

HI3120 DOCSIS 3.1 eMTA WiFi Gateway

# Guia do Usuário

*Versão 1.1 - 09/2019*



# Sobre este Guia do Usuário

## Público-alvo

Este manual destina-se a pessoas que desejam configurar os recursos do HI3120 através de sua Interface Gráfica de Usuário (GUI).

## Documentação relacionada

- ▶ **Guia de instalação rápida:** consulte isso para obter informações sobre como colocar seu HI3120 em funcionamento imediatamente. Inclui informações sobre os requisitos do sistema, conteúdo do pacote, o procedimento de instalação e dicas básicas de solução de problemas.
- ▶ **Ajuda on-line :** cada tela na Interface gráfica do Usuário (GUI) da HI3120 contém um botão **Ajuda**. Clique neste botão para ver informações adicionais sobre a configuração da tela.

## Convenções documentais

Este Guia do Usuário usa várias convenções e estilos tipográficos para indicar o tipo de conteúdo:

- ▶ Parágrafos com balas são usados para listar itens e para indicar opções.
- 1 Parágrafos numerados indicam etapas processuais.

NOTA: As notas fornecem informações adicionais sobre um assunto.

 avisos fornecem informações sobre ações que podem prejudicar você ou seu dispositivo.

Rótulos de produtos, rótulos de campo, opções de campo, etc. são do tipo **negrito**. Por exemplo:

Selecione **UDP** para usar o Protocolo de Datagrama do Usuário.

Um clique do mouse na Interface Gráfica do Usuário (GUI) é denotado por um suporte de ângulo reto ( > ). Por exemplo:

Clique **em Configurações > Configurações avançadas**.

significa que você deve clicar em **Configurações** na GUI e, em seguida, **configurações avançadas**.

Um traçado-chave é denotado por suportes quadrados e texto maiúsculo. Por exemplo:

Pressione [ENTER] para continuar.

## Suporte ao cliente

Para obter assistência técnica ou outros problemas de suporte ao cliente, consulte seu representante da Hitron.

## Detalhes de login padrão

O endereço IP padrão e as credenciais de login do HI3120 são as seguintes.

Tabela 1: [Credenciais padrão](#)

Endereço IP	192.168.0.1	
Usuário	CLARO_XXXXXX	XXXXXX = 6 últimos dígitos do Endereço MAC
Senha	XXXXXXXXXXXX	XXXXXXXXXXXX = Endereço MAC completo

Copyright ©2019 Hitron Technologies. Todos os direitos reservados. Todas as marcas comerciais e marcas registradas utilizadas são de propriedade de seus respectivos proprietários.

AVISO: As informações neste Guia do Usuário são precisas no momento da escrita. Este Guia do Usuário é fornecido "como está" sem garantia expressa ou implícita de qualquer tipo. Nem a Hitron Technologies nem seus agentes assumem qualquer responsabilidade por imprecisões neste Guia do Usuário, ou perdas incorridas pelo uso ou uso indevido das informações neste Guia do Usuário.

## Sumário

Sobre este Guia do Usuário .....	2
<b>Introdução .....</b>	<b>8</b>
1.1 Visão geral do HI3120/CHITA .....	8
1.1.1 Principais características.....	8
1.2 Conexões de hardware .....	10
1.3 Leds 14	
1.4 Configuração de endereço IP.....	16
1.4.1 Configuração manual do endereço IP .....	18
1.5 Login no HI3120.....	19
1.6 Visão geral do GUI .....	20
1.7 Redefinindo o HI3120 .....	21
<b>Status.....</b>	<b>22</b>
2.1 Visão geral do status .....	22
2.1.1 Docsis .....	22
2.1.2 Endereços IP e Sub-redes .....	23
2.1.3 DHCP .....	25
2.1.4 Locação DHCP .....	26
2.1.5 Endereços MAC .....	26
2.1.6 Modo de roteamento .....	27
2.1.7 Arquivos de configuração.....	27
2.1.8 Transmissões downstream e upstream.....	27
2.1.9 Frequências de cabos .....	27
2.1.10 Modulação.....	28
2.1.11 TDMA, FDMA e SCDMA.....	28
2.2 Informações do sistema.....	29
2.3 Provisionamento DOCSIS .....	30
2.4 DOCSIS WAN .....	31
2.5 Eventos DOCSIS.....	34
2.6 Status Wi-Fi.....	36
2.7 MTA38	
<b>Básico.....</b>	<b>40</b>

3.1 Visão geral básica.....	40
3.1.1 O sistema de nomes de domínio .....	40
3.1.2 Encaminhamento de portas .....	41
3.1.3 Acionamento de portas .....	41
3.1.4 DMZ41	
3.1.5 Modo de roteamento .....	41
3.2 Configuração LAN.....	42
3.3 Função de gateway .....	45
3.4 Encaminhamento da porta .....	45
3.4.1 Adicionar ou editar uma regra de encaminhamento de portas	48
3.5 Acionamento da porta .....	50
3.5.1 Adicionar ou editar uma regra de acionamento de portas	51
3.6 DMZ53	
3.7 DNS 55	
Wi-Fi.....	57
4.1 Visão geral sem fio .....	57
4.1.1 Noções básicas de rede sem fio .....	57
4.1.2 Arquitetura .....	57
4.1.3 Padrões sem fio .....	60
4.1.4 Conjuntos de serviços e SSIDs .....	60
4.1.5 Segurança sem fio .....	61
4.1.6 WMM .....	62
4.2 Configurações básicas Wi-Fi.....	63
4.2.1 Configurações 2.4G .....	63
4.2.2 Configurações 5G.....	67
4.3 WPS .....	70
4.4 Controle de acesso .....	73
Admin.....	77
5.1 Visão geral do administrador.....	77
5.1.1 Depuração (Ping e Traceroute) .....	77
5.2 Diagnóstico .....	78
5.3 Cópia de Segurança .....	80
5.4 Reinicialização do dispositivo.....	81
5.5 DDNS .....	82
5.6 IP Passthrough.....	83
Segurança.....	84
6.1 Visão geral da segurança .....	84

6.1.1 Firewall .....	84
6.1.2 Sistema de detecção de intrusões .....	85
6.1.3 Filtragem do dispositivo .....	85
6.1.4 Filtragem de serviço .....	85
6.2 A tela de firewall .....	85
6.3 Bloqueio de portas .....	87
6.3.1 Adicionar ou editar uma regra do bloqueio de portas .....	90
6.3.2 Adicionar ou editar uma regra do dispositivo confiável do bloqueio de porta.....	94
6.4 Filtro do dispositivo .....	95
6.4.1 Adicionar ou editar um dispositivo gerenciado .....	97
6.5 Filtro de palavras-chave.....	99
6.5.1 Adicionar ou editar uma regra do dispositivo confiável do filtro de palavras-chave .....	102
Solucionando problemas .....	111

# 1

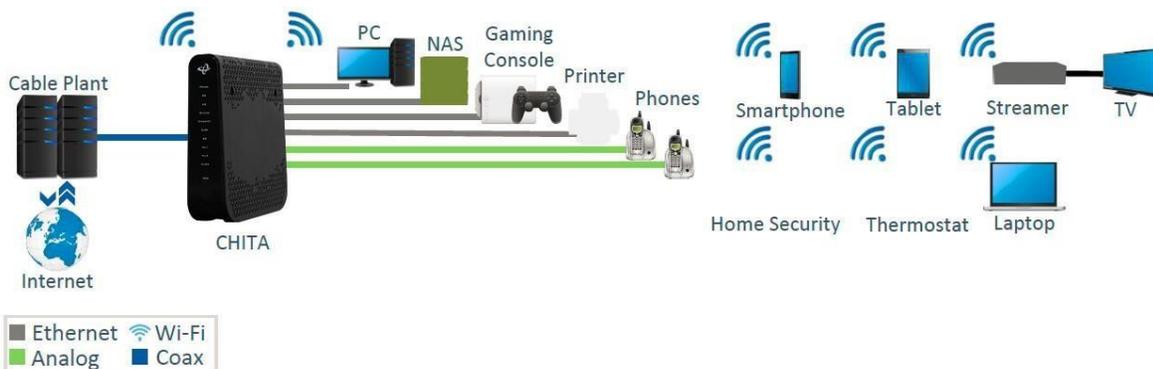
## Introdução

Este capítulo apresenta o HI3120 e sua GUI (Interface Gráfica do Usuário).

### 1.1 Visão geral do HI3120/CHITA

Seu HI3120 é um cable modem DOCSIS, roteador, adaptador multimídia embarcado (eMTA) e ponto de acesso sem fio que permite conectar seu Ethernet a cabo, dispositivos sem fio e telefones uns aos outros e à Internet através da conexão a cabo.

Figura 1: Visão geral do aplicativo



#### 1.1.1 Principais características

O HI3120 fornece:

- ▶ Conformidade DOCSIS/EuroDOCSIS 3.0

- ▶ IEEE 802.11ac WiFi ponto de acesso 3x3 antenas internas MIMO de banda dupla
- ▶ Conexão de rede local através de quatro portas Ethernet de 10/1000/1000 Mbps
- ▶ Duas portas telefônicas analógicas FXS usando SIP ou MGCP
- ▶ Porta de host USB 2.0
- ▶ Qualidade do Serviço (QoS) para o melhor desempenho de vídeo e dados
- ▶ LEDs externos exibindo claramente dispositivo e rede status
- ▶ Controle completo do operador via arquivo de configuração e SNMP
- ▶ TR-069 e HNAP prontos para fácil configuração e gerenciamento remoto
- ▶ Segurança sem fio: criptografia WEP, WPA-PSK e WPA2-PSK, botão de pressão (Wifi Protected Setup) e configuração PIN, filtragem MAC
- ▶ Configurações de backup e restauração
- ▶ Interface de configuração segura, acessível pelo navegador Da Web

## 1.2 Conexões de hardware

Esta seção descreve as portas e botões físicos do HI3120.

Figura 2: Conexões de hardware



Tabela 2: Conexões de hardware

<p>Wps</p>	<p>Pressione este botão para iniciar o procedimento PBC (Push-Button Configuration, configuração de botão de configuração de botão protegido pelo WiFi).</p> <p>Pressione o botão PBC em seus clientes sem fio na área de cobertura dentro de dois minutos para permitir que eles se juntem à rede sem fio.</p> <p>O <b>LED WPS</b> exibe o status de conexão de configuração protegida pelo WiFi da seguinte forma:</p> <ul style="list-style-type: none"> <li>▶ <b>Bicolor</b>, piscando: a conexão WPS está processando.</li> <li>▶ <b>Verde</b>, estável: a conexão WPS foi bem sucedida.</li> <li>▶ <b>Vermelho, estável</b>: a conexão WPS falhou ou ocorreu um erro.</li> <li>▶ <b>Off</b>: WPS não está ativo.</li> </ul> <p>Consulte WPS para obter mais informações.</p>
<p>Usb</p>	<p>O HI3120 fornece uma porta de host USB 2.0, permitindo que você conecte discos flash USB para montagem e compartilhamento através das interfaces LAN através do protocolo Samba (bairro de rede).</p> <p>O HI3120 suporta os seguintes sistemas de arquivos Windows:</p> <ul style="list-style-type: none"> <li>▶ FAT16</li> <li>▶ FAT32</li> <li>▶ Ntfs</li> </ul> <p> <b>dispositivos USB não devem drenar mais de 500mA da porta USB. Os dispositivos USB que requerem mais de 500mA devem ser fornecidos com suas próprias fontes de energia.</b></p>
<p>Linha</p>	<p>Use essas portas para conectar seus telefones analógicos para serviços VoIP, usando cabos com conectores RJ11.</p>

Tabela 2: Conexões de hardware

Reset	<p>Use este botão para reiniciar ou redefinir seu HI3120 para suas configurações padrão de fábrica.</p> <p>Para reiniciar o HI3120, pressione o botão e segure-o por menos de cinco segundos. O HI3120 reinicia, usando as configurações existentes.</p> <p>Para reiniciar o HI3120, pressione o botão e segure-o por mais de dez segundos. Todas as configurações configuradas pelo usuário são excluídas e o HI3120 é reiniciado usando suas configurações padrão de fábrica.</p>
LAN1	<p>Use essas portas para conectar seus computadores e outros dispositivos de rede, usando cabos Ethernet de categoria 5 ou 6 com conectores RJ45.</p>
LAN2	
LAN3	
LAN4	
Cabo	<p>Use isso para se conectar à Internet através de um cabo RF tipo F.</p>

Tabela 2: Conexões de hardware

Energia	<p>Use a porta <b>POWER</b> para conectar ao adaptador de energia 12v/2.5A (30W) que veio com o seu HI3120. Use o interruptor <b>POWER</b> para ligar ou desligar o HI3120.</p> <p>O <b>LED POWER</b> exibe o status de energia da seguinte forma:</p> <ul style="list-style-type: none"><li>▶ <b>Verde</b>, estável: a potência da HI3120 está desligada.</li><li>▶ <b>Desligado</b>: a energia da HI3120 está desligada.</li></ul> <p> <b>NUNCA use outro adaptador de energia com o seu HI3120. Fazer isso pode prejudicar sua HI3120.</b></p> <p>Figura 3: Adaptador de energia</p> 
---------	--

## 1.3 Leds

Esta seção descreve os LEDs (luzes) da HI3120.

Figura 4: LEDs

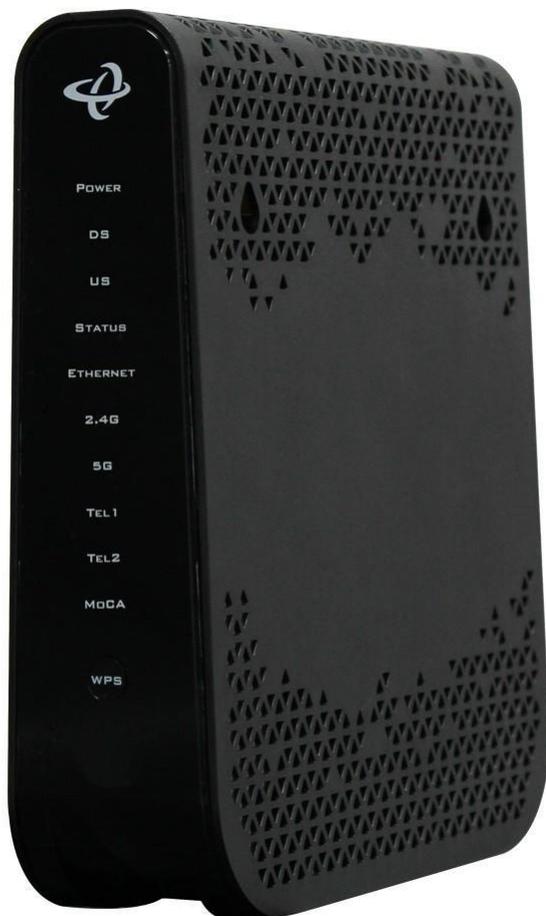


Tabela 3: LEDs

POWER	Indica se o produto está energizado.	
	Verde-Aceso	O modem está ligado.
	Desligado	Sem fonte de alimentação.
DS	Indica o estado da conexão do produto à internet para que seja possível a transmissão de dados no sentido da rede da operadora para o terminal (Tráfego Downstream).	
	Verde-Piscando	Procurando canal downstream.
	Âmbar-Aceso	Frequência de download sincronizada. (Apenas 1 canal)
	Verde-Aceso	Frequência de download sincronizada. (bonding)
	Verde-Aceso	DOCSIS3.1 OFDM
	Desligado	A inicialização não foi iniciada ou falhou.
US	Indica o estado da conexão do produto à internet para que seja possível a transmissão de dados no sentido do terminal para a rede da operadora (Tráfego Upstream).	
	Verde-Piscando	Procurando canal upstream.
	Âmbar-Aceso	Frequência de upload sincronizada. (Apenas 1 canal)
	Verde-Aceso	Frequência de upload sincronizada. (bonding)
	Verde-Aceso	DOCSIS3.1
	Desligado	A inicialização não foi iniciada ou falhou.
ONLINE	Indica se o produto está ou não conectado à internet.	
	Verde- Piscando	Processo de registro na empresa prestadora de serviços.
	Verde-Aceso	Serviço de internet disponível.
	Desligado	A inicialização não foi iniciada ou falhou.
ETHERNET	Indica se o cabo está conectado à porta Ethernet.	
	Verde-Piscando	Ethernet ativada.
	Desligado	Ethernet desativada.
2.4GHz / 5GHz	Indica o estado e se há tráfego de dados na rede sem fio de 2.4GHz e 5GHz.	
	Verde-Piscando	A rede WiFi de 2.4GHz / 5GHz está ativa e está recebendo ou enviando dados.

	Verde-Aceso	A rede WiFi de 2.4GHz / 5GHz está ativa, mas não há transmissão de dados.
	Desligado	Rede desligada.
TEL 1 / TEL 2	Indica se a linha telefônica está registrada e se o telefone está ou não em uso.	
	Verde-Piscando	A linha de telefone está em uso.
	Verde-Aceso	O serviço de telefone está disponível.
	Desligado	O serviço de telefone não está disponível.
WPS	Botão WPS que permitirá que o usuário se conecte de maneira segura e fácil ao Wi-Fi.	
	Verde-Piscando	Está procurando um dispositivo WPS.
	Verde-Aceso	Um dispositivo WPS foi encontrado e a conexão foi bem-sucedida.
	Desligado	A funcionalidade WPS está desativada.

NOTA: Para obter informações sobre o comportamento dos LEDs do botão **WPS** e **POWER**, consulte a Tabela 2.

## 1.4 Configuração de endereço IP

Antes de entrar na GUI do HI3120, o endereço IP do seu computador deve estar na mesma sub-rede que o HI3120. Isso permite que seu computador se comunique com o HI3120.

NOTA: Consulte endereços IP e Subnets para formação em segundo plano.

Se o computador estiver configurado para obter um endereço IP automaticamente ou se você não tiver certeza, tente fazer login no HI3120 (consulte visão geral da GUI).

- ▶ Se a tela de login for exibida, o computador já está configurado corretamente.
- ▶ Se a tela de login não for exibida, o computador não será configurado corretamente.  
Siga o procedimento na Configuração manual de endereços IP e defina seu computador para obter um endereço IP automaticamente. Tente registrar novamente. Se você não puder fazer login, siga novamente o procedimento de configuração de endereço IP manual e defina um endereço IP específico conforme mostrado. Tente fazer login de novo.

NOTA: Se você ainda não puder ver a tela de login, as configurações ip do seu HI3120 podem ter sido alteradas de seus padrões. Se você não conhece o novo endereço da HI3120, você deve devolvê-lo aos padrões de fábrica. Consulte [Redefinindo o HI3120](#). Tenha em mente que todas as configurações configuradas pelo usuário são perdidas.

### 1.4.1 Configuração manual do endereço IP

Por padrão, o endereço IP local do seu HI3120 é **192.168.0.1**. Se o seu HI3120 estiver usando o endereço IP padrão, você deve definir o endereço IP do seu computador entre **192.168.0.2** e **192.168.0.254**.

Tome as seguintes etapas para configurar manualmente o endereço IP do seu computador para se conectar ao HI3120:

NOTA: [Este exemplo usa o Windows XP; o procedimento para o seu sistema operacional pode ser diferente.](#)

- 1 Clique em **Iniciar**, em seguida, clique em Painel de **Controle**.
- 2 Na janela que exibe, clique duas vezes em **Conexões de Rede**.
- 3 Clique com o botão direito da sua conexão de rede (geralmente **conexão local**) e clique em **Propriedades**.
- 4 Na guia Geral **Esta conexão usa a** seguinte lista de itens, role para baixo e selecione Protocolo da **Internet (TCP/IP)**. Clique em **Propriedades**.
- 5 Você pode obter um endereço IP automaticamente ou especificar um manualmente:
  - ▶ Se sua rede tiver um servidor DHCP ativo, selecione **Obter um endereço IP automaticamente**.
  - ▶ Se sua rede não tiver um servidor DHCP ativo, selecione **Usar o seguinte endereço IP**. No campo de **endereços IP**, digite um valor entre **192.168.0.2** e **192.168.0.254** (padrão). No campo da **máscara Sub-rede**, digite **255.255.255.0** (padrão).

NOTA: [Se o seu HI3120 não estiver usando o endereço IP padrão, digite um endereço IP e uma máscara de sub-rede que coloque seu computador na mesma sub-rede que o HI3120.](#)

- 6 Clique em **OK**. A janela Protocolo **da Internet (TCP/IP)** fecha. Na janela **Propriedades de Conexão da Área Local**, clique em **OK**.

Seu computador agora obtém um endereço IP do HI3120 ou usa o endereço IP especificado e pode se comunicar com o HI3120.

## 1.5 Login no HI3120

Tome as seguintes medidas para fazer login na GUI da HI3120.

NOTA: Você pode fazer login na GUI da HI3120 através da interface sem fio. No entanto, é fortemente recomendável que você configure o HI3120 através de uma conexão com fio na LAN.

- 1 Abra uma janela do navegador.
- 2 Digite o endereço IP da HI3120 (padrão **192.168.0.1**) na barra de URL. A tela de **Login**.

Figura 5: Login



HI3120 CONECTE-SE Claro

Nome do usuário  
Insira nome de usuário

Senha  
Digite a senha

Lembrar de mim neste dispositivo

- 3 Digite o Nome **de Usuário** e **Senha**. O nome de usuário de login padrão é **admin**, e a senha padrão é administrador .

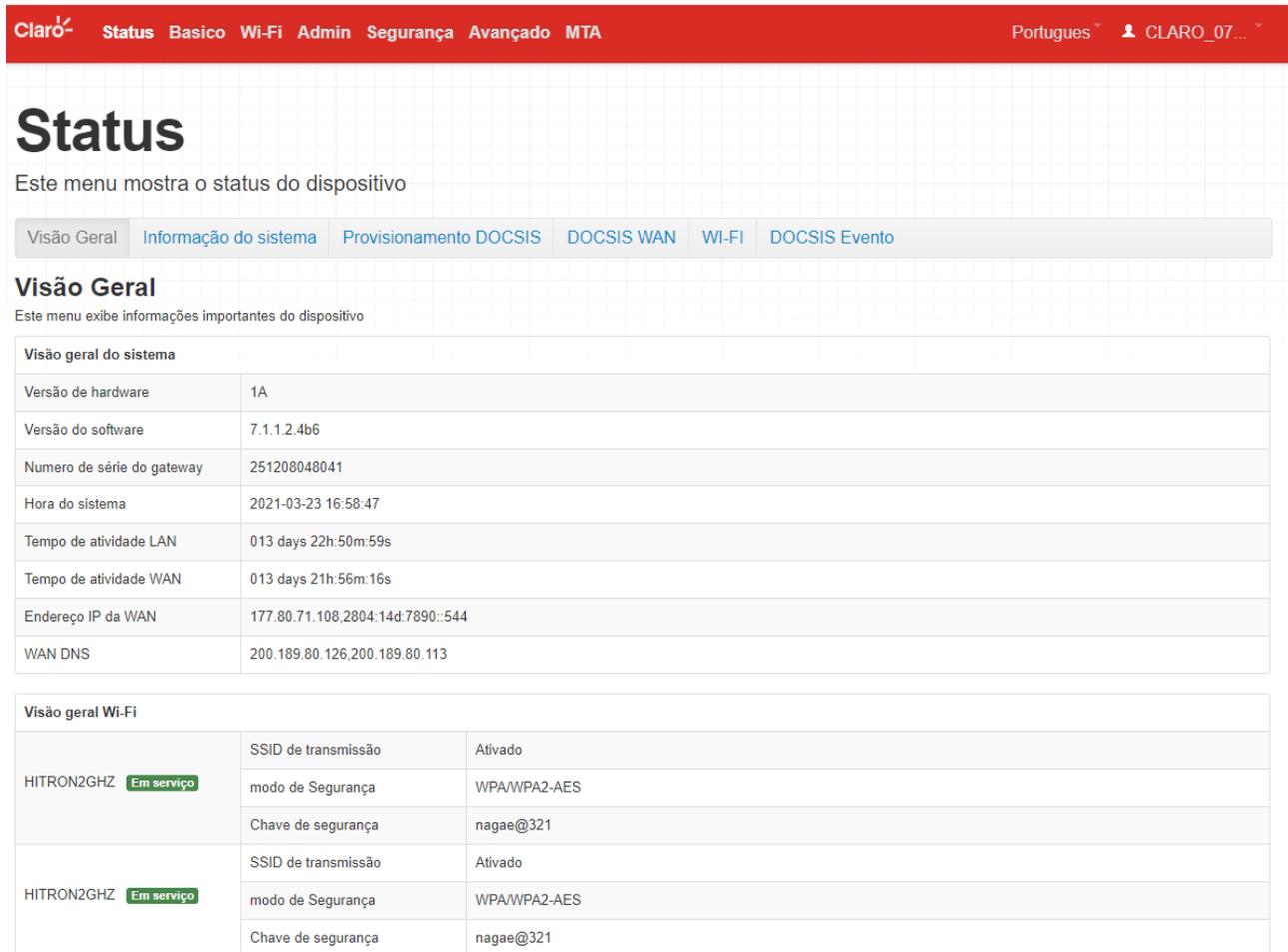
NOTA: O nome de usuário e a senha são sensíveis a casos; "administrador" não é o mesmo que "Administrador".

- 4 Clique **em Login**. A tela **de informações do sistema** é exibida (consulte a tela de informações do sistema).

## 1.6 Visão geral do GUI

Esta seção descreve a GUI da HI3120.

Figura 6: Visão geral da GUI



Claro Status Básico Wi-Fi Admin Segurança Avançado MTA Portuguese CLARO\_07...

# Status

Este menu mostra o status do dispositivo

Visão Geral Informação do sistema Provisionamento DOCSIS DOCSIS WAN WI-FI DOCSIS Evento

## Visão Geral

Este menu exibe informações importantes do dispositivo

Visão geral do sistema	
Versão de hardware	1A
Versão do software	7.1.1.2.4b6
Numero de série do gateway	251208048041
Hora do sistema	2021-03-23 16:58:47
Tempo de atividade LAN	013 days 22h:50m:59s
Tempo de atividade WAN	013 days 21h:56m:16s
Endereço IP da WAN	177.80.71.108,2804:14d:7890::544
WAN DNS	200.189.80.126,200.189.80.113

Visão geral Wi-Fi		
HITRON2GHZ <span>Em serviço</span>	SSID de transmissão	Ativado
	modo de Segurança	WPA/WPA2-AES
	Chave de segurança	nagae@321
HITRON2GHZ <span>Em serviço</span>	SSID de transmissão	Ativado
	modo de Segurança	WPA/WPA2-AES
	Chave de segurança	nagae@321

Tabela 4: [Visão geral da GUI](#)

Barra de Navegação Primária	Use esta seção para passar de uma parte da GUI para outra.
Barra de Navegação Secundária	Use esta seção para mover de uma tela relacionada para outra.
Janela Principal	Use esta seção para ler informações sobre a configuração do seu HI3120 e fazer alterações de configuração.

## 1.7 Redefinindo o HI3120

Quando você redefine o HI3120 para seus padrões de fábrica, todas as configurações configuradas pelo usuário são perdidas e o HI3120 é devolvido ao seu estado de configuração inicial.

Para redefinir o HI3120, clique em **Administrador** > **Reset do dispositivo**. Na tela que é exibida, clique no botão **Redefinir de fábrica**.

O HI3120 desliga e liga novamente, usando suas configurações padrão de fábrica.

NOTA: [Dependendo da configuração anterior do seu HI3120, você pode precisar reconfigurar as configurações ip do seu computador; consulte configuração de endereço IP.](#)

# 2

## Status

Este capítulo descreve as telas que exibem quando você clicar em **Status** na barra de ferramentas. Ele contém as seguintes seções:

- ▶ [Visão geral do status](#)
- ▶ [Informações do sistema](#)
- ▶ [Provisionamento DOCSIS](#)
- ▶ [DOCSIS WAN](#)
- ▶ [Eventos DOCSIS](#)
- ▶ [Status Wi-Fi](#)
- ▶ [MTA](#)

### 2.1 Visão geral do status

Esta seção descreve alguns dos conceitos relacionados às telas **status**.

#### 2.1.1 Docsis

A Especificação de Interface de Serviço de Dados sobre Cabo (DOCSIS) é uma norma de telecomunicações que define a prestação de serviços de dados (acesso à Internet) em uma rede tradicional de TV a cabo (CATV).

Seu HI3120 suporta docsis versão 3.0.

## 2.1.2 Endereços IP e Sub-redes

Todos os computadores da Internet devem ter um endereço IP (Internet Protocol) exclusivo. O endereço IP funciona muito parecido com um endereço de rua, na qual identifica um local específico para o qual as informações são transmitidas. Nenhum computador em uma rede pode ter o mesmo endereço IP.

### 2.1.2.1 Formato de endereço IP

Os endereços IP consistem em quatro octetos (valores numéricos de 8 bits) e geralmente são representados em notação decimal, por exemplo **192.168.1.1**. Em notação decimal, isso significa que cada octeto tem um valor mínimo de 0 e um máximo valor de 255.

Um endereço IP carrega duas informações básicas: o "número de rede" (o endereço da rede como um todo, análogo a um nome de rua) e o "Host ID" (análogo a um número de casa) que identifica o computador específico (ou outro dispositivo network).

### 2.1.2.2 Atribuição de endereço IP

Os endereços IP podem vir de três lugares:

- ▶ A Agência de Números Atribuídos à Internet (IANA)
- ▶ Seu provedor de serviços de Internet
- ▶ Você (ou seus dispositivos de rede)

O IANA é responsável pela alocação de endereços IP em escala global e seu ISP atribui endereços IP a seus clientes. Você nunca deve tentar definir seus próprios endereços IP em uma rede pública, mas você é livre para fazê-lo em uma rede privada.

No caso da HI3120:

- ▶ A rede pública (Wide Area Network ou WAN) é o link entre o conector de cabo e seu Provedor de Serviços de Internet. O endereço IP do seu HI3120 nesta rede é atribuído pelo seu provedor de serviços.

- ▶ A rede privada é a sua Rede de Área Local (LAN) e Rede de Área Local Sem Fio (WLAN), se habilitada. Você é livre para atribuir endereços IP a computadores na LAN e WLAN manualmente, ou para permitir que o HI3120 os atribua automaticamente via DHCP (Dynamic Host Configuration Protocol). A IANA reservou os seguintes blocos de endereços IP para serem usados apenas para redes privadas:

Tabela 5: [Faixas privadas de endereços IP](#)

De...	... Para
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Se você atribuir endereços manualmente, eles devem estar dentro da sub-rede LAN da HI3120.

### 2.1.2.3 Sub-redes

Uma sub-rede é, como o nome sugere, uma seção separada de uma rede, distinta da rede principal da qual faz parte. Uma sub-rede pode conter todos computadores em um escritório local corporativo, por exemplo, enquanto a rede principal inclui vários escritórios.

Para definir a extensão de uma sub-rede e diferenciá-la da rede principal, é usada uma máscara de sub-rede. Esta "mascara" a parte do endereço IP que se refere à rede principal, deixando a parte do endereço IP que se refere à sub-rede.

Cada máscara de sub-rede tem 32 bits (dígitos binários), assim como cada endereço IP:

- ▶ Um valor binário de **1** na máscara de sub-rede indica que o bit correspondente no endereço IP faz parte da rede principal.
- ▶ Um valor binário de **0** na máscara de sub-rede indica que o bit correspondente no endereço IP faz parte da sub-rede.

Por exemplo, a tabela a seguir mostra o endereço IP de um computador (**192.168.1.1**) expresso em decimal e binário (cada célula na tabela indica um octeto):

Tabela 6: [Endereço IP: Decimal e Binário](#)

192	168	0	1
11000000	10101000	00000000	00000001

A tabela a seguir mostra uma máscara de sub-rede que "mascara" os primeiros vinte e quatro bits do endereço IP, tanto em sua notação decimal quanto binária.

Tabela 7: **Máscara de Sub-rede: Decimal e Binário**

255	255	255	0
11111111	11111111	11111111	00000000

Isso mostra que nesta sub-rede, os três primeiros octetos (**192.168.1**, no exemplo endereço IP) definem a rede principal, e o octeto final (**1**, no exemplo endereço IP) define o endereço do computador na sub-rede.

As notações decimais e binárias dão as duas formas comuns de escrever uma máscara de sub-rede:

- ▶ Decimal: a máscara de sub-rede é escrita da mesma forma que o endereço IP: **255.255.255.0**, por exemplo.
- ▶ Binário: a máscara de sub-rede é indicada após o endereço IP (precedido por uma barra dianteira), especificando o número de dígitos binários que ele mascara. A máscara de sub-rede **255.255.255.0** mascara os primeiros vinte e quatro bits do endereço IP, por isso seria escrito como follows: **192.168.1.1/24**.

## 2.1.3 DHCP

O Dynamic Host Configuration Protocol, ou DHCP, define o processo pelo qual os endereços IP podem ser atribuídos a computadores e outros dispositivos de rede automaticamente, a partir de outro dispositivo na rede. Este dispositivo é conhecido como um servidor DHCP e fornece redes adicionais a todos os dispositivos cliente DHCP.

Para receber um endereço IP via DHCP, um computador deve primeiro solicitar um do servidor DHCP (esta é uma solicitação de transmissão, o que significa que ele é enviado para toda a rede, em vez de apenas um endereço IP). O servidor DHCP ouve as solicitações e responde atribuindo um endereço IP ao computador que o solicitou.

Se um computador não estiver configurado para solicitar um endereço IP via DHCP, você deve configurar um endereço IP manualmente se quiser acessar outros computadores e dispositivos na rede. Consulte configuração de endereço IP para obter mais informações.

Por padrão, o HI3120 é um cliente DHCP na WAN (a conexão CATV). Ele transmite um endereço IP pela rede de tv a cabo e recebe um do provedor de serviços. Por padrão, o HI3120 é um servidor DHCP na LAN; ele fornece endereços IP para computadores na LAN que os solicitam.

## 2.1.4 Locação DHCP

"Locação DHCP" refere-se ao período de tempo para o qual um servidor DHCP permite que um cliente DHCP use um endereço IP. Normalmente, um cliente DHCP solicitará uma renovação de locação DHCP antes do fim do tempo de locação, e pode continuar a usar o endereço IP para um período adicional. No entanto, se o cliente não solicitar uma renovação, o servidor DHCP deixa de permitir que o cliente use o endereço IP.

Isso é feito para evitar que os endereços IP sejam usados por computadores que não os requerem mais, uma vez que o pool de endereços IP disponíveis é finito.

## 2.1.5 Endereços MAC

Cada dispositivo de rede possui um endereço MAC (Media Access Control, controle de acesso de mídia). Este é um código alfanumérico único, dado ao dispositivo na fábrica, que na maioria dos casos não pode ser alterado (embora alguns dispositivos sejam capazes de "falsificação MAC", onde se passam pelo endereço MAC de outro dispositivo).

Os endereços MAC são a maneira mais confiável de identificar dispositivos de rede, uma vez que os endereços IP tendem a mudar ao longo do tempo (seja manualmente alterado ou atualizado via DHCP).

Cada endereço MAC é exibido como seis grupos de dois dígitos hexadecimais separados por colons (ou, ocasionalmente, traços) por exemplo **00:AA:FF:1A:B5:74**.

NOTA: Cada grupo de dois dígitos hexadecimais é conhecido como um "octeto", uma vez que representa oito bits.

Tenha em mente que um endereço MAC não representa precisamente um computador em sua rede (ou em outro lugar), ele representa um dispositivo de rede, que pode ser parte de um computador (ou outro dispositivo). Por exemplo, se um único computador tiver uma placa Ethernet (para se conectar ao seu HI3120 através de uma das portas **LAN**) e também tiver uma placa sem fio (para se conectar ao seu HI3120 através da interface sem fio), os endereços MAC das duas placas serão diferentes. No caso do HI3120, cada módulo interno (modem de cabo module, módulo Ethernet, módulo sem fio, etc.) possui seu próprio endereço MAC

### 2.1.6 Modo de roteamento

Quando seu HI3120 está no modo de roteamento, ele age como um gateway para computadores na LAN acessarem a Internet. O provedor de serviços atribui um endereço IP ao HI3120 na WAN, e todo o tráfego para computadores LAN é enviado para esse endereço IP. O HI3120 atribui endereços IP privado aos computadores LAN (quando o DHCP está ativo), e transmite o tráfego relevante para cada endereço IP privado.

NOTA: Quando o DHCP não estiver ativo no modo HI3120 no modo de roteamento, cada computador na LAN deve receber um endereço IP na sub-rede manualmente.

Quando o HI3120 não está no modo de roteamento, o provedor de serviços atribui um endereço IP a cada computador conectado diretamente ao HI3120. O HI3120 não realiza nenhuma operação de roteamento, e o tráfego flui entre os computadores e o provedor de serviços.

O modo de roteamento não é configurável pelo usuário; ele é especificado pelo provedor de serviços no arquivo de configuração do HI3120.

### 2.1.7 Arquivos de configuração

O arquivo de configuração (ou config) da HI3120 é um documento que o HI3120 obtém automaticamente pela Internet a partir do servidor do provedor de serviços, que especifica as configurações que o HI3120 deve usar. Ele contém uma variedade de configurações que não estão presentes na Interface gráfica de usuário (GUI) configurável pelo usuário e podem ser especificadas apenas pelo serviço do provedor.

### 2.1.8 Transmissões downstream e upstream

Os termos "downstream" e "upstream" referem-se aos fluxos de tráfego de dados e indicam a direção em que o tráfego está viajando. "Downstream" refere-se ao tráfego do provedor de serviços para o HI3120, e "upstream" refere-se ao tráfego da HI3120 para o provedor de serviço.

### 2.1.9 Frequências de cabos

Assim como as transmissões de rádio, as transmissões de dados sobre a rede de cabos devem existir em diferentes frequências, a fim de evitar interferências entre os sinais.

A faixa de tráfego de dados é separada da banda de TV, e cada canal data é separado de outros canais de dados.

## 2.1.10 Modulação

As transmissões sobre a rede de cabos são baseadas em uma forma de onda periódica de alta frequência conhecida como "onda portadora". Esta onda portadora é assim chamada porque "carrega" o sinal de dados. O sinal de dados em si é definido por variações na onda portadora. O processo de variar a onda portadora (a fim de transportar sinal de dados informação) é conhecida como "modulação". O sinal de dados é, portanto, conhecido como "sinal modulador".

As transmissões de cabo utilizam uma variedade de métodos para realizar a modulação (e a "decodificação" do sinal recebido, ou "demodulação"). Os métodos de modulação definidos no DOCSIS 3 são os seguintes:

- ▶ **QPSK**: Chave de fase de quadratura
- ▶ **QAM**: Modulação de Amplitude de Quadratura
- ▶ **QAM TCM** : Modulação da amplitude de quadratura de trellis

Em muitos casos, um número precede o tipo de modulação (por exemplo **16 QAM**). Este número refere-se à complexidade da modulação. Quanto maior o número, mais dados podem ser codificados em cada símbolo.

NOTA: [Em sinais modulados, cada caractere modulado distinto \(por exemplo, cada tom audível produzido por um modem para transmissão sobre linhas telefônicas\) é conhecido como um símbolo.](#)

Uma vez que mais informações podem ser representadas por um único caractere, um número alto seu indica uma taxa de transferência de dados mais alta.

## 2.1.11 TDMA, FDMA e SCDMA

O Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) e Synchronous Code Division Multiple Access (SCDMA) são métodos de acesso ao canal que permitem que vários usuários compartilhem o mesmo canal de frequência.

- ▶ O TDMA permite que vários usuários compartilhem o mesmo canal de frequência dividindo transmissões por tempo. Cada usuário é alocado uma série de faixas horárias e transmite durante esses horários.
- ▶ O FDMA permite que vários usuários compartilhem o mesmo canal de frequência atribuindo uma faixa de frequência dentro do canal existente a cada usuário.

- ▶ O SCDMA permite que vários usuários compartilhem o mesmo canal de frequência, atribuindo um código ortogonal exclusivo a cada usuário.

## 2.2 Informações do sistema

Use esta tela para ver a formação geral sobre o hardware do seu HI3120, seu software e sua conexão com a Internet.

Clique em **Status>Informações do sistema**. O visor de tela a seguir.

Figura 7: Status: Informações do sistema

**Status**

Este menu mostra o status do dispositivo

Visão Geral | Informação do sistema | Provisionamento DOCSIS | DOCSIS WAN | WI-FI | DOCSIS Evento

**Informação do sistema**

Este menu exibe informações gerais do dispositivo

Versão de hardware	1A	Endereço IP da WAN	191.186.110.20,2804:14d:10::7
Versão do software	7.1.1.2.5b1	WAN recebendo	228.75G Bytes
Numero de série do gateway	251208072639	Envio de WAN	47.53G Bytes
Endereço MAC HFC	90:AA:C3:07:33:00	Endereço IP da LAN privada	192.168.0.1/24
Hora do sistema	2021-04-09 15:13:28	Recepção LAN	467.83M Bytes
Fuso horário	UTC-03: 00 Terra Nova, Groenlândia, Brasil Leste	Envio de LAN	575.61M Bytes
Tempo de atividade LAN	007 days 22h:59m:22s	Tempo de atividade WAN	000 days 00h:06m:29s

A tabela a seguir descreve os rótulos nesta tela.

Tabela 8: Status: Informações do sistema

Versão de hardware	Isso exibe o número da versão do hardware físico do HI3120.
Versão de software	Isso exibe o número da versão do software que controla o HI3120.

Número de série do Gateway	Isso exibe um número que identifica exclusivamente o dispositivo.
Endereço MAC HFC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) do módulo HFC (Hybrid-Fiber Coax) da HI3120. Este é o módulo que se conecta à Internet através da conexão <b>CATV</b> .
Tempo do sistema	Isso exibe a data e a hora atuais.
Tempo de up do sistema	Isso mostra a quantidade de tempo que se passou desde que o HI3120 foi reiniciado pela última vez.
WAN IP	Isso exibe o endereço IP WAN da HI3120. Este endereço IP é automaticamente atribuído ao HI3120
Wan Recebendo	Isso exibe a quantidade de dados recebidos sobre a conexão WAN desde que o dispositivo foi iniciado pela última vez.
Wan Envio	Isso exibe a quantidade de dados transmitidos sobre a conexão WAN desde que o dispositivo foi iniciado pela última vez.
Sub-rede privada LAN IPv4	Isso exibe as informações ip da sub-rede LAN da HI3120.
Recebimento de LAN	Isso exibe a quantidade de dados recebidos sobre a conexão LAN desde que o dispositivo foi iniciado pela última vez.
Lan Enviando	Isso exibe a quantidade de dados transmitidos sobre a conexão LAN desde que o dispositivo foi iniciado pela última vez.

## 2.3 Provisionamento DOCSIS

Esta tela exibe os passos dados com sucesso para se conectar à Internet pela **Conexão** de cabo.

Use esta tela para fins de solução de problemas para garantir que o HI3120 tenha se conectado com sucesso à Internet; se ocorreu um erro, você pode identificar o estágio em que a falha ocorreu. Clique em **Status** > **Provisionamento DOCSIS**. A tela a seguir é exibida.

Figura 8: Status: Provisionamento DOCSIS

Claro Status Básico Wi-Fi Admin Segurança Avançado MTA Portuguese CLARO\_07...

## Status

Este menu mostra o status do dispositivo

Visão Geral Informação do sistema Provisionamento DOCSIS DOCSIS WAN WI-FI DOCSIS Evento

### Status de provisionamento DOCSIS

Este menu exibe o status de conectividade do modem e seu estado de inicialização

HW init	Sucesso
encontrar Downstream	Sucesso
classificação	Sucesso
DHCP	Sucesso
Hora do dia	Sucesso
Download modem Config File	Sucesso
Registro	Sucesso
EAE status	Desabilitado
BPI status	AUTH:inicio, TEK:inicio

Para cada etapa:

- ▶ **O** processo é exibido quando o HI3120 está tentando completar uma etapa de conexão.
- ▶ **O sucesso é exibido quando o HI3120 completou uma etapa** de conexão.
- ▶ **Desativar** displays quando o recurso relevante tiver sido desativado.

## 2.4 DOCSIS WAN

Use esta tela para descobrir informações sobre:

- ▶ A natureza da conexão upstream e downstream entre o HI3120 e o dispositivo ao qual está conectado através da interface **CABLE**.
- ▶ Detalhes IP da conexão WAN da HI3120.

Clique em **Status > DOCSIS WAN**. A tela a seguir é exibida. Clique em **Status > DOCSIS WAN**. A tela a seguir é exibida.

Figura 9: Status: DOCSIS WAN

**Status**

Este menu mostra o status do dispositivo

Visão Geral | Informação do sistema | Provisionamento DOCSIS | **DOCSIS WAN** | WI-FI | DOCSIS Evento

**DOCSIS WAN**

Este menu exibe os parâmetros de sinal upstream e downstream

Visão geral DOCSIS	
Acesso a rede	Permitido
Endereço de IP	10.13.12.27
Máscara de sub-rede	255.255.192.0
Endereço IP do gateway	10.13.0.1
Tempo de concessão de DHCP	D: 06 H: 164 M: 32 S: 11

Visão geral downstream								
Porta ID	Frequência (Hz)	Modulação	RX (dBmV)	ID do canal	SNR (dB)	Bytes	Corretos	Incorretos
1	567000000	256QAM	8.599	42	40.946	0	0	0
2	573000000	256QAM	8.800	90	40.366	840160332	0	0
3	579000000	256QAM	8.500	91	40.366	2707572268	0	0
4	585000000	256QAM	8.500	92	40.946	915597232	0	0
5	591000000	256QAM	8.599	93	40.946	2702540227	0	0
6	597000000	256QAM	8.199	94	40.366	1238926420	0	0
7	603000000	256QAM	8.199	95	40.946	2704519705	0	0
8	609000000	256QAM	8.199	96	40.946	978862774	0	0
9	615000000	256QAM	8.000	97	40.946	2473801198	0	0

A tabela a seguir descreve os rótulos nesta tela.

Tabela 9: Status: WAN DOCSIS

Visão geral do DOCSIS	
Acesso à rede	<p>Isso mostra se o seu provedor de serviços permite ou não acessar a Internet pela conexão CABO.</p> <ul style="list-style-type: none"> <li>▶ <b>Permitido</b> será exibido se você puder acessar a Internet.</li> <li>▶ <b>Negado</b> será exibido se você não conseguir acessar a Internet.</li> </ul>

Tabela 9: [Status: WAN DOCSIS \(continuação\)](#)

Endereço IP	Isso exibe o endereço IP WAN da HI3120. Este endereço IP é automaticamente atribuído ao HI3120
Máscara de Sub-rede	Isso exibe a máscara de sub-rede WAN da HI3120.
Tempo de locação do DHCP	Isso exibe o tempo que se passa antes do término da locação de endereços IP do seu dispositivo, e um novo endereço IP é atribuído a ele pelo servidor DHCP.
Visão geral a jusante	
NOTA: <a href="#">O sinal a jusante é o sinal transmitido ao HI3120.</a>	
Forçar a frequência a jusante (MHz)	Use-o para configurar o HI3120 para usar uma frequência específica a jusante. Digite a frequência desejada em Mega-hertz (MHz) e clique em <b>Aplicar</b> .
Porta	Isso exibe o número de identificação da porta da conexão a jusante.
Frequência (Hz)	Isso exibe a frequência real em Hertz (Hz) de cada canal de dados a jusante ao qual o HI3120 está conectado.
Modulação	Isso exibe o tipo de modulação que cada canal a jusante usa.
Potência (dbmV)	Isso exibe a potência do sinal de cada canal de dados a jusante ao qual o HI3120 está conectado, no decibéis (decibéis acima/abaixo de 1 milivolt).
SNR (dB)	Isso exibe a Relação Sinal para Ruído (SNR) de cada canal de dados a jusante ao qual o HI3120 está conectado, em dB (decibéis).
Canal	Isso exibe o número de identificação de cada canal no qual o sinal a jusante é transmitido.
Visão geral upstream	
NOTA: <a href="#">O sinal a montante é o sinal transmitido do HI3120.</a>	
Forçar a frequência a jusante (MHz)	Use-o para configurar o HI3120 para usar uma frequência upstream específica. Digite a frequência desejada em Mega-hertz (MHz) e clique em <b>Aplicar</b> .
Porta	Isso exibe o número de identificação da porta da conexão upstream.
Frequência (Hz)	Isso exibe a frequência real em Hertz (Hz) de cada canal de dados upstream ao qual o HI3120 está conectado.

Tabela 9: [Status: WAN DOCSIS \(continuação\)](#)

Modulação	Isso exibe o tipo de modulação que cada canal upstream usa.
Potência (debmV)	Isso exibe a potência do sinal de cada canal de dados a montante ao qual o HI3120 está conectado, no decibéis (decibéis acima/abaixo de 1 milivolt).
SNR (dB)	Isso exibe a Relação Sinal para Ruído (SNR) de cada canal de dados a montante ao qual o HI3120 está conectado, em dB (decibéis).
Canal	Isso exibe o número de identificação de cada canal no qual o sinal upstream é transmitido.

## 2.5 Eventos DOCSIS

Use esta tela para visualizar informações sobre eventos locais de atividades WAN. Clique **em Status** > Tela **DOCSIS Evento**. A tela a seguir é exibida.

Figura 10: Status: DOCSIS Evento

Claro
Portugues CLARO\_07...

Status
Basico Wi-Fi Admin Segurança Avançado MTA

## Status

Este menu mostra o status do dispositivo

Visão Geral
Informação do sistema
Provisionamento DOCSIS
DOCSIS WAN
Wi-Fi
DOCSIS Evento

### DOCSIS Logs

Os logs de eventos DOCSIS são mostrados aqui

No.	Tempo	Tipo	Undefined	Evento
1	Tue Mar 9 18:04:25 2021	82001200	5	RNG-RSP CCAP Commanded Power in Excess of 6 dB Below the Value Corresponding to the Top of the DRW;CM-MAC=90:aa:c3:07:0d:20;CM-TS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
2	Thu Jan 1 00:01:25 1970	84020100	4	Missing Mandatory MDD TLV on primary DS Channel;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
3	Tue Mar 9 18:10:36 2021	90000000	5	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
4	Tue Mar 9 18:10:36 2021	73040100	6	TLV-11 - unrecognized OID;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
5	Tue Mar 9 18:10:36 2021	68001102	3	Config File Rejected due to Invalid or Unexpected TLV 11;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
6	Tue Mar 9 18:10:38 2021	73050400	5	REG-RSP-MP Mismatch Between Calculated Value for P1.6hi Compared to CCAP Provided Value;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
7	Tue Mar 9 18:10:38 2021	82001200	5	RNG-RSP CCAP Commanded Power in Excess of 6 dB Below the Value Corresponding to the Top of the DRW;CM-MAC=90:aa:c3:07:0d:20;CM-TS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
8	Tue Mar 9 18:40:17 2021	68010600	6	DHCP Renew - lease parameters tftp file-^1/290A62AE/ modified;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
9	Tue Mar 9 19:02:01 2021	82000700	3	Unicast Ranging Received Abort Response - initializing MAC;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
10	Tue Mar 9 19:02:01 2021	82000200	3	No Ranging Response received - T3 time-out;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;
11	Tue Mar 9 19:02:49 2021	90000000	5	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=90:aa:c3:07:0d:20;CMTS-MAC=00:9e:1e:58:4d:5e;CM-QOS=1.1;CM-VER=3.1;

A tabela a seguir descreve os rótulos neste Tela.

Tabela 10: Status: DOCSIS Evento

Não	Isso exibe o número de índice arbitrário e incremental atribuído ao evento.
Hora	Isso mostra a data e a hora em que o evento ocorreu.
Tipo	Isso mostra a natureza do evento.
Prioridade	Isso mostra a gravidade do evento.
Evento	Isso exibe uma descrição do evento.
Claro	Clique nisso para remover todos os registros de eventos DOCSIS do sistema.

## 2.6 Status Wi-Fi

Use esta tela para visualizar informações sobre a rede sem fio da HI3120.

Clique em **Status** > **Wi-Fi**. A tela a seguir é exibida.

Figura 11: Status: Status Wi-Fi

The screenshot shows the 'Status Wi-Fi' page in a web interface. At the top, there is a navigation bar with 'Claro' and menu items: 'Status', 'Basico', 'Wi-Fi', 'Admin', 'Segurança', 'Avançado', 'MTA'. The user is logged in as 'CLARO\_07...'. The main heading is 'Status', with a sub-heading 'Este menu mostra o status do dispositivo'. Below this are tabs for 'Visão Geral', 'Informação do sistema', 'Provisionamento DOCSIS', 'DOCSIS WAN', 'Wi-Fi', and 'DOCSIS Evento'. The 'Status Wi-Fi' section is active, with the sub-heading 'Este menu exibe o status Wi-Fi atual'. It is divided into two main sections: '2.4 GHz Status Wi-Fi' and '5 GHz Status Wi-Fi'. Each section contains a table with configuration details. The 2.4 GHz section shows 'Status Wi-Fi (2.4 GHz)' as 'ON', 'modo Wi-fi (2.4 GHz)' as '802.11 g/n Mixed', and 'Canal Wi-Fi (2.4 GHz)' as 'Auto(11)'. The 5 GHz section shows 'Status Wi-Fi (5 GHz)' as 'ON', 'modo Wi-fi (5 GHz)' as '802.11 a/n/ac Mixed', and 'Canal Wi-Fi (5 GHz)' as 'Auto(16T)'. Below these are two 'Visão geral do SSID' sections, one for 2.4 GHz and one for 5 GHz, both for the SSID 'HITRON2GHZ' (marked 'Em serviço'). Each SSID section contains a table with 'SSID de transmissão' (Ativado), 'WMM(QOS)' (Ativado), 'modo de Segurança' (WPA/WPA2-AES), and 'Chave de segurança' (nagae@321).

2.4 GHz Status Wi-Fi	
Status Wi-Fi (2.4 GHz)	ON
modo Wi-fi (2.4 GHz)	802.11 g/n Mixed
Canal Wi-Fi (2.4 GHz)	Auto(11)

5 GHz Status Wi-Fi	
Status Wi-Fi (5 GHz)	ON
modo Wi-fi (5 GHz)	802.11 a/n/ac Mixed
Canal Wi-Fi (5 GHz)	Auto(16T)

Visão geral do SSID		
HITRON2GHZ <span>Em serviço</span>	SSID de transmissão	Ativado
	WMM(QOS)	Ativado
	modo de Segurança	WPA/WPA2-AES
	Chave de segurança	nagae@321

Visão geral do SSID (5 GHz)		
HITRON2GHZ <span>Em serviço</span>	SSID de transmissão	Ativado
	WMM(QOS)	Ativado
	modo de Segurança	WPA/WPA2-AES

A tabela a seguir descreve os rótulos neste Tela.

Tabela 11: [Status: Status Wi-Fi](#)

2.4G	<p>O HI3120 opera dentro das bandas de rede 2.4Ghz e 5GHz. Use essas guias para visualizar informações sobre a rede relevante.</p> <ul style="list-style-type: none"> <li>▶ Clique <b>2.4G</b> para ver informações sobre a rede de 2.4GHz da HI3120.</li> <li>▶ Clique em <b>5G</b> para ver informações sobre a rede de 5GHz da HI3120.</li> </ul> <p>Os campos que exibem são idênticos para ambas as redes.</p>
5G	
Visão geral básica	
Modo sem fio	Isso exibe o tipo de rede sem fio que o HI3120 está usando.
Canal Sem Fio	Isso exibe o canal sem fio no qual o A rede sem fio da HI3120 está transmitindo e recebendo.
Visão geral do SSID	
(SSID)	<p>Isso exibe o identificador de conjunto de serviços da rede sem fio. Este é o nome da rede sem fio, à qual os clientes sem fio se conectam.</p> <ul style="list-style-type: none"> <li>▶ <b>Em Serviço</b> é exibido quando a rede está ativa.</li> <li>▶ <b>Desativado</b> é exibido quando a rede não está ativa.</li> </ul>
SSID de transmissão	Este campo é <b>exibido ativado</b> quando o SSID da rede sem fio está sendo transmitido e é exibido <b>desativado</b> quando não está.
Wmm	Este campo é <b>exibido ativado</b> quando o WiFi MultiMedia está ativo e é exibido <b>desativado</b> quando não está.
Modo de segurança	Isso exibe o tipo de segurança que a rede sem fio da HI3120 está usando atualmente.
Chave de segurança	Isso exibe a senha da rede sem fio da HI3120.

## 2.7 MTA

Use esta tela para ver informações gerais sobre o módulo adaptador de terminal multimídia incorporado da HI3120.

Clique em **Status > MTA**. O visor de tela a seguir.

Figura 12: Status: Tela MTA

Procedimento de Inicialização	
Telefonia DHCP	[N/A]
segurança de telefonia	BASIC
Telefonia TFTP	Process
Telephony Registration Complete	Fail
Status da linha	
Line1	Not Registered
Line2	Not Registered

A tabela a seguir descreve os rótulos neste Tela.

Tabela 12: Status: MTA

Procedimento de provisionamento de telefonia	
DHCP	Este campo exibe o status do servidor DHCP de telefonia remota.
Tipo de fluxo de provisionamento	Isso exibe o tipo de segurança usada para chamadas de voz através do HI3120.
Configuração TFTP	Este campo exibe o status do servidor TFTP de telefonia remota.
Registro	Este campo exibe o status geral do registro de chamada de voz.
Status de registro de linha	
Linha 1	Esses campos exibem o status atual de cada telefone conectado ao HI3120.
Linha 2	
Status de chamada	

Tabela 12: [Status: MTA \(Continuação\)](#)

Linha 1	Esses campos exibem o status atual de quaisquer chamadas que estão sendo realizadas nos telefones conectados ao HI3120.
Linha 2	

# 3

## Básico

Este capítulo descreve as telas que exibem quando você clica em **Básico** na barra de ferramentas. Ele contém as seguintes seções:

- ▶ [Visão geral básica](#)
- ▶ [Configuração LAN](#)
- ▶ [Função gateway](#)
- ▶ [Encaminhamento da porta](#)
- ▶ [Ativação da porta](#)
- ▶ [DMZ](#)
- ▶ [DNS](#)

### 3.1 Visão geral básica

Esta seção descreve alguns dos conceitos relacionados às telas **Básico** (veja também a visão geral do status ).

#### 3.1.1 O sistema de nomes de domínio

Um domínio é um local em uma rede, por **exemplo, example.com**. Na Internet, os nomes de domínio são mapeados para os endereços IP aos quais devem ser encaminhados pelo DNS (Domain Name System, sistema de nomes de domínio). Isso permite que você insira "www.example.com" em seu navegador e alcance o lugar correto na Internet mesmo que o endereço IP do servidor do site tenha sido alterado.

### 3.1.2 Encaminhamento de portas

O encaminhamento de porta permite que um computador em seu LAN receba comunicações específicas de WAN. Normalmente, isso é usado para permitir certos aplicativos (como jogos) através do firewall, para um computador específico na LAN. O encaminhamento de portas também é comumente usado para executar um servidor HTTP público de uma rede privada.

Você pode configurar uma regra de encaminhamento de porta para cada aplicativo para o qual deseja abrir portas no firewall. Quando o HI3120 recebe tráfego de entrada da WAN com uma porta de destino que corresponde a uma regra de encaminhamento de portas, ele encaminha o tráfego para o endereço IP lan e o número da porta especificado na regra de encaminhamento da porta.

NOTA: [Para obter informações sobre as portas, você precisa abrir para um determinado aplicativo, consulte a documentação desse aplicativo.](#)

### 3.1.3 Acionamento de portas

O acionamento de portas é um meio de automatizar o encaminhamento de portas. O HI3120 verifica o tráfego de saída (da LAN para o WAN) para ver se alguma das portas de destino do tráfego corresponder às especificadas nas regras de acionamento da porta que você configura. Se alguma das portas corresponder, o HI3120 abre automaticamente as portas de entrada especificadas na regra, antecipando-se ao tráfego de entrada.

### 3.1.4 DMZ

Em rede, a Zona Desmilitarizada (DMZ) é uma parte do seu LAN que foi isolada do resto da LAN, e aberta à WAN. O termo vem da designação militar para um pedaço de território, geralmente localizado entre duas forças opostas, que é isolado de ambos e ocupado por nenhum dos dois.

### 3.1.5 Modo de roteamento

Quando seu HI3120 está no modo de roteamento, ele age como um gateway para computadores na LAN acessarem a Internet. O provedor de serviços atribui um endereço IP ao HI3120 na WAN, e todo o tráfego para computadores LAN é enviado para esse endereço IP. O HI3120 atribui endereços IP privados a computadores LAN (quando o DHCP está ativo), e transmite o tráfego relevante para cada endereço IP privado.

NOTA: Quando o DHCP não estiver ativo no modo HI3120 no modo de roteamento, cada computador na LAN deve receber um endereço IP na sub-rede do HI3120 manualmente.

Quando o HI3120 não está no modo de roteamento, o provedor de serviços atribui um endereço IP a cada computador conectado diretamente ao HI3120. O HI3120 não realiza nenhuma operação de roteamento, e o tráfego flui entre os computadores e o provedor de serviços.

### 3.2 Configuração LAN

Use esta tela para:

- ▶ Ver informações sobre a conexão do HI3120 com o WAN
- ▶ Configure o servidor DHCP interno do HI3120
- ▶ Defina como o HI3120 atribui endereços IP na LAN
- ▶ Veja informações sobre os dispositivos de rede conectados ao HI3120 na LAN.

Clique **em Básico** > **Configuração de LAN**. A tela a seguir é exibida.

Figura 13: Básico: Configuração da LAN

Claro Status Básico WI-Fi Admin Segurança Avançado MTA Portuguese CLARO\_07...

## Configurações básicas

Este menu mostra as configurações básicas do dispositivo

Configuração da LAN Configuração da WAN Funcao de Gateway Encaminhamento de porta Acionamento de Porta DMZ DNS

### Configuração de LAN privada

Endereço IP da LAN privada	<input type="text" value="192.168.0.1"/>
Máscara de sub-rede	<input type="text" value="255.255.255.0"/>
Status do DHCP da LAN	<input checked="" type="radio"/> <b>Ativado</b> <input type="radio"/> Desativado <input type="button" value="Reserva DHCP"/>
Tempo de concessão de DHCP	<input type="text" value="1 Semana"/>
IP de inicio do DHCP	<input type="text" value="192.168.0.2"/>
IP final do DHCP	<input type="text" value="192.168.0.253"/>

### Dispositivos conectados

Nome de HOST	Endereço de IP	Endereço MAC	Tipo	Interface	Status
--------------	----------------	--------------	------	-----------	--------

A tabela a seguir descreve os rótulos nesta tela.

Tabela 13: Básico: Configuração da LAN

Configuração lan privada	
Endereço IP LAN privado	Use este campo para definir o endereço IP do HI3120 na LAN.
Máscara de Sub-rede	Use este campo para definir a sub-rede LAN. Use notação decimal pontilhada (por exemplo, <b>255.255.255,0</b> ).
LAN DHCP Status	Use este campo para configurar se o servidor DHCP do HI3120 está ativo ou não. <ul style="list-style-type: none"> <li>▶ Para ativar o servidor DHCP, clique em <b>Habilitar</b>.</li> <li>▶ Para desativar o dhcp server, clique em <b>Desativar</b>.</li> </ul>

Tabela 13: [Básico: Configuração da LAN \(continuação\)](#)

Tempo de locação	Use isso para selecionar o tempo que se passa antes do término da locação de endereços IP do seu dispositivo, e um novo endereço IP é atribuído a ele pelo servidor DHCP.
IP de início do DHCP	Use este campo para especificar o endereço IP no qual o HI3120 começa a atribuir endereços IP a dispositivos na LAN (quando o DHCP estiver ativado).
IP final do DHCP	Use este campo para especificar o endereço IP no qual o HI3120 para de atribuir endereços IP a dispositivos na LAN (quando o DHCP estiver ativado).  NOTA: Os dispositivos que solicitam endereços IP uma vez que o pool DHCP esteja esgotado não recebem um endereço IP.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.
Computadores Conectados	
Nome do anfitrião	Isso exibe o nome de cada dispositivo de rede conectado na LAN.
Endereço IP	Isso exibe o endereço IP de cada dispositivo de rede conectado na LAN.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada dispositivo de rede conectado na LAN.
Tipo	Isso mostra se o endereço IP do dispositivo foi atribuído pelo DHCP( <b>DHCP-IP</b> )ou <b>auto-atribuído</b> .
Interface	Isso mostra se o dispositivo está conectado na LAN( <b>Ethernet</b> ) ou no WLAN (Wireless(x), onde <b>x</b> denota o modo sem fio; <b>b</b> , <b>g</b> ou <b>n</b> ).
Status	Isso é <b>exibido Ativo</b> quando o computador conectado está on-line e <b>inativo</b> quando o computador conectado está desligado.

### 3.3 Função de gateway

Use esta tela para ativar ou desativar o gateway residencial da HI3120 e as funções UPnP (Universal Plug n Play).

Desativar o recurso de gateway residencial define o aparelho apenas para usar o modo ponte. Use este modo quando sua rede já estiver usando outro roteador.

Clique em **Básico>Função de Gateway**. O visor de tela a seguir.

Figura 14: Básico: Função de Gateway



A tabela a seguir descreve os rótulos neste Tela.

Tabela 14: Básico: Função de Gateway

UPnP	Selecione a caixa de seleção para ativar os recursos do Dispositivo Universal Plug n Play Internet Gateway da HI3120 ou desmarque a caixa de seleção para desabilitá-los.
------	---

### 3.4 Encaminhamento da porta

Use esta tela para configurar o encaminhamento da porta entre computadores no WAN e computadores na LAN. Você pode ativar ou desativar a porta e configurar novas e existentes regras de encaminhamento de portas.

Clique em **Básico** > **Encaminhamento de porta**. O visor de tela a seguir.

Figura 15: **Básico: Encaminhamento de porta**



A tabela a seguir descreve os rótulos nesta tela.

Tabela 15: **Básico: Encaminhamento de porta**

Todas as regras de encaminhamento de portas	Use este campo para ligar ou desligar a porta. ▶ Seleccionar <b>ativado</b> para ativar o encaminhamento da porta. ▶ Seleccionar <b>desativado</b> para desativar o encaminhamento da porta.
Regras de encaminhamento de portas	
Selecione	Selecione o botão de rádio de uma regra de encaminhamento da porta antes de clicar em <b>Editar</b> ou <b>Excluir</b> .
Não	Isso exibe o número de identificação arbitrária atribuído à regra de encaminhamento da porta.
Nome	Isso exibe o nome arbitrário atribuído à regra quando a criou.

Tabela 15: Básico: Encaminhamento de porta (continuação)

Público	<p>Esses campos exibem as portas às quais a regra se aplica:</p> <ul style="list-style-type: none"> <li>▶ O campo <b>Público</b> exibe o alcance de porta de entrada. Estas são as portas em que o HI3120 recebeu tráfego do host originário na WAN.</li> <li>▶ O campo <b>Private</b> exibe o alcance da porta para o qual o HI3120 encaminha o tráfego para o dispositivo na LAN.</li> </ul>
Privada	
Protocolo	<p>Este campo exibe o protocolo ou protocolos aos quais esta regra se aplica:</p> <ul style="list-style-type: none"> <li>▶ <i>Protocolo de Controle de Transmissão</i> (TCP)</li> <li>▶ <i>Protocolo de Datagrama do Usuário</i> (UDP)</li> <li>▶ <i>Protocolo de Controle de Transmissão e Protocolo de Datagrama do Usuário</i> (TCP/UDP)</li> </ul> <p>encapsulamento de roteamento genérico (GRE)</p> <ul style="list-style-type: none"> <li>▶ Encapsular o Protocolo de Segurança (ESP)</li> </ul>
Endereço IP local	<p>Isso exibe o endereço IP do computador na LAN para o qual o tráfego em conformidade com as condições de alcance e <b>protocolo de porta pública</b> é encaminhado.</p>
Status	<p>Use isso para ativar ou desativar a regra de encaminhamento da porta.</p> <ul style="list-style-type: none"> <li>▶ Selecione <b>ON</b> para ativar a regra de encaminhamento da porta.</li> <li>▶ Selecione <b>OFF</b> para desativar a regra de encaminhamento da porta.</li> </ul>
Adicionar	<p>Clique nisso para definir uma nova regra de encaminhamento de portas. Consulte Adicionar ou Editar uma regra de encaminhamento de portas para obter informações na tela que exibe.</p>
Editar	<p>Selecione o botão de rádio de uma regra de encaminhamento de porta e clique nisso para fazer alterações na regra. Consulte Adicionar ou Editar uma regra de encaminhamento de portas para obter informações na tela que exibe.</p>
Excluir	<p>Selecione o botão de rádio de uma regra de encaminhamento de porta e clique nisso para remover a regra. As informações da regra excluída não podem ser recuperadas.</p>
Ajuda	<p>Clique nisso para ver informações sobre os campos nesta tela.</p>

### 3.4.1 Adicionar ou editar uma regra de encaminhamento de portas

- ▶ Para adicionar uma nova regra de encaminhamento de portas, clique em **Adicionar** no **Básico > Encaminhamento de Porta** Tela.
- ▶ Para editar uma regra de encaminhamento de porta existente, selecione o botão de rádio da regra no **Básico > Tela de encaminhamento de porta** e clique no botão **Editar**.

NOTA: **Certifique-se de que `habilitado` está selecionado na tela `Básico>Porta de encaminhamento` para adicionar ou editar regras de encaminhamento da porta.**

A tela a seguir é exibida.

Figura 16: **Básico: Adicionar/editar encaminhamento de porta**

Adicione uma regra para serviços de encaminhamento de porta pelo usuário	
Aplicativo comum	-SERVICES-
Nome da Aplicação	
Protocolo	UDP
Faixa de Portas Publicas	
Faixa de portas privadas	
Endereço IP local	
Endereço IP remoto	<input checked="" type="radio"/> Qualquer <input type="radio"/> Específico
Status da regra	<input checked="" type="radio"/> ON <input type="radio"/> OFF
<input type="button" value="Aplique"/> <input type="button" value="Fechar"/>	

A tabela a seguir descreve os rótulos nesta tela.

Tabela 16: **Básico: Adicionar/editar encaminhamento de portas.**

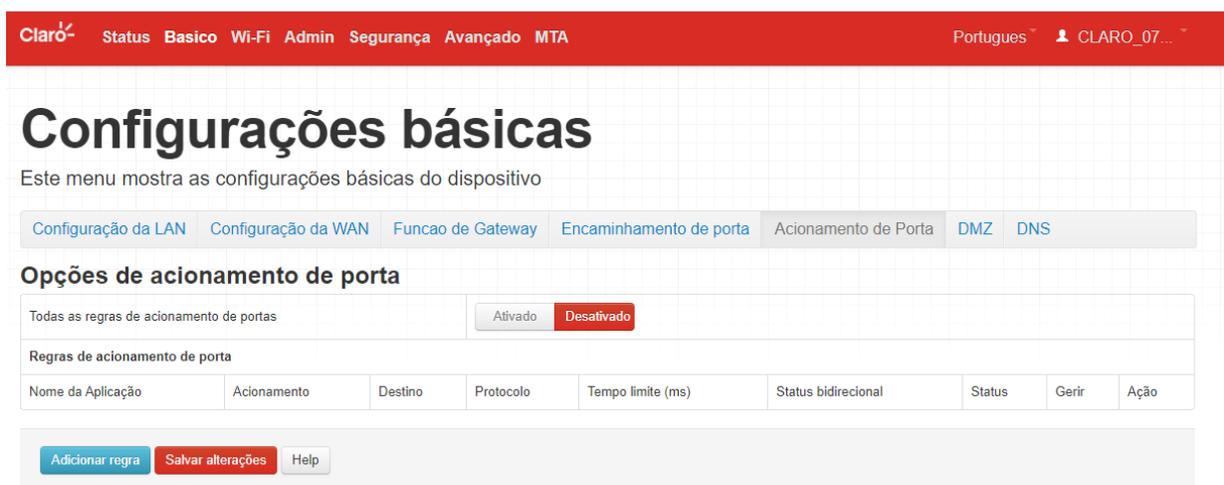
Aplicação Comum	Use este campo para selecionar o aplicativo para o qual deseja criar uma regra de encaminhamento de porta, se desejar.
Nome da aplicação	Digite um nome para o aplicativo para o qual deseja criar a regra.  NOTA: Este nome é arbitrário e não afeta a funcionalidade de forma alguma.
Protocolo	Use este campo para especificar se o HI3120 deve encaminhar o tráfego através de: <ul style="list-style-type: none"> <li>▶ Protocolo de Controle de Transmissão (<b>TCP</b>)</li> <li>▶ Protocolo de Datagrama do Usuário (<b>UDP</b>)</li> <li>▶ Protocolo de Controle de Transmissão e Protocolo de Datagrama do Usuário(<b>TCP/UDP</b>)</li> <li>▶ Encapsulamento de Roteamento Genérico (<b>GRE</b>)</li> <li>▶ Protocolo de Segurança Encapsulado (<b>ESP</b>)</li> </ul> NOTA: Em caso de dúvida, deixe este campo à sua disposição (TCP/UDP).
Faixa de Porto Público	Use esses campos para especificar o alcance da porta de entrada. Estes são os portos em que o HI3120 recebe tráfego do host originário na WAN.  Digite o número da porta inicial no primeiro campo e o número da porta final no segundo campo.  Para especificar apenas uma única porta, digite seu número em ambos os campos.
Faixa de Porta Privada	Use esses campos para especificar as portas para as quais o tráfego recebido deve ser encaminhado.  Digite o número da porta inicial no primeiro campo. O número de portas deve corresponder ao especificado na <b>Faixa de Porta Pública</b> , de modo que o HI3120 completa o segundo campo automaticamente.
Endereço IP local	Use este campo para inserir o endereço IP do computador na LAN para a qual deseja encaminhar o tráfego.
Aplicar	Clique nisso para salvar suas alterações nos campos nesta tela.
Perto	Clique nisso para retornar à tela <b>de encaminhamento de porta</b> sem salvar suas alterações na regra.

## 3.5 Acionamento da porta

Use esta tela para configurar o acionamento da porta. Você pode ativar ou desativar as portas e configurar regras de acionamento de portas novas e existentes.

Clique em **Básico > Acionamento de porta**.

Figura 17: Básico: Acionamento de portas



A tabela a seguir descreve os rótulos nesta tela.

Tabela 17: Básico: Acionamento de portas

Todas as regras de acionamento de portas	Use este campo para ligar ou desligar a porta. <ul style="list-style-type: none"> <li>▶ Selecione <b>Habilitado</b> para ativar o acionamento da porta.</li> <li>▶ Selecione <b>Desativado</b> para desativar a porta.</li> </ul>
Regras de acionamento de portas	
(Botão de rádio)	Selecione o botão de rádio de uma regra de encaminhamento da porta antes de clicar em <b>Editar</b> ou <b>Excluir</b> .
Não	Isso exibe o número de identificação arbitrária atribuído à regra de encaminhamento da porta.
Nome da aplicação	Isso exibe o nome atribuído à regra quando a criou.
Gatilho	Isso exibe a gama de portas de saída. Quando o HI3120 detecta atividade (tráfego de saída) nessas portas a partir de computadores na LAN, ele abre automaticamente as portas <b>Target</b> .

Tabela 17: **Básico: Acionamento da porta (continuação)**

Alvo	Isso exibe a gama de portas acionadas. Essas portas são abertas de forma automatizada quando o HI3120 detecta a atividade nas portas <b>Trigger</b> a partir de computadores na LAN.
Protocolo	Isso exibe o protocolo da regra de acionamento da porta( <b>TCP, UDP</b> ou <b>Both</b> ).
Tempo limite (ms)	Isso exibe o tempo (em milissegundos) após o HI3120 abrir as portas <b>Target</b> que deve fechá-las.
Status de Twoway	Normalmente, uma regra de acionamento de porta funciona para dois endereços IP; quando uma regra é ativada, outros IPs também poderão usar a regra como gatilho.
Status	Use este campo para ativar ou <b>desativar</b> regra .
Adicionar	Clique nisso para definir uma nova regra de acionamento da porta. O acionamento da porta deve ser primeiro definido <b>como Habilitado</b> . Consulte Adicionar ou Editar uma regra de acionamento de porta para obter informações na tela que exibe.
Editar	Selecione o botão de rádio da regra de acionamento da porta e clique nisso para fazer alterações na regra. O acionamento da porta deve ser primeiro definido como <b>Habilitado</b> . Consulte Adicionar ou Editar uma regra de acionamento de porta para obter informações na tela que exibe.
Excluir	Selecione o botão de rádio de uma regra de encaminhamento de porta e clique nisso para remover a regra. As informações da regra excluída não podem ser recuperadas.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

### 3.5.1 Adicionar ou editar uma regra de acionamento de portas

- ▶ Para adicionar uma nova regra de acionamento de porta, clique em **Adicionar** no **Básico > Acionamento de porta**.
- ▶ Para editar uma regra de acionamento de porta existente, selecione o botão de rádio da regra no **Básico > Tela de acionamento de** porta e clique no botão **Editar**.

NOTA: Certifique-se de que **habilitado** está selecionado na tela **Basico** > **Acionamento de portas**, a fim de adicionar ou editar regras de acionamento da porta.

A tela a seguir é exibida.

Figura 18: [Básico: Adicionar/editar acionamento de porta](#)



A tabela a seguir descreve os rótulos nesta tela.

Tabela 18: [Básico: Adicionar/editar acionamento de porta](#)

<p>Nome da aplicação</p>	<p>Digite um nome para o aplicativo para o qual deseja criar a regra.</p> <p>NOTA: Este nome é arbitrário e não afeta a funcionalidade de forma alguma.</p>
<p>Alcance da porta de gatilho</p>	<p>Use esses campos para especificar as portas de gatilho. Quando o HI3120 detecta a atividade em qualquer uma dessas portas originárias de um computador na LAN, ela abre automaticamente as portas alvo na expectativa de tráfego de entrada.</p> <p>Digite o número da porta inicial no campo first e o número da porta final no segundo campo.</p> <p>Para especificar apenas uma única porta, digite seu número em ambos os campos.</p>

Tabela 18: **Básico: Adicionar/editar acionamento de porta (continuação)**

Alcance de porta alvo	<p>Use esses campos para especificar as portas-alvo. O HI3120 abre essas portas na expectativa de entrada de tráfego sempre que detecta atividade em qualquer uma das portas <b>trigger</b>. O tráfego de entrada é encaminhado para essas portas no computador conectado à LAN.</p> <p>Entre com o número da porta inicial no primeiro campo, e o número da porta final no segundo campo.</p> <p>Para especificar apenas uma única porta, digite seu número em ambos os campos.</p>
Protocolo	<p>Use este campo para especificar se o HI3120 deve ativar este gatilho quando detectar atividade através de:</p> <ul style="list-style-type: none"> <li>▶ Protocolo de Controle de Transmissão (<b>TCP</b>)</li> <li>▶ Protocolo de Datagrama do Usuário (<b>UDP</b>)</li> <li>▶ Protocolo de Controle de Transmissão e Protocolo de Datagrama do Usuário (<b>Ambos</b>)</li> </ul> <p>NOTA: Em caso de dúvida, deixe este campo à sua revelia (<b>Ambos</b>).</p>
Tempo limite(ms)	<p>Digite o tempo (em milissegundos) após o HI3120 abrir as portas <b>Alvo</b> que deve fechá-las.</p>
Aplicar	<p>Clique nisso para salvar suas alterações nos campos nesta tela.</p>
Perto	<p>Clique nisso para retornar à tela <b>Direcionamento de porta</b> sem salvar suas alterações na regra.</p>

## 3.6 DMZ

Use esta tela para configurar a Zona Desmilitarizada (DMZ) da sua rede.

NOTA: Apenas um dispositivo pode estar no DMZ de cada vez.

Clique em **Básico>DMZ**. A tela a seguir é exibida.

Figura 19: Básico: DMZ



A tabela a seguir descreve os rótulos nesta tela.

Tabela 19: Básico: DMZ

Habilitar o DMZ	Use este campo para ligar ou desligar o DMZ. <ul style="list-style-type: none"> <li>▶ Selecione <b>Habilitado</b> para ativar o DMZ.</li> <li>▶ Selecione <b>Desativado</b> para desativar o DMZ. Computadores que estavam anteriormente no DMZ estão agora na LAN.</li> </ul>
Anfitrião DMZ	Digite o endereço IP do computador que deseja adicionar ao DMZ.
Dispositivos conectados	Clique nisso para ver uma lista dos computadores atualmente conectados ao HI3120 na LAN.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

## 3.7 DNS

Use esta tela para configurar as configurações LAN DNS da HI3120, incluindo sua máscara de sub-rede, sufixo de domínio e nome de host proxy.

Clique em **Básico**>**DNS**. O visor de tela a seguir

Figura 20: Básico: DNS

Claro Status Básico Wi-Fi Admin Segurança Avançado MTA Portuguese CLARO\_07...

# Configurações básicas

Este menu mostra as configurações básicas do dispositivo

Configuração da LAN Configuração da WAN Função de Gateway Encaminhamento de porta Acionamento de Porta DMZ DNS

## Configurações de DNS

Defina suas configurações de DNS

DNS Obtém	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
DNS1	<input type="text" value="Endereço IP do DNS"/>
DNS2	<input type="text" value="Endereço IP do DNS"/>
Obter DNS IPv6	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

A tabela a seguir descreve os rótulos neste Tela.

Tabela 20: Básico: DNS

Obtenção de DNS LAN	<p>Use-a para selecionar se deve obter informações de DNS automaticamente Não, não, não rede Sim Para definir-para Manualmente.</p> <ul style="list-style-type: none"><li>▶ <b>Selecione Auto</b> Para obter informações de DNS Automaticamente.</li><li>▶ <b>Selecionar Manual</b> para obter informações de DNS manualmente.</li></ul>
LAN DNS Proxy Status	<p>Use isso para ativar ou desativar o proxy DNS na LAN. Quando o proxy DNS é ligado (padrão) o servidor DHCP fornece o endereço IP LAN da HI3120 como o servidor DNS para resolução de nome.</p> <ul style="list-style-type: none"><li>▶ Selecionados <b>Habilitado</b> para ativar o proxy DNS.</li><li>▶ desativado selecionado para desativar o proxy DNS.</li></ul>
Sufixo de domínio	<p>Use este campo para definir o domínio que você pode inserir em um navegador da Web (em vez de um endereço IP) para alcançar o HI3120 na LAN.</p> <p>NOTA: É sugerido que você anote o sufixo de domínio do seu dispositivo caso precise acessar a GUI do HI3120 sem saber seu endereço IP.</p>
Nome do host proxy 1	<p>Quando o <b>DNS Obter LAN</b> for definido como <b>Manual</b>, digite os endereços IP de até dois computadores para os quais você deseja adicionar manualmente ao DNS.</p>
Nome do host proxy 2	
Salvar alterações	<p>Clique nisso para salvar suas alterações nos campos nesta tela.</p>
Cancelar	<p>Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.</p>
Ajuda	<p>Clique nisso para ver informações sobre os campos nesta tela.</p>

# 4

## Wi-Fi

Este capítulo descreve as telas que exibem quando você clica em **Wi-Fi** na barra de ferramentas. Ele contém as seguintes seções:

- ▶ Visão geral sem fio
- ▶ Configurações básicas sem fio
- ▶ WPS
- ▶ Controle de acesso

### 4.1 Visão geral sem fio

Esta seção descreve alguns dos conceitos relacionados às telas **Wi-Fi**.

#### 4.1.1 Noções básicas de rede sem fio

A rede sem fio do seu HI3120 faz parte da Rede local de área (LAN), conhecida como LAN Sem Fio (WLAN). O WLAN é uma rede de links de rádio entre o HI3120 e os outros computadores e dispositivos que se conectam a ele.

#### 4.1.2 Arquitetura

A rede sem fio consiste em dois tipos de dispositivo: pontos de acesso (APs) e clientes.

- ▶ O ponto de acesso controla a rede, fornecendo uma conexão sem fio a cada cliente.

- ▶ Os clientes sem fio se conectam ao ponto de acesso para receber uma conexão sem fio à WAN e à LAN com fio.

O HI3120 é o ponto de acesso, e os computadores que você conecta ao HI3120 são os clientes sem fio.

### 4.1.3 Padrões sem fio

A forma como os dispositivos sem fio se comunicam entre si é padronizada pelo Instituto de Engenheiros Elétricos e Eletrônicos (IEEE). Os padrões IEEE relativos a LANs sem fio são identificados por sua designação 802.11. Existem uma variedade de padrões WLAN, mas o HI3120 suporta o seguinte (por ordem de adoção - de antiga para nova - e velocidades de transferência de dados - de baixa a alta):

- ▶ IEEE 802.11b
- ▶ IEEE 802.11g
- ▶ IEEE 802.11n
- ▶ IEEE 802.11ac

### 4.1.4 Conjuntos de serviços e SSIDs

Cada rede sem fio, incluindo todos os dispositivos que a compõem, é conhecida como service set.

NOTA: Dependendo de seus recursos e configuração, um único ponto de acesso sem fio pode controlar vários conjuntos de serviços; isso é frequentemente feito para fornecer diferentes níveis de serviço ou segurança para diferentes clientes.

Cada conjunto de serviços é identificado por um service Set Identifier (SSID). Este é o nome da rede. Os clientes sem fio devem conhecer o SSID para poder se conectar ao AP. Você pode configurar o HI3120 para transmitir o SSID (nesse caso, qualquer cliente que escaneia as ondas de rádio pode descobrir o SSID), ou para "ocultar" o SSID (nesse caso não é transmitido, e apenas usuários que já conhecem o SSID podem se conectar).

### 4.1.5 Segurança sem fio

O rádio é inerentemente um meio inseguro, uma vez que pode ser interceptado por qualquer pessoa na área de cobertura com um receptor de rádio. Portanto, existem uma variedade de técnicas para controlar a autenticação (identificando quem deve ser autorizado a entrar na rede) e criptografia (embaralhamento de sinal para que apenas usuários autenticados possam decodificar os dados transmitidos). A sofisticação de cada método de segurança varia, assim como sua eficácia. O HI3120 suporta os seguintes protocolos de segurança sem fio (por ordem de eficácia):

- ▶ **WEP** (Protocolo de Equivalência Wired): este protocolo usa uma série de "chaves" ou strings (letras) de dados para autenticar o cliente sem fio com o AP e criptografar dados enviados pelo link sem fio. O WEP é um protocolo preterido, e só deve ser usado quando for o padrão de segurança suportado pelos clientes sem fio.  
O WEP fornece apenas um nível nominal de segurança, uma vez que existe um software amplamente disponível que pode quebrá-lo em questão de minutos. Além disso, o uso do WEP limita a velocidade da rede sem fio a uma velocidade de 54Mbps (velocidade de 802,11g).
- ▶ **WPA-PSK** (WiFi Protected Access - Pré-Shared Key): O WPA foi criado para resolver as inadequações do WEP. Existem dois tipos de WPA: a versão "enterprise" (conhecida simplesmente como WPA) requer o uso de um banco de dados de autenticação central, enquanto a versão "pessoal" (suportada pela HI3120) permite que os usuários autenticuem usando uma "chave pré-compartilhada" ou senha.  
Embora o WPA forneça uma boa segurança, ele ainda é vulnerável a tentativas de adivinhação de senhas de "força bruta" (em que um invasor simplesmente ataca o AP com solicitações de junção usando diferentes senhas), então para uma segurança ideal é aconselhável que você use uma senha aleatória de treze caracteres ou mais, contendo nenhuma palavra "dicionário".
- ▶ **WPA2-PSK**: WPA2 é uma melhoria no WPA. A diferença de primária é que o WPA usa o padrão de criptografia Do Protocolo de Integridade da Chave Temporal (TKIP) (que tem sido mostrado ter certas possíveis fraquezas), enquanto o WPA2 usa o Padrão Avançado de Criptografia (AES) mais forte no modo Contador com o Protocolo de Código de Autenticação de Mensagem de Codificação de Blocos cifrados (CCMP), que recebeu o selo de aprovação do governo dos EUA para comunicações até o nível de segurança do serviço secreto. Uma vez que o WPA2-PSK usa o mesmo mecanismo de chave pré-compartilhado que o WPA-PSK, aplica-se a mesma ressalva contra o uso de senhas inseguras ou simples.

NOTA: O HI3120 pode ser configurado para usar o padrão de criptografia TKIP; no entanto, isso limita a velocidade da rede sem fio a 54Mbps (velocidade de 802,11g).

#### 4.1.5.1 WPS

WiFi-Protected Setup (WPS) é um método padronizado de permitir que dispositivos sem fio se juntem rapidamente e facilmente às redes sem fio, mantendo um bom nível de segurança. O HI3120 fornece dois métodos de autenticação WPS:

- ▶ **Configuração de botão de botão (PBC):** quando o usuário pressiona o botão **PBC** no AP (um botão físico ou um botão virtual na GUI), qualquer usuário de um cliente sem fio que suporta WPS pode pressionar o botão **PBC** correspondente no cliente dentro de dois minutos para se juntar à rede.
- ▶ **Configuração do número de identificação pessoal (PIN):** todos os dispositivos compatíveis com WPS possuem um PIN (geralmente para ser encontrado impresso em um adesivo na carcaça do dispositivo). Quando você configura outro dispositivo para usar o mesmo PIN, os dois dispositivos autenticam um com o outro.

Uma vez autenticados, os dispositivos que se juntaram a uma rede via WPS usam o padrão de segurança WPA2.

#### 4.1.6 WMM

WiFi MultiMedia (WMM) é um aprimoramento de Qualidade de Serviço (QoS) que permite a priorização de certos tipos de dados sobre a rede wireless. O WMM fornece quatro classificações de tipo de dados (em ordem prioritária; mais alta para a menor):

- ▶ Voz
- ▶ Vídeo
- ▶ Melhor esforço
- ▶ Fundo

Se você deseja melhorar o desempenho de voz e vídeo (em detrimento de outros aplicativos menos sensíveis ao tempo, como navegação na Internet e transferências ftp), você pode habilitar wmm. Você também pode editar os parâmetros WMM QoS, mas são desaconselhados a fazê-lo a menos que você tem uma razão extremamente boa para fazer as alterações.

## 4.2 Configurações básicas Wi-Fi

Use esta tela para configurar as configurações básicas de 2.4GHz e 5GHz do seu HI3120. Você pode ligar ou desativar os módulos sem fio, selecionar o modo sem fio e canal para configurar as configurações SSID das redes sem fio.

O HI3120 tem redes sem fio separadas de 2,4 GHz e 5GHz:

- ▶ Para configurar a rede sem fio de 2.4GHz da HI3120, clique **em Wi-Fi > Configurações básicas**, e clique na guia **2.4G**. Consulte configurações 2.4G para obter informações na tela que exibe.
- ▶ Para configurar a rede sem fio de 5GHz da HI3120, clique **em Wi-Fi > Configurações básicas**, e clique na guia **5G**. Consulte configurações 5G para obter informações na tela que exibe.

### 4.2.1 Configurações 2.4G

Use esta tela para configurar a rede sem fio de 2.4GHz da HI3120.

Clique em **Wi-Fi > Configurações básicas**, e clique na guia **2.4G**. A tela a seguir é exibida.

Figura 21: Wi-Fi: Configurações básicas de 2.4GHz



Claro Status Básico **Wi-Fi** Admin Segurança Avançado MTA Portuguese CLARO\_07...

# WI-FI

Este menu mostra as configurações Wi-Fi

Configuracoes basicas Controle de acesso ATF

2.4G 5G WPS

## Configuracoes basicas

Wi-Fi ativado	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
modo Wi-fi	802.11 g/n misto
Largura de banda do canal	20 MHz <input checked="" type="checkbox"/> 20/40 MHz <input type="checkbox"/> 40 MHz
Canal Wi-Fi	Auto (11)
WPS ativado	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF

## Várias configurações de SSID

2.4G SSID primário

Nome da rede (SSID)	HITRON2GHZ
Habilitar	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
SSID de transmissão	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
WMM(QOS)	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
modo de Segurança	WPA-Personal
Modo de autenticação	Auto (WPA-PSK or WPA2-PSK)
Senha	nagae@321

Salvar alterações Cancelar Help

A tabela a seguir descreve os rótulos nesta tela. Tabela

### 21: Wi-Fi: Configurações básicas de 2.4GHz

Configurações básicas	
Modo sem fio	<p>Selecione o tipo de rede sem fio de 2.4GHz que deseja usar:</p> <ul style="list-style-type: none"><li>▶ <b>802.11 11b Somente:</b> usar o IEEE 802.11b</li><li>▶ <b>802.11 11g Somente:</b> usar o IEEE 802.11g</li><li>▶ <b>802.11 11n Somente:</b> usar o IEEE 802.11n</li><li>▶ <b>802.11 B/G/N Misto:</b> usar IEEE 802.11b, 802.11g e 802.11n</li><li>▶ <b>802.11 G/N Misto:</b> usar IEEE 802.11g e 802.11n</li></ul> <p>Nota: Apenas clientes sem fio que suportam o protocolo de rede selecionado podem se conectar à rede sem fio. Em caso de dúvida, use <b>11B/G/N Misto</b> (padrão).</p>
Largura de banda do canal	<p>Este campo permite configurar a largura do canal de rádio que o HI3120 usa para comunicar com seus clientes sem fio (somente IEEE 802.11n). O uso da largura de banda completa de 40MHz pode dobrar a velocidade de dados.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>20 MHz</b> para usar apenas uma banda de 20 mega-hertz.</li><li>▶ Selecione <b>20/40 MHz</b> para usar uma banda de 40 mega-hertz quando possível, e uma banda de 20 mega-hertz quando uma banda de 40Mhz não estiver disponível.</li><li>▶ Selecione <b>40 MHz</b> para usar apenas uma banda de 40 mega-hertz.</li></ul>
Canal Sem Fio	<p>Selecione o canal sem fio de 2.4GHz que deseja usar ou selecione <b>Auto</b> Para que o HI3120 eleja o canal ideal para usar.</p> <p>NOTA: Use a configuração Auto, a menos que você tenha uma razão específica para fazer o contrário.</p>
Configurações SSID	

Tabela 21: Wi-Fi: Configurações básicas de 2.4GHz (continuação)

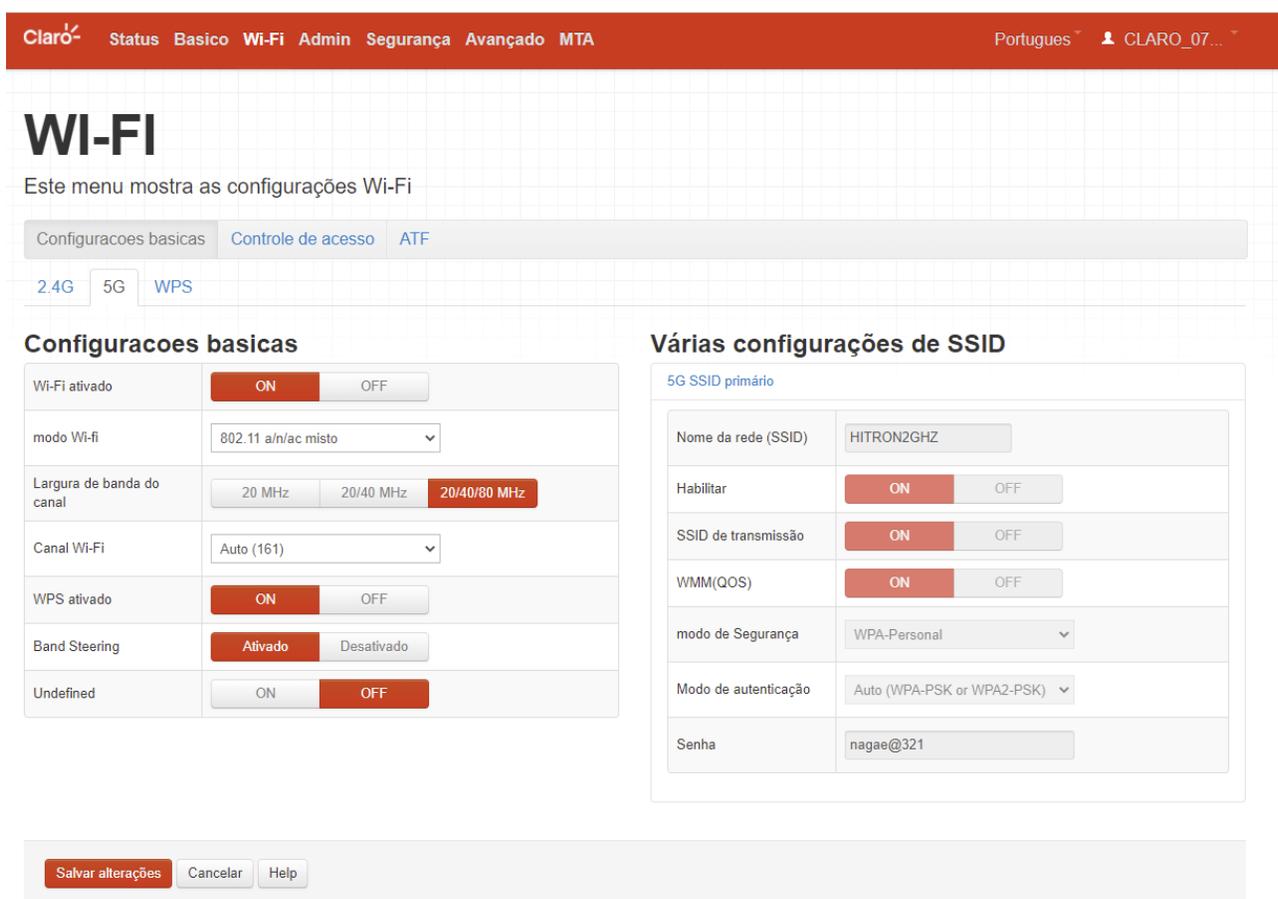
Nome da rede (SSID)	<p>Digite o nome que deseja usar para este SSID. Este é o nome que identifica sua rede e ao qual os clientes sem fio se conectam.</p> <p>NOTA: Sugere-se que você altere o SSID de seu padrão, por razões de segurança.</p>
Permitir	<p>Use este campo para ativar ou desativar o SSID.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>ON</b> para ativar o SSID.</li><li>▶ Selecione <b>OFF</b> para desativar o SSID.</li></ul>
SSID de transmissão	<p>Use este campo para tornar este SSID visível ou invisível para outros dispositivos sem fio.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>ON</b> se quiser que seu nome de rede (SSID) seja público. Qualquer pessoa com um dispositivo sem fio na área de cobertura pode descobrir o SSID e tentar se conectar à rede.</li><li>▶ Selecione <b>OFF</b> se você não quiser que o HI3120 transmita o nome da rede (SSID) para todos os dispositivos sem fio na área de cobertura. Quem quiser se conectar à rede deve conhecer o SSID.</li></ul>
WMM(QoS)	<p>Este campo exibe se as configurações de Qualidade de Serviço (QoS) do Wifi MultiMedia (WMM) estão ativadas ou <b>desativadas</b> neste SSID.</p>
Salvar alterações	<p>Clique nisso para salvar suas alterações nos campos nesta tela.</p>
Cancelar	<p>Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.</p>
Ajuda	<p>Clique nisso para ver informações sobre os campos nesta tela.</p>

## 4.2.2 Configurações 5G

Use esta tela para configurar a rede sem fio de 5GHz da HI3120.

Clique em **Wi-Fi** > **Configurações básicas**, em seguida, clique na guia **5G**. A tela a seguir é exibida.

Figura 22: Wi-Fi: Configurações básicas de 5GHz



The screenshot displays the 'WI-FI' configuration page for a Hitron device. The top navigation bar includes 'Claro', 'Status', 'Basico', 'WI-FI', 'Admin', 'Segurança', 'Avançado', and 'MTA'. The user is logged in as 'CLARO\_07...'. The main heading is 'WI-FI', with a sub-heading 'Este menu mostra as configurações Wi-Fi'. Below this, there are tabs for 'Configuracoes basicas', 'Controle de acesso', and 'ATF'. The '5G' tab is selected. The page is divided into two main sections: 'Configuracoes basicas' and 'Várias configurações de SSID'.

**Configuracoes basicas**

Wi-Fi ativado	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
modo Wi-fi	802.11 a/n/ac misto
Largura de banda do canal	<input type="checkbox"/> 20 MHz <input type="checkbox"/> 20/40 MHz <input checked="" type="checkbox"/> 20/40/80 MHz
Canal Wi-Fi	Auto (161)
WPS ativado	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Band Steering	<input checked="" type="checkbox"/> Ativado <input type="checkbox"/> Desativado
Undefined	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

**Várias configurações de SSID**

5G SSID primário

Nome da rede (SSID)	HITRON2GHZ
Habilitar	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
SSID de transmissão	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
WMM(QOS)	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
modo de Segurança	WPA-Personal
Modo de autenticação	Auto (WPA-PSK or WPA2-PSK)
Senha	nagae@321

At the bottom, there are buttons for 'Salvar alterações', 'Cancelar', and 'Help'.

A tabela a seguir descreve os rótulos nesta tela.

Tabela 22: Wi-Fi: Configurações básicas de 5GHz

Configurações básicas	
Modo sem fio	<p>Selecione o tipo de rede sem fio de 5GHz que deseja usar:</p> <ul style="list-style-type: none"> <li>▶ <b>802.11 11n 5G</b>: usar IEEE 802.11n (5GHz)</li> <li>▶ <b>802.11 11a</b>: use IEEE 802.11a</li> <li>▶ <b>802.11 a/n Misto</b>: usar IEEE 802.11a e 802.11n</li> <li>▶ <b>802.11 11am</b>: utilizar o IEEE 802.11ac (somente 5GHz)</li> <li>▶ <b>802.11 n/E Misto</b>: usar IEEE 802.11n e 802.11ac.</li> </ul> <p>Nota: <a href="#">Apenas clientes sem fio que suportam o protocolo de rede selecionado podem se conectar à rede sem fio.</a></p>
Largura de banda do canal	<p>Este campo permite configurar a largura do canal de rádio que a HI3120 usa para se comunicar com seus clientes sem fio. O uso da largura de banda completa de 40MHz pode dobrar a velocidade de dados.</p> <ul style="list-style-type: none"> <li>▶ Selecione <b>20 MHz</b> para usar apenas uma banda de 20 mega-hertz.</li> <li>▶ Selecione <b>40 MHz</b> para usar apenas uma banda de 40 mega-hertz.</li> <li>▶ Selecione <b>80 MHz</b> para usar apenas uma Banda de 80 mega-hertz.</li> </ul>
Dfs	<p>Use este campo para ativar ou desativar a Seleção dinâmica de frequência (DFS) na rede de 5GHz. O DFS permite que a interferência entre dispositivos sem fio seja minimizada selecionando largura de banda não usada.</p> <ul style="list-style-type: none"> <li>▶ Selecione <b>ON</b> para ativar o DFS.</li> <li>▶ Selecione <b>OFF</b> para desativar o Dfs.</li> </ul>
Canal Sem Fio	<p>Selecione o canal sem fio de 5GHz que deseja usar ou selecione <b>Auto</b> Para que o HI3120 selecione o canal ideal para usar.</p> <p>NOTA: <a href="#">Use a configuração Auto, a menos que você tenha uma razão específica para fazer o contrário.</a></p>

Tabela 22: Wi-Fi: Configurações básicas de 5GHz (continuação)

WPS Enabled	<p>Use este campo para ativar ou desativar a Configuração Protegida do Wifi (WPS) na rede de 5GHz.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>ON</b> para ativar WPS.</li><li>▶ Selecione <b>OFF</b> para desativar wps.</li></ul> <p>Consulte a tela WPS para obter mais informações sobre o uso do WPS.</p>
Configurações SSID	
Nome da rede (SSID)	<p>Digite o nome que deseja usar para este SSID. Este é o nome que identifica sua rede e ao qual os clientes sem fio se conectam.</p> <p>NOTA: Sugere-se que você altere o SSID de seu padrão, por razões de segurança.</p>
Permitir	<p>Use este campo para ativar ou desativar o SSID.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>ON</b> para ativar o SSID.</li><li>▶ Selecione <b>OFF</b> para desativar o SSID.</li></ul>
SSID de transmissão	<p>Use este campo para tornar este SSID visível ou invisível para outros dispositivos sem fio.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>ON</b> se quiser que seu nome de rede (SSID) seja público. Qualquer pessoa com um dispositivo sem fio na área de cobertura pode descobrir o SSID e tentar se conectar à rede.</li><li>▶ Selecione <b>OFF</b> se você não quiser que o HI3120 transmita o nome da rede (SSID) para todos os dispositivos sem fio na área de cobertura. Quem quiser se conectar à rede deve conhecer o SSID.</li></ul>
WMM(QoS)	<p>Este campo exibe se as configurações de Qualidade de Serviço (QoS) do Wifi MultiMedia (WMM) estão ativadas ou <b>desativadas</b> neste SSID.</p>
Salvar alterações	<p>Clique nisso para salvar suas alterações nos campos nesta tela.</p>
Cancelar	<p>Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.</p>
Ajuda	<p>Clique nisso para ver informações sobre os campos nesta tela.</p>

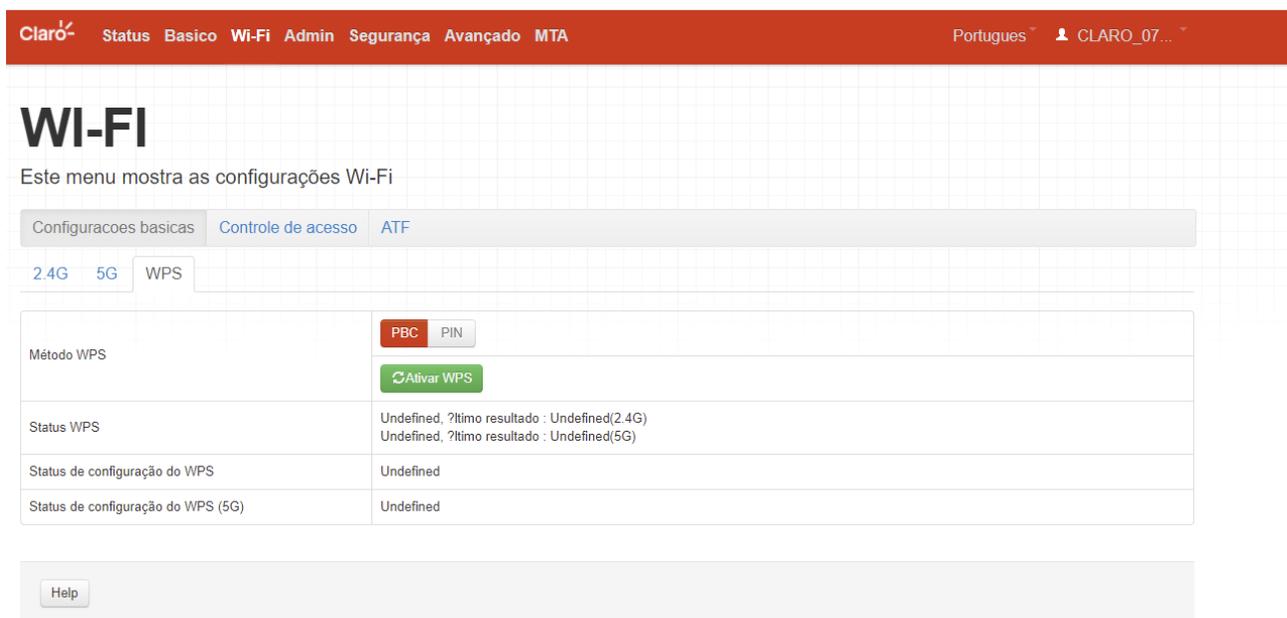
## 4.3 WPS

Use esta tela para configurar a autenticação e criptografia das redes sem fio de 2,4 GHz e 5GHz da sua HI3120 e gerenciar a configuração protegida por Wifi (WPS).

NOTE: É fortemente recomendável que você configure segurança em sua rede; caso contrário, qualquer pessoa na área de cobertura de rádio pode acessar sua rede.

Clique em **Wi-Fi** > **WPS**. O visor de tela a seguir.

Figura 23: Wi-Fi: WPS



The screenshot shows the WPS configuration page in the Hitron web interface. The page has a red header with the 'Claro' logo and navigation tabs: Status, Básico, Wi-Fi, Admin, Segurança, Avançado, MTA. The user is logged in as 'CLARO\_07...'. The main content area is titled 'WI-FI' and contains the following elements:

- Sub-menu: Configurações básicas, Controle de acesso, ATF
- Frequency tabs: 2.4G, 5G, WPS
- WPS Method section: Radio buttons for 'PBC' (selected) and 'PIN', and a green 'Ativar WPS' button.
- Status WPS: Undefined, 7ltimo resultado : Undefined(2.4G), Undefined, 7ltimo resultado : Undefined(5G)
- Status de configuração do WPS: Undefined
- Status de configuração do WPS (5G): Undefined
- Help button at the bottom.

A tabela a seguir descreve as etiquetas nesta tela.

Tabela 23: Wi-Fi: WPS

2.4G	<p>O HI3120 opera dentro das bandas de rede 2.4Ghz e 5GHz. Use essas guias para visualizar informações sobre a rede relevante.</p> <ul style="list-style-type: none"> <li>▶ Clique <b>2.4G</b> para ver informações sobre a rede de 2.4GHz da HI3120.</li> <li>▶ Clique em <b>5G</b> para ver informações sobre a rede de 5GHz da HI3120.</li> </ul> <p>Os campos que exibem são idênticos para ambas as redes.</p>
5G	
Configurações WPS	
WPS	<p>Use esses botões para ativar ou desativar a Configuração Protegida do Wifi (WPS).</p> <ul style="list-style-type: none"> <li>▶ Selecione <b>ON</b> para ativar WPS.</li> <li>▶ Selecione <b>OFF</b> para desativar wps.</li> </ul>
Método WPS	<p>Use estes botões para executar a configuração protegida por Wifi (WPS):</p> <ul style="list-style-type: none"> <li>▶ Clique no botão <b>PBC</b> e, em seguida, <b>pressione o botão</b> para iniciar o processo de configuração do botão de pressão. Em seguida, pressione o botão PBC em dispositivos sem fio do cliente dentro de dois minutos, a fim de registrá-los em sua rede sem fio.</li> <li>▶ Clique no botão <b>PIN</b> para iniciar o processo de configuração PIN. Na tela que exibe, digite o PIN WPS que deseja usar para o HI3120 ou o PIN WPS do dispositivo cliente que deseja adicionar à rede.</li> </ul>
WPS Status	Isso mostra se o HI3120 está usando ou não a configuração protegida por Wifi.
WPS Configurar status	Isso exibe a configuração de configuração protegida por Wifi.
Configurações de segurança	
(SSID)	Sua HI3120 tem vários SSIDs. Clique no SSID que deseja configurar para ver seus campos de segurança.

Tabela 23: Wi-Fi: WPS (continuação)

Modo de segurança sem fio	<p>Selecione o tipo de segurança que deseja usar.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>Nenhum</b> para não usar segurança. Qualquer pessoa na área de cobertura pode entrar na sua rede.</li><li>▶ Selecione <b>WEP</b> para usar o protocolo de segurança de privacidade equivalente com fio.</li><li>▶ Selecione <b>WPA-Personal</b> para usar o protocolo de segurança WiFi Protected Access (Personal).</li></ul> <p>NOTA: Devido a vulnerabilidades de segurança inerentes, é sugerido que você use <b>WEP</b> apenas se for o único suporte de segurança que seus clientes sem fio suportam. Em quase todas as circunstâncias, você deve usar a opção <b>WPA</b>. Além disso, o uso do <b>WEP</b> limita a velocidade da rede sem fio a 54Mbps (velocidade de 802,11g).</p>
Autenticação	<p>Selecione o tipo de autenticação que deseja usar.</p> <ul style="list-style-type: none"><li>▶ Selecione <b>WPA-PSK</b> para usar o protocolo de segurança WiFi Protected Access (Personal).</li><li>▶ Selecione <b>WPA2-PSK</b> para usar o protocolo de segurança WiFi Protected Access 2 (Personal).</li><li>▶ Selecione <b>Auto (WPA-PSK ou WPA2-PSK)</b> para usar os protocolos de segurança WPA e WPA2; clientes que suportam WPA2 se conectam usando este protocolo, enquanto aqueles que suportam apenas WPA se conectam usando este protocolo.</li></ul>

Tabela 23: Wi-Fi: WPS (continuação)

Modo de criptografar	<p>Selecione o tipo de criptografia que deseja usar. As opções que exibem dependem das opções selecionadas nos outros campos desta tela.</p> <p><b>WEP:</b></p> <ul style="list-style-type: none"><li>▶ Selecione <b>WEP64</b> para usar uma chave de segurança de dez dígitos.</li><li>▶ Selecione <b>WEP128</b> para usar uma chave de segurança de 26 dígitos.</li></ul> <p><b>WPA-PSK, WPA2-PSK e Auto:</b></p> <ul style="list-style-type: none"><li>▶ Selecione <b>TKIP</b> para usar o Protocolo de Integridade da Chave Temporal.</li><li>▶ Selecione <b>AES</b> para usar o Padrão avançado de criptografia.</li><li>▶ Selecione <b>TKIP/AES</b> para permitir que os clientes que usam qualquer tipo de criptografia se conectem ao HI3120.</li></ul> <p>NOTA: O uso do padrão de criptografia TKIP limita a velocidade da rede sem fio a 54Mbps (velocidade de 802,11g).</p>
Frase de senha	<p>Digite a chave de segurança ou senha que deseja usar para sua rede sem fio. Você precisará inserir essa chave em seus clientes sem fio, a fim de permitir que eles se conectem à rede.</p>
Salvar alterações	<p>Clique nisso para salvar suas alterações nos campos nesta tela.</p>
Cancelar	<p>Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.</p>
Ajuda	<p>Clique nisso para ver informações sobre os campos nesta tela.</p>

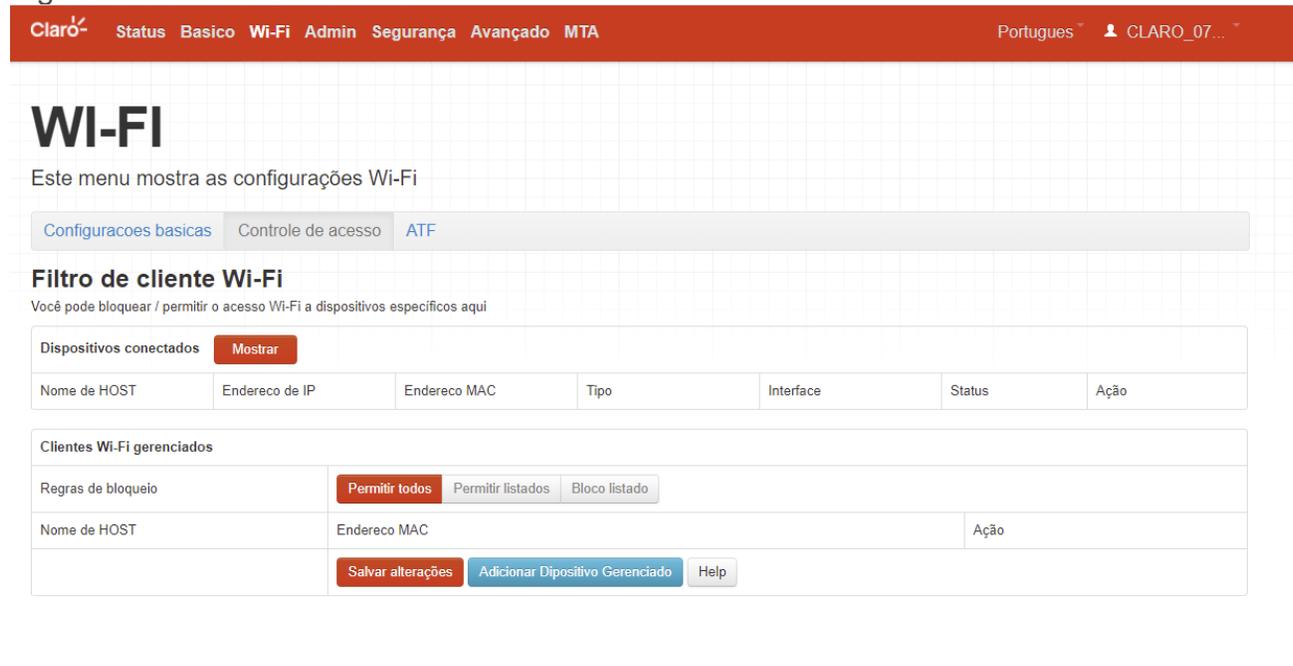
## 4.4 Controle de acesso

Use esta tela para modificar os Identificadores de Conjunto de Serviços (SSIDs) das redes sem fio da HI3120 e gerenciar os dispositivos que se conectam à rede sem fio.

NOTA: Esta tela é exibida somente quando a configuração protegida por Wifi (WPS) é desligada.

Clique em **Wi-Fi > Controle de Acesso**. A tela a seguir é exibida. Clique na guia **2.4G** para ver informações sobre a rede sem fio de 2.4GHz ou clique na guia **5G** para ver informações sobre a rede sem fio de 5GHz.

Figura 24: **Wi-Fi: Controle de acesso**



A tabela a seguir descreve as etiquetas nesta tela.

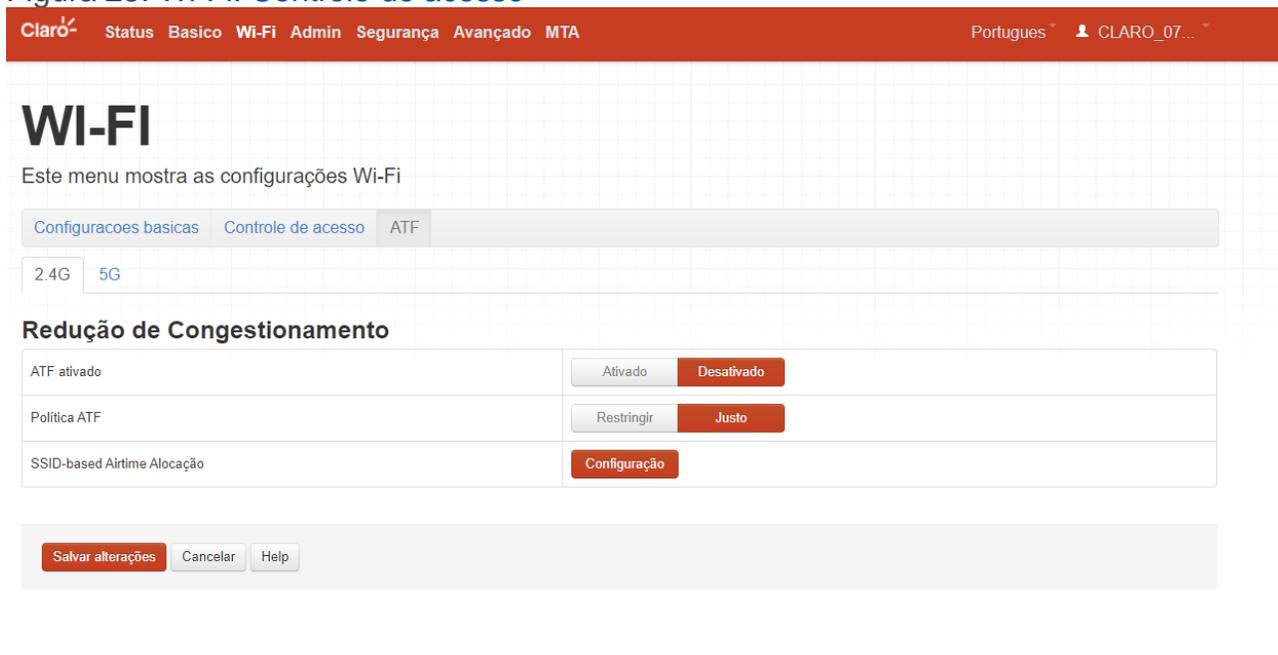
Tabela 24: **Wi-Fi: Controle de acesso**

Dispositivos conectados	
Nome do anfitrião	Isso exibe o nome de cada dispositivo de rede conectado na rede sem fio.
Endereço IP	Isso exibe o endereço IP de cada dispositivo de rede conectado na rede sem fio.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada dispositivo de rede conectado na rede sem fio.
Tipo	Isso mostra se o endereço IP do dispositivo foi atribuído pelo DHCP( <b>DHCP-IP</b> ) ou <b>auto-atribuído</b> .
Interface	Isso exibe o nome da interface na qual o dispositivo relevante está conectado.

Tabela 24: Wi-Fi: Controle de acesso (continuação)

Status	Isso mostra se o dispositivo conectado está ou não ativo.
Ação	Clique <b>em Gerenciar</b> para fazer alterações no status de filtragem do dispositivo; consulte Adicionar ou Editar um dispositivo gerenciado para informações sobre a tela que exibe.
Dispositivos Gerenciados	
Regras do bloco	Use estes botões para controlar a ação a ser tomada para os dispositivos listados: <ul style="list-style-type: none"><li>▶ Selecionar <b>permitir que todos</b> ignorem os dispositivos <b>gerenciados</b> listar e deixar todos os dispositivos conectados ao HI3120.</li><li>▶ Selecione <b>Permitir que listados permitam</b> apenas dispositivos adicionados à lista de dispositivos <b>gerenciados</b> para acessar o HI3120 e a rede. Todos os outros dispositivos têm acesso negado.</li><li>▶ Selecione <b>Negar</b> para permitir todos os dispositivos, exceto aqueles que você adicionou à lista de dispositivos <b>gerenciados</b> para acessar o HI3120 e a rede. Os dispositivos especificados são negados acesso.</li></ul>
Nome do anfitrião	Isso exibe o nome de cada dispositivo de rede na lista.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada dispositivo de rede da lista.
Ação	Clique <b>em Gerenciar</b> para fazer alterações em uma regra de dispositivo gerenciado (consulte Adicionar ou Editar um dispositivo gerenciado ).
Adicionar dispositivo gerenciado	Clique nisso para adicionar uma nova regra de dispositivo gerenciado (consulte Adicionar ou Editar um dispositivo gerenciado ).
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

Figura 25: Wi-Fi: Controle de acesso



A tabela a seguir descreve as etiquetas nesta tela.

Tabela 25: Wi-Fi: Avançado

Recursos avançados sem fio	
Pesquisa do site wifi	Isso escaneia o ambiente para todas as SSID próximas.
Clientes sem fio	Ele exibe uma lista de clientes conectados à rede sem fio.

# 5

## Admin

Este capítulo descreve as telas que exibem quando você clica em **Admin** na barra de ferramentas. Ele contém as seguintes seções:

- ▶ Visão geral do administrador
- ▶ Traceroute: esta ferramenta permite que você veja a rota tomada por pacotes de dados do HI3120 até o destino especificado. Você pode usar esta ferramenta para resolver problemas de roteamento ou identificar firewalls que podem estar bloqueando seu acesso a um computador ou serviço.
- ▶ Diagnóstico
- ▶ Backup
- ▶ Reinicialização do dispositivo
- ▶ DDNS
- ▶ IP Passthrough

### 5.1 Visão geral do administrador

Esta seção descreve alguns dos conceitos relacionados com as telas **do Admin**.

#### 5.1.1 Depuração (Ping e Traceroute)

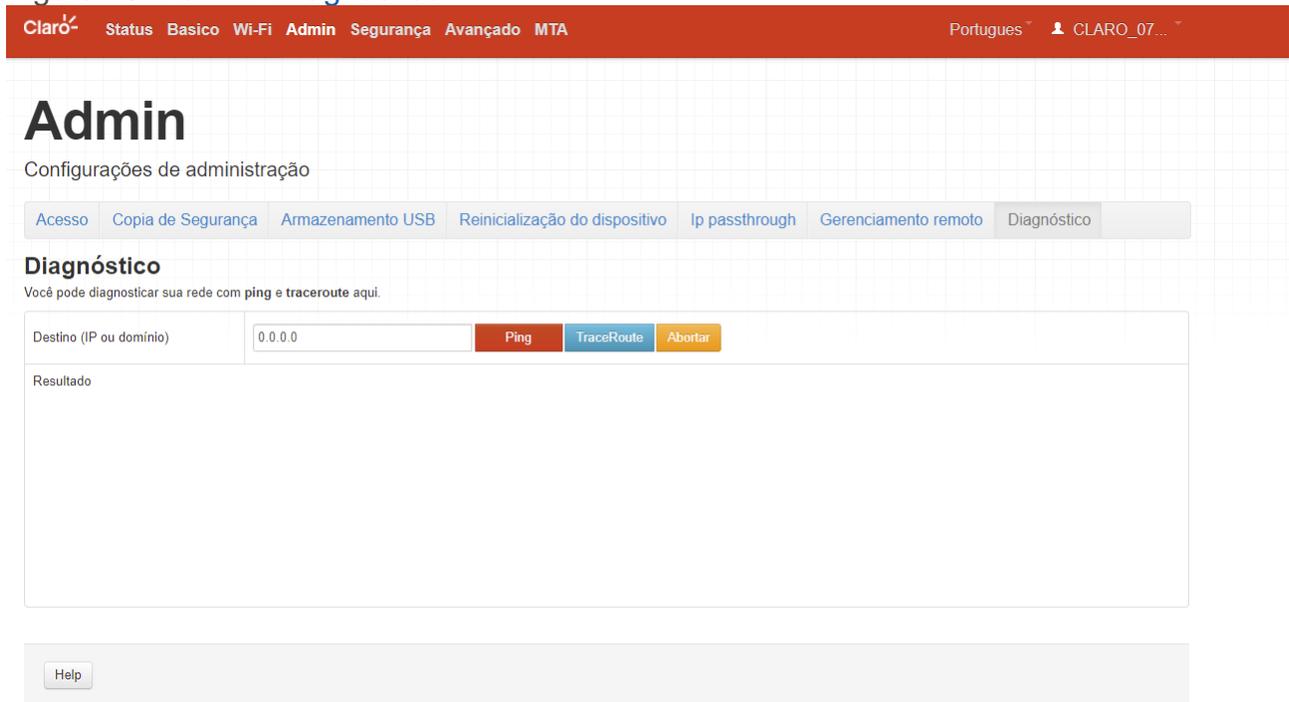
O HI3120 oferece um par de ferramentas para permitir que você realize diagnósticos de rede na LAN:

- ▶ Ping: esta ferramenta permite que você insira um endereço IP e veja se um computador (ou outro dispositivo de rede) responde com esse endereço na rede. O nome vem do pulso que o SUBMARINO SONAR emite ao digitalizar objetos subaquáticos, já que o processo é bastante semelhante. Você pode usar esta ferramenta para ver se um endereço IP está em uso ou para descobrir se um dispositivo (cujo endereço IP você conhece) está funcionando corretamente.
- ▶ Traceroute: esta ferramenta permite que você veja a rota tomada por pacotes de dados para obter da HI3120 para a nação destaque você especificar. Você pode usar esta ferramenta para resolver problemas de roteamento ou identificar firewalls que podem estar bloqueando seu acesso a um computador ou serviço.

## 5.2 Diagnóstico

Use esta tela para realizar testes de rastreamento e rastreamento em endereços IP ou URLs. Clique **em Admin > Diagnósticos**. A tela a seguir é exibida.

Figura 26: Admin: Diagnóstico



A tabela a seguir descreve os rótulos nesta tela.

Tabela 26: Admin: Diagnóstico

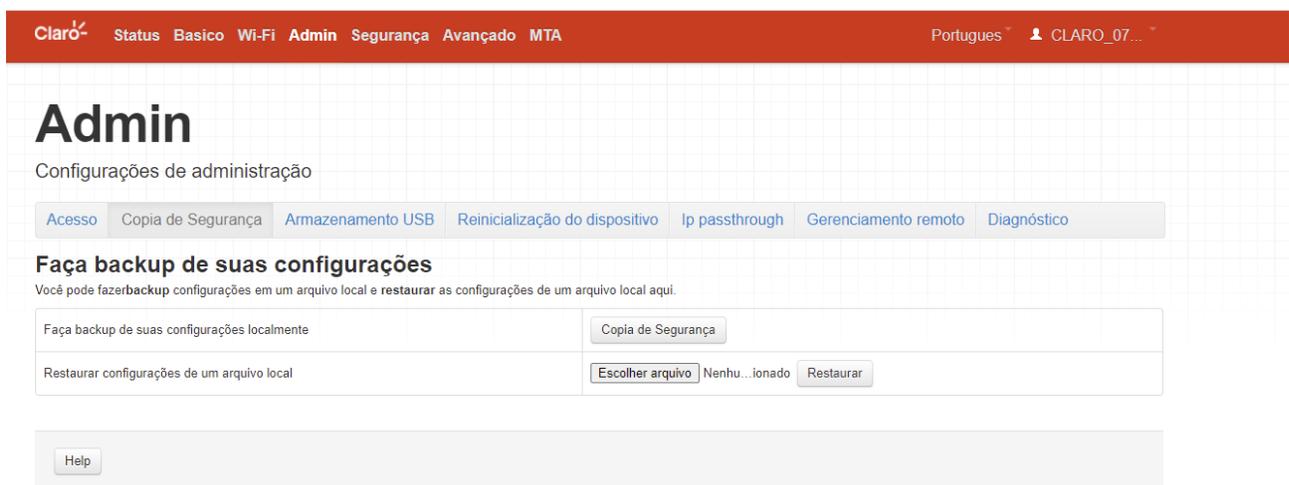
Destino (IP ou Domínio)	Digite o endereço IP ou URL que deseja testar.
Ping	Selecione o tipo de teste que você deseja executar no <b>Destino</b> que você especificou.
Traceroute	
Resultado	Este campo exibe um relatório do teste mais recentemente realizado.
Cancelar	Clique nisso para encerrar um teste em andamento.

## 5.3 Cópia de Segurança

Use esta tela para fazer backup das configurações do SEU HI3120 no computador ou carregar as configurações de um backup que você criou anteriormente.

Clique em **Admin > Cópia de Segurança**. O visor de tela a seguir.

Figura 27: Admin: Cópia de Segurança



A tabela a seguir descreve os rótulos nesta tela.

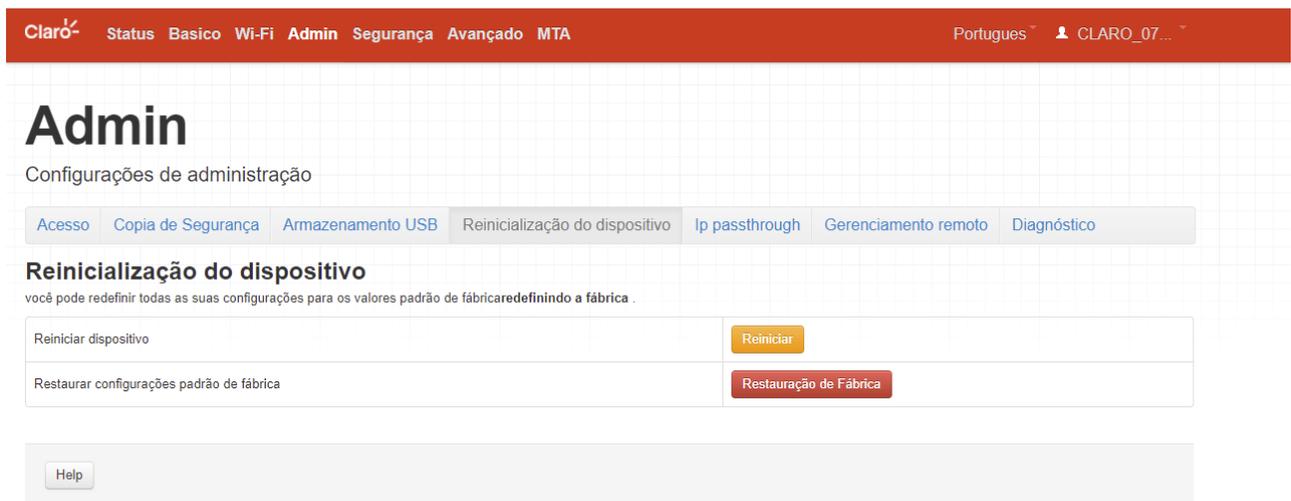
Tabela 27: Admin: Cópia de Segurança.

Fazer backup de suas configurações localmente	Clique nisso Para criar Para Backup Todos Como configurações do seu RIO HI3120 Não seu computador.
Restaurar configurações de um arquivo local	Use esses campos para retornar as configurações do seu HI3120 para as especificadas em um backup que você criou anteriormente.  Clique em <b>Procurar</b> para selecionar um backup e clique em <b>Restaurar</b> para retornar as configurações do HI3120 para as especificadas no backup.

## 5.4 Reinicialização do dispositivo

Use esta tela para reiniciar seu HI3120 ou para devolvê-lo às configurações padrão de fábrica. Clique em **Admin > Reinicialização do dispositivo**. A tela a seguir é exibida.

Figura 29: Admin: Reinicialização do dispositivo



A tabela a seguir descreve os rótulos nesta tela.

Tabela 29: Admin: Reinicialização do dispositivo

Dispositivo de reinicialização	Clique nisso para reiniciar seu HI3120.
Restaurar configurações padrão de fábrica	Clique nisso para retornar seu HI3120 às configurações padrão de fábrica. Quando você faz isso, todas as configurações configuradas pelo usuário são perdidas e não podem ser recuperadas.

## 5.5 DDNS

Use esta tela para configurar configurações DNS (Dynamic DNS). O DDNS permite que você resolva nomes de domínio para endereços IP, o que é valioso se desejar hospedar um servidor conectado ao HI3120.

Clique em **Admin > DDNS**. O visor de tela a seguir

Figura 30: [Avançado: DDNS](#)



The screenshot shows the DDNS configuration page in the Hitron web interface. The top navigation bar is red and contains the following items: Claro logo, Status, Básico, Wi-Fi, Admin, Segurança, Avançado (highlighted), MTA, Portuguese, and a user profile icon labeled CLARO\_0. Below the navigation bar, the page title is "Configurações avançadas para o gateway". There are four tabs: "Configuração de Switch", "DDNS" (selected), "Localização do dispositivo", and "Controle RIP". The main heading is "Configurações DDNS" with a sub-heading "Configure esta página para permitir que o roteador funcione como um cliente DNS dinâmico." The configuration form consists of the following fields:

Ativar DDNS	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Provedor de serviço	dyndns@dyndns.org ▼
Nome do usuário	<input type="text"/>
Senha	<input type="password"/>
Nome de Host	<input type="text"/>
Forçar Intervalo de Atualização	1 Day ▼

A tabela a seguir descreve os rótulos neste Tela.

Tabela 30: [DDNS](#)

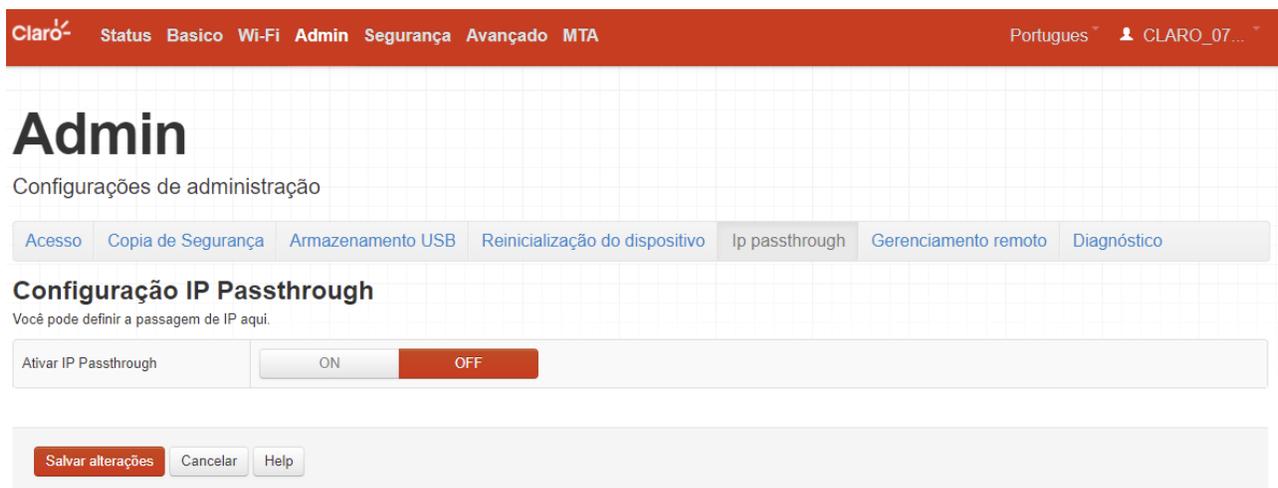
DDNS	Use estes botões para ativar ou desativar o DDNS. ▶ Clique <b>em ON</b> para ativar o DDNS. ▶ Clique <b>em OFF</b> para desativar o DDNS.
Provedor de Serviços	Selecione o provedor de serviços DDNS com quem você tem uma conta.  NOTA: <a href="#">Os dados que você precisa inserir dependerão do Provedor de Serviços selecionado.</a>
Sistema	Digite o nome do sistema DNS, se necessário.
Nome de Servidor	Digite o nome do servidor DNS, se necessário.
Servidor URL	Digite a URL do servidor do sistema DNS, se necessário.
Servidor IP	Digite a URL do servidor IP, se necessário.
Nome do usuário	Digite o nome de usuário de sua conta DDNS.
Senha	Digite a senha da sua conta DDNS.
Nome do anfitrião	Digite seu nome de domínio.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

## 5.6 IP Passthrough

Use esta tela para configurar clientes com a função IP Passthrough. O IP Passthrough pode fazer com que alguma porta ou CPE seja executado sob o modo ponte quando o gateway estiver no modo roteador.

Clique em **Admin > IP Passthrough**. A tela a seguir é exibida.

Figura 31: Admin: IP Passthrough



A tabela a seguir descreve os rótulos nesta tela.

Tabela 31: Admin: IP Passthrough

Passar ip através do MAC	Digite o endereço MAC do dispositivo para definir com a função de passagem IP.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

# 6

## Segurança

Este capítulo descreve as telas que exibem quando você clica em **Segurança** na barra de ferramentas. Ele contém as seguintes seções:

- ▶ [Visão geral de segurança](#)
- ▶ [Firewall](#)
- ▶ [Filtro de serviço](#)
- ▶ [Filtro do dispositivo](#)
- ▶ [Filtro de palavras-chave](#)

### 6.1 Visão geral da segurança

Esta seção descreve alguns dos conceitos relacionados às telas **de segurança**.

#### 6.1.1 Firewall

O termo "firewall" vem de uma técnica de construção projetada para evitar a propagação do fogo de uma sala para outra. Da mesma forma, o firewall do seu 1.1 evita tentativas de intrusão e outras atividades indesejáveis originárias da WAN, mantendo os computadores em sua LAN seguros. Você também pode usar técnicas de filtragem para especificar os computadores e outros dispositivos que deseja permitir na LAN e impedir que certos tráfegos vão da LAN para o WAN.

## 6.1.2 Sistema de detecção de intrusões

Um sistema de detecção de intrusões monitora a atividade da rede, procurando violações de políticas e atividades maliciosas ou suspeitas. O sistema de detecção de intrusões da HI3120 registra toda essa atividade na tela **Security > Logs**.

## 6.1.3 Filtragem do dispositivo

Cada dispositivo de rede tem um endereço MAC (Media Access Control, controle de acesso de mídia) exclusivo que o identifica exclusivamente na rede. Quando você habilita a filtragem de endereço MAC no firewall do HI3120, você pode configurar uma lista de dispositivos, identificados por seus endereços MAC e, em seguida, especificar se você deseja:

- ▶ Negar o acesso dos dispositivos na lista ao HI3120 e à rede (nesse caso todos os outros dispositivos podem acessar a rede)

Ou

- ▶ Permita que os dispositivos da lista acessem a rede (nesse caso nenhum outro dispositivo pode acessar a rede).

## 6.1.4 Filtragem de serviço

A filtragem de serviços é uma maneira de impedir que os usuários na LAN se conectem com dispositivos na WAN através de serviços específicos, protocolos ou aplicativos. Ele consegue isso permitindo ou negando que o tráfego da LAN passe para a WAN, com base na porta-alvo.

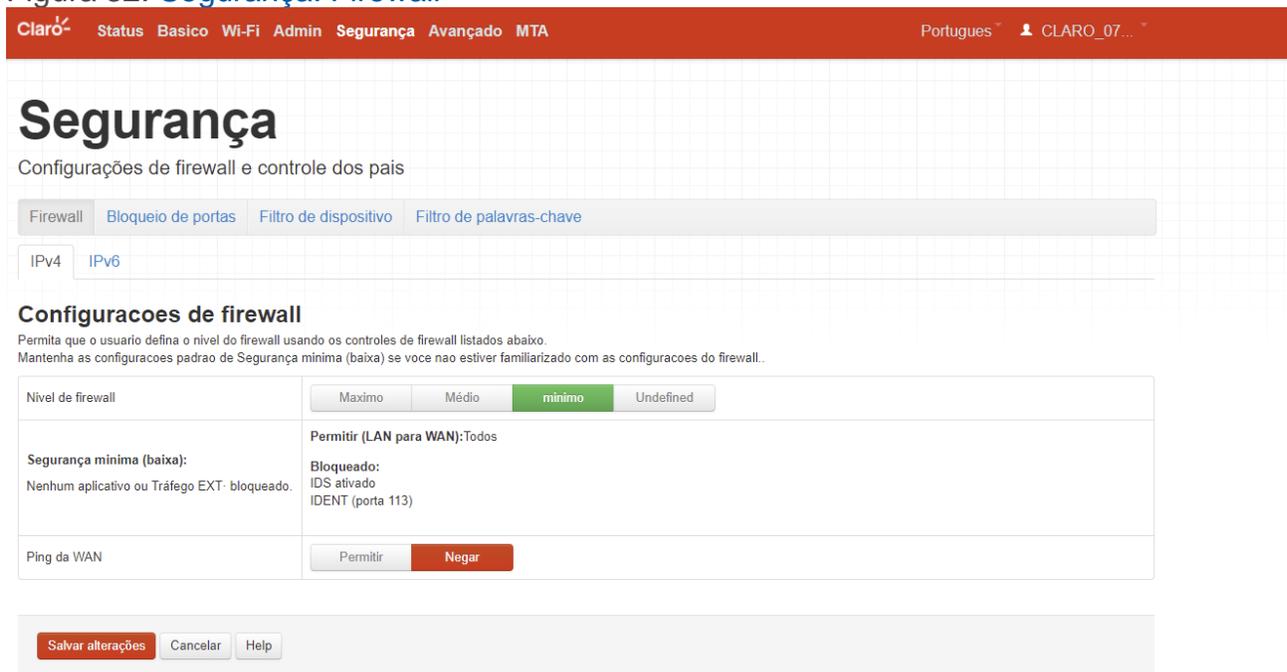
## 6.2 A tela de firewall

Use esta tela para ativar ou desativar os recursos de firewall e para permitir ou permitir certos aplicativos e protocolos. Você pode selecionar o nível de proteção de firewall a partir de opções pré-definidas ou criar um perfil de proteção personalizado.

NOTA: [Para bloquear portas específicas](#), use a tela do filtro de serviço (consulte a tela do filtro de serviço).

Clique em **Segurança > Firewall**. A tela a seguir é exibida.

Figura 32: Segurança: Firewall



Claro Status Basico Wi-Fi Admin **Segurança** Avançado MTA Portuguese CLARO\_07...

## Segurança

Configurações de firewall e controle dos pais

Firewall Bloqueio de portas Filtro de dispositivo Filtro de palavras-chave

IPv4 IPv6

### Configuracoes de firewall

Permita que o usuário defina o nível do firewall usando os controles de firewall listados abaixo. Mantenha as configurações padrão de Segurança mínima (baixa) se você não estiver familiarizado com as configurações do firewall.

Nível de firewall	Maximo Médio <b>minimo</b> Undefined
Segurança mínima (baixa): Nenhum aplicativo ou Tráfego EXT. bloqueado.	Permitir (LAN para WAN): Todos Bloqueado: IDS ativado IDENT (porta 113)
Ping da WAN	Permitir <b>Negar</b>

Salvar alterações Cancelar Help

© 2021 Hitron Technologies Inc. Todos os direitos reservados.

Os recursos de firewall IPv4 e IPv6 são configurados separadamente. Clique na guia **IPv4** (que é exibida por padrão) para configurar os recursos de firewall do IPv4 ou clique na guia **IPv6** para configurar os recursos de firewall do IPv6. Os campos que exibem em cada guia são idênticos.

A tabela a seguir descreve os rótulos neste Tela.

Tabela 32: **Segurança: Firewall**

Nível de firewall	Selecione o nível de proteção de firewall que deseja aplicar à sua LAN. Detalhes sobre o nível de proteção são exibidos sob os botões.
(Nível de segurança)	Esses campos descrevem os protocolos e aplicativos específicos que são permitidos ou negados pelo nível de segurança de firewall selecionado.  Quando você seleciona <b>Personalizado</b> Não campo <b>Nível Firewall</b> a exibição de campos adicionais que permitem alternar recursos específicos on ou off:  ▶ <b>Firewall completo</b> : selecione <b>ON</b> para ativar a proteção de segurança de firewall ou selecione <b>OFF</b> para desabilitá-lo (não recomendado).
Ping de WAN	Use este campo para permitir ou proibir as solicitações de eco do Protocolo de Mensagem de Controle da Internet (ICMP) da WAN para a LAN.  ▶ Selecione <b>Permitir</b> o ping da WAN.  ▶ Selecione <b>Negar</b> para proibir o ping do WAN. Os pedidos de Echo da WAN para a LAN são ignorados silenciosamente.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

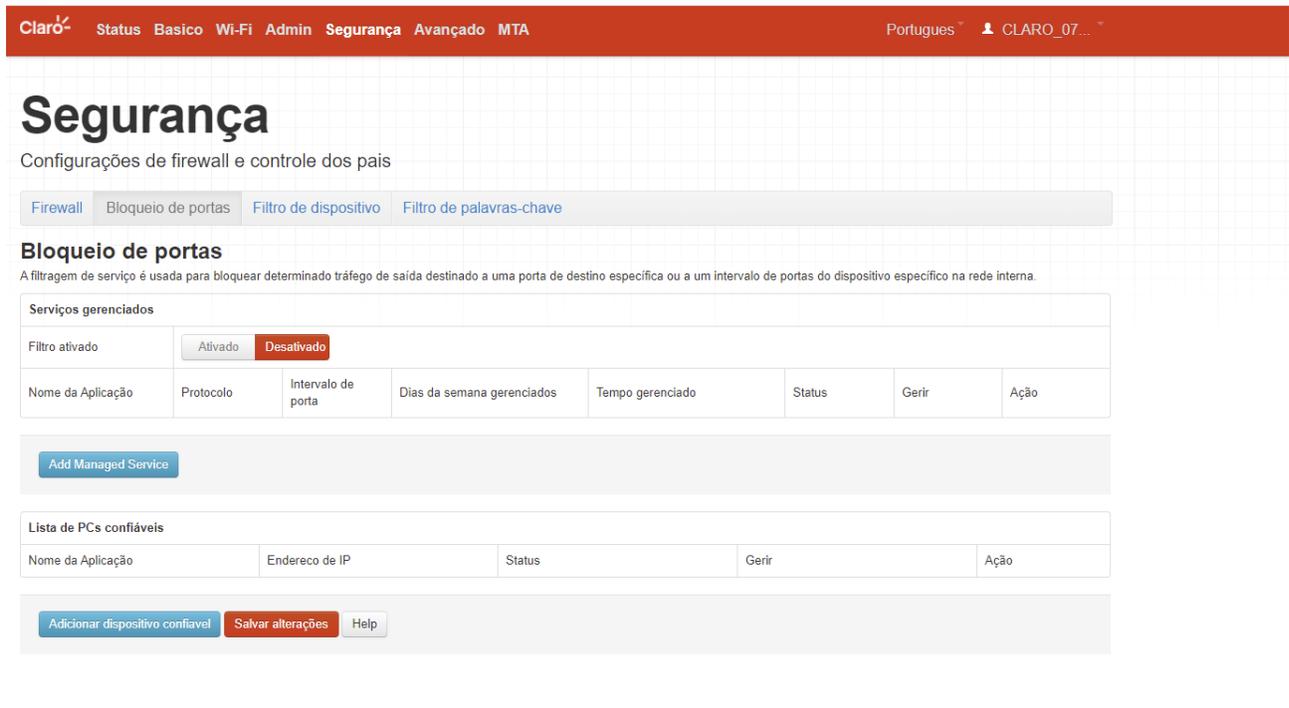
## 6.3 Bloqueio de portas

Use esta tela para configurar a filtragem do serviço. Você pode ativar ou desativar a filtragem do serviço e configurar regras novas e existentes de filtragem de serviços.

Você também pode criar e editar regras confiáveis do dispositivo. Dispositivos confiáveis são aqueles aos quais as regras de filtragem de serviço não são aplicadas.

Clique em **Segurança > Bloqueio de portas**. A tela a seguir é exibida.

Figura 33: Segurança: Bloqueio de portas



Claro Status Básico Wi-Fi Admin **Segurança** Avançado MTA Portuguese CLARO\_07...

## Segurança

Configurações de firewall e controle dos pais

Firewall Bloqueio de portas Filtro de dispositivo Filtro de palavras-chave

### Bloqueio de portas

A filtragem de serviço é usada para bloquear determinado tráfego de saída destinado a uma porta de destino específica ou a um intervalo de portas do dispositivo específico na rede interna.

Serviços gerenciados

Filtro ativado  Ativado  Desativado

Nome da Aplicação	Protocolo	Intervalo de porta	Dias da semana gerenciados	Tempo gerenciado	Status	Gerir	Ação
-------------------	-----------	--------------------	----------------------------	------------------	--------	-------	------

Add Managed Service

Lista de PCs confiáveis

Nome da Aplicação	Endereço de IP	Status	Gerir	Ação
-------------------	----------------	--------	-------	------

Adicionar dispositivo confiável Salvar alterações Help

© 2021 Hitron Technologies Inc. Todos os direitos reservados.

A tabela a seguir descreve os rótulos nesta tela.

Tabela 33: [Segurança: Bloqueio de portas](#)

Serviços Gerenciados	
Filtro ativado	Use este campo para ativar ou desativar a filtragem do serviço. <ul style="list-style-type: none"><li>▶ Selecione <b>Habilitado</b> para ativar a filtragem do serviço.</li><li>▶ Selecione <b>Desativado</b> para desativar a filtragem do serviço.</li></ul>
Nome do aplicativo	Isso exibe o nome atribuído à regra de filtragem quando você a criou.
Protocolo	Este campo exibe o protocolo ou protocolos aos quais esta regra de filtragem se aplica: <ul style="list-style-type: none"><li>▶ Protocolo de Controle de Transmissão (<b>TCP</b>)</li><li>▶ Protocolo de Datagrama do Usuário (<b>UDP</b>)</li></ul>
Faixa de porta	Isso exibe a porta de início e extremidade para a qual esta regra de filtragem se aplica.
Dias semanais gerenciados	Isso exibe os dias da semana em que esta regra se aplica.
Tempo gerenciado	Isso exibe o início ( <b>De</b> ) e o final ( <b>Para</b> ) do período durante o qual esta regra se aplica, nos dias de <b>semana gerenciados especificados</b> .

Tabela 33: [Segurança: Bloqueio de portas \(continuação\)](#)

Ação	Clique em <b>Gerenciar</b> para fazer alterações em uma regra de filtragem (consulte Adicionar ou Editar uma regra de filtro de serviço ).
Adicionar serviço gerenciado	Clique nisso para adicionar uma nova regra de filtragem de serviço (consulte Adicionar ou Editar uma regra do filtro de serviço ).
Lista de PC confiável	
Nome do anfitrião	Isso exibe o nome arbitrário de cada PC confiável configurado.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada PC confiável. Cada dispositivo de rede tem um endereço MAC que o identifica exclusivamente.
Status	Isso mostra se o dispositivo é atualmente confiável( <b>Ativado</b> ) ou não (Desativado).
Gerenciar	Clique em <b>Gerenciar</b> para fazer alterações na regra do dispositivo confiável. Consulte Adicionar ou Editar uma regra de dispositivo confiável do filtro de serviço para obter informações na tela que exibe.
Ação	Clique em <b>Excluir</b> para remover a regra do dispositivo confiável.
Adicionar dispositivo confiável	Clique nisso para criar uma nova regra de dispositivo confiável. Consulte Adicionar ou Editar uma regra de dispositivo confiável do filtro de serviço para obter informações na tela que exibe.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

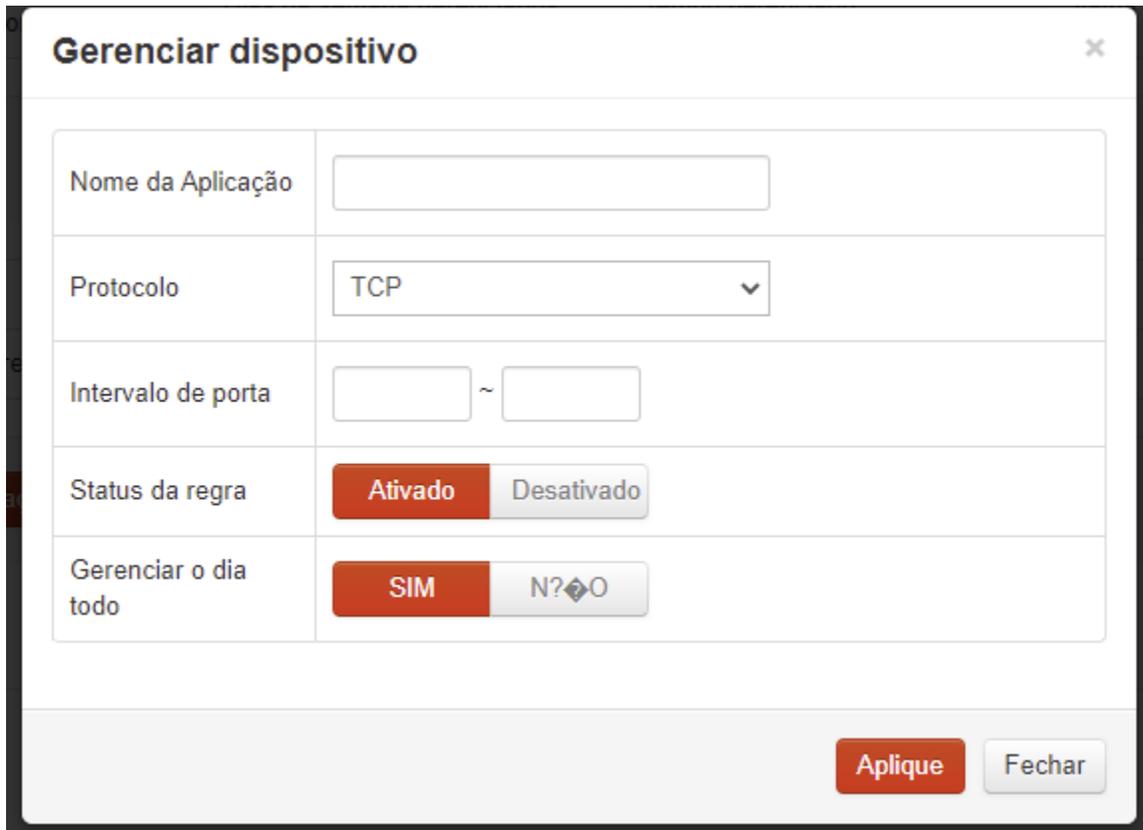
### 6.3.1 Adicionar ou editar uma regra do bloqueio de portas

- ▶ Para adicionar uma nova regra de filtro de serviço, clique em **Adicionar serviço gerenciado** na **Segurança > Tela do bloqueio de portas**.
- ▶ Para editar uma regra de filtro de serviço existente, localize a regra na tela **De Segurança > Bloqueio de portas** e clique no botão **Gerenciar**.

NOTA: Certifique-se de que **habilitado** está selecionado na tela **Segurança > Filtro de Serviço**, a fim de adicionar ou editar regras de filtragem do serviço.

A tela a seguir é exibida.

Figura 34: [Segurança: Adicionar/editar bloqueio de porta](#)



The screenshot shows a dialog box titled "Gerenciar dispositivo" with a close button (X) in the top right corner. The dialog contains a form with the following fields and controls:

Nome da Aplicação	<input type="text"/>
Protocolo	TCP <input type="button" value="v"/>
Intervalo de porta	<input type="text"/> ~ <input type="text"/>
Status da regra	<input checked="" type="button" value="Ativado"/> <input type="button" value="Desativado"/>
Gerenciar o dia todo	<input checked="" type="button" value="SIM"/> <input type="button" value="N?O"/>

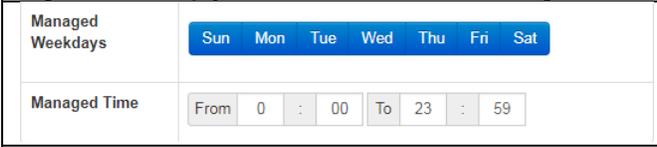
At the bottom right of the dialog, there are two buttons: "Aplique" (Apply) and "Fechar" (Close).

A tabela a seguir descreve os rótulos nesta tela.

Tabela 34: [Segurança: Adicionar/editar bloqueio de porta](#)

Nome da aplicação	<p>Digite um nome para o aplicativo para o qual deseja criar a regra.</p> <p>NOTA: Este nome é arbitrário e não afeta a funcionalidade de forma alguma.</p>
Protocolo	<p>Use este campo para especificar se o HI3120 deve filtrar através de:</p> <ul style="list-style-type: none"><li>▶ Protocolo de Controle de Transmissão (<b>TCP</b>)</li><li>▶ Protocolo de Datagrama do Usuário (<b>UDP</b>)</li></ul> <p>NOTA: Em caso de dúvida, deixe este campo à sua disposição (TCP).</p>
Faixa de porta	<p>Use esses campos para especificar a porta de início e extremidade para a qual esta regra de filtragem se aplica. Estes são os portos para onde o tráfego será bloqueado.</p> <p>Digite o número da porta inicial no primeiro campo e o número da porta final no segundo campo.</p> <p>Para especificar apenas uma única porta, digite seu número em ambos os campos.</p>

Tabela 34: **Segurança: Adicionar/editar filtro de serviço**

Status da regra	Use este campo para selecionar se a regra de filtragem deve estar ativa ou não. <ul style="list-style-type: none"> <li>▶ Selecione <b>Ativado</b> para ativar a regra. O tráfego correspondente será bloqueado.</li> <li>▶ Selecione <b>Desativado</b> para desativar a regra. O tráfego correspondente não será bloqueado.</li> </ul>
Gerenciar o dia todo	Use este campo para especificar se a regra de filtragem deve ser aplicada em todos os dias da semana, em todos os momentos , ou se a regra deve ser aplicada apenas em determinados momentos. <ul style="list-style-type: none"> <li>▶ Selecione <b>SIM</b> para aplicar a regra o tempo todo .</li> <li>▶ Selecione <b>NÃO</b> para aplicar a regra apenas em determinados momentos. Os campos adicionais são exibidos, permitindo especificar os horários em que a regra deve ser aplicada.</li> </ul> <p>Figura 35: <b>Opções adicionais de filtragem de serviços</b></p>  <p>Use os campos <b>gerenciados durante</b> a semana para especificar os dias em que a regra deve ser aplicada. Um fundo vermelho indica que a regra será aplicada (o tráfego será bloqueado), e um fundo verde indica que a regra não será aplicada (o tráfego não será bloqueado). Clique em um dia para alternar a regra sobre ou desligado para o dia relevante.</p> <p>Use os campos <b>Gerenciar tempo de partida</b> para especificar o período durante o qual a regra deve ser aplicada. Digite o tempo de início nos campos <b>de início</b>, usando notação de 24 horas, e digite o tempo final nos campos de <b>fim</b>.</p>
Aplicar	Clique nisso para salvar suas alterações nos campos nesta tela.
Perto	Clique nisso para retornar à tela <b>do Filtro de serviço</b> sem salvar suas alterações na regra.

### 6.3.2 Adicionar ou editar uma regra do dispositivo confiável do bloqueio de porta

- ▶ Para adicionar uma nova regra de dispositivo confiável, clique em **Adicionar PC confiável** na tela **segurança > bloqueio de porta > adicionar**.
- ▶ Para editar uma regra de dispositivo confiável existente, localize a regra na tela **De segurança > Bloqueio de porta** e clique no botão **Gerenciar**.

A tela a seguir é exibida.

Figura 36: [Segurança: Adicionar/editar filtro de serviço de dispositivo confiável](#)



A tabela a seguir descreve os rótulos nesta tela.

Tabela 35: [Segurança: Adicionar/editar dispositivo confiável do bloqueio de porta](#)

Nome do anfitrião	Digite um nome para identificar o dispositivo.
Endereço MAC	Digite o endereço MAC (Media Access Control, controle de acesso de mídia) do dispositivo.
Status da regra	Use este campo para definir se a regra do dispositivo confiável deve estar ativa ou não. <ul style="list-style-type: none"> <li>▶ Selecione <b>Ativado</b> para ativar a regra do dispositivo confiável.</li> <li>▶ Selecione <b>Desativado</b> para desativar a regra do dispositivo confiável.</li> </ul>
Aplicar	Clique nisso para salvar suas alterações nos campos nesta tela.
Perto	Clique nisso para retornar à tela <b>do Filtro de serviço</b> sem salvar suas alterações na regra.

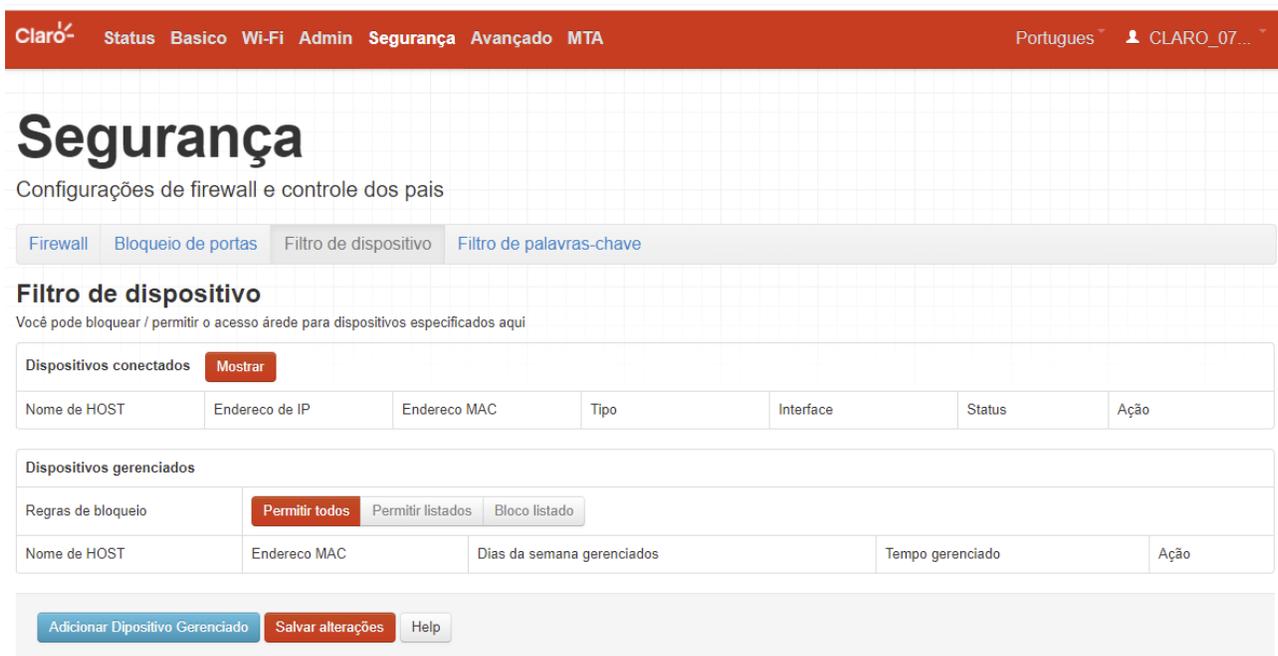
## 6.4 Filtro do dispositivo

Use esta tela para configurar a filtragem de endereços MAC (Media Access Control, controle de acesso de mídia) na LAN e para configurar a filtragem IP.

NOTA: Para configurar a filtragem de endereço MAC na rede sem fio, consulte a tela de controle de acesso Wi-Fi.

Clique em **Segurança > Filtro do dispositivo**. O visor de tela a seguir.

Figura 37: Segurança: Filtro do dispositivo



A tabela a seguir descreve os rótulos nesta tela. Tabela

36: Segurança: Filtro do dispositivo

Dispositivos conectados	
Nome do anfitrião	Isso exibe o nome de cada dispositivo de rede conectado na LAN.

Tabela 36: **Segurança: Filtro do dispositivo (continuação)**

IP Address	Isso exibe o endereço IP de cada dispositivo de rede conectado na LAN.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada dispositivo de rede conectado na LAN.
Tipo	Isso mostra se o endereço IP do dispositivo foi atribuído pelo DHCP( <b>DHCP-IP</b> ) ou <b>autoatribuído</b> .
Interface	Isso exibe o nome da interface na qual o dispositivo relevante está conectado.
Status	Isso mostra se o dispositivo conectado está ou não ativo.
Ação	Clique <b>em Gerenciar</b> para fazer alterações no status de filtragem do dispositivo; consulte Adicionar ou Editar um dispositivo gerenciado para obter informações na tela que exibe.
Dispositivos Gerenciados	
Regras do bloco	Use estes botões para controlar a ação a ser tomada para os dispositivos listados: <ul style="list-style-type: none"><li>▶ Selecionar <b>permitir que todos</b> ignorem os dispositivos <b>gerenciados</b> listar e deixar todos os dispositivos conectados ao HI3120.</li><li>▶ Selecione <b>Permitir que listados permitam</b> apenas dispositivos adicionados à lista De dispositivos <b>gerenciados</b> para acesso o HI3120 e a rede. Todos os outros dispositivos têm acesso negado.</li><li>▶ Selecione <b>Negar</b> para permitir todos os dispositivos, exceto aqueles que você adicionou à lista de dispositivos <b>gerenciados</b> para acessar o HI3120 e a rede. Os dispositivos especificados são negados acesso.</li></ul>
Nome do anfitrião	Isso exibe o nome de cada dispositivo de rede na lista.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada dispositivo de rede da lista.
Dias semanais gerenciados	Isso exibe os dias da semana em que o dispositivo é gerenciado.

Tempo gerenciado	Isso exibe o início ( <b>De</b> ) e o final ( <b>Para</b> ) do período durante o qual o dispositivo é gerenciado, nos dias de semana <b>gerenciados especificados</b> .
Ação	Clique em <b>Gerenciar</b> para fazer alterações em uma regra de dispositivo gerenciado (consulte Adicionar ou Editar um dispositivo gerenciado ).
Adicionar dispositivo gerenciado	Clique nisso para adicionar uma nova regra de dispositivo gerenciado (consulte Adicionar ou Editar um dispositivo gerenciado ).
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

### 6.4.1 Adicionar ou editar um dispositivo gerenciado

- ▶ Para adicionar um novo dispositivo LAN gerenciado, clique em **Adicionar dispositivo gerenciado** na **segurança** > **Tela do filtro do dispositivo**.
- ▶ Para editar um dispositivo LAN gerenciado existente, localize o dispositivo no **Security** > **Tela do filtro do dispositivo** e clique no botão **Gerenciar**.
- ▶ Para adicionar um novo dispositivo de rede sem fio gerenciado, clique em **Adicionar dispositivo gerenciado** na tela **Wireless** > **Access Control**.
- ▶ Para editar um dispositivo de rede sem fio gerenciado existente, localize o dispositivo no **Tela wireless** > **Access Control** e clique no botão **Gerenciar**.

A tela a seguir é exibida.

Figura 38: **Segurança: Adicionar/editar o filtro do dispositivo**

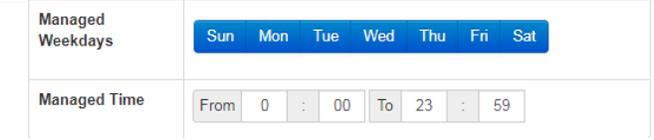


A tabela a seguir descreve os rótulos nesta tela.

Tabela 36: **Segurança: Adicionar / Editar Filtro de Dispositivo**

Nome do anfitrião	<p>Se você estiver gerenciando um dispositivo já conectado através da LAN, este campo exibirá o nome do dispositivo.</p> <p>Alternativamente, se você está gerenciando um dispositivo que não está conectado através da LAN, você pode inserir seu nome aqui se você o conhece.</p>
Endereço MAC	<p>Se você estiver gerenciando um dispositivo já conectado através da LAN, este campo exibirá o endereço MAC (Media Access Control) do dispositivo. Alternativamente, se você estiver gerenciando um dispositivo que não está conectado através da LAN, você pode inserir seu endereço MAC aqui se você conhece ele.</p>
Gerenciado pelo dispositivo	<p>Use este campo para definir se o dispositivo deve ter seus privilégios de acesso filtrados ou não.</p> <ul style="list-style-type: none"><li>▶ Clique <b>em Sim</b> para filtrar os privilégios de acesso do dispositivo.</li><li>▶ Clique <b>em Não</b> para não filtrar os privilégios de acesso do dispositivo.</li></ul> <p>Quando um dispositivo não está sendo gerenciado, o campo <b>Gerenciar o Dia todo</b> e campos relacionados não são exibidos.</p>

Tabela 36: Segurança: Adicionar / Editar Filtro de Dispositivo (continuação)

<p>Gerenciar o dia todo</p>	<p>Use este campo para especificar se o dispositivo deve ser gerenciado em todos os dias da semana, em todos os momentos , ou se o dispositivo deve ser gerenciado apenas em determinados momentos.</p> <ul style="list-style-type: none"> <li>▶ Selecione <b>SIM</b> para gerenciar o dispositivo o tempo todo.</li> <li>▶ Selecione <b>NÃO</b> para gerenciar o dispositivo apenas em determinados momentos. Os campos adicionais são exibidos, permitindo especificar os horários em que o dispositivo deve ser gerenciado.</li> </ul> <p>Figura 39: Opções adicionais de filtragem de serviços</p>  <p>Use os campos <b>gerenciados durante</b> a semana para especificar os dias em que o dispositivo deve ser gerenciado. Um fundo vermelho indica que o dispositivo será gerenciado (o acesso será bloqueado), e um fundo verde indica que o dispositivo não será gerenciado (o acesso não será bloqueado). Clique em um dia para alternar a regra dentro ou fora para o dia relevante.</p> <p>Use os campos <b>Gerenciar tempo de partida</b> para especificar o período durante o qual o dispositivo deve ser gerenciado. Digite o tempo de início nos campos <b>de From</b>, usando notação de 24 horas, e digite o tempo final nos campos <b>de To</b>.</p>
<p>Aplicar</p>	<p>Clique nisso para salvar suas alterações nos campos nesta tela.</p>
<p>Perto</p>	<p>Clique nisso para retornar à tela <b>do Filtro do Dispositivo</b> sem salvar suas alterações na regra.</p>

## 6.5 Filtro de palavras-chave

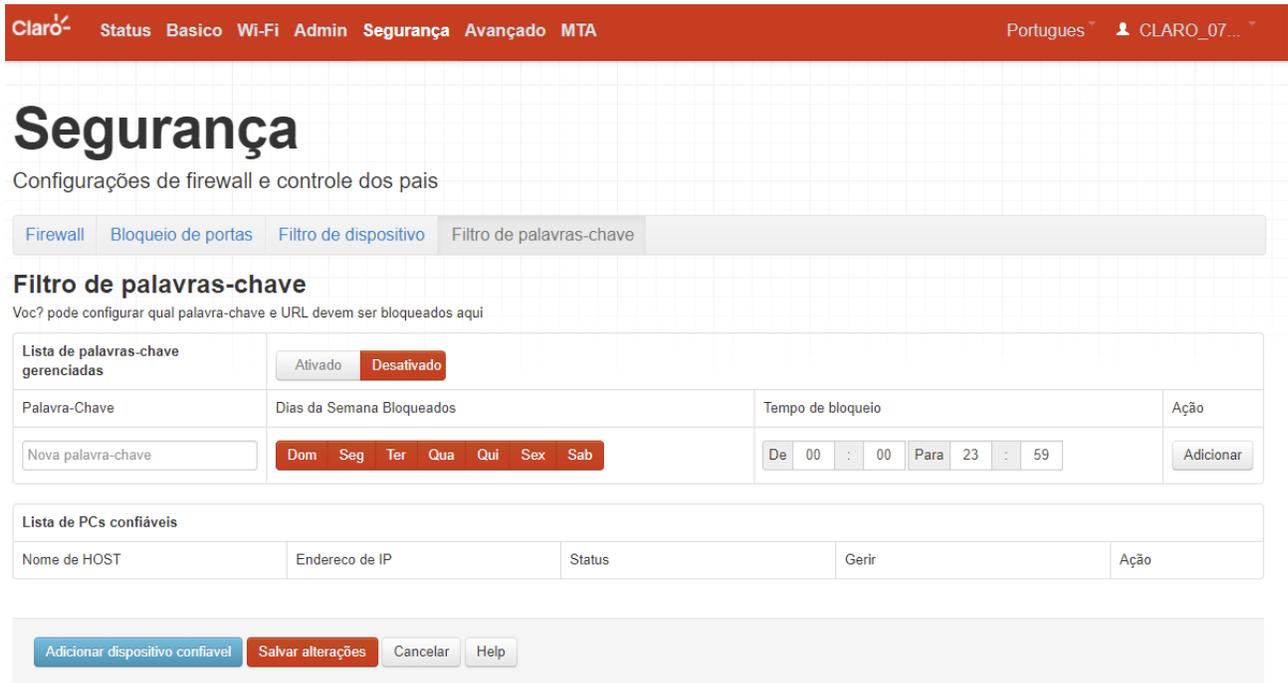
Use esta tela para bloquear o acesso da LAN a sites cujos URLs (endereços web) e conteúdo de página (texto) contêm determinadas palavras-chave. Você pode criar várias regras de bloqueio de palavras-chave e defini-las para aplicar em determinados dias e em determinados momentos.

Você também pode criar e editar regras confiáveis do dispositivo. Dispositivos

confiáveis são aqueles aos quais as regras de filtragem de palavras-chave não são aplicadas.

Clique em **Segurança > Filtro de palavras-chave**. O visor da tela a seguir.

Figura 40: [Segurança: Filtro de palavras-chave](#)



A tabela a seguir descreve os rótulos neste Tela.

Tabela 38: [Filtro de palavras-chave](#)

<p>Lista de palavras-chave gerenciadas</p>	<p>Use este campo para ativar ou desativar a filtragem de palavras-chave.</p> <ul style="list-style-type: none"> <li>▶ Selecione <b>Habilitado</b> para fazer filtragem de palavras-chave.</li> <li>▶ Selecione <b>Desativado</b> para desativar a filtragem da palavra-chave.</li> </ul>
<p>Palavra</p>	<p>Digite a palavra-chave que deseja bloquear. O HI3120 examina tanto a URL (endereço da Internet) da página quanto o conteúdo da página (texto).</p>

Tabela 38: Filtro de palavras-chave (continuação)

Dias de semana bloqueados	Use esses campos para especificar os horários em que a palavra-chave deve ser bloqueada. Um fundo vermelho indica que a regra será aplicada (o acesso será bloqueado) e um fundo verde indica que o dispositivo não será aplicado (o acesso não será bloqueado). Clique em um dia para alternar a regra dentro ou fora para o dia relevante.
Tempo bloqueado	Use esses campos para especificar o período durante o qual a regra deve ser aplicada. Digite o tempo de início nos campos De 24 horas, e digite o tempo final nos campos De <b>Para</b> .
Ação	Clique em <b>Adicionar</b> para criar uma nova regra de bloqueio de palavras-chave; uma nova linha de exibição de campos .
Lista de PC confiável	
Nome do anfitrião	Isso exibe o nome arbitrário de cada PC confiável configurado.
Endereço MAC	Isso exibe o endereço MAC (Media Access Control, controle de acesso de mídia) de cada PC confiável. Cada dispositivo de rede tem um endereço MAC que o identifica exclusivamente.
Status	Isso mostra se o dispositivo é atualmente confiável( <b>Ativado</b> ) ou não ( <b>Desativado</b> ).
Gerenciar	Clique em <b>Gerenciar</b> para fazer alterações na regra do dispositivo confiável. Consulte Adicionar ou Editar uma regra de dispositivo confiável do filtro de palavras-chave para obter informações na tela que é exibida.
Ação	Clique em <b>Delete</b> para remover a regra do dispositivo confiável.
Adicionar dispositivo confiável	Clique nisso para criar uma nova regra de dispositivo confiável. Consulte Adicionar ou Editar uma regra de dispositivo confiável do filtro de palavras-chave na página 100 para obter informações na tela que é exibida.
Salvar alterações	Clique nisso para salvar suas alterações nos campos nesta tela.
Cancelar	Clique nisso para retornar os campos nesta tela aos seus últimos valores salvos sem salvar suas alterações.
Ajuda	Clique nisso para ver informações sobre os campos nesta tela.

### 6.5.1 Adicionar ou editar uma regra do dispositivo confiável do filtro de palavras-chave

- ▶ Para adicionar uma nova regra de dispositivo confiável, clique em **Adicionar PC confiável** no **Security >** Tela de filtro de palavras-chave.
- ▶ Para editar uma regra de dispositivo confiável existente, localize a regra na tela do filtro de **palavras-chave de segurança** e clique no botão **Gerenciar**.

A tela a seguir é exibida.

Figura 41: Segurança: Adicionar / Editar Dispositivo Confiável do Filtro de Palavra-chave



dispositivo de gerenciamento confiável	
Nome de HOST	<input type="text" value="Nome de HOST"/>
Endereço de IP	<input type="text" value="Endereço de IP"/>
Status da regra	<input checked="" type="radio"/> Ativado <input type="radio"/> Desativado
<input type="button" value="Aplicar"/> <input type="button" value="Fechar"/>	

A tabela a seguir descreve os rótulos nesta tela.

Tabela 39: [Segurança: Adicionar / Editar Dispositivo Confiável do Filtro de Palavra-chave](#)

Nome do anfitrião	Digite um nome para identificar o dispositivo.
Endereço MAC	Digite o endereço MAC (Media Access Control, controle de acesso de mídia) do dispositivo.
Status da regra	Use este campo para definir se a regra do dispositivo confiável deve estar ativa ou não. <ul style="list-style-type: none"><li>▶ Selecione <b>Ativado</b> para ativar a regra do dispositivo confiável.</li><li>▶ Selecione <b>Desativado</b> para desativar a regra do dispositivo confiável.</li></ul>
Aplicar	Clique nisso para salvar suas alterações nos campos nesta tela.
Perto	Clique nisso para retornar à tela <b>do filtro de palavras-chave</b> sem salvar suas alterações na regra.

# 7

## Solucionando problemas

Use esta seção para resolver problemas comuns com o HI3120 e sua rede. Ele contém as seguintes seções:

- ▶ Nenhum dos LEDs liga
- ▶ Um dos LEDs não exibe como esperado
- ▶ Esqueci o endereço IP da HI3120
- ▶ Esqueci o nome de usuário ou senha do administrador do HI3120
- ▶ Não posso acessar o HI3120 ou a Internet
- ▶ Não posso conectar meu dispositivo sem fio

### Problema: Nenhum dos LEDs liga

O HI3120 não está recebendo energia, ou há uma falha no dispositivo.

- 1 Certifique-se de que está usando o adaptador de alimentação correto.  
 **Usar um adaptador de energia diferente do que veio com o seu HI3120 pode danificar o seu HI3120.p**
- 2 Certifique-se de que o adaptador de alimentação esteja conectado ao HI3120 e à tomada de parede (ou outra fonte de energia) corretamente.
- 3 Certifique-se de que a fonte de energia está funcionando corretamente. Substitua quaisquer fusíveis quebrados ou reinicie quaisquer disjuntores

tropeçados.

- 4 Desconecte e reconecte o adaptador de energia à fonte de alimentação e ao HI3120.
- 5 Se nenhuma das etapas acima resolver o problema, consulte seu fornecedor.

### **Problema: Um dos LEDs não mostra como o esperado**

- 1 Certifique-se de entender o comportamento normal do LED (consulte LEDs).
- 2 Certifique-se de que o hardware do HI3120 esteja conectado corretamente; consulte o Guia de Instalação Rápida.
- 3 Desconecte e reconecte o adaptador de energia ao HI3120.
- 4 Se nenhuma das etapas acima resolver o problema, consulte seu fornecedor.

### **Problema: Esqueci o endereço IP da HI3120**

- 1 O endereço IP LAN padrão da HI3120 é **192.168.0.1**.
- 2 Dependendo do seu sistema operacional e da sua rede, você pode ser capaz de encontrar o endereço IP da HI3120 procurando o gateway padrão do seu computador. Para fazer isso em (a maioria)máquinas Windows, clique em **Iniciar > Executar**, digite "cmd", e depois digite "ipconfig". Obtenha o endereço IP do **Gateway Padrão** e digite-o na barra de endereços do seu navegador.

### **Problema: Esqueci o nome de usuário ou senha do administrador da HI3120**

O nome de usuário padrão é **administrador**, e a senha padrão é administrador.

### **Problema: Eu não posso acessar o HI3120 ou a Internet**

- 1 Certifique-se de que está usando o endereço IP correto para o HI3120.
- 2 Verifique as conexões de hardware da sua rede e que os LEDs da HI3120 são exibidos corretamente (consulte LEDs).
- 3 Certifique-se de que o computador está na mesma sub-rede que o HI3120; ver Configuração de endereço IP.

- 4 Se você está tentando se conectar pela rede sem fio, pode haver um problema com a conexão sem fio. Conecte-se através de uma porta **LAN** em vez disso.
- 5 Se as etapas acima não funcionarem, você precisa redefinir o HI3120. Consulte Redefinindo o HI3120. Todos os dados configurados pelo usuário são perdidos e o HI3120 é devolvido às configurações padrão. Se você anteriormente apoiou uma versão mais recente do seu HI3120, agora você pode enviá-las para o HI3120; ver A tela de backup.
- 6 Se o problema persistir, entre em contato com seu fornecedor.

### **Problema: Não consigo conectar meu dispositivo sem fio**

- 1 Certifique-se de que seu dispositivo cliente sem fio está funcionando corretamente e está configurado corretamente. Consulte a documentação do cliente sem fio, se não tiver certeza.
- 2 Certifique-se de que o cliente sem fio está dentro da área de cobertura de rádio da HI3120. Tenha em mente que obstruções físicas (paredes, pisos, árvores, etc.) e interferência elétrica (outros transmissores de rádio, fornos de micro-ondas, etc) reduzem sua área de qualidade e cobertura de sinais da HI3120.
- 3 Certifique-se de que o HI3120 e o cliente sem fio estejam definidos para usar o mesmo modo sem fio, SSID e configurações de segurança (consulte a tela de configurações básicas sem fio e a tela WPS & Segurança).
- 4 Reinsira quaisquer credenciais de segurança (teclas WEP, senha WPA(2)-PSK ou PIN WPS).
- 5 Se você estiver usando o recurso PBC (configuração de botão) do WPS, certifique-se de que você está pressionando o botão no HI3120 e o botão no cliente sem fio dentro de 2 minutos um do outro.