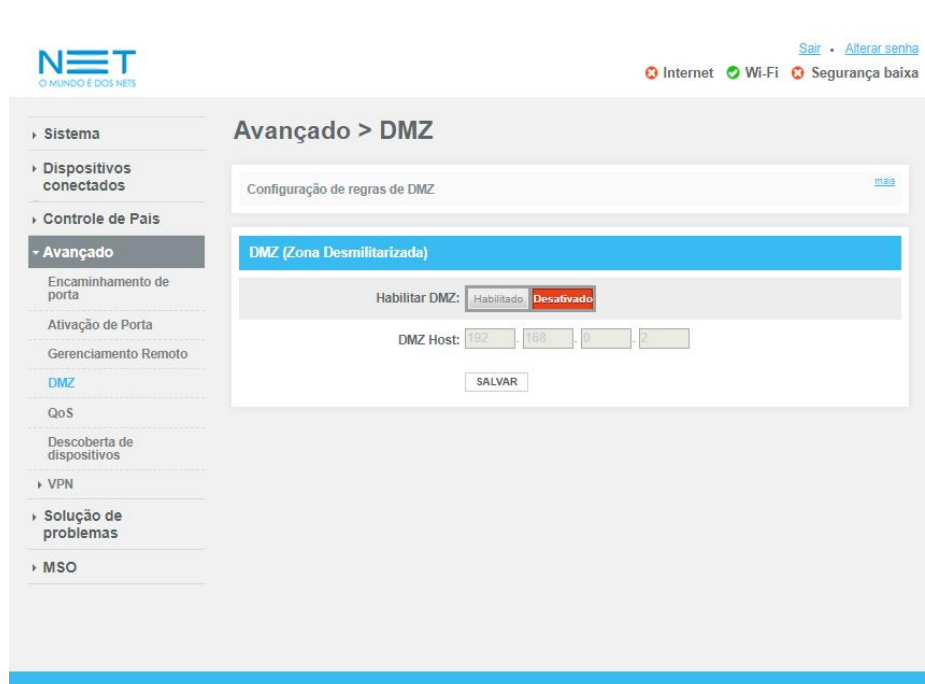
The screenshot shows the 'Avançado > Remote Management' configuration page in a web interface. The top left features the 'NET' logo with the tagline 'O MUNDO É DOS NETS'. The top right has links for 'Sair' and 'Alterar senha', along with status indicators for 'Internet', 'Wi-Fi', and 'Segurança baixa'. A left sidebar contains a navigation menu with items like 'Sistema', 'Dispositivos conectados', 'Controle de Pais', 'Avançado', 'Encaminhamento de porta', 'Ativação de Porta', 'Gerenciamento Remoto', 'DMZ', 'QoS', 'Descoberta de dispositivos', 'VPN', 'Solução de problemas', and 'MSO'. The main content area is titled 'Avançado > Remote Management' and includes a sub-header 'Configuração do Acesso Remoto'. It contains several configuration sections: 'Gerenciamento Remoto HTTP' (Desativado, Porta: 80), 'Gerenciamento Remoto HTTPS' (Desativado, Porta: 843), and 'Gerenciamento Remoto ping WAN' (Habilitado). Below these are fields for 'Endereço do Gerenciamento Remoto' (0.0.0.0) and 'Gerenciamento Remoto IPv6'. A 'Remote Access Allowed From' section offers radio button options for 'Trust Select Dispositivo' and 'Qualquer dispositivo', with a note explaining the security risk of the latter. A 'SALVAR' button is located at the bottom of the configuration area.

Página Remote Management

DMZ

Advanced > DMZ

Se tiver um computador cliente local que não possa executar um aplicativo da Internet corretamente atrás do firewall, será possível configurar o computador para acesso bidirecional irrestrito à Internet, definindo-o como um host DMZ virtual. Um DMZ permite que um único computador da LAN exponha suas portas à Internet. Ao fazer isso, o computador exposto não estará mais “atrás” do firewall. Portanto, colocar um computador na área DMZ deve ser considerado algo temporário porque o firewall não será mais capaz de oferecer segurança a ele.



Página DMZ

Opções da página DMZ

Opções	Descrição
Enable DMZ	Ativa ou desativa o ajuste DMZ do Gateway. As opções são: <ul style="list-style-type: none">• Enabled = ativar o recurso DMZ do gateway.• Disabled = desativar o recurso DMZ do gateway. Esta seleção torna o campo DMZ Host indisponível
DMZ Host	Digite o endereço IP do computador a ser usado como o servidor DMZ.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvá-los.

QoS

Advanced > QoS

A página de QoS permite configurar o Gateway para fornecer melhor controle de reserva de recursos. As redes sem fio oferecem uma oportunidade igual para todos os dispositivos transmitirem dados a partir de qualquer tipo de aplicativo.

Embora isso seja aceitável para a maioria dos aplicativos, os aplicativos de áudio e vídeo multimídia são particularmente sensíveis às variações de atraso e taxa de transferência que resultam desse método de acesso sem fio de “igualdade de oportunidades”. Para que os aplicativos de multimídia funcionem bem em uma rede sem fio, é necessário um mecanismo de Qualidade de Serviço (QoS) para priorizar os tipos de tráfego e fornecer um método de acesso sem fio de “maior oportunidade”.

A página de QoS permite ativar ou desativar as configurações de QoS.

Observação: É possível alterar as configurações de QoS sem precisar reinicializar o Gateway.

The screenshot shows the NET router's web interface. The top left features the NET logo with the tagline 'O MUNDO E DOS NETS'. The top right has links for 'Sair' and 'Alterar senha', along with status indicators for 'Internet', 'Wi-Fi', and 'Segurança baixa'. A left sidebar menu includes categories like 'Sistema', 'Dispositivos conectados', 'Controle de Pais', 'Avançado', 'Encaminhamento de porta', 'Ativação de Porta', 'Gerenciamento Remoto', 'DMZ', 'QoS', 'Descoberta de dispositivos', 'VPN', 'Solução de problemas', and 'MSO'. The main content area is titled 'Avançado > QoS' and contains a sub-header 'Configurar QoS de Wi-Fi privada e LAN'. Below this, there are two toggle switches: 'QoS para WiFi Multimedia (WMM)' which is currently 'Habilitado' (green), and 'QoS para LAN' which is currently 'Desativado' (red).

Página QoS

Opções da página QoS

Opções	Descrição
QoS for WiFi Multimedia (WMM)	Determina se o Gateway ativa ou desativa a QoS para WMM. As opções são: <ul style="list-style-type: none">• Enabled = ativa QoS para WMM.• Disabled = desativa QoS para WMM.
QoS for LAN	Determina se o Gateway ativa ou desativa a QoS para a rede local (LAN). As opções são: <ul style="list-style-type: none">• Enabled = ativa QoS para a LAN.• Disabled = desativa QoS para a LAN.

Descoberta de dispositivo

Advanced > Device Discovery

O Universal Plug and Play (UPnP) é uma arquitetura que permite a conectividade dinâmica entre dispositivos em uma rede. O objetivo do UPnP é oferecer suporte a redes "invisíveis" de dispositivos de configuração zero, incluindo dispositivos inteligentes, PCs, impressoras e outros dispositivos inteligentes que utilizam protocolos padrão.

Usando o UPnP, os dispositivos podem se conectar dinamicamente a uma rede, sem precisar de intervenção ou configuração do usuário. Um dispositivo compatível com UPnP pode obter um endereço IP, divulgar seus recursos, aprender sobre outros dispositivos UPnP conectados e se comunicar diretamente com esses dispositivos. O mesmo dispositivo pode encerrar sua conexão de forma simples quando desejar sair da comunidade UPnP.

Usando a página Device Discovery, é possível configurar o gateway para descobrir dispositivos na rede compatíveis com UPnP.

The screenshot shows the NET router's configuration interface. At the top left is the NET logo with the tagline 'O MUNDO É DOS NETS'. At the top right, there are status indicators for Internet (red X), Wi-Fi (green checkmark), and Segurança baixa (red X). Below the logo is a navigation menu with categories: Sistema, Dispositivos conectados, Controle de Pais, Avançado (selected), Encaminhamento de porta, Ativação de Porta, Gerenciamento Remoto, DMZ, QoS, Descoberta de dispositivos, VPN, Solução de problemas, and MSO. The main content area is titled 'Avançado > Descoberta de dispositivos'. It contains a text box: 'Habilitar o UPnP para que o gateway descubra os dispositivos cliente habilitados de UPnP automaticamente.' Below this is a toggle switch for 'Habilitar UPnP:' set to 'Habilitado'. There are two input fields: 'Tempo de Anúncio:' set to '60' segundos and 'Tempo de Vida:' set to '4' hops. A 'SALVAR' button is at the bottom left of the configuration area.

Página Device Discovery

Opções da página Device Discovery

Opções	Descrição
Enable UPnP	Determina se os recursos UPnP do Gateway estão ativados ou desativados. As opções são: Enabled = ativar os recursos UPnP do gateway. Disabled = desativar os recursos UPnP do gateway.
Advertisement Period	Especifique com que frequência, em segundos, o Gateway transmitirá suas informações UPnP. Esse valor pode variar de 1 a 2147483648 segundos. Durações menores garantem que os pontos de controle tenham status de dispositivo atual à custa de tráfego de rede adicional. Longos períodos podem comprometer a atualização do status do dispositivo, mas podem reduzir significativamente o tráfego da rede.
Time To Live	O tempo de duração do anúncio é medido em saltos (etapas) para cada pacote UPnP enviado. O tempo de vida da contagem de saltos é o número de etapas que um pacote transmitido pode propagar para cada anúncio UPnP antes que ele desapareça. O número de saltos pode variar de 1 a 255. O valor padrão de quatro saltos deve estar bom para a maioria das redes domésticas. Se alguns dispositivos não estiverem sendo atualizados ou alcançados corretamente, aumente levemente esse valor.
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.

VPN

Advanced > VPN

É possível configurar vários túneis VPN em vários computadores clientes. Diferentes túneis podem ser configurados e armazenados, mas não habilitados para facilidade de uso com conexões e/ou computadores clientes que não são usados constantemente. Para cada configuração de túnel, seus parâmetros IPsec exclusivos são armazenados usando o menu IPsec Config na parte inferior da página.

The screenshot shows the NET router configuration interface. The top left features the NET logo with the tagline "O MUNDO É DOS NETS". The top right includes links for "Sair" and "Alterar senha", along with status indicators for "Internet", "Wi-Fi", and "Segurança baixa". A left sidebar menu lists various system settings, with "Avançado" expanded to show "VPN Configurações Gerais" selected. The main content area is titled "Avançado > VPN > Configurações Gerais" and contains two sections: "Configuração PPTP" and "Configuração IPSEC". Both sections have a "Habilitar" toggle set to "Habilitado". The PPTP section includes a table with columns for "Índice", "Nome", and "Grupo", and an "ADICIONAR ÍNDICE" button.

NET
O MUNDO É DOS NETS

Sair · [Alterar senha](#)
Internet Wi-Fi Segurança baixa

▶ Sistema
▶ Dispositivos conectados
▶ Controle de País
▼ Avançado
Encaminhamento de porta
Ativação de Porta
Gerenciamento Remoto
DMZ
QoS
Descoberta de dispositivos
▼ VPN
VPN Configurações Gerais
Tabela do túnel IPSEC
▶ Solução de problemas
▶ MSO

Avançado > VPN > Configurações Gerais

Definir a configuração geral de VPN.

Configuração PPTP

Habilitar PPTP : Habilitado Desativado

Índice	Nome	Grupo
--------	------	-------

Configuração IPSEC

Habilitar IPSEC : Habilitado Desativado

Menu Troubleshooting

O menu Troubleshooting fornece as seguintes páginas para ajudá-lo a identificar e resolver problemas:

- Logs –
- Diagnostic Tools – permite solucionar problemas.
- Restore/Reboot – restaura os ajustes do gateway ou reinicializa o gateway.
- Change Password – altera a senha usada para efetuar login na interface de gerenciamento da Web.

Ferramentas de diagnóstico de rede

Troubleshooting > Diagnostic Tools

Pode haver ocasiões em que se encontre um problema ao tentar alcançar um determinado destino. Se examinar a configuração e a operação do Gateway e tudo parecer certo, o problema pode estar em um roteador no fio que parte do Gateway ou com o próprio fio.

Para ajudá-lo a identificar esses problemas, use a página Network Diagnostic Tools para testar a conectividade com um destino ou endereço IP.

NET
O MUNDO É DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Solução de problemas > Ferramentas de Diagnósticos

Solucionar problemas do gateway e suas conexões usando ferramentas de diagnóstico [mais](#)

Packet Sniffer Test

Sniffer Interface: l2sd0.2

START SNIFFER STOP SNIFFER DOWNLOAD SNIFFER DATA

Resultados do Teste de Conectividade

Conectividade: Inativo

Pacotes Enviados: 0

Pacotes Recebidos: 0

Endereço de destino:

TESTE DE CONECTIVIDADE

Página Network Diagnostic Tools

Teste da conectividade com um endereço de destino

Para testar a conectividade do gateway com um endereço de destino:

1. Na página Network Diagnostic Tools, em **Test Connectivity Results**, insira o endereço IP de um site ativo conhecido no campo **Destination Address**.

Observação: Esse procedimento pressupõe que o endereço de destino inserido seja válido e operacional.

2. Clique no botão **TEST CONNECTIVITY**. Uma mensagem é exibida com os resultados. Clique em **OK** para remover a mensagem. Os contadores **Packets Sent** e **Packets Received** mostram o número de pacotes enviados e recebidos durante o teste.

Se o teste for bem-sucedido, isto significa que o destino que apresenta dificuldade para ser alcançado está ativo e fisicamente acessível. Se houver roteadores entre o gateway e o destino e houver dificuldade de acesso, o problema pode estar em um dos roteadores.

Se o Gateway tiver enviado pacotes para um endereço de destino, mas não tiver recebido nenhum retorno, será exibida uma mensagem de erro. Clique em **OK** para dispensar a mensagem e confirmar se digitou um endereço de destino válido.

Restaurar/Reiniciar

Troubleshooting > Restore/Reboot

A página Restore / Reboot fornece botões para executar as seguintes atividades:

- **REBOOT** = reinicia o Gateway, mas mantém as substituições feitas nas configurações padrão de fábrica.
- **RESET WI-FI Router** = remove as substituições feitas somente nos ajustes do roteador Wi-Fi do Gateway e faz que essas configurações retornem aos valores padrão. Todos os outros ajustes do Gateway permanecem inalterados.
 - **RESTORE WIFI SETTINGS** = remove as substituições feitas nos ajustes sem fio do Gateway e faz que os ajustes sem fio retornem aos valores padrão. Todos os outros ajustes do Gateway permanecem inalterados.
- **RESTORE FACTORY SETTINGS** = remove substituições feitas em todos os ajustes do Gateway, incluindo senhas, controles parentais e firewall, e faz que o Gateway retorne aos valores padrão de fábrica.



NET
O MUNDO E DOS MEUS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Solução de problemas > Restaurar / Reiniciar

Reiniciar / restaurar seu Gateway Wi-Fi [mais](#)

Restaurar / Reiniciar

REINICIAR	Selecionar 'Reiniciar' para reiniciar o dispositivo
RESTAURAR WI-FI	Selecione 'Restaurar Configurações Wi-Fi' para ativar suas configurações padrão do gateway apenas para Wi-Fi. Apenas as definições de Wi-Fi serão perdidas.
RESTAURAR FÁBRICA	Selecione 'Restaurar Configurações de Fábrica' para ativar suas configurações padrão do gateway. Todas as configurações anteriores serão perdidas.

Página Restore/Reboot

Alterar senha

Troubleshooting > Change Password

A página Change Password permite alterar a senha usada para efetuar login na interface da Web do gateway. Por segurança, recomendamos alterar a senha de login padrão na primeira vez que efetuar login na interface de gerenciamento da Web para proteger o Gateway contra usuários não autorizados.

Esta página também está disponível ao clicar no link **Change Password** na área superior direita da interface de gerenciamento da Web.

Observação: Para alterar a senha da rede Wi-Fi, acesse a página Gateway > Connection > WiFi.

NET
O MUNDO É DOS NETS

Sair • Alterar senha
Internet Wi-Fi Segurança baixa

Solução de problemas > Alterar Senha

Alterar senha do usuário para ter acesso as configurações do equipamento. [mais](#)

Senha

Tipo do usuário: ms0

Senha atual:

Nova Senha de Rede:

Re-insira nova senha:

SALVAR CANCELAR

Página Change Password

Opções da página Change Password

Opções	Descrição
User Type	Use esta lista suspensa para selecionar o tipo de usuário.
Current Password	Digite a senha atual que diferencia maiúsculas e minúsculas. Por motivos de segurança, todo caractere digitado é mascarado como um ponto (D) .
New Password	Digite a nova senha que diferencia maiúsculas de minúsculas que deseja usar. A nova senha faz distinção entre maiúsculas e minúsculas e pode conter de 8 a 20 caracteres alfanuméricos, mas sem espaços ou caracteres especiais. Por motivos de segurança, todo caractere digitado é mascarado como um ponto (D) .
Re-enter New Password	Digite a mesma senha que diferencia entre maiúsculas e minúsculas digitada no campo New Password. Por motivos de segurança, todo caractere digitado é mascarado como um ponto (D) .
Botão SAVE	Depois de configurar os ajustes nesta página, clique neste botão para salvar suas configurações.
Botão CANCEL	Clique neste botão para descartar as alterações nesta página e retornar às configurações da página anterior.