

Manual do Usuário

Introdução

Bem-vindo ao mundo instigante da Internet de alta velocidade e do serviço de telefonia digital de alta qualidade. Seu gateway doméstico HUMAX oferece conectividade wireless selecionável ou simultânea dupla para alta capacidade e usuários adicionais. Você pode realizar chamada de voz dependendo do tipo dos serviços VoIP.

A banda dupla selecionável suporta somente uma rede wireless, 2.4GHz ou 5GHz. Um roteador wireless de banda dupla é um roteador de banda simples com dois canais selecionáveis; você pode usar qualquer dos canais, mas não ambos ao mesmo tempo. Com um roteador de banda dupla selecionável, todos os dispositivos wireless em sua residência deverão compartilhar uma rede wireless simples.

Bandas duplas concomitantes suportam duas redes wireless separadas simultaneamente, utilizando tanto 2.4GHz como 5GHz. O equipamento não só dobra a largura da banda disponível como também permite a criação de uma rede wireless dedicada e confiável para vídeo e jogos. Quando forem conectados vários dispositivos, manter duas conexões de rede wireless separadas evita o congestionamento e a interferência, permitindo maior flexibilidade para a melhor conexão possível.

Benefícios e Recursos

Seu gateway residencial HG100R(E) oferece os seguintes benefícios e recursos excelentes.

- ▶ Conformidade com DOCSIS e Euro-DOCSIS 1.x/2.0/3.0, assim como com a norma Euro-Packet Cable 1.0/1.5 para proporcionar um desempenho de alta qualidade e confiabilidade ao usuário.
- ▶ Conectividade wireless de banda dupla selecionável/ simultânea para 2.4GHz e 5GHz projetada em conformidade com as normas 802.11a/b/g/n
- ▶ Adaptador de voz digital embutido para serviços de telefonia VoIP
- ▶ Portas Gigabit Ethernet para fornecer conectividade com fio
- ▶ Funções de classe estendida, tais como identificador de chamadas, chamada em espera, chamada em conferência, mensagens de voz e fax etc.
- ▶ Atualizações automáticas do software pelo seu provedor de serviços
- ▶ Menu de controle dos pais configurável pelo usuário para bloquear o acesso a sites de Internet indesejáveis

Aviso

Obrigado por adquirir um produto HUMAX. Por favor, leia esse manual do usuário cuidadosamente para que instalar o produto de forma segura, utilizando-o e mantendo-o com o máximo de desempenho. Guarde este manual de usuário com seu produto para consulta futura. As informações constantes neste manual de usuário estão sujeitas a alterações sem aviso prévio.

Direitos Autorais (Copyright © 2014 HUMAX Corporation)

O manual não deve ser copiado, utilizado ou traduzido, no todo ou em parte, sem consentimento prévio da HUMAX, por escrito, ressalva a aprovação de titularidade de direito autoral e das leis de direitos autorais.

Informações de Segurança e de Regulamentação

Este guia de usuário do gateway HUMAX residencial contém informações importantes de segurança, reciclagem, garantia e licença. Se você desejar mais detalhes sobre como seu gateway residencial funciona, consulte o manual de usuário. Você pode fazer o download do manual na página <http://www.humaxdigital.com/gateway/>.

Instruções de Segurança

Por favor, leia estas instruções antes de utilizar o seu gateway residencial. Não queremos que você se machuque nem que seu gateway residencial seja danificado.

- Não utilize o seu gateway residencial em local próximo de água. Mantenha o seu gateway residencial seco. Se você precisar limpá-lo, não utilize uma toalha úmida. Limpe seu gateway residencial com um pano limpo e seco. Nunca utilize fluidos de limpeza ou produtos químicos similares. Não borrife sprays de limpeza diretamente no gateway residencial, nem utilize aspiradores para remover a poeira.
- Não coloque o seu gateway residencial perto de fontes de calor, tais como aparelhos com temperatura elevada, tais como aquecedores e radiadores, outros aparelhos eletrônicos como computadores e aparelhos de som, ou dentro de sua lareira. Seu gateway residencial é frio e assim deve ser mantido.
- Não cubra o seu gateway residencial, nem bloqueie o fluxo de ar para o gateway com outros objetos. Mantenha o gateway residencial longe de calor e umidade excessivos, bem como livres de vibração e poeira.
- O gateway residencial é somente de uso em interiores. Por favor, não tente utilizá-lo em ambientes externos.
- Não tente abrir, modificar ou reparar o seu gateway residencial. Isso pode lhe causar um choque elétrico ou uma lesão. Qualquer alteração pelo consumidor não expressamente aprovada pela HUMAX invalida a sua autorização para operar o equipamento e anulará a garantia do seu gateway residencial. Se você acredita que algo está errado com o seu gateway residencial, entre em contato com o suporte da HUMAX RG.
- Conecte somente cabos e acessórios especificados e da forma indicada pela HUMAX gateway.
- Proteja o seu cabo de força permitindo que ele seja mantido solto, pendendo livremente entre o gateway residencial e a tomada. Não o estique nem o comprima entre outros objetos.
- Manuseie seu gateway residencial com cuidado. Não derrube nem chacoalhe seu gateway residencial.
- É esperado que seu gateway residencial esquente, porém o equipamento necessita de ventilação para continuar funcionando corretamente. Não bloqueie a ventilação. É importante que o gateway residencial seja instalado em uma superfície sólida e desobstruída. Não coloque seu gateway residencial em superfície macia, como o chão revestido de carpete, que possa bloquear sua ventilação.
- Esse gateway residencial foi qualificado em condições de teste que incluíram o uso de cabos fornecidos entre os componentes do sistema. Para garantir a conformidade regulatória e de segurança, use apenas os cabos de alimentação e de interface fornecidos, instalando-os adequadamente.

Advertência

- Adie a instalação até que não haja risco de tempestade ou raios na região.
- Evite utilizar um telefone (que não seja do tipo sem fio) durante descargas elétricas. Pode haver um risco remoto de choque elétrico causado por raios. Para proteção adicional, desligue o gateway residencial da tomada e desconecte seus cabos para evitar danos devido a relâmpagos e picos de energia.
- Após a conclusão de qualquer serviço ou reparo neste gateway residencial, peça ao técnico para executar verificações de segurança para determinar se o gateway residencial está em condições seguras de operação.

Riscos de Asfixia

Choking hazards

A embalagem do gateway residencial pode incluir sacos e presilhas de plástico. Favor descartá-los corretamente, mantendo-os longe de crianças, pois podem representar um risco de asfixia. Mantenha o gateway residencial, seus cabos e acessórios fora do alcance das crianças pequenas.

Instalação

Índice

Instalação

Acessórios

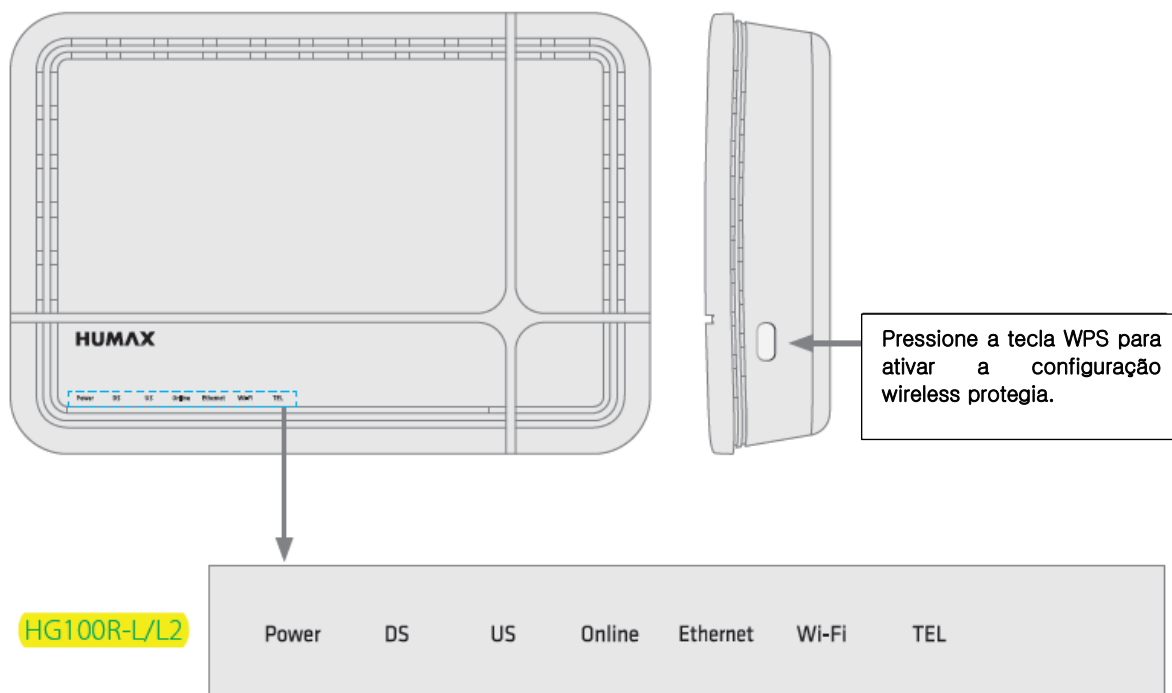
Guia de Instalação Rápida

Adaptador de corrente DC

Cabo Ethernet

Painel Frontal

Obs.: A imagem pode diferir do produto real.



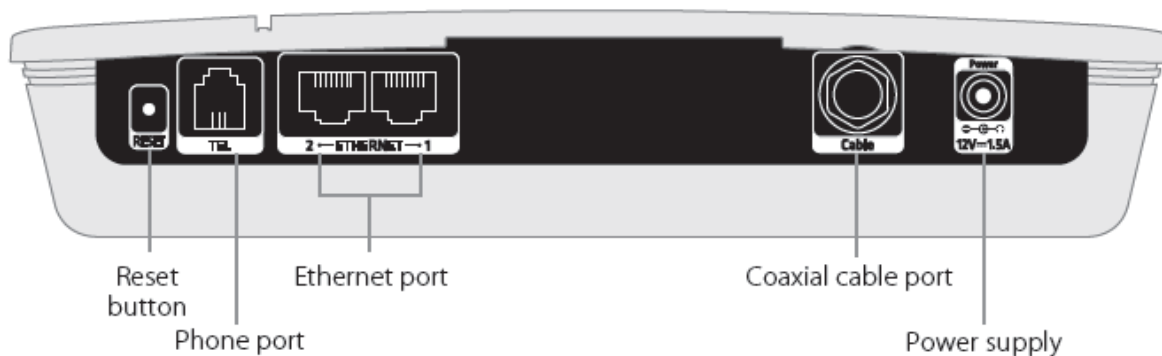
Instalação

Depois que o gateway tiver sido registrado na rede com êxito, os LEDs acendem continuamente, indicando que o gateway está ativo e em operação integral.

LED		Operação
Energia	Verde ligada	Corrente desligada
	Vermelha ligada	Corrente está fraca
	Desligado	Corrente desligada
DS	Verde ligada	Canal de sinal downstream travado.
	Verde piscante	Escaneamento downstream em andamento. Atualização de software em andamento.
	Amarela ligada	Canal downstream agregado está travado.
	Desligado	Não há nenhum sinal RF.
US	Verde ligada	Sinal de canal upstream em busca.
	Verde piscante	Busca upstream em andamento. Atualização de software em andamento
	Amarelo ligada	Canal de agregação upstream em busca.
	Desligado	Não há nenhum sinal RF.
Online	Verde ligada	<i>Acesso à rede está habilitado.</i>
	Vermelho piscante	Não há nenhum sinal RF
	Verde piscante	Acesso à rede está desabilitado.
Ethernet	Verde ligada	Links LAN até 10/100Mbps.
	Amarela ligada	Links LAN até 1000Mbps.
	Desligado	LAN está desconectada.
Wi-Fi	Verde ligada	WLAN está habilitada.
	Verde piscante	Tráfego de dados em curso.
	Desligado	WLAN está desabilitada.
TEL	Verde ligada	Telefone habilitado.
	Verde piscante	Telefone inicializado ou em uso.
	Desligado	Telefone está desabilitado

Painel traseiro

HG100R-L2



Item	Descrição
RESET	Mantenha a tecla de reinicialização pressionada por 7 segundos para retornar às configurações de fábrica.
TEL	Conectar um telefone para uso do serviço VoIP.
Porta Ethernet	Conecte as portas Ethernet aos computadores locais.
Cabo	Conecte um cabo coaxial para usar o serviço de TV a cabo.
Energia	Conecte um adaptador de corrente DC do conector de energia à tomada na parede.

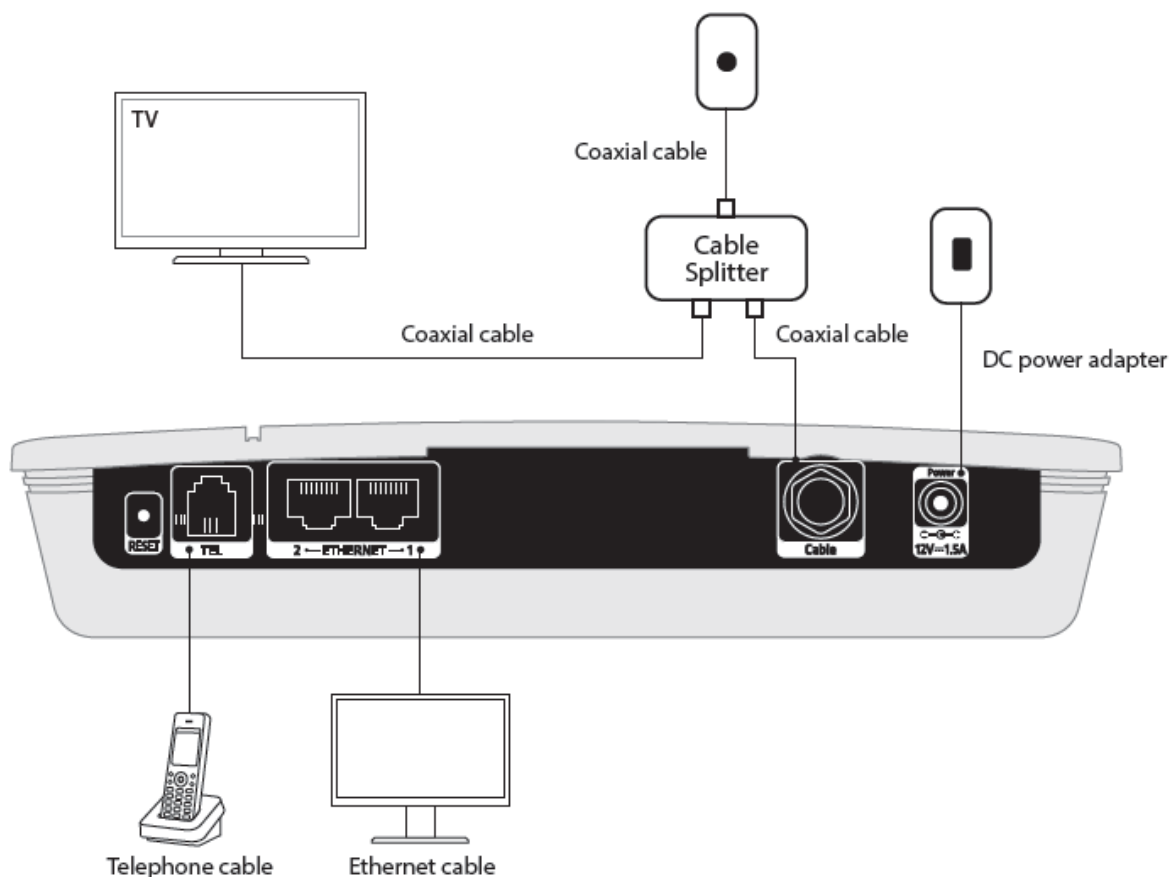
Nota: A tecla de reinicialização é somente para fins de manutenção. Não a utilize, a menos que seja instruído a fazê-lo por seu provedor de serviços. Sua utilização pode acarretar a perda das configurações do modem a cabo que você tenha selecionado.

Conexões

Seu gateway residencial suporta tanto os serviços de Internet quanto de telefonia ao mesmo tempo. Esta seção descreve como conectar o seu gateway residencial para combinar com seus dispositivos de rede e obter um melhor desempenho.

Advertência:

- Conecte todos os dispositivos antes de ligar qualquer cabo de energia na tomada. Sempre desligue o gateway residencial e os dispositivos de rede antes de conectar ou desconectar qualquer cabo.
- Tensões elétricas perigosas podem existir nas portas de telefone no gateway residencial e em qualquer fiação conectada, incluindo a fiação da Ethernet, a fiação de telefone e o cabo coaxial.



Conectando a TV

1. Utilize um cabo coaxial para conectar sua TV a um splitter de cabo (adquirido separadamente).
2. Utilize outro cabo coaxial para conectar o gateway residencial ao splitter de cabo.
3. Utilize o outro cabo coaxial para conectar o divisor de cabo à saída do cabo.

Conectando os PCs

Utilize cabos para conectar seus computadores ao gateway residencial. Se você utilizar um computador ou HUB de Ethernet, você pode conectar mais de 200 PCs.

Nota: Talvez você precise verificar com o seu provedor de serviços a possibilidade de conexão de múltiplos computadores.

Conectando o Telefone

Conecte o cabo do telefone diretamente do telefone ao gateway residencial.

Nota:

- É recomendável que você verifique com seu provedor de serviços como proceder para utilizar o serviço de telefonia.
- Você pode conectar um telefone, máquina de fax, secretária eletrônica, caixa de identificador de chamadas etc.

Connecting the Network

Conectando a Rede

Após conectar seus dispositivos de rede, você conectar seu gateway residencial à rede utilizando um cabo coaxial ou um cabo de Ethernet.

Utilizando um cabo coaxial

Conecte um cabo coaxial da tomada na parede ao gateway residencial.

Nota: Se você já tiver conectado os cabos coaxiais conforme descrito em *Conectando a TV*, a conexão de rede já estará concluída.

Utilizando um cabo de Ethernet

Conecte um cabo de Ethernet do roteador ao gateway residencial.

Ligando o equipamento

1. Conecte o adaptador DC do conector de energia à tomada na parede.
2. Se a corrente passar, acenderá um LED verde no painel frontal.

Nota: Utilize somente o adaptador de energia DC fornecido junto com esse produto. Utilizar outros adaptadores pode danificar o produto.

Requisitos para o Serviço de Internet e Telefonia

Para configurar o cabo do modem do gateway residencial, você precisará das informações adiante. Você pode obter as informações com seu provedor de serviço (ISP – Provedor de Serviço de Internet).

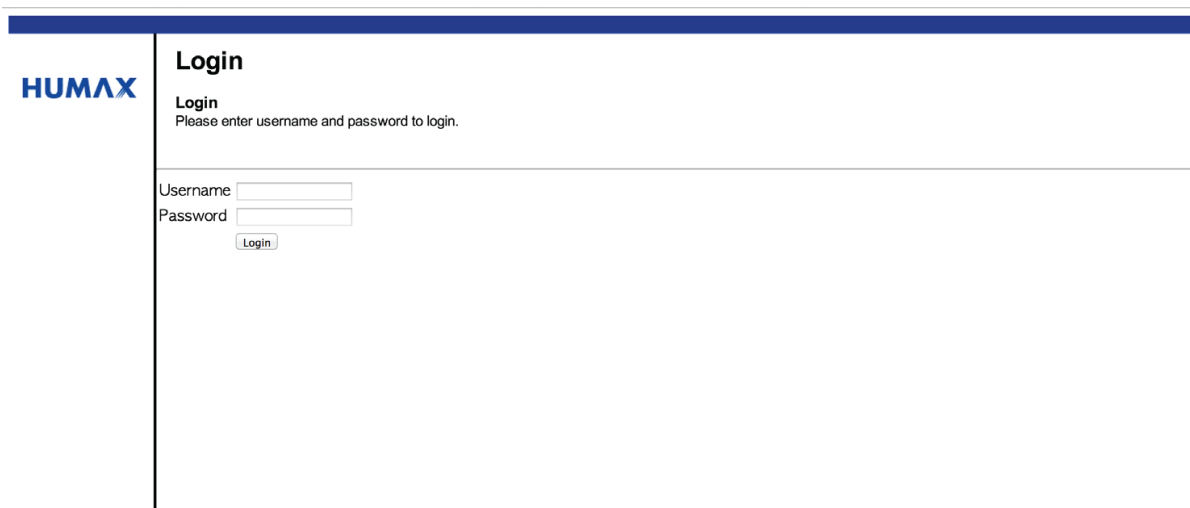
1. Se o seu provedor de serviço de internet não utilizar um servidor de DHCP - Protocolo de configuração dinâmica de host, você precisará:
 - O endereço de IP estático que é atribuído ao seu computador pelo seu ISP
 - A máscara de sub-rede que é automaticamente atribuída à sua WAN pelo seu ISP
 - O endereço de IP do gateway padrão
 - Os endereços de IP dos servidores DNS primário e secundário

2. Seu ISP pode exigir as seguintes informações:
 - O endereço MAC do modem a cabo
 - O endereço MAC do computador que está registrado com o ISP
 - O nome do host que está registrado com o ISP
 - O nome de domínio que é usado pelo seu ISP

Acesso ao Gateway Residencial

O endereço de IP do gateway residencial é 192.168.1.1 ou 192.168.100.1. Para configurar o gateway residencial, siga os passos abaixo.

1. Obtenha um endereço de IP a partir do servidor DHCP embutido para o seu computador para conectar o seu gateway residencial.
2. Abra o navegador (Internet Explorer, Chrome, Mozilla, etc.) no seu computador.
3. Digite o endereço de IP <http://192.168.0.1> ou <http://192.168.100.1> e, em seguida, a página de autenticação semelhante à ilustrada abaixo será exibida.



HUMANX

Login

Login
Please enter username and password to login.

Username

Password

©2013 HUMANX Co., Ltd.. All rights reserved.


Nota: O nome de usuário e a senha padrão são "admin" e "password".

Configuração Básica

Status ➔ [Conexão](#)

Após o login, a página de status da conexão será exibida conforme a ilustração abaixo. Você pode verificar as informações sobre o seu modem a cabo e conectividade de rede.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA
--------	-------	----------	----------	------------------	-----	----------	-----



Status

Connection

This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	507000000 Hz Locked	
Connectivity State	OK	Operational
Boot State		
Configuration File	OK	
Security	Disabled	Disabled

Downstream Bonded Channels

Channel	Lock	Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1			QAM256		507000000 Hz	18.9 dBmV	50.0 dB	0	0
2			QAM256		513000000 Hz	19.1 dBmV	49.9 dB	0	0
3			QAM256		519000000 Hz	19.3 dBmV	49.9 dB	0	0
4			QAM256		525000000 Hz	19.5 dBmV	49.9 dB	0	0
5			QAM256		531000000 Hz	19.5 dBmV	49.9 dB	0	0
6			QAM256		537000000 Hz	19.2 dBmV	49.9 dB	0	0
7			QAM256		543000000 Hz	18.7 dBmV	49.9 dB	0	0
8			QAM256		549000000 Hz	18.3 dBmV	49.8 dB	0	0

Total Correctables	Total Uncorrectables
0	0

Upstream Bonded Channels

Channel	Lock	Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1			ATDMA		2560 Ksym/sec	39600000 Hz	21.7 dBmV
2			ATDMA		2560 Ksym/sec	30000000 Hz	21.2 dBmV
3			ATDMA		2560 Ksym/sec	33200000 Hz	21.5 dBmV
4			ATDMA		2560 Ksym/sec	36400000 Hz	21.2 dBmV

CM IP Address	Duration	Expires
	D: -- H: -- M: -- S: --	-----:--:--

Current System Time: Wed Feb 12 17:32:38 2014

©2013 HUMAX Co., Ltd.. All rights reserved.

Nota: As informações nesta página podem ser alteradas a qualquer momento pela atualização do seu navegador.

Básica ➔ [Configuração](#)

Você pode configurar as funções básicas do gateway residencial e a conectividade de rede. Insira as informações necessárias nos campos para configurar o seu gateway residencial.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA	Log
--------	-------	----------	----------	------------------	-----	----------	-----	-----

HUMAX

Basic

Setup

This page allows you to configure the basic features of your residential gateway related to your ISP connection.

Network Configuration

LAN

IPv6 Address: Unspecified
 IPv6 Prefix: ::
 IPv4 Address: 192 . 168 . 0 . 1
 MAC Address: 00:30:0d:90:12:05

Interface/Prefix
 None Specified

WAN

IPv6 Address: fe80::230:dff:fe90:1203/64
 IPv4 Address: 20.20.20.105
 MAC Address: 00:30:0d:90:12:03
 Duration: D: 00 H: 01 M: 00 S: 00
 Expires: Wed Feb 12 18:28:01 2014
 IPv4 DNS Servers: 8.8.8.8
 IPv6 DNS Servers: None

WAN Connection Type:

Ipv4 MTU Size: (256-1500 octets, 0 = use default)

Spoofed MAC Address: : : : : :

©2013 HUMAX Co., Ltd.. All rights reserved.

LAN

- Endereço IPv6: Digite o endereço IPv6 do seu gateway residencial em sua LAN privada.
- Prefixo IPv6: Formato de endereço / comprimento pré-fixado
- Endereço IPv4: Digite o endereço IPv4 do seu gateway residencial em sua LAN privada.
- Endereço MAC: O endereço de controle de acesso de mídia exibe.

WAN

1. Selecione o tipo de conexão WAN.
 - DHCP: Digite o nome do host e o nome de domínio.
 - IP Estático: Digite as informações fornecidas pelo seu provedor de Internet para o endereço IP estático, máscara de IP estático, gateway padrão, DNS primário e DNS secundário.
2. Clique em Aplicar para salvar suas alterações. Neste ponto, o gateway residencial está configurado para utilização básica. Para conectar-se à Internet, siga os passos abaixo:
 - Ligue o gateway residencial e aguarde até que ele faça o registro no CMTS e obtenha um endereço de IP Internet roteável.
 - Obtenha uma concessão de IP do servidor DHCP interno para cada computador conectado ao gateway residencial.

Nota: A comunicação na LAN funciona independentemente de a conexão WAN fornecida pelo modem a cabo estar funcionando. No entanto, você não pode acessar a Internet até que a conexão WAN esteja habilitada e tenha um endereço de IP.

Inicialização Rápida

Mudanças de Configuração

Alguns ajustes de configuração são recuperados somente uma vez do armazenamento não volátil quando o gateway residencial for ligado pela primeira vez. Uma configuração dessas altera os parâmetros de endereço estático de IP WAN. Quaisquer alterações destes ajustes forçarão a reinicialização do gateway residencial de modo que a nova configuração possa ser lida do armazenamento não volátil.

Quando essa reinicialização for necessária, uma interface da web informará o seguinte:



The device has been reset...[RELOAD](#)

Simplesmente aguarde o gateway residencial reiniciar e clique no link RELOAD para inserir novamente a interface web onde você tiver feito sua última modificação. A maioria dos itens de configuração pode ser alterada em tempo real sem necessidade de reinicialização.

Várias páginas de status estão disponíveis no servidor da web para auxiliar na resolução de problemas que você experimentar com seu gateway residencial. Informações gerais sobre o gateway residencial são encontradas nas Páginas de Status do Software; informações de conectividade e resolução de problemas são encontradas nas Páginas de Conexão e Diagnóstico; e informações sobre reinicialização do modem segundo as configurações padrão de fábrica são encontradas na Página Segurança.

Status do Software

Status ➔ [Software](#)

Você pode verificar as informações sobre a versão do hardware, versão do software, endereço MAC, endereço IP do modem a cabo, número de série, sistema de backup e status de registro rede.

The screenshot shows the HUMANIX web interface. At the top, there is a navigation bar with tabs: Status (highlighted), Basic, Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMANIX logo and a list of menu items: Software (highlighted), Connection, Switch Mode, Password, Diagnostics, and Factory Defaults. The main content area is titled 'Status' and 'Software'. It contains the text: 'This page displays information on the current system software.' Below this, there are two sections: 'Information' and 'Status'. The 'Information' section contains a table with the following data:

Standard Specification Compliant	DOCSIS 3.0
Hardware Version	V1.0
Software Version	VER 1.0.1
Cable Modem MAC Address	00:30:0d:90:12:01
Cable Modem Serial Number	901201
CM certificate	Not Installed
EMTA Type	NCS

The 'Status' section contains a table with the following data:

System Up Time	0 days 00h:05m:32s
Network Access	Allowed
Cable Modem IP Address	-----

Status da Conexão

Status ➔ [Conexão](#)

Você pode verificar as informações sobre os canais RF upstream e downstream, inclusive as frequências downstream do canal, IDs de canal upstream e potência do sinal upstream e downstream, além de modulação. Você também pode verificar as informações de concessão de IP, incluindo o endereço IP atual do modem por cabo, a duração de ambas as concessões, o tempo de validade de ambas as concessões, e a hora atual do sistema do servidor de tempo DOCSIS.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA
--------	-------	----------	----------	------------------	-----	----------	-----

HUMAX

- Software
- Connection
- Switch Mode
- Password
- Diagnostics
- Factory Defaults

Status

Connection

This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	507000000 Hz Locked	
Connectivity State	OK	Operational
Boot State		
Configuration File	OK	
Security	Disabled	Disabled

Downstream Bonded Channels

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1		QAM256		507000000 Hz	18.9 dBmV	50.0 dB	0	0
2		QAM256		513000000 Hz	19.1 dBmV	49.9 dB	0	0
3		QAM256		519000000 Hz	19.3 dBmV	49.9 dB	0	0
4		QAM256		525000000 Hz	19.5 dBmV	49.9 dB	0	0
5		QAM256		531000000 Hz	19.5 dBmV	49.9 dB	0	0
6		QAM256		537000000 Hz	19.2 dBmV	49.9 dB	0	0
7		QAM256		543000000 Hz	18.7 dBmV	49.9 dB	0	0
8		QAM256		549000000 Hz	18.3 dBmV	49.8 dB	0	0

Total Correctables	Total Uncorrectables
0	0

Upstream Bonded Channels

Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1		ATDMA		2560 Ksym/sec	39600000 Hz	21.7 dBmV
2		ATDMA		2560 Ksym/sec	30000000 Hz	21.2 dBmV
3		ATDMA		2560 Ksym/sec	33200000 Hz	21.5 dBmV
4		ATDMA		2560 Ksym/sec	36400000 Hz	21.2 dBmV

CM IP Address	Duration	Expires
	D: -- H: -- M: -- S: --	-----

Current System Time: Wed Feb 12 17:32:38 2014

©2013 HUMAX Co., Ltd.. All rights reserved.

Nota: As informações desta página podem ser alteradas a qualquer tempo atualizando seu navegador.

Status

Status do Modo de Comutação

Status ➔ [Modo de Comutação](#)

Você pode definir o modo de comutação para configurar links Ethernet.

The screenshot shows the HUMANX web interface. At the top, there is a navigation bar with tabs: Status (highlighted), Basic, Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMANX logo and several menu items: Software, Connection, Switch Mode (highlighted), Password, Diagnostics, and Factory Defaults. The main content area is titled 'Status' and 'Switch Mode'. It contains the text 'This page displays switch mode.' and a dropdown menu for 'Switch Mode' currently set to 'IPv4+IPv6 Mode'. Below the dropdown is an 'Apply' button.

©2013 HUMANX Co., Ltd.. All rights reserved.

Modo Desabilitado: Opera em modo ponte

- Modo IPv4 Somente: Opera em modo NAT, quando utiliza o endereço IPv4
- Modo IPv6 Somente: Opera em modo NAT, quando utiliza o endereço IPv6
- Modo IPv4+IPv6: Opera em modo NAT, quando utiliza os endereços IPv4 e IPv6.
- Modo Legado RG IPv4: Opera em modo NAT, quando utiliza o endereço IPv4

Status de Segurança

Status ➔ [Senha](#)

Você pode definir os privilégios de acesso do administrador alterando sua senha.

- Para alterar a senha,
Primeiro insira um ID de usuário para alterar a senha atual. Insira uma nova senha e a nova senha novamente, e depois a senha atual. Clique em Aplicar para salvar as suas alterações.

The screenshot shows the HUMANIX web interface. At the top, there is a navigation bar with tabs: Status (highlighted), Basic, Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a vertical menu with buttons for Software, Connection, Switch Mode, Password (highlighted), Diagnostics, and Factory Defaults. The main content area is titled 'Status' and 'Password'. Below the title, it says 'This page allows you to configure the login password.' There are four input fields: 'Password Change User ID', 'New Password', 'Re-Enter New Password', and 'Current User ID Password'. An 'Apply' button is located below the 'Current User ID Password' field.

©2013 HUMANIX Co., Ltd.. All rights reserved.

Nota: O nome de usuário e a senha padrão são "admin" e "password".

Status de Diagnóstico

Status ➔ Diagnóstico

A resolução de problemas de conectividade pode ser acessada visualizando a página Diagnóstico, exibida abaixo. Duas ferramentas são disponibilizadas para a solução de problemas de conectividade de rede:

- Ping: Você pode verificar a conectividade entre o gateway residencial e os dispositivos da rede local.
- Traceroute: Você pode mapear o caminho de rede do gateway residencial para um host público, permitindo controles alternativos para ferramenta *traceroute*.

Status

Diagnostics

This page displays information on the status of the cable modem's HFC and IP network connectivity.

Utility: Ping

Ping Test Parameters

Target:

Ping Size: 64 bytes

No. of Pings: 3

Ping Interval: 1000 ms

Start Test Abort Test Clear Results

Results
Waiting for input...

©2013 HUMAX Co., Ltd.. All rights reserved.

Nota: Para rodar qualquer ferramenta, faça quaisquer mudanças nos parâmetros padronizados e selecione a opção Iniciar Teste. A janela será automaticamente atualizada à medida que os resultados forem exibidos na tabela de Resultados.

Status ➔ [Configurações Padronizadas de Fábrica](#)

Você pode restaurar as configurações padronizadas de fábrica de seu gateway residencial.

- Para restaurar as configurações de fábrica, Selecione Sim para Restaurar as Configurações de Fábrica e clique em Aplicar.

The screenshot shows the HUMANX web interface. At the top, there is a navigation bar with tabs: Status (highlighted), Basic, Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a vertical menu with buttons for Software, Connection, Switch Mode, Password, Diagnostics, and Factory Defaults (highlighted). The main content area is titled 'Status' and 'Factory Defaults'. It contains the text: 'This page allows you to reset configuration as factory defaults.' Below this, there is a form with the label 'Restore Factory Defaults' and two radio buttons: 'Yes' and 'No' (selected). An 'Apply' button is located below the radio buttons.

©2013 HUMANX Co., Ltd.. All rights reserved.

Advertência: Uma vez restauradas as configurações padronizadas de fábrica, todos os dados do usuário serão cancelados.

Embora você possa configurar seu gateway residencial seguindo a seção Inicialização Rápida, você pode configurar mais funções avançadas, como segue:

- Configuração de seu Servidor DHCP para mudar para a configuração LAN padronizada ou permitir que concessões sejam provisionadas por um servidor DHCP separado na LAN
- Suporte do Sistema de Nome de Domínio Dinâmico (DDNS)
- Back-up e restauração dos ajustes de configuração

Configuração de Servidor DHCP

Básica ➔ **DHCP**

Você pode mudar a configuração do servidor DHCP.

Se você tiver o próprio servidor DHCP atendendo o lado LAN (ou escolha definir por código resistente todos os endereços IP de seus computadores), desabilite o servidor interno DHCP selecionando Não para o Servidor DHCP. Fazendo isso, você garante que o endereço IP atribuído a seu gateway residencial seja o mesmo na sub-rede externa que o servidor DHCP externo (a máscara de sub-rede é sempre 255.255.255.0) ou você não conseguirá acessar o gateway residencial em LAN. Você pode configurar o endereço IP do Gateway residencial na página de Configurações Básicas.

Você também pode programar o endereço IP para que as concessões IP disponíveis em LAN e mudando o número de computadores suportado pela LAN. No caso acima, os endereços 192.168.1.33 a 192.168.1.64 podem ser utilizados como endereços IP resistentes, sem medo de que o endereço IP conflite com o pool DHCP. Os endereços configurados do servidor WINS também podem ser passados para CPEs depois do gateway residencial, via DHCP.

Status Basic Advanced Firewall Parental Control VPN Wireless MTA Logout

HUMANIX

Basic

DHCP

This page allows you to configure the status of the optional internal DHCP server for the LAN.

DHCP Server Yes No

Starting Local Address

Number of CPEs

Lease Time

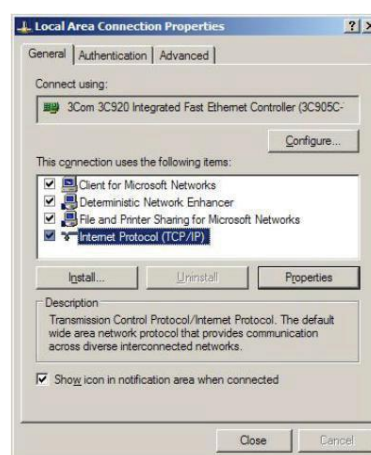
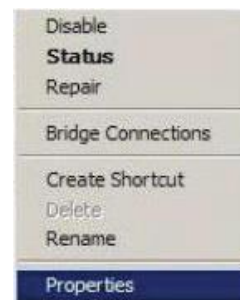
DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
0026b9c7a1ea	192.168.0.010	255.255.255.000	D:00 H:01 M:00 S:00	Wed Feb 12 18:28:29 2014	<input type="radio"/>

Current System Time: Wed Feb 12 17:34:13 2014

Como codificar o endereço IP do seu Computador

1. Para codificar um endereço IP resistente em seu computador no Microsoft Windows XP, por exemplo, vá para Meus Locais de Rede, clique com o botão direito e selecione Propriedades.
2. A janela Conexões de Rede aparecerá mostrando todos os adaptadores de rede disponíveis do seu Computador. Clique com o botão direito no adaptador habilitado que você conectou ao gateway residencial e selecione Propriedades.
3. Depois de selecionar Propriedades, a janela de Propriedades de Conexão de LAN para aquela Interface de Rede abrirá, conforme indicado à direita.
4. Selecione Protocolo de Internet (TCP/IP) para o adaptador e clique no botão Propriedades. Isso abrirá a janela de Propriedades de TCP/IP para aquela Interface de Rede que você está configurando.
5. Se Obter um endereço de IP automaticamente estiver selecionado, então o DHCP estará ativado. Para codificar o seu adaptador de rede, selecione Utilizar o seguinte endereço de IP e digite o endereço apropriado. Neste exemplo, o Computador recebeu o código resistente 192.168.1.35. A máscara de sub-rede deve ser sempre 255.255.255.0, o gateway de Internet padrão deve ser sempre 192.168.0.1 (ou o lado privado da LAN do gateway residencial), e o servidor de DNS também é 8.8.8.8. Clique em OK e seu Computador terá agora um código resistente, devendo ser capaz de acessar a Internet sem a necessidade contar com o servidor DHCP interno para lhe fornecer um endereço.



Configuração Básica

Protocolo de Configuração de Hospedagem Dinâmica para IPv6 (DHCPv6)

Básica ➔ [DHCPv6](#)

DHCPv6 é um protocolo de rede que é utilizado para configurar hosts IPv6 com endereços de IP, prefixos de IP e/ou outra configuração necessária para operar em uma rede IPv6.

Você pode configurar uma chave pré-partilhada configurada entre o servidor DHCP e o cliente DHCP.

The screenshot shows the HUMANIX web interface for DHCPv6 configuration. The top navigation bar includes Status, Basic (selected), Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. The left sidebar contains buttons for Setup, DHCP, DHCPv6 (highlighted), LAN IPv6, DDNS, and Backup. The main content area is titled 'Basic' and 'DhcpV6'. It includes a description: 'This page allows configuration of the internal DhcpV6 server for the LAN. When modifying the System Delegated Prefix, set the System Delegated Prefix first, and press Apply so that the system can calculate its LAN Delegated Prefix.' Below this are input fields for 'System Delegated Prefix' and a checkbox for 'User defined prefix'. The 'Server Settings' section includes a note: 'LAN Delegated Prefix will be derived from System Delegated Prefix and Start Address will have the same prefix as the LAN Delegated Prefix.' It features a checked 'Enabled' checkbox, input fields for 'LAN Delegated Prefix' and 'Start Address', a 'Number of addresses' field set to 255, a 'Valid Lifetime' field set to 60, and checkboxes for 'Enable Rapid Commit' (checked) and 'Enable Unicast'. 'Apply' and 'Restore DhcpV6 Defaults' buttons are at the bottom.

©2013 HUMANIX Co., Ltd.. All rights reserved.

Rede de Área Local para IPv6 (LAN IPv6)

Básica ➔ [LAN IPv6](#)

Você pode ver as informações sobre a autoconfiguração IPv6 sem status.

The screenshot shows the HUMANIX web interface for LAN IPv6 configuration. The top navigation bar is the same as the previous page. The left sidebar highlights the 'LAN IPv6' button. The main content area is titled 'Basic' and 'LAN IPv6'. It includes a description: 'This page displays information related to IPv6 on the LAN.' Below this is the 'Stateless Auto Configuration' section, which contains a table with columns for 'IP Address', 'MAC Address', and 'Reachability State'. The table is currently empty.

©2013 HUMANIX Co., Ltd.. All rights reserved.

Suporte ao DNS dinâmico

Básico ➔ **DDNS**

DNS dinâmico (DDNS) permite que um endereço IP dinâmico receba um nome de host estático, pré-definido, de forma que o host possa ser facilmente contatado por outros hosts na Internet mesmo que o endereço IP mude. O gateway residencial suporta um cliente DNS dinâmico compatível com o Serviço DNS Dinâmico (<http://www.dyndns.com/>).

The screenshot shows the HUMANX router's configuration interface. At the top, there is a navigation bar with tabs: Status, Basic (selected), Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMANX logo and several menu items: Setup, DHCP, DHCPv6, LAN IPv6, DDNS (highlighted in yellow), and Backup. The main content area is titled 'Basic' and 'DDNS'. It contains a description: 'This page allows you to configure the status of the optional internal DHCP server for the LAN.' Below this, there are several fields: 'DDNS Service:' with a dropdown menu set to 'Disabled', 'User Name:', 'Password:', and 'Host Name:' (all with empty input boxes). The 'IP Address:' is set to '20.20.20.105'. The 'Status:' is 'DDNS service is not enabled.' There is an 'Apply' button at the bottom of the form.

©2013 HUMANX Co., Ltd.. All rights reserved.

Como ativar o Cliente DNS

1. Vá para <http://www.dyndns.com> e crie uma conta para o Serviço DNS Dinâmico.
 - Conecte-se a DynDNS com o número de usuário e senha
 - Vá para Minha Conta > Meus Serviços > Acrescentar Serviços de Host
 - Digite o nome do host de seu servidor e selecione o domínio DNS dinâmico para atribuir a seu host
 - Verifique o intervalo para a nova tentativa em que o gateway residencial tentar repetidos contatos com o servidor do nome de domínio.
 - Verifique o endereço IP atual de seu host. Este é o endereço IP WAN que foi designado a seu CMG durante o provisionamento (Ver o endereço IP Wan no Menu Básico / Configuração).
2. Na página DDNS, selecione www.DynDNS.org na lista de Serviços DDNS para habilitar o serviço, insira as informações de sua conta e clique em Aplicar.
3. O Cliente DDNS notificará o serviço DDNS sempre que o endereço IP WAN mudar, de forma que o nome escolhido para o seu host será resolvido adequadamente pelos hosts que o consultarem.

Backup/Restauração de Configurações

Básico ➔ [Backup](#)

Você pode salvar as configurações atuais do gateway residencial em um computador local. Mais tarde, se precisar, você poderá restaurar uma configuração específica ou recuperar alterações que tenham gerado um efeito indesejável.

The screenshot shows the HUMAX web interface. At the top, there is a navigation bar with tabs: Status, Basic (selected), Advanced, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMAX logo and a list of menu items: Setup, DHCP, DHCPv6, LAN IPv6, DDNS, and Backup (highlighted in yellow). The main content area is titled 'Basic' and 'Backup/Restore Settings'. It contains the text: 'This page allows you to save your current settings locally on your PC or restore the settings previously saved.' Below this text, there is a file selection interface with a 'Choose File' button, the text 'No file chosen', and 'Restore' and 'Backup' buttons.

©2013 HUMAX Co., Ltd.. All rights reserved.

Para fazer o backup da configuração atual, clique em Salvar e siga o processo.

Para restaurar a configuração anterior, clique em Escolher Arquivo e utilize a janela de navegação para localizar o arquivo. (Normalmente GatewaySettings.bin, a menos que você mude o nome antes de salvar). Assim que o arquivo for localizado, clique em Restaurar para restaurar as configurações.

Nota: Assim que as configurações forem restauradas, o gateway residencial será reinicializado.

O gateway residencial suporta recursos avançados adicionais, conforme segue:

- Suporta bloqueio opcional de WAN, passagem de IPSec, passagem de PPTP, administração remota e habilitação de modos multicast
- Filtro de endereço de IP de LAN, endereço MAC e número de porta
- Encaminhamento e ativação de WAN para LAN
- Suporta hospedagem DMZ (ou host exposto)
- Habilita o modo de operação

Modos Opcionais

Avançado ➔ [Opções](#)

Você pode operar o seu gateway residencial em vários modos que ajustam a forma como as rotas de IP do dispositivo trafegam.

HUMANX **Advanced**

Options

This page allows you to configure the advanced features of the residential gateway.

WAN Blocking	<input checked="" type="checkbox"/> Enable
Ipsec PassThrough	<input type="checkbox"/> Enable
PPTP PassThrough	<input type="checkbox"/> Enable
Remote Config Management	<input checked="" type="checkbox"/> Enable
Multicast Enable	<input checked="" type="checkbox"/> Enable
UPnP Enable	<input type="checkbox"/> Enable
NAT ALG Status	
RSVP	<input checked="" type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable
Kerb88	<input checked="" type="checkbox"/> Enable
NetBios	<input checked="" type="checkbox"/> Enable
IKE	<input checked="" type="checkbox"/> Enable
RTSP	<input checked="" type="checkbox"/> Enable
Kerb1293	<input checked="" type="checkbox"/> Enable
H225	<input checked="" type="checkbox"/> Enable
PPTP	<input checked="" type="checkbox"/> Enable
MSN	<input checked="" type="checkbox"/> Enable
SIP	<input checked="" type="checkbox"/> Enable
ICQ	<input checked="" type="checkbox"/> Enable
IRC666x	<input checked="" type="checkbox"/> Enable
ICQTalk	<input checked="" type="checkbox"/> Enable
Net2Phone	<input checked="" type="checkbox"/> Enable
IRC7000	<input checked="" type="checkbox"/> Enable
IRC8000	<input checked="" type="checkbox"/> Enable

PassThrough Mac Addresses (example: 01:23:45:67:89:AB)

Addresses entered: 0/32

- Bloqueio WAN impede que o gateway residencial ou os Computadores a ele conectados fiquem visíveis na WAN. Por exemplo, os pings para o endereço IP WAN do gateway residencial ou os Computadores por detrás dele não são devolvidos. Portanto, será mais difícil para hackers descobrir seu endereço de IP da WAN para iniciar um ataque à sua LAN privada.
- Passagem IpSec e Passagem PPTP permitem que esses protocolos sejam utilizados por meio do gateway residencial, de tal forma que um dispositivo VPN ou software possa comunicar-se adequadamente com a WAN.

Configuração Avançada

- Passagem IpSec e Passagem PPTP permitem a utilização desses protocolos através do gateway residencial de tal forma que um dispositivo VPN ou software possa se comunicar adequadamente com a WAN.
- Gerenciamento de Configuração Remota permite que o gateway residencial seja gerenciado (configurado) pela WAN surfando para o endereço IP WAN na porta 8080 do gateway de qualquer lugar na Internet (p/ ex. na janela do browser URL, entrar em <http://WanIPAddress:8080/> para acessar o gateway residencial remotamente).
- Habilitar Multicast permite o tráfego multicast específico (indicado por um endereço multicast específico) para ser passado de e para o computador na rede privada por detrás do gateway residencial .
- Habilitar UPnP habilita o agente UPnP no gateway residencial . Se você estiver rodando um aplicativo CPE que requer UPnP, marque essa caixa.

Para ativar um recurso, clique na caixa de seleção e, em seguida Aplicar. Estas características são alteradas sem reinicializar o sistema.

Filtros

Avançado ➔ [Filtro de IP](#)

Você pode configurar o gateway residencial para evitar que computadores locais tenham acesso à WAN, especificando os endereços IP que devem ser filtrados.

HUMAX

Advanced

IP Filtering

This page allows you to configure the IP address filtering to block access to specific network devices on the LAN.

Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Apply

©2013 HUMAX Co., Ltd.. All rights reserved.

- Insira as faixas de endereço IP iniciais e finais para configurar os computadores locais que não terão acesso à WAN.

Nota: Insira o LSB (Byte menos significativo) do endereço de IP. Os bytes superiores do endereço IP são ajustados automaticamente do endereço IP do gateway residencial.

Para ativar o filtro de endereço IP, selecione Habilitado e, em seguida, clique em Aplicar.

Avançado ➔ [Filtro MAC](#)

Você pode impedir que computadores enviem tráfego TCP / UDP de saída para a WAN por meio de seu endereço MAC.

The screenshot shows the HUMANX web interface. At the top, there is a navigation bar with tabs: Status, Basic, **Advanced**, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMANX logo and a list of menu items: Options, IP Filtering, **MAC Filtering**, Port Filtering, Forwarding, Port Triggers, and DMZ Host. The main content area is titled "Advanced" and "MAC Filtering". It contains the following text: "This page allows you to configure the MAC address filtering to block access to specific network devices on the LAN. This configuration is applied to IPv4 only." Below this text, there is a section for "MAC Addresses (example: 01:23:45:67:89:AB)". It features a text input field, an "Add MAC Address" button, a list area (currently empty), and a "Remove MAC Address" button. At the bottom right of this section, it says "Addresses entered: 0/20" and there is a "Clear All" button. At the very bottom of the page, there is a copyright notice: "©2013 HUMANX Co., Ltd.. All rights reserved."

Isto é útil pelo fato de que o endereço MAC de uma placa NIC específica nunca muda, ao contrário de seu endereço IP, que pode ser atribuído através de um servidor DHCP ou codificado em forma resistente para vários endereços ao longo do tempo.

Avançado ➔ [Filtro de Porta](#)

Você pode impedir que computadores enviem tráfego TCP / UDP de saída para a WAN em números IP específicos de portas.

The screenshot shows the HUMANX web interface. At the top, there is a navigation bar with tabs: Status, Basic, **Advanced**, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. Below this, the 'Advanced' section is active, displaying 'Port Filtering'. A sidebar on the left contains several menu items: Options, IP Filtering, MAC Filtering, **Port Filtering**, Forwarding, Port Triggers, and DMZ Host. The main content area has the title 'Advanced Port Filtering' and a description: 'This page allows you to configure the port filtering to block access to specific network devices on the LAN.' Below the description is a table with the following structure:

Port Filtering			
Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Below the table is an 'Apply' button.

©2013 HUMANX Co., Ltd.. All rights reserved.

- Introduza um intervalo de porta inicial e final para determinar qual o tráfego TCP / UDP permitido para a WAN por porta.
Por exemplo, se você quiser bloquear o acesso de todos os computadores da LAN privada a sites HTTP (ou de “surfando na rede”), você pode configurar a Porta Inicial em 80, a Porta Final em 80, o Protocolo de TCP, selecionar Habilitado e clicar em Aplicar.
- Nota:* Os intervalos de portas especificados são bloqueados para todos os computadores e esta definição não é o endereço IP ou o endereço MAC específico.

Envio por Porta

Avançado ➔ Envio

Você pode rodar um servidor publicamente acessível na LAN especificando o mapeamento de portas TCP / UDP para um computador local.

Application Port

HTTP	80
FTP	21
TFTP	69
SMTP	25
POPS	110
NNTP	119
Telnet	23
IRC	194
SNMP	161
Finger	79
Gopher	70
Whois	43
rlogin	107
LDAP	389
UUCP	540

©2013 HUMANX Co., Ltd.. All rights reserved.

- Para especificar um mapeamento, digite o intervalo de números de portas que devem ser encaminhados localmente, e o endereço de IP para o qual o tráfego para essas portas deve ser enviado. Uma tabela de números de Porta normalmente utilizadas é fornecida na página para sua conveniência.

Nota: Se você quer apenas uma única especificação de porta, digite o mesmo número de porta nos locais de início e fim daquele endereço IP.

- Se ambos os números das portas externas e locais / internas estiverem presentes, o número da porta Local é um campo obrigatório e o número da porta externa é opcional. Se o número da porta externa for utilizado, o gateway residencial traduzirá o número da porta externa para o número da porta interna.

Ativação da Porta

Avançada ➔ [Ativações da Porta](#)

A Ativação da Porta é similar ao Envio pela Porta, exceto pelo fato de que não são portas estáticas mantidas abertas todo o tempo. Quando o gateway residencial detectar dados de saída em um número de porta de IP específico configurado na Faixa de Ativação, as portas resultantes configuradas na Faixa-Alvo são abertas para dos que chegam (ou às vezes denominadas portas bidirecionais). Se nenhum tráfego de saída for detectado nas portas da Faixa de Ativação or 10 minutos, as portas da Faixa-Alvo se encerrarão. Este é o método para a abertura de portas específicas para aplicações especiais (p/ ex. programas de videoconferência, jogos interativos, transferência de arquivos em programas de chat, etc.) pois elas são ativadas dinamicamente, não sendo mantidas constantemente abertas nem deixadas abertas por equívoco por um administrador de roteador e expostas para que potenciais hackers as descubram.

The screenshot shows the 'Advanced' configuration page for 'Port Triggers'. The navigation bar at the top includes: Status, Basic, **Advanced**, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left, a sidebar contains buttons for: Options, IP Filtering, MAC Filtering, Port Filtering, Forwarding, **Port Triggers**, and DMZ Host. The main content area is titled 'Advanced Port Triggers' and contains the following text: 'This page allows you to configure dynamic triggers to the specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messenger program features may require these special settings.' Below the text is a 'Create' button and a table with the following structure:

Trigger		Target		Prot	Description	Enabled	Remove All
Start Port	End Port	Start Port	End Port				

DMZ Hosting

Avançada ➔ [Host DMZ](#)

Hosting em DMZ (Zona desmilitarizada) (também referida geralmente como "host exposto") permite que você especifique o destinatário padrão de tráfego WAN que o NAT não é capaz de traduzir para um computador local conhecido. Isto também pode ser descrito como um computador ou uma pequena sub-rede que fica entre a LAN interna privada confiável e a Internet pública não confiável.

The screenshot shows the HUMANX web interface. At the top, there is a navigation bar with tabs: Status, Basic, **Advanced**, Firewall, Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMANX logo and a list of menu items: Options, IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers, and **DMZ Host**. The main content area is titled "Advanced" and "DMZ Host". It contains the following text: "This page allows you to configure a specific network device to be exposed directly to the WAN. This may be used when problem applications do not work with port triggers. If there are no exposed hosts, enter 0." Below this text is a form field for "DMZ Address" with the value "192.168.0.0" and an "Apply" button.

©2013 HUMANX Co., Ltd.. All rights reserved.

Você pode configurar um computador para ser o host DMZ. Essa configuração é geralmente utilizada para computadores que utilizam números de portas aleatórios e não funcionam corretamente com ativações específicas de portas ou configurações de envio por porta mencionados anteriormente. Se um computador específico é configurado como um host DMZ, lembre-se de definir a configuração de volta a 0 quando encerrada a aplicação necessária, uma vez que este computador ficará efetivamente exposto à Internet pública, embora ainda protegido contra ataques de Recusa de Serviço por meio do firewall.

O gateway residencial contém uma aplicação embutida de firewall para proteger a LAN privada contra ataques mal-intencionados (DoS, etc.) da interface WAN. Os filtros de conteúdo e os filtros de SPAM também estão incluídos para permitir controle dos pais acionado manualmente.

Configuração Básica

Firewall ➔ [Básica](#)

A página de Filtro da Web tem diversas configurações relacionadas ao bloqueio ou exclusivamente à permissão de diferentes tipos de dados por meio do gateway residencial da WAN para a LAN.

The screenshot shows the HUMANIX Firewall configuration interface. At the top, there is a navigation bar with tabs: Status, Basic, Advanced, Firewall (highlighted), Parental Control, VPN, Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMANIX logo and three buttons: Basic (highlighted), Local Log, and Remote Log. The main content area is titled "Firewall" and "Basic". It contains a descriptive paragraph: "This page allows you to configure the firewall. It is highly recommended that the firewall is enabled at all times for protection against the denial of service attacks." Below this, there are several configuration options: "IPv4 Firewall Protection" set to "Off", "IPv6 Firewall Protection" set to "On", "Block Fragmented IP Packets" with an "Enable" checkbox, "Port Scan Detection" with an "Enable" checkbox, and "IP Flood Detection" with an "Enable" checkbox. To the right of these options is a box titled "Allowed Services" containing the text "No Ports Restricted". At the bottom of the configuration area is an "Apply" button.

©2013 HUMANIX Co., Ltd.. All rights reserved.

Proteção de Firewall

Você pode ajustar as opções de proteção de firewall.

- Baixa não bloqueia nenhum serviço/porta, porém protege contra pacotes inválidos e ataques conhecidos.
- Média pode fazer o firewall derrubar um pacote, a menos que seja uma porta específica de serviços permitidos. Os serviços permitidos estão listados na mesma página.
- Alta é semelhante à Média, porém permite o acesso a um número ainda menor de serviços.
- Desligado permite que todo o tráfego passe.

Bloqueio de Pacotes de IP Fragmentados

Você pode assinalar Habilitar para impedir todos os pacotes de IP fragmentados de passar pelo firewall.

Deteção por Escaneamento de Porta

Você pode assinalar Habilitar para detectar e bloquear a atividade de escaneamento da porta proveniente tanto de LAN como de WAN.

Deteção de Invasões de IPs

Você pode assinalar Habilitar para fazer o firewall detector os ataques na forma de invasão de IPs.

Log de Eventos Locais

Firewall ➔ [Log Local](#)

O Log Local pode enviar relatórios de ataque a firewall de duas formas diferentes.

Os E-mails Individuais podem ser enviados automaticamente, a cada vez que o firewall estiver sob ataque, e também um log de evento local estiver armazenado no modem e for exibido no formulário da tabela na página de Log de Eventos Locais.

Para habilitar os alertas automáticos de E-mails:

- Inserir seu endereço de E-mail.
- Inserir o endereço do servidor de mensagens SMTP (Saída) associado à conta de e-mail e as credenciais de autenticação, se exigido (disponibilizado por seu ISP),
- Clicar em Habilitado e então clicar em Aplicar.

Os E-mails Individuais serão agora enviados ao endereço especificado cada vez que um ataque for detectado. Cada ataque também é registrado na tabela da página de Log de Eventos. Se desejado, um resumo da Tabela de Log de Eventos pode ser enviada ao endereço de contato de E-mail especificado clicando na tecla de Log de E-Mail. O clique na tecla Limpar Log também pode limpar a tabela.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA	Logout										
HUMAX																		
Firewall																		
Local Log																		
This page allows you to configure the firewall event log which is reported via Email or on the local log page.																		
Contact Email Address <input type="text"/>																		
SMTP Server Name <input type="text"/>																		
SMTP Username <input type="text"/>																		
SMTP Password <input type="password"/>																		
E-mail Alerts <input type="checkbox"/> <i>Enable</i>																		
<input type="button" value="Apply"/>																		
<table border="1"><thead><tr><th>Description</th><th>Count</th><th>Last Occurrence</th><th>Target</th><th>Source</th></tr></thead><tbody><tr><td colspan="5"><input type="button" value="E-mail Log"/> <input type="button" value="Clear Log"/></td></tr></tbody></table>									Description	Count	Last Occurrence	Target	Source	<input type="button" value="E-mail Log"/> <input type="button" value="Clear Log"/>				
Description	Count	Last Occurrence	Target	Source														
<input type="button" value="E-mail Log"/> <input type="button" value="Clear Log"/>																		

Log de Eventos Remotos

Firewall ➔ [Log Remoto](#)

O Log Remoto pode enviar diferentes relatórios de ataques para um servidor SysLog padronizado de forma que muitas instâncias possam estar logadas ao longo de um período de tempo extenso. Você pode selecionar ataque individual ou itens de configuração para enviar ao servidor SysLog, de forma que somente os itens de interesse possam ser monitorados. Você pode fazer o log com as conexões permitidas, com as conexões bloqueadas, tipos de ataque de Internet conhecidos e eventos de configuração do gateway residencial. O servidor SysLog deve estar na mesma rede que a LAN privada, atrás do gateway residencial (normalmente 192.168.0.x). Para ativar a função de monitoramento SysLog, verifique todos os tipos de eventos que deseja monitorar e insira o último byte do endereço IP do servidor SysLog. Normalmente, o endereço IP deste servidor SysLog deve ter codificação resistente, de forma que o endereço não se altera e sempre confere com a inserção nesta página.

©2013 HUMANX Co., Ltd.. All rights reserved.

Uma lista completa dos tipos passíveis de ataque/notificação Sys/Log a servidor e seu formato está abaixo. O formato genérico das mensagens sysLog para tráfego ou eventos relacionados à administração é:

```
MMM DD HH:MM:SS YYYY SYSLOG[0]: [Host HostIP] Protocol SourceIP,SourcePort
--> DestIP, DestPort EventText
```

Onde:

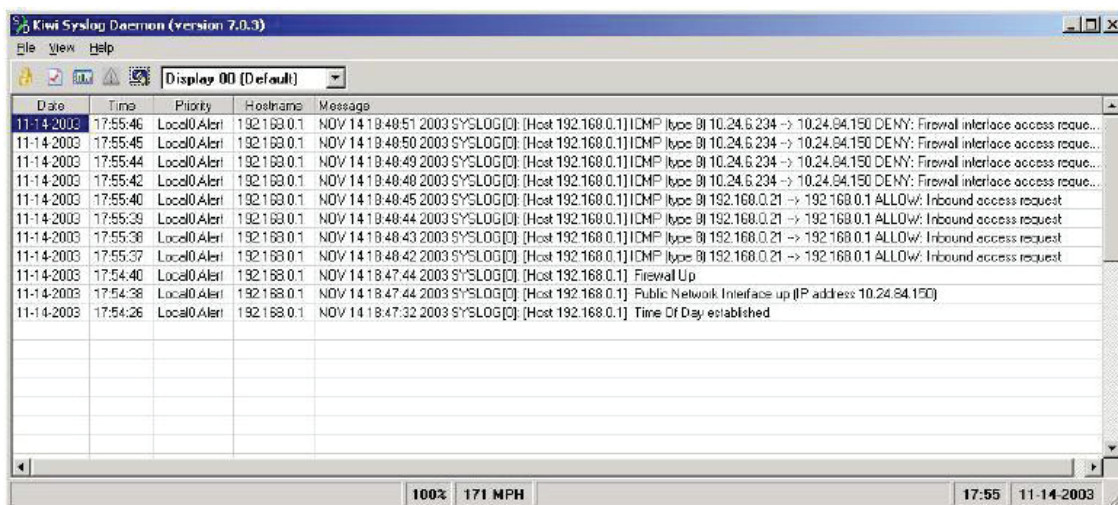
- MMM é a forma abreviada de três letras para o mês (p/ ex., JUN, JUL AGO, etc.)
- DD é a forma de representação do dia do mês, com dois dígitos (p/ ex. 01, 02, 03, etc.)
- HH:MM:SS é a hora exibida em valores de dois dígitos para a hora, minuto e segundo, respectivamente
- YYYY é o ano, com quatro dígitos
- HostIP é o endereço IP do RGCM que envia o evento SysLog. Este é um Endereço IP LAN na página web da Configuração Básica.
- Protocolo é um dos seguintes: "TCP", "UDP", "ICMP", "IGMP" ou "OUTROS". No caso de "OUTROS", o tipo de protocolo é exibido entre parênteses (). Para os pacotes ICMP, o tipo ICMP é exibido entre parênteses.
- SourceIP é o endereço IP do originador da sessão/pacote.
- SourcePort é a porta de origem no originador.
- DestIP é o endereço IP do destinatário da sessão/pacote.
- DestPort é a porta de destino no destinatário.
- EventText é uma descrição textual do evento.

Firewall

O formato das mensagens SysLog para eventos informativos é simplificado:

MMM DD HH:MM:SS YYYY SYSLOG[0]: [Host HostIP] EventText

A ilustração abaixo mostra um exemplo de captura de tela dos SysLogs recebidos por um Servidor.



The screenshot shows the Kiwi Syslog Daemon interface with a table of log entries. The table has columns for Date, Time, Priority, Hostname, and Message. The messages include ICMP deny and allow events, firewall status changes, and network interface events.

Date	Time	Priority	Hostname	Message
11-14-2003	17:55:46	Local0.Alert	192.168.0.1	NOV 14 18:49:51 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 10.24.6.234 -> 10.24.64.150 DENY: Firewall interface access request
11-14-2003	17:55:45	Local0.Alert	192.168.0.1	NOV 14 18:49:50 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 10.24.6.234 -> 10.24.64.150 DENY: Firewall interface access request
11-14-2003	17:55:44	Local0.Alert	192.168.0.1	NOV 14 18:49:49 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 10.24.6.234 -> 10.24.64.150 DENY: Firewall interface access request
11-14-2003	17:55:42	Local0.Alert	192.168.0.1	NOV 14 18:49:48 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 10.24.6.234 -> 10.24.64.150 DENY: Firewall interface access request
11-14-2003	17:55:40	Local0.Alert	192.168.0.1	NOV 14 18:49:45 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 192.168.0.21 -> 192.168.0.1 ALLOW: Inbound access request
11-14-2003	17:55:39	Local0.Alert	192.168.0.1	NOV 14 18:49:43 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 192.168.0.21 -> 192.168.0.1 ALLOW: Inbound access request
11-14-2003	17:55:38	Local0.Alert	192.168.0.1	NOV 14 18:48:42 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 192.168.0.21 -> 192.168.0.1 ALLOW: Inbound access request
11-14-2003	17:55:37	Local0.Alert	192.168.0.1	NOV 14 18:48:42 2003 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 8) 192.168.0.21 -> 192.168.0.1 ALLOW: Inbound access request
11-14-2003	17:54:40	Local0.Alert	192.168.0.1	NOV 14 18:47:44 2003 SYSLOG[0]: [Host 192.168.0.1] Firewall Up
11-14-2003	17:54:38	Local0.Alert	192.168.0.1	NOV 14 18:47:44 2003 SYSLOG[0]: [Host 192.168.0.1] Public Network Interface up (IP address: 10.24.64.150)
11-14-2003	17:54:26	Local0.Alert	192.168.0.1	NOV 14 18:47:32 2003 SYSLOG[0]: [Host 192.168.0.1] Time Of Day established

Configuração de Usuário


Controle dos Pais ➔ [Configuração de Usuário](#)

Você pode realizar as configurações de usuário. A opção 'Somente Lista Escrita' limita o usuário à visita somente aos sites especificados na Lista de Domínios Permitida de sua regra de conteúdo.

A Página de Configuração do Usuário de Controle dos Pais é a página máster à qual cada usuário individual é conectado em uma regra de acesso por um período de tempo especificado, regra de filtro de conteúdo e senha de login para chegar ao conteúdo filtrado. Cada usuário especificado também pode ser habilitado como usuário de confiança, o que significa que aquela pessoa terá acesso a todo o conteúdo da Internet, independentemente dos filtros que possam ter sido configurados. Esta caixa de verificação poderá ser utilizada como uma desabilitação simples para garantir ao usuário acesso integral, porém ainda terá a capacidade de manter as configurações anteriores de filtragem armazenadas e disponíveis. Os cronômetros de duração da sessão podem também ser programados para permitir um período de tempo finito durante o qual um usuário tem acesso à Internet por meio das regras lançadas uma vez que tenham inserido sua senha para acessar a internet pela primeira vez.

Isto permite o acesso à Internet por um usuário definido sem a necessidade de inserir uma senha toda vez que uma nova página da web é oferecida ao cliente. De forma correspondente, existe um cronômetro de inatividade da senha se não houver acesso à internet pelo tempo especificado em minutos, exigindo que o usuário faça um novo login no fim da sessão para continuar utilizando a Internet. Esses logins cronometrados garantem que um usuário específico esteja utilizando o gateway da Internet para acesso, e a conexão/acesso sejam disponibilizados adequadamente. Se a qualquer momento uma mudança for efetuada nessa página para um usuário específico, clique Aplicar para ativar e armazenar as configurações.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	M
--------	-------	----------	----------	------------------	-----	----------	---



Parental Control

User Setup

This page allows you to configure a specific user allowing the content policy and the time access policy. In white list only, you can set a user to visit a specific site which is allowed according to the user's content rule.

User Configuration

User Settings

1. Default Enable

Password:

Re-Enter Password:

Trusted User: Enable

Content Rule: White List Access Only 1. Default

Time Access Rule:

Session Duration: 0 min

Inactivity time: 0 min

Trusted Computers

Optionally, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer.

00 : 00 : 00 : 00 : 00 : 00

No Trusted Computers

Configuração de Usuário

- Clique em Acrescentar Usuário para configurar os controles para um usuário específico.

Configurações de Usuário

- Verificar Habilitar para selecionar o usuário.
- Clique em Remover Usuário para excluir o usuário do Controle dos Pais.
- Senha: Insira uma senha de usuário para entrar na Internet.
- Reinsira a Senha: Inserir a senha novamente para confirmação.
- Usuário de Confiança: O usuário selecionado terá acesso integral ao conteúdo da Internet, desabilitando assim quaisquer filtros configurados.
- Regra de Conteúdo: Utilizada para especificar os websites que um usuário selecionado tem permissão para acessar. Somente Acesso da Lista Branca e escolha um usuário da lista de rolagem automática.
- Regra de Tempo de Acesso: Você pode escolher uma regra que restrinja o horário em que o usuário selecionado pode usar a Internet.
- Duração da Sessão: Você pode configurar o intervalo de tempo em que um usuário selecionado pode usar a Internet.
- Período de Inatividade: Você pode configurar o tempo de inatividade antes do encerramento automático da Internet para um usuário selecionado.

Clientes de Confiança


- Clique em Acrescentar quando tiver terminado de inserir o endereço MAC.
- Clique em Remover para apagar o usuário configurado.

Configuração Básica

Controle dos Pais ➔ [Básico](#)

Você pode configurar as regras básicas para bloquear determinado conteúdo da Internet e determinados websites. Quando você mudar suas configurações de controle dos pais, clique em Aplicar, Acrescentar ou Remover para que suas novas configurações passem a valer. Se você atualizar a tela do seu browser, poderá ver as configurações ativas no momento.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA
--------	-------	----------	----------	------------------	-----	----------	-----



- User Setup
- Basic**
- ToD Filter
- Local Log

Parental Control

Basic Setup

Parental control menu has three submenus which consist of content policy, time access policy and user. In the content policy menu, you can enter the domains you want to block. In the time access policy menu, you can set the day of week and time you want to block access on. In the user menu, you can set the content policy and the time access policy for each user.

This page allows you to configure the basic setup to block certain internet content or web sites.

Parental Control Activation

This box must be checked to turn on Parental Control

Enable Parental Control

Content Policy Configuration

Content Policy List

1. Default

Keyword List	Blocked Domain List	Allowed Domain List
<input type="text" value="anonymizer"/>	<input type="text" value="anonymizer.com"/>	<input type="text"/>
<input type="text"/> <input type="button" value="Add Keyword"/>	<input type="text"/> <input type="button" value="Add Domain"/>	<input type="text"/> <input type="button" value="Add Allowed Domain"/>
<input type="button" value="Remove Keyword"/>	<input type="button" value="Remove Domain"/>	<input type="button" value="Remove Allowed Domain"/>

Override Password

If you encounter a blocked website, you can override the block by entering the following password

Password	<input type="password" value="....."/>
Re-Enter Password	<input type="password" value="....."/>
Access Duration	<input type="text" value="30"/>
<input type="button" value="Apply"/>	

Ativação do Controle dos Pais

- Verifique Habilitar Controle dos Pais para ativar a função Controle dos Pais.
- Clique em Aplicar para salvar.

Configuração da Política de Conteúdo

- Insira o nome da regra e clique em Acrescentar Nova Política para criar uma nova política.

Lista da Política de Conteúdo

- Clique em Remover Política para deletar a regra da política selecionada.
- Lista de palavras-chave: Lista a palavra-chave da URL
- Clique em Acrescentar palavra-chave para inserir uma nova palavra-chave.
- Clique em Remover Palavra-Chave para excluir uma palavra-chave existente
- Lista de Domínios Bloqueados: Lista de domínios que deve ser bloqueada
- Clique em Acrescentar domínio para acrescentar um novo domínio.
- Clique em Remover Domínio para excluir um domínio existente.
- Lista de Domínios Permitidos: Lista branca, com permissão para visitas dos usuários
- Clique em Acrescentar Domínio Permitido para inserir uma nova lista branca.
- Clique em Remover Domínio Permitido para excluir a lista de URL selecionada.

Filtro ToD [Hora do Dia]

Controle dos Pais ➔ [Filtro ToD](#)

Você pode configurar as políticas de acesso para bloquear todo o tráfego de Internet direcionado a dispositivos de rede específicos e dali originados com base nas configurações de hora do dia.

The screenshot shows the HUMANX web interface for Parental Control. The top navigation bar includes: Status, Basic, Advanced, Firewall, Parental Control (highlighted), VPN, Wireless, MTA, and Logout. On the left, there is a sidebar with the HUMANX logo and navigation buttons for User Setup, Basic, ToD Filter (highlighted), and Local Log. The main content area is titled 'Parental Control' and 'Time of Day Access Policy'. It contains a description: 'This page allows you to configure the time access policy to block all internet traffic to and from the specific network devices according to the day and time settings.' Below this is the 'Time Access Policy Configuration' section, which includes a text input field and an 'Add New Policy' button. The 'Time Access Policy List' section shows a filter dropdown set to 'No filters entered', an 'Enabled' checkbox, and a 'Remove' button. Under 'Days to Block', there are checkboxes for Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The 'Time to Block' section has an 'All day' checkbox and time pickers for Start (12:00 AM) and End (12:00 AM). The 'Ports to Block' section has an 'Enabled' checkbox, 'Port Start' and 'Port End' input fields (both set to 0), and a 'Protocol' dropdown set to UDP. An 'Apply' button is at the bottom of the configuration area.

©2013 HUMANX Co., Ltd., All rights reserved.

Configuração da Política de Acesso por Horário

- Insira um novo nome na política de acesso por horário e clique em Acrescentar Nova Política para criar uma nova regra da política de horário.

Lista da Política de Acesso Horário

Você pode habilitar ou remover uma regra da política de acesso horário.

- Assinale Habilitado para ativar a regra da política de acesso horário.
- Clique em Remover para excluir a regra da política de acesso horário.
- Dias a Bloquear: Selecione um dia para bloquear um website naquele dia específico.
- Horário a Bloquear: Configure um horário detalhado para bloquear um website durante aquele período.
- Assinale Habilitado para bloquear uma porta específica e então configure o início da porta, o fim da porta e o tipo de protocolo.

Log Local

Controle dos Pais ➔ [Log Local](#)

Esta página exibe o relatório de logs de eventos.

HUMANX

Parental Control

Event Log

This page displays the parental control event log report.

Last Occurrence	Action	Target	User	Source
-----------------	--------	--------	------	--------

©2013 HUMANX Co., Ltd.. All rights reserved.

Log de Eventos

- Última ocorrência: Exibe o horário em que o último evento ocorreu
 - Ação: Exibe como processar o pacote detectado
 - Alvo: Exibe o endereço IP de destino de uma determinada solicitação de acesso
 - Usuário: Exibe o usuário que desencadeou este log de evento
 - Fonte: Exibe a fonte do endereço IP deste evento
- Clique em Excluir Log para excluir todo o log de eventos.

O gateway residencial HUMAX suporta diversos protocolos de Redes Privadas Virtuais (VPN), dependendo das opções de tempo de compilação.

Resumo VPN

VPN ➔ [Básico](#)

Você pode criar, configurar e controlar túneis VPN IPSEC. A tabela a seguir apresenta o status dos túneis atualmente definidos.

HUMAX VPN

Basic

This page allows you to configure VPN protocols and VPN tunnels.

IPsec

IPsec Endpoint

#	Name	Status	Control	Configure
<input type="text" value="Add New Tunnel..."/>				

©2013 HUMAX Co., Ltd.. All rights reserved.

A tabela de status apresenta uma lista dos túneis definidos, permitindo que você controle e configure cada um deles.

- Nome: Exibe um nome de túnel definido pelo usuário
- Status: Exibe um estado de conexão atual
- Controle: Exibe as teclas Habilitar, Conectar ou Desconectar com base no estado de conexão do túnel atual.
- Configurar: Traz teclas de Editar e Apagar para gerenciamento das configurações


Clique em Acrescentar Novo Túnel para criar uma nova configuração de túnel e anexá-la à tabela. O nome e concepções do túnel podem ser então acrescentados pressionando-se a tecla Edit para aquele túnel.

Configuração e Ajuste VPN

VPN ➔ [IPsec](#)

Você pode configurar múltiplos túneis VPN em vários PCs de clientes. Diferentes túneis podem ser configurados e armazenados, porém não podem ser habilitados para facilidade de uso com conexões e/ou PCs de clientes que não são constantemente utilizados. Para cada configuração de túnel armazenada, seus parâmetros IPSEC únicos são armazenados utilizando-se o menu dos Ajustes IPSEC no rodapé da página. Também há um menu de ajustes avançados que aparece no rodapé da página quando a tecla é clicada. Essas características avançadas controlam o gerenciamento da chave IPSEC e a negociação com o terminal longínquo.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless
--------	-------	----------	----------	------------------	-----	----------



VPN

IPsec

This page allows you to configure the IPsec tunnels.

Tunnel: Tunnel list is EMPTY Delete Tunnel

Name: Add New Tunnel

Disabled Apply

Local endpoint settings

Address group type: IP subnet

Subnet:

Mask:

Identity type: IP address

Identity:

Remote endpoint settings

Address group type: IP subnet

Subnet:

Mask:

Identity type: IP address

Identity:

Network address type: IP address

Remote Address:

IPsec settings

Pre-shared key:

Phase 1 DH group: Group 1 (768 bits)

Phase 1 encryption: DES

Phase 1 authentication: MD5

Phase 1 SA lifetime: seconds

Phase 2 encryption: DES

Phase 2 authentication: MD5

Phase 2 SA lifetime: seconds

Show Advanced Settings

Túnel

Este menu de rolagem seleciona túneis pré-configurados por seu nome pré-estabelecido na seleção abaixo. Isto permite que cada túnel seja configurado individualmente.

Nome

O nome é um nome de usuário genérico especificado para um grupo de ajustes para um único túnel. Uma vez que o nome apropriado do túnel seja inserido pela primeira vez, a tecla Acrescentar Novo Túnel pode ser pressionada para criar um título para os ajustes de túnel que podem ser selecionados, utilizando-se a rolagem do "Túnel" acima. Caso nenhum nome seja inserido, os túneis serão nomeados sequencialmente 1, 2, 3 e assim por diante.

Habilitar

Uma vez que um túnel VPN específico seja nomeado e configurado, ele poderá ser deixado armazenado e desabilitado ou habilitado pelo menu de rolagem “Habilitar/Desabilitar”. A tecla Aplicar tornará válido aquele ajuste.

Local Endpoints Settings **Ajustes do Terminal Local**

Tipo de Endereço do Grupo

O grupo de acesso VPN local pode ser ajustado aqui para que seja um único endereço IP específico de um computador, uma gama de endereços IP para abranger uma pequena gama de computadores ou uma sub-rede/rede inteira.

- Caso selecione Sub-rede IP, você poderá inserir as informações de sub-rede e de máscara.
- Caso selecione Endereço IP único, você poderá inserir somente aquele endereço IP específico.
- Caso selecione Gama de Endereços IP, você poderá inserir os endereços IP iniciais e finais para formar um pool de endereços IP consecutivos que terá acesso ao túnel VPN.

Tipo de Identidade

Você poderá definir o tipo de identidade do nó terminal local para usar automaticamente o endereço IP WAN do roteador ou como um usuário de endereço IP especificado, com nome de domínio inteiramente qualificado (FQDN) ou endereço de e-mail. Esta é a identidade que o nó terminal distante utilizará para identificação do ponto de terminação e aperto de mão. O nó terminal VPN do lado oposto do túnel deve conferir com os ajustes aqui com seus ajustes de nó terminal remoto.

Identidade

Uma vez que o tipo de identidade seja selecionado entre os acima, a string de identificação deve ser inserida aqui. Para o modo endereço IP, simplesmente x.x.x.x é inserido. Para FQDN, “yourdomain.com” seria inserido e a identidade de seu endereço de Email, “yourname@yourdomain.com” seria inserida. O nó terminal VPN remoto do outro lado do túnel deve conferir com os ajustes aqui com seus ajustes de nó terminal remoto.

Remote Endpoint Settings **Ajustes de Nó Terminal Remoto**

Esses ajustes dizem ao nó terminal local (roteador CableMedea router) como fazer a conexão com o ponto de terminação VPN distante (o outro lado do túnel VPN).

Tipo de Grupo de Endereços

O grupo de acesso VPN pode ser ajustado aqui para um único endereço IP específico de um computador, uma gama de endereços IP para abranger uma pequena gama de computadores, ou toda a sub-rede/rede.

- Caso selecione Sub-rede IP, você poderá inserir as informações de sub-rede e de máscara.
- Caso selecione Endereço IP único, você poderá inserir somente aquele endereço IP específico.
- Caso selecione Gama de Endereços IP, você poderá inserir os endereços IP iniciais e finais para formar um pool de endereços IP consecutivos que terá acesso ao túnel VPN. O nó terminal VPN remoto do outro lado do túnel deve ter ajustes aqui que conferem com seus ajustes de seu nó terminal local.

Tipo de Identidade

Você poderá definir o tipo de identidade do nó terminal local para usar automaticamente o endereço IP do nó terminal remoto ou como um usuário de endereço IP especificado, com nome de domínio inteiramente qualificado (FQDN), ou endereço de e-mail. Esta é a identidade que o nó terminal distante utilizará para a identificação do ponto de terminação VNP e aperto de mão. O nó terminal VPN remoto do outro lado do túnel devem conferir com os ajustes aqui para seus ajustes de nó terminal local.

Identidade

Uma vez que a identidade seja selecionada entre as acima, a string da identidade deve ser inserida aqui. Para o modo de endereço IP, simplesmente x.x.x.x é inserido. Para FQDN, “yourdomain.com” deve ser inserido e, para identidade de endereço de e-mail, “yourname@yourdomain.com” seria inserido. O nó terminal VPN remoto do outro lado do túnel deve conferir ter ajustes aqui que conferem com os ajustes para seu nó terminal local.

Tipo de Endereço de Rede

Você pode selecionar Endereço IP ou Nome de Domínio Inteiramente Qualificado (FQDN) para o tipo de endereço WAN do nó terminal remoto.

Endereço Remoto

Você pode inserir o endereço IP do nó terminal remoto ou seu FQDN, dependendo de que tipo de Endereço de Rede for selecionado acima.

Ajustes IPSEC

Com os túneis VPN, existem duas etapas de Associação de Segurança (AS). A etapa 1 é utilizada para criar um SA IKE. Depois que a Etapa 1 for concluída, a Etapa 2 será utilizada para criar uma ou mais SAs IPSEC, que são então utilizadas para as sessões IPSEC.

Chave Pré-Partilhada

Caso um lado do túnel VPN esteja utilizando um identificador único de firewall (ou Chave Pré-Partilhada), isto deve ser inserido no campo “Chave Pré-Partilhada”.

Etapa 1 Grupo DH

Existem três grupos Diffie-Hellman para escolher: 768 bits, 1024 bits e 1536 bits. Diffie-Hellman é uma técnica de encriptação que utiliza chaves públicas e privadas para encriptação e descriptação. Quanto mais alto o número de bits selecionado, tanto mais seguro.

Etapa 1 Encriptação

A encriptação é assegurada para garantir a conexão VPN entre os nós terminais. Cinco tipos diferentes de encriptação estão disponíveis: DES, 3DES, AES-128, AES-192 e AES-256. Qualquer forma fora da encriptação pode ser selecionada, desde que os nós terminais distantes confirmem entre si. Um dos ajustes mais comuns aqui é o 3DES;

O AES, contudo, também é um método bem forte de encriptação.

Etapa 1 Autenticação

A autenticação funciona como outro nível de segurança. Os dois tipos de autenticação disponíveis são o MD5 e o SHA. O SHA é recomendado por ser mais seguro. O tipo de autenticação pode ser utilizado, desde que a outra extremidade do túnel VPN utilize o mesmo método.

Fase 1 Vida Útil da AS

Neste campo, a vida útil das chaves rotativas individuais é especificada. Insira o número desejado de segundos para que a chave dure até que uma negociação de nova chave entre cada nó terminal esteja negociada. Vidas úteis mais curtas em geral são mais seguras, pois darão a um atacante um tempo menor para tentar quebrar a chave, porém a negociação de chave efetivamente consome largura de banda, de forma que o rendimento da rede será sacrificado com vidas úteis curtas. As inserções aqui são normalmente de milhares ou dezenas de milhares de segundos. O ajuste padrão é 28.000 segundos.

Etapa 2 Encriptação

A encriptação é utilizada para garantir a conexão VPN entre os nós terminais. Cinco tipos diferentes de encriptação estão disponíveis: DES, 3DES, AES-128, AES-192 e AES-256. Qualquer forma fora da encriptação poderá ser selecionada, desde que os nós terminais confirmem. Um dos ajustes mais comuns aqui é o 3DES;

O AES, contudo, também é um método de encriptação bastante sólido, sendo recomendado por ser muito difícil de quebrar.

Etapa 2 Autenticação

A autenticação funciona como outro nível de segurança. Os três tipos de autenticação disponíveis são MD5, SHA e Nulo (nenhum). SHA é recomendado por ser mais seguro. Qualquer desses tipos de autenticação pode ser utilizado desde que a outra extremidade do túnel VPN utilize o mesmo método.

Etapa 2 SA Vida Útil

Neste campo, a vida útil das chaves rotativas individuais é especificada. Insira o número desejado de segundos para que a chave dure até uma negociação de nova chave entre cada nó terminal. Vidas úteis mais curtas são geralmente mais seguras, uma vez que proporcionariam a um atacante um período mais curto para tentar quebrar a chave, porém a negociação da chave efetivamente consome largura de banda, de forma que o rendimento será sacrificado com tempos de vida mais curtos. As inserções aqui são normalmente em milhares de segundos. O ajuste padrão é de 3.600 segundos.

Advanced Tunnel Settings

Ajustes de Túneis Avançados

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless
--------	-------	----------	----------	------------------	-----	----------

HUMAX

VPN

IPsec

This page allows you to configure the IPsec tunnels.

Tunnel: Tunnel list is EMPTY. Delete Tunnel

Name: (null) Add New Tunnel

Enabled/Disabled Apply

Local endpoint settings

Address group type: IP subnet

Subnet: 192 . 168 . 0 . 0

Mask: 255 . 255 . 255 . 0

Identity type: IP address

Identity: (null)

Remote endpoint settings

Address group type: IP subnet

Subnet: 0 . 0 . 0 . 0

Mask: 0 . 0 . 0 . 0

Identity type: IP address

Identity: (null)

Network address type: IP address

Remote Address: 0.0.0.0

IPsec settings

Pre-shared key: (null)

Phase 1 DH group: Group 1 (768 bits)

Phase 1 encryption: DES

Phase 1 authentication: MD5

Phase 1 SA lifetime: 0 seconds

Phase 2 encryption: DES

Phase 2 authentication: MD5

Phase 2 SA lifetime: 0 seconds

Gerenciamento da Chave

Para uma encriptação bem-sucedida, ambas as extremidades do túnel VPN têm de concordar sobre o tipo de encriptação e a desencriptação no lado remoto. Isto é obtido partilhando-se uma chave para o código de encriptação.

- Selecione Auto (IKE) para usar o Gerenciamento Automático de Chave. Certifique-se de que existe uma Chave Pré-Partilhada inserida nos ajustes IPSEC ao utilizar este ajuste.
- Selecione Manual para usar o Gerenciamento Manual de Chave. Isto permite ao usuário selecionar ou gerar ele próprio as chaves. A chave deve ser inserida no campo de Chave de Encriptação Manual. Em seguida, a “Chave de Autenticação” deve ser inserida neste campo. Esses campos devem conferir com as informações inseridas no nó terminal VPN remoto. Até 16 dígitos hexadecimais podem ser inseridos no campo de Chave de Encriptação Manual. Até 32 dígitos hexadecimais podem ser inseridos no campo de Chave de Autenticação Manual. O campo SPI de entrada deve conferir com o SPI de saída no nó terminal VNP remoto. De forma oposta, o campo SPI de saída deve conferir com o SPI de entrada no nó terminal VPN remoto. Somente números podem ser utilizados nos campos SPI de Entrada/Saída. Clique em Aplicar para validar os ajustes.

Modo de Negociação IKE

Você pode selecionar modos de negociação IKE que trocam as mesmas cargas IKE em diferentes sequências.

O modo principal é o mais comum e mais seguro.

O modo agressivo é mais rápido.

O modo principal normalmente é utilizado e exige mais autenticação que o modo Agressivo.

Perfect Forward Secrecy (PFS)

Quando esta função está habilitada, ela assegura o intercâmbio inicial da chave e as propostas IKE estão seguros utilizando-se uma Chave Pré-Partilhada dos ajustes IPSEC. Este ajuste somente é válido ao utilizar o gerenciamento de chave (IKE) Auto.

Etapa 2 Grupo DH

Este ajuste é ativado quando PFS está selecionado.

Existem três grupos Diffie-Hellman entre os quais escolher: 768 bits, 1024 bits e 1536 bits. A Diffie-Hellman é uma técnica de encriptação que utiliza chaves públicas e privadas para encriptação e desencriptação. Quanto maior o número de bits selecionado, tanto mais segura a encriptação.

Detecção de Repetição

Selecione Habilitado para monitorar os números em sequência nos pacotes assim que chegam, de forma a garantir a segurança em nível de pacote IP. Quaisquer violações são reportadas no Log de Evento VPN.

Envio de Transmissão NETBIOS

Selecione Habilitado para habilitar o tráfego NetBIOS a passar pelo túnel VPN para as funções de rede do Windows.

Log de Evento VPN

VPN ➔ [Log de Evento](#)

Você pode visualizar um histórico das conexões VPN e da atividade em ordem cronológica, assim como o endereço IP em ambos os nós terminais no túnel (remoto e local).

Clique em Atualizar para obter a atualização da tabela de Log de Eventos, então você poderá verificar quaisquer mudanças desde que a página da web foi carregada pela última vez.

Clique em Limpar para excluir da tabela de log seu conteúdo atual, quando então serão exibidos os dados mais recentes.

The screenshot shows the HUMAN VPN Event Log interface. At the top, there is a navigation bar with tabs: Status, Basic, Advanced, Firewall, Parental Control, VPN (highlighted), Wireless, MTA, and Logout. On the left side, there is a sidebar with the HUMAN logo and three buttons: Basic, IPsec, and Event Log (highlighted). The main content area is titled 'VPN Event Log' and contains the text: 'This page allows you to view the VPN event log.' Below this text is a table with two columns: 'Time' and 'Description'. The table contains one row with the text 'Event log is empty.' At the bottom of the table, there are two buttons: 'Refresh' and 'Clear'.

O gateway residencial também serve como um ponto de acesso (PA) sem fio IEEE 802.11. Quando um cartão wireless é instalado, o conjunto completo de páginas de configuração wireless descrito abaixo é exibido sob o menu.

Os usos HG100R-L2-Dual selecionáveis de banda dupla que suportam somente uma rede Wi-Fi, de 2.4GHz ou 5GHz.

Ajustes de Rádio

Wireless ➔ [Rádio](#)

Você pode configurar os parâmetros físicos de sua rede wireless. O endereço MAC da interface wireless é exibido no topo da página.

The screenshot shows the 'Wireless' configuration page for a HUMANX device. The page is titled 'Wireless' and '802.11 Radio'. It includes a navigation menu on the left with options like 'Radio', 'Primary Network', 'Advanced', 'Access Control', 'WMM', and 'WDS'. The main content area contains the following configuration options:

- Wireless MAC Address : 2C:D0:5A:69:BE:57 [2.4 GHz]
- Wireless : On Off
- Country : BRAZIL
- Output Power : 100%
- 802.11 Band : 2.4 Ghz (Current : 2.4 GHz)
- 802.11 n-mode : Auto
- 802.11 N Support Required : Off
- Bandwidth : 20 Mhz (Current : 20MHz)
- Sideband for Control Channel (40 Mhz only) : None
- Control Channel : 1 (Current : 1 ***Interference Level: Acceptable)
- Regulatory Mode : Off
- TPC Mitigation (db) : 0 (Off)
- OBSS Coexistence : 1 (Enabled)
- STBC Tx : Auto

Buttons at the bottom include 'Apply', 'Restore Wireless Defaults', and 'Scan Wireless APs'.

©2013 HUMANX Co., Ltd.. All rights reserved.

Interfaces Wireless

Você pode ajustar a identificação básica do conjunto de serviço (BSSID) da interface para a configuração Wi-Fi.

Wireless

Você pode habilitar ou desabilitar a interface wireless selecionada acima.

País

Você pode selecionar um país para restringir o conjunto de canais com base nas exigências regulatórias do país.

Potência de Saída

Você pode ajustar a potência de saída do radio para controlar o alcance da PA.

Banda 802.11

Você pode selecionar se o rádio vai operar em banda de 2.4 GHz ou 5 GHz. Pode haver menos interferência de outras redes wireless e utensílios domésticos na banda de 5 GHz, porém dispositivos 802.11b/g não poderão ser conectados.

Modo 802.11 n

Você pode ajustar o modo 802.11 n em Desligar para forçar a PA a operar no modo 802.11g.

Suporte N Exigido 802.11 N

Apêndice

- Selecione Ligar, somente estações habilitadas em .n podem ser associadas ao CM.
- Selecione Desligar, b/g/n não são permitidos.

Largura de Banda

- Os canais 802.11b/g têm largura de somente 20 MHz.
- Os canais 802.11n podem ter largura de 40 MHz. Existem algumas questões de compatibilidade reversa com os canais 40 MHz, contudo. É mais fácil encontrar esse problema em banda de 2.4 GHz quando os dispositivos do legado (802.11b/g) podem estar operando utilizando canais de 20 MHz.

Banda Lateral para Canal de Controle (40 MHz somente)

Você pode programar se o canal de controle de 20 MHz usará a metade superior ou inferior do canal de 40 MHz. Se você mudar este ajuste, o ajuste do canal de controle poderá ser mudado. Por exemplo (na banda 2.4 GHz), se a metade superior 20 MHz for selecionada como banda lateral para o canal de controle, o canal de controle mais baixo disponível seria o canal 5, para permitir um 20 MHz menor para dados.

Canal de Controle

Você pode selecionar o canal de controle para a operação PA. A lista dos canais disponíveis depende do país selecionado.

Modo de Regulagem

Você pode selecionar os modos de operação 802.11d ou 802.11h.

- 802.11d permite que as estações operem em qualquer país sem qualquer reconfiguração.
- 802.11h permite que menos de três opções sejam ativadas. Utilizados na banda 5GHz UNII. Essas são alterações das especificações do 802.11 para resolver questões de interferência com outros sistemas de transmissão, tais como satélite ou radar, além de exigências de transmissão em diferentes partes do mundo.

Atenuação TPC (dB)

Atenuação TPC (dB) refere-se ao fator de atenuação de controle de potência em dB. O Controle do Poder de Transmissão é utilizado automaticamente para reduzir o poder de transmissão quando as demais redes estiverem dentro do alcance. Este ajuste somente é utilizado quando o Modo de Regulagem ainda estiver ajustado para 802.11h.

Coexistência OBSS

A coexistência OBSS diz respeito à capacidade da PA de suportar dispositivos de 20 MHz dentro de canais de 40 MHz. Ela também permite que a PA lide melhor com os dispositivos 20 MHz ao seu redor que estejam interferindo em parte de seu canal de 40 MHz.

Escanear PAa Wireless

Forçar o Ponto de Acesso dos Modems a escanear outras PAs dentro da mesma faixa.

Ajustes de Rede Principais

Wireless ➔ [Rede Primária](#)

Você pode configurar a rede wireless primária e seus ajustes de segurança.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA
--------	-------	----------	----------	------------------	-----	----------	-----

HUMAX

Wireless

802.11 Primary Network

This page allows you to configure the primary wireless network and its security settings.

Wireless Radio 2.4 GHz
 Primary Network On Off

Network Name (SSID)

Closed Network

AP Isolate

WPA

WPA-PSK

WPA2

WPA2-PSK

WPA/WPA2 Encryption

WPA Pre-Shared Key Show Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

WEP Encryption

Shared Key Authentication

802.1x Authentication

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Automatic Security Configuration

WPS

WPS Config State: Unconfigured

The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS).

Device Name

WPS Setup AP

UUID: 82cc80507ea6bf151c34fa29304c6cf9

PIN:

WPS Add Client

Add a client:

Client PIN:

Authorized Client MAC:

Rede Primária

Você pode selecionar Ligar ou Desligar para ajustar o modo de operação da rede primária.

Nome da Rede (SSID)

Você pode ajustar o nome da rede (também conhecido como SSID) da rede primária. Você pode inserir até 32 caracteres ASCII

Nota: O nome da rede deve ser idêntico àqueles de todos os dispositivos na rede wireless.

Rede Fechada

Você pode ocultar o nome da rede. O nome da rede não é transmitido pela PA em uma rede fechada. Portanto, somente os clientes que já conhecem o nome da rede podem se conectar.

WPA

O Acesso Wi-Fi Protegido é um algoritmo um pouco mais antigo e menos seguro para garantir a segurança de uma rede wireless. Esta é a variante da empresa que requer a configuração de um servidor RADIUS.

WPA-PSK

O modo de Chave Pré-Partilhada do algoritmo WPA, que não requer o uso de um servidor RADIUS. Este também é conhecido como WPA Personal. WPA e WPA-PSK não podem ser usados ao mesmo tempo.

WPA2

Uma forma avançada de WPA que é mais segura. Este é o modo Empresa do WPA2 que requer o uso de um servidor RADIUS. O WPA2 e o WPA podem ser usados ao mesmo tempo para conferir compatibilidade reversa com dispositivos que não suportam o WPA2.

WPA2-PSK

Os modos de Chave Pré-Partilhada do WPA2, também conhecido como WPA2 Pessoal, WPA2 e WPA2-PSK não podem ser utilizados ao mesmo tempo para conferir compatibilidade reversa com dispositivos que não suportam WPA2.

Encriptação WPA/WPA2

Você pode ajustar os modos de encriptação AES ou TKIP + AES ao utilizar qualquer dos esquemas de autenticação WPA. AES oferece a encriptação mais sólida, ao passo que a TKIP oferece encriptação sólida com compatibilidade reversa melhorada. O modo TKIP + AES permite que tanto os clientes capacitados com TKIP e com AES consigam se conectar.

Chave WPA Pré-Partilhada

Você pode ajustar a Chave WPA Pré-Partilhada (PSK). Esta é uma string de caracteres 8-63 ASCII ou um número hexa de 64 dígitos. Isto é ativado quando o método de Autenticação de Rede é o WPA-PSK ou o WPA2-PSK.

Servidor RADIUS

Você pode ajustar o endereço IP do servidor RADIUS para utilizar a autenticação de cliente. O servidor RADIUS pode estar na rede pública (WAN) ou na rede privada (LAN). Isto se aplica somente aos modos WPA ou WPA2 (Empresa).

Porta RADIUS

Você pode ajustar o número da porta UDP do servidor RADIUS. O padrão é 1812.

RADIUS Key

Você pode ajustar o segredo partilhado para a conexão RADIUS. A chave é uma string ASCII de 0 a 255 caracteres.

Intervalo de Rotação da Chave do Grupo

O intervalo de rotação diz respeito à frequência com que as chaves de transmissão giram por segundo.

Caso esteja ajustada em zero, o rechaveamento periódico está desabilitado.

Intervalo de Nova Autenticação WPA/WPA2

Este valor refere-se à frequência com que uma estação que utiliza a segurança Enterprise tem de contatar o servidor RADIUS.

Encriptação WEP

Você pode ajustar o modo de encriptação WEP. Tanto os modos de encriptação de 64-bits e de 128-bits são suportados. Ao rodar a Chave Partilhada ou a autenticação 802.1x, a encriptação WEP deve estar habilitada. A encriptação WEP não pode ser utilizada ao mesmo tempo que a WPA ou WPA2.

Network Key 1 a Network Key 4

Você pode ajustar as chaves de encriptação WEP quando a encriptação WEP estiver habilitada.

- Inserir 5 caracteres ASCII ou 10 dígitos hexadecimais para uma chave de 64 bits.
- Inserir 13 caracteres ASCII ou 26 dígitos hexadecimais para uma chave de 128 bits.

Chave de Rede Corrente

Você pode selecionar a chave de encriptação (transmitir) quando a encriptação WEP estiver habilitada.

PassPhrase

Você pode ajustar o texto para usar a geração de chave WEP.

Geração de Chaves WEP

Se você clicar em Gerar Chaves WEP quando a encriptação WEP estiver habilitada, a frase-senha inserida para um conjunto de chaves WEP é convertida.

Configuração Automática de Segurança

- Ajuste Wi-Fi Protegido (WPS) – Este é o método padronizado para atingir a mesma meta que os SES HUMAN. O protocolo é desativado em uma especificação emitida pela Wi-Fi Alliance.
- Nome do Dispositivo – Este é anunciado para as estações wireless.

Ajuste PA WPS

Você pode ajustar o PIN. Clique em Gerar PA PIN nesta seção ao utilizar um Registro Externo.

Acrescentar Cliente WPS

Apêndice

Para acrescentar um novo cliente wireless utilizando o Registro Externo, você pode usar a tecla ou o método PIN.

Ajustes Avançados

Wireless ➔ Avançado

Você pode configurar os ajustes wireless avançados. A maioria dos usuários não precisam mudar esses ajustes.

The screenshot shows the HUMANX Wireless 802.11 Advanced configuration page. The page title is "Wireless" and "802.11 Advanced". Below the title, it says "This page allows you to configure the data rates and Wi-Fi thresholds." The configuration options are as follows:

- 54g™ Mode: 54g Auto
- XPress™ Technology: Enabled
- 802.11n Protection: Auto
- Short Guard Interval: Auto
- Basic Rate Set: Default
- Multicast Rate: Auto
- NPHY Rate: Auto
- Legacy Rate: Auto
- Beacon Interval: 100
- DTIM Interval: 1
- Fragmentation Threshold: 2346
- RTS Threshold: 2347

There is an "Apply" button at the bottom of the configuration area.

©2013 HUMANX Co., Ltd.. All rights reserved.

Modo 54g™

Você pode ajustar o modo de rede.

- O 54g Auto aceita clientes 54g, 802.11g e 802.11b, porém otimiza o desempenho com base no tipo de clientes conectados.
- O 54g Performance aceita somente clientes 54g™ e oferece o rendimento mais alto; as redes 802.11b ao redor podem apresentar desempenho deteriorado.
- O 54g LRS interopera com a mais ampla variedade de clientes 54g™, 802.11g e 802.11b;
- O 802.11b aceita somente clientes 802.11b.

Tecnologia XPress™

Você pode habilitar o método de reconhecimento de bloqueio de frame de propriedade exclusiva da para frames 802.11g. Esta característica pode melhorar o rendimento, porém pode causar problemas.

Proteção 802.11n

Esta opção é similar à proteção 54g, ressaltando-se que se aplica aos dispositivos 802.11n.

Intervalo de Guarda Curto

Você pode ajustar o intervalo de guarda para evitar a perda de dados por interferência ou atrasos em múltiplas vias.

Ajuste da Taxa Básica

Você pode verificar as taxas básicas anunciadas e ajustar todas as taxas disponíveis como taxas básicas. O modo padronizado utiliza os padrões do driver.

Multicast Rate

Você pode ajustar a taxa multicast à qual os pacotes multicast são transmitidos às estações. Os pacotes multicast não são reconhecidos.

Taxa NPHY

Você pode selecionar a taxa 802.11n para ser aplicada a todos os pacotes unicast.

Taxa de Legado

Você pode forçar a taxa em que a PA opera. Esta opção é ativada quando o modo 802.11n está ajustado em Desligado.

Intervalo Beacon

Você pode ajustar o intervalo beacon em milissegundos para a AP. O modo padronizado é 100, que é adequada para quase todas as aplicações.

Intervalo DTIM

Apêndice

Você pode ajustar o intervalo de despertar para os clientes no modo de economia de energia. Quando o cliente está rodando em modo de economia de energia, os valores menores conferem rendimento mais alto, porém reduzem a vida útil da bateria do cliente, ao passo que valores mais altos resultam em desempenho inferior, porém em vida útil de bateria mais longa.

Limiar de Fragmentação

Você pode ajustar o limiar de fragmentação. Os pacotes que excedem o limiar são fragmentos em pacotes de tamanho não superior ao limiar antes da transmissão de pacotes.

Limiar RTS

Você pode ajustar o limiar RTS. Os pacotes que excedam esse limiar podem fazer a PA realizar uma troca RTS/CTS para reservar o meio wireless antes da transmissão dos pacotes.

Ajustes de Controle de Acesso

Wireless ➔ [Controle de Acesso](#)

Você pode controlar os clientes wireless que podem acessar sua rede wireless. Também são oferecidas informações sobre os clientes wireless conectados a seu ponto de acesso.

©2013 HUMANIX Co., Ltd.. All rights reserved.

Modo MAC Restrito

Você pode programar a permissão ou negação de acesso wireless a clientes wireless com endereço MAC especificado. Para permitir todos os clientes, selecione Desabilitado.

Endereços MAC

Você pode listar os endereços MAC de clientes wireless para permitir ou recusar acesso com base no ajuste de Modo Restrito. Os formatos MAC que constituem alimentação de dados válida são XX:XX:XX:XX:XX:XX e XX-XX-XX-XX-XX-XX.

Clientes Conectados

Uma lista de clientes wireless conectados é exibida. Quando um cliente se conectar (associar) à rede, ele é acrescentado à lista; quando um cliente deixa (desassocia) a rede, ele é removido da lista. Para cada cliente, a idade (em segundos), a força média estimada do sinal de recepção (em dBm), o endereço IP e o nome do host são apresentados. A idade é o intervalo de tempo transcorrido desde a data em que os dados foram transmitidos ao cliente ou dele recebidos.

Ajustes WMM

Wireless ➔ [WMM](#)

Você pode configurar Wi-Fi Multimídia (WMM). WMM é uma implantação da Qualidade do Serviço (QoS), a qual é definida pela norma IEEE 802.11e.

O Suporte WMM prevê a priorização de pacotes de dados wireless de diferentes aplicações com base em quatro categorias de acesso: Default, Jogos, Vídeo e Definição pelo Usuário. As informações dependentes de tempo tem mais prioridade que o tráfego normal.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA
--------	-------	----------	----------	------------------	-----	----------	-----

HUMAX

Wireless

802.11 Wi-Fi Multimedia

This page allows you to configure the Wi-Fi Multimedia Quality of Service (QoS).

WMM Support ▼

No-Acknowledgement ▼

Power Save Support ▼

EDCA AP Parameters:	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
AC_BE	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="button" value="Off"/> ▼
AC_BK	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="button" value="Off"/> ▼
AC_VI	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1"/>	<input type="text" value="6016"/>	<input type="text" value="3008"/>	<input type="button" value="Off"/> ▼
AC_VO	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1"/>	<input type="text" value="3264"/>	<input type="text" value="1504"/>	<input type="button" value="Off"/> ▼
EDCA STA Parameters:						
AC_BE	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	
AC_BK	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	
AC_VI	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="2"/>	<input type="text" value="6016"/>	<input type="text" value="3008"/>	
AC_VO	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="2"/>	<input type="text" value="3264"/>	<input type="text" value="1504"/>	
WMM TXOP Parameters:						
	Short Retry Limit	Short Fallbk Limit	Long Retry Limit	Long Fallbk Limit	Max Rate in 500kbps	
AC_BE	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="0"/>	
AC_BK	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="0"/>	
AC_VI	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="0"/>	
AC_VO	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="0"/>	

©2013 HUMAX Co., Ltd.. All rights reserved.

Suporte WMM

Você pode ajustar o suporte WMM. Se você ajustar o Padrão, o suporte WMM estará habilitado e, assim, o Elemento de Informações WME é incluído no frame beacon.

Inexistência de Reconhecimento

Você pode ajustar o Suporte ao Não Reconhecimento para Ligado ou Desligado. Caso habilitados, os reconhecimentos para os dados não serão transmitidos.

Suporte à Economia de Energia

Você pode ajustar o Suporte à Economia de Energia para Ligado ou Desligado. Se habilitada, A PA enfileira os pacotes para STAs que estejam em modo de economia de energia. Os pacotes enfileirados são transmitidos quando o STA informar PA de que saiu do modo de economia de energia.

Parâmetros EDCA AP

Você pode especificar os parâmetros de transmissão para o tráfego transmitido da PA para o STA para as quatro Categorias de Acesso: Melhores Esforços (AC_BE), Histórico (AC_BK), Vídeo (AC_VI) e Voz (AC_VO). Os parâmetros de transmissão incluem a Janela de Contenção (CWmin e CWmax), Arbitramento de Número de Espaçamento entre Frames (AIFSN) e Limite de Oportunidade de Transmissão (Limite TXOP).

Também há dois ajustes específicos de PA: Controle de Admissão e Descarte dos mais Antigos Primeiro.

- O controle de admissão especifica se o controle de admissão está em vigor para as Categorias de Acesso.
- Descartar os mais Antigos Primeiro é a política de descarte para as filas.
On descarta os mais antigos primeiro; Off descarta os mais recentes primeiro.

Parâmetros EDCA STA

Você pode especificar os parâmetros para o tráfego transmitidos da STA para a PA para as quatro Categorias de Acesso: Melhores Esforços (AC_BE), Histórico (AC_BK), Vídeo (AC_VI) e Voz (AC_VO). Os parâmetros de transmissão incluem a Janela de Contenção (CWmin e CWmax), Arbitramento de Número de Espaçamento entre Frames (AIFSN) e Limite de Oportunidade de Transmissão (Limite TXOP).

Ajustes WDS

Wireless ➔ [WDS](#)

Você pode ajustar o Sistema de Distribuição Wireless (WDS), que também é conhecido como ponte wireless. O WDS permite que você conecte múltiplos pontos de acesso wireless juntos para formar uma única rede que utiliza links wireless ponto-a-ponto.

The screenshot shows the HUMANAX web interface for configuring WDS. At the top, there is a navigation bar with tabs: Status, Basic, Advanced, Firewall, Parental Control, VPN, Wireless (highlighted), MTA, and Logout. On the left side, there is a sidebar with buttons for Radio, Primary Network, Advanced, Access Control, WMM, and WDS. The main content area is titled 'Wireless' and '802.11 WDS'. Below the title, it says 'This page allows you to configure the WDS features.' There is a dropdown menu for 'Wireless Bridging' set to 'Disabled'. Below that, there are three input fields for 'Remote Bridges' and an 'Apply' button. At the bottom left of the page, there is a copyright notice: '©2013 HUMANAX Co., Ltd. All rights reserved.'

Ponte Wireless

Você pode ajustar a ponte wireless para habilitá-la ou desabilitá-la.

Pontes Remotas

Você pode inserir os endereços MAC de ponte remota autorizados a estabelecer uma ponte wireless. Até quatro pontes remotas podem ser conectadas. Normalmente, você terá de inserir o endereço MAC de sua PA na ponte remota também.

O Adaptador do Terminal Multimídia (MTA) no gateway residencial oferece serviços de voz sobre IP. Você pode fazer ligações telefônicas na Internet. As funções telefônicas básicas, tais como espera, chamadas tridirecionais, correio de voz e transmissões de fac-símile são suportadas com esta conexão no gateway residencial. Você pode clicar em quaisquer submenus MTA para visualizar as informações do status para aquela opção.


Nota: Este menu está disponível somente quando seu gateway residencial suportar serviços VoIP.

Status MTA

MTA ➔ [Status](#)

Você pode visualizar o status atual do MTA embutido. Esta página exibe os status do Registro/Provisionamento e das linhas.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA	Logout
--------	-------	----------	----------	------------------	-----	----------	------------	--------



Status

DHCP

QoS

Provisioning

Event Log

MTA

Status

This page displays the initialization status of the MTA.

Startup Procedure	
Task	Status
Telephony DHCP	In Progress
Telephony Security	[Error: FAIL]
Telephony TFTP	In Progress
Telephony Call Server Registration	L1: No Security Association / L2: No Security Association
Telephony Registration Complete	In Progress


MTA Line State			
Lines	Hook State	Expiration Time	Re-registration Time
Line 1	N/A (Endpoint Disabled)	[Error: FAIL]	[Error: FAIL]
Line 2	N/A (Endpoint Disabled)	[Error: FAIL]	[Error: FAIL]

Protocolo de Configuração Dinâmica do Host (DHCP)

MTA ➔ [DHCP](#)

Você pode visualizar as informações sobre o status do cliente DHCP, cliente tftp e endereço IP do servidor DNS. Os cronômetros de tempo concedido e os valores da opção DHCP também são exibidos.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA	Logout
--------	-------	----------	----------	------------------	-----	----------	-----	--------



MTA

DHCP

This page displays the MTA DHCP lease information.

Status

DHCP

QoS

Provisioning

Event Log

Lease Parameters

FQDN	
IP Address/Submask	0.0.0.0 / 0.0.0.0
Gateway	0.0.0.0
Bootfile	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Lease Timers

Lease Time Remaining	D: 00 H: 00 M: 00 S: 00
Rebind Time Remaining	D: 00 H: 00 M: 00 S: 00
Renew Time Remaining	D: 00 H: 00 M: 00 S: 00

PacketCable DHCP Option 122

SNMP Entity (Sub-option 3)	
Kerberos Realm (Sub-option 6)	
Provisioning Timer (Sub-option 8)	


©2013 HUMAX Co., Ltd.. All rights reserved.

Qualidade do Serviço (QoS)

MTA ➔ [QoS](#)

Você pode visualizar as informações sobre erros FEC Downstream, contrainformações do Fluxo de Serviço e o estado da Supressão do Cabeçalho da Carga.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA	Logout
--------	-------	----------	----------	------------------	-----	----------	-----	--------



MTA

QoS

This page displays the MTA Quality of Service (QoS) parameters.

Status

DHCP

QoS

Provisioning

Event Log

Error Codewords

Unerrored Codewords	59946314
Correctable Codewords	2
Uncorrectable Codewords	0

Payload Header Suppression

PHS Status	ON
------------	----

Service Flows

SFID	Service Class Name	Direction	Primary Flow	Packets
9		Upstream	No	2018
65545		Downstream	No	0


©2013 HUMAX Co., Ltd.. All rights reserved.

Provisionamento

MTA ➔ [Provisionamento](#)

Você pode visualizar o conteúdo do arquivo de configuração MTA. O valor dos MIBs MTA selecionados também é exibido.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	MTA
--------	-------	----------	----------	------------------	-----	----------	-----



- Status
- DHCP
- QoS
- Provisioning
- Event Log

MTA

Provisioning

This page displays the MTA provisioning details.

MTA Config File

Filename	
Contents	

Enterprise MIBs

OID	Value
emtaInhibitSwDownloadDuringCall	false(2)
emtaFirewallEnable	true(1)
emtaRingWithDCOffset	false(2)
emtaIncludedInCmMaxCpe	false(2)
emtaDhcpOption	cableLabsClientConfiguraton(122)
emtaUseAlternateTelephonyRootCert	false(2)
emtaEnableDQoSLife	true(1)
emtaInhibitNcsSyslog	true(1)
emtaMaintenanceWindowBegin	Thu Jan 01 00:00:00 1970
emtaMaintenanceWindowDuration	0
emtaMaintenanceControlMask	0x10 [maintenanceOnCMSLoss(3)]
emtaMaintenanceQuarantineTimeout	120
emtaMaintenanceDisconnectedTimeout	120
emtaMaintenanceRFDisconnectTimeout	300
emtaSignalingAnnouncementCtrl	0x00
emtaSignalingVoiceJitterBufferType	jitterBufferTypeAdaptive(2)
emtaSignalingVoiceJitterNomValue	0
emtaSignalingVoiceJitterMinValue	0
emtaSignalingVoiceJitterMaxValue	0
emtaSignalingDataJitterNomValue	60
emtaSignalingDtmfToneRelayRFC2833Support	true(1)
emtaSignalingRtpBaseReceiveUdpPort	53456
emtaSignalingEndptConnectionCleanupTimeout	0
emtaSignalingEmaResetCleanupTimeout	0
emtaSignalingT38FaxRelaySupport	true(1)

Log de Eventos

MTA ➔ [Log de Eventos](#)

Você pode visualizar o log de eventos MTA e as informações detalhadas. Clique em Salvar Log para salvar o conteúdo atual.

HUMANX

MTA

Event Log

This page displays the MTA event log.

Time	Priority	ID	Text	Endpoint
------	----------	----	------	----------

Especificações

RF Downstream		
	DOCSIS	EuroDOCSIS
Faixa de Frequência	108 - 1002 MHz	108 - 1002 MHz
Demodulação	64/256 QAM	64/256 QAM
Faixa de Potência de Entrada	-15 dBmV/+15 dBmV	-17dBmV ~ +13dBmV (64QAM), -13dBmV ~ +17dBmV
Taxa Máx. de Dados por Canal	344Mbps(8 canais) / 43Mbps(único) @256QAM	444.96Mbps (8 canais) / 55.62 Mbps(canal único) @256 QAM
Taxa Símbolo	5.056941Msps(64QAM), 5.360537Msps(256QAM)	6.952 Msps
Largura de banda	6MHz	8MHz
Potência total de entrada	<30 dBmV	<30 dBmV
Impedância de Entrada	75 Ohms	75 Ohms
RF Upstream		
	DOCSIS	EuroDOCSIS
Faixa de Frequência	5MHz- 42MHz	5MHz ~ 65MHz
Modulação	QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM	QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM
Taxa de Dados máxima por canal:	131 Mbps(4 canais) / 32.78 Mbps (único)	131 Mbps(4 channels) / 32.78 Mbps (Single)
Taxa Símbolo	160, 320, 640, 1,280, 2,560, 5,120Ksym/seg	160, 320, 640, 1,280, 2,560, 5,120Ksym/seg
Largura de banda	200KHz, 400KHz, 800 KHz, 1.6 MHz, 3.2 MHz, 6.4 MHz	200KHz, 400KHz, 800 KHz, 1.6 MHz, 3.2 MHz, 6.4 MHz
Potência de Saída	Um canal no TCS TDMA Pmin a +57 dBmV (32 QAM, 64 QAM) Pmin a +58 dBmV (8 QAM, 16 QAM) Pmin a +61 dBmV (QPSK) S-CDMA Pmin a +56 dBmV (todas as modulações), onde: Pmin = +17 dBmV, 1280 kHz taxa de modulação Pmin = +20 dBmV, 2560 kHz taxa de modulação Pmin = +23 dBmV, 5120 kHz taxa de modulação Dois canais no TCS TDMA Pmin a +54 dBmV (32 QAM, 64 QAM) Pmin a +55 dBmV (8 QAM, 16 QAM) Pmin a +58 dBmV (QPSK) S-CDMA Pmin a +53 dBmV (todas as modulações), onde: Pmin = +17 dBmV, 1280 kHz taxa de modulação Pmin = +20 dBmV, 2560 kHz taxa de modulação Pmin = +23 dBmV, 5120 kHz taxa de modulação	Um canal no TCS TDMA Pmin a +57 dBmV (32 QAM, 64 QAM) Pmin a +58 dBmV (8 QAM, 16 QAM) Pmin a +61 dBmV (QPSK) S-CDMA Pmin a +56 dBmV (todas as modulações), onde: Pmin = +17 dBmV, 1280 kHz taxa de modulação Pmin = +20 dBmV, 2560 kHz taxa de modulação Pmin = +23 dBmV, 5120 kHz taxa de modulação Dois canais no TCS TDMA Pmin a +54 dBmV (32 QAM, 64 QAM) Pmin a +55 dBmV (8 QAM, 16 QAM) Pmin a +58 dBmV (QPSK) S-CDMA Pmin a +53 dBmV (todas as modulações), onde: Pmin = +17 dBmV, 1280 kHz taxa de modulação Pmin = +20 dBmV, 2560 kHz taxa de modulação Pmin = +23 dBmV, 5120 kHz taxa de modulação

	Três ou quatro canais no TCS TDMA Pmin a +51 dBmV (32 QAM, 64 QAM) Pmin a +52 dBmV (8 QAM, 16 QAM) Pmin a +55 dBmV (QPSK) S-CDMA Pmin a +53 dBmV (todas as modulações), onde: Pmin = +17 dBmV, 1280 kHz de taxa de modulação Pmin = +20 dBmV, 2560 kHz de taxa de modulação Pmin = +23 dBmV, 5120 kHz de taxa de modulação	Três ou quatro canais no TCS TDMA Pmin a +51 dBmV (32 QAM, 64 QAM) Pmin a +52 dBmV (8 QAM, 16 QAM) Pmin a +55 dBmV (QPSK) S-CDMA Pmin a +53 dBmV (todas as modulações), onde: Pmin = +17 dBmV, 1280 kHz de taxa de modulação Pmin = +20 dBmV, 2560 kHz de taxa de modulação Pmin = +23 dBmV, 5120 kHz de taxa de modulação
Impedância de Saída	75 Ohms	75 Ohms
Rede		
Gateway	Camada de Aplicação: Cliente/Servidor DHCP; DNS (Proxy & Dinâmico), HTTP, FTP, TFTP; SNMPv1/2, Telnet, SSH Camada de Transporte: TCP (TACACS), UDP(RADIUS) Camada de Rede: ARP, ICMP, IPv4, IPv6, IPSec, RIPv1/2 Camada de Link de Dados: ponte transparente 802.1d, Passagem VPN, PAT, VLAN, Roteamento Estático; ARP; QoS Camada Física: Ethernet 10/100/1000Base T	
Wireless LAN	WiFi 802.11a/b /g/ n Dual Band Dual concorrente 2T2R(2.4GHz/5GHz) 300Mbps PHY taxa de dados Suporta IEEE 802.11e WiFi Multimedia (WMM) Suporta 8 SSIDs WMM-QoS WPS, WPA, WEP (64/128-bit), TKIP,AES, Filtros MAC WPS tecla para Configuração WiFi Protegida com PIN Controle de Acesso Endereço MAC	
Alimentação de Energia		
Tensão de Entrada	100V–240V ~ 50/60Hz	
Tipo	Adaptador	
Consumo de Potência	12V 1.5A	
Proteção	Fusível interno separado. A alimentação deve ser protegida contra queda de raios.	
Especificações físicas		
Tamanho (c/l/h)	225mm (C) x 155 mm (L) x 44 mm (H)	
Peso	Peso líquido 620g +/- 10g	
Temperatura de Operação	0° a 40°C	
Umidade de Operação	20% a 90%	
Temperatura de Armazenagem	-20° a 70°C	

Glossário

Ponto de acesso Um dispositivo que oferece conectividade WLAN a clientes wireless (estações).

Adaptador Um dispositivo ou cartão que faz a conexão de um computador, impressora ou outro dispositivo periférico à rede ou a algum outro dispositivo. Um adaptador wireless conecta um computador à WLAN.

ASCII O Código Padronizado Estadunidense para o Intercâmbio de Informações faz referência a dados alfanuméricos para o processamento e a compatibilidade de comunicação entre diversos dispositivos; normalmente utilizado para transmissão assíncrona.

Autenticação Um processo por meio do qual CMTS verifica se o acesso é autorizado, utilizando uma senha, um endereço IP de confiança ou um número serial.

Autorização Parte do processo entre uma CMTS e o modem de cabo ou gateway para habilitar a Privacidade da Linha Básica.

Largura de Banda A capacidade de transmissão de um meio em termos de uma faixa de frequências. Uma largura de banda maior indica a capacidade de transmitir mais dados ao longo de um determinado período de tempo.

Ponte Um dispositivo de rede de camada 2 OSI que conecta duas LANs utilizando protocolos similares. Ele filtra os frames com base no endereço MAC para reduzir o volume de tráfego. Uma ponte pode ser colocada entre dois grupos de hosts que se comunicam bastante juntos, porém nem tanto com os hosts de outros grupos. A ponte examina o destino de cada pacote para determinar se o transmitirá ao outro lado.

Transmissão Transmissão simultânea para dispositivos de rede múltiplos; um mecanismo de protocolo suporta o grupo e o endereçamento universal.

Modem de cabo Um dispositivo instalado em um local de assinante para oferecer comunicações de dados sobre uma rede HFC. A menos que haja disposição em contrário, todas as referências a “modem de cabo” nesta documentação constituem referência aos modems de cabo DOCSIS ou Euro-DOCSIS somente.

Cliente Em uma arquitetura cliente/servidor, um cliente é um computador que solicita arquivos ou serviços, tais como transferência de arquivos, login remoto ou impressão do servidor. Também chamado um CPE. Em rede WLAN, um cliente é qualquer host que possa se comunicar com o ponto de acesso. Um cliente wireless também é chamado de uma “estação”.

CMTS Um sistema de terminação de modem de cabo é um dispositivo na cabeceira do sistema de cabo que promove a interface da rede HFC com uma rede local ou IP remota para conectar hosts IP, modems a cabo ou gateways e os assinantes. Ele gerencia toda a largura de banda do modem a cabo. Às vezes, é chamado de roteador de extremidade.

Cabo coaxial Um tipo de cabo que consiste de um fio central coberto por isolamento e uma blindagem aterrada de fios coaxiais trançados. A blindagem minimiza a interferência elétrica e de radiofrequência. O cabo coaxial tem grande largura de banda e pode suportar a transmissão por longas distâncias.

CPE Equipamento das dependências de cliente, normalmente computadores, impressoras, etc. que é conectado a um modem a cabo ou gateway no local do assinante. O CPE pode ser disponibilizado pelo assinante ou pelo provedor de Serviços de Internet, também chamado de um cliente.

DHCP Um servidor de Protocolo de Configuração Dinâmica de Host atribui dinamicamente endereços IP a hosts de clientes em uma rede IP. O DHCP elimina a necessidade de designar manualmente endereços IP estáticos por meio da “concessão” de um endereço IP e máscara de sub-rede para cada cliente. Ele permite a reutilização automática de endereços IP não utilizados. Um servidor DHCP na cabeceira do sistema de cabos atribui um endereço IP ao gateway residencial e, opcionalmente, a clientes no gateway residencial LAN. O gateway residencial contém um servidor embutido que atribui endereços IP privativos a clientes.

DMZ Uma “zona desmilitarizada” consiste de um ou mais hosts localizados logicamente entre uma LAN privada e a Internet. A DMZ impede o acesso direto por nossos usuários externos a dados privados. (O termo deriva das áreas tampão localizadas entre países em conflito, tais como a Coreia do Norte e a Coreia do Sul). Em uma configuração pequena típica DMZ, o host DMZ recebe solicitações de usuários de LAN privada para acessar websites externos e iniciar sessões para essas solicitações. O host DMZ não pode iniciar uma sessão de volta para a LAN privada. Os usuários de Internet fora da LAN privada somente podem acessar o host DMZ. Você pode usar um DMZ para configurar um servidor de web ou para jogos sem a exposição de dados confidenciais.

DNS O Sistema de Nome de Domínio é o sistema de Internet para a conversão de nomes de domínio em endereços IP. Um servidor DNS contém uma tabela que cruza os nomes de domínio, tais como Internetname.com, com os endereços IP, tais como 192.169.9.1. Quando você acessa a rede mundial, um servidor DNS traduz o URL exibido no browser ao endereço IP do website de destino. A tabela de consulta DNS é uma base de dados distribuída da Internet; nenhum servidor DNS lista todos os nomes de domínio com os endereços IP correspondentes.

DOCSIS Especificação da Interface de Serviço de Dados por Cabo define os padrões da interface para modems a cabo, gateways e equipamentos de suporte para entregar dados entre uma rede HFC e sistemas de computadores ou aparelhos de televisão. Para enfatizar seu uso como um padrão de modem a cabo, o DOCSIS é agora chamado de Modems a Cabo Certificados CableLabs. O Euro-DOCSIS é o DOCSIS adaptado para uso na Europa.

Downstream Em uma rede de dados a cabo, o sentido dos dados recebidos pelo computador da Internet.

Endereço IP dinâmico Um endereço IP que é temporariamente concedido a um host por um servidor DHCP. O oposto de endereço IP estático.

Encriptar Codificar dados.

Nó terminal Um nó terminal VPN termina o VPN no roteador, de forma que os computadores no gateway residencial LAN não precisam do software do cliente VPN para a ligação em túnel pela Internet até o servidor VPN.

Ethernet O tipo mais amplamente utilizado de LAN, também conhecido como IEEE 802.3. As redes Ethernet mais comuns são baseadas em 10Base-T, que oferecem velocidades de transmissão de até 10 Mbps, em geral sobre fios não blindados, de pares torcidos, com conectores RJ-45. A Fast Ethernet (100Base-T) oferece velocidades de até 100 Mbps. “Base” significa a “tecnologia baseada em banda” e “T” significa “par de cabos torcidos”. Cada porta Ethernet tem um endereço físico denominado endereço MAC.

Euro-DOCSIS Um padrão ComLabs adaptado ao DOCSIS para uso na Europa.

Evento Uma mensagem gerada por um dispositivo para informar um operador ou sistema de gerenciamento de rede de que alguma coisa ocorreu.

Firewall Um sistema de software de segurança no gateway residencial que faz cumprir uma política de controle de acesso entre a Internet e o gateway residencial LAN.

Frame Uma unidade de dados transmitida entre os nós da rede que contém dados de controle de endereçamento e protocolo. Alguns frames de controle não contêm nenhum dado.

Frequência Número de vezes em que um sinal eletromagnético repete um ciclo idêntico em uma unidade de tempo, normalmente um segundo, medida em Hz, kHz, MHz ou GHz

Gateway Um dispositivo que habilita a comunicação entre redes que utilizam diferentes protocolos. Ver também roteador.

Endereço IP do Gateway . O endereço do roteador padrão do Gateway na Internet.

Hexadecimal Um sistema de numeração com base em 16 dígitos que utiliza 16 números sequenciais (0 a 9 e as letras A a F) como unidades de base, antes de acrescentar uma nova posição. Em computadores, o sistema hexadecimal é uma forma conveniente de expressar números binários.

Host Em IP, um host é qualquer computador que suporta aplicações de usuário final ou serviços com acesso à rede bidirecional completa. Cada host tem um número único que, quando combinado com o número da rede, forma seu endereço IP.

Host também pode significar:

- Um computador que roda um servidor web que atende a páginas de um ou mais web sites pertencentes à(s) organização(ões) ou pessoas físicas.
- Uma empresa que presta esse serviço
- Em ambientes IBM, um computador mainframe On e uma rede HFC, um hub é uma cabeceira de rede de escala reduzida que realiza algumas ou todas as funções de cabeceira para parte do sistema.

Hz Hertz — um ciclo por segundo. A unidade para medir a frequência com que um sinal eletromagnético alternado completa ciclos em sua amplitude mais alta e mais baixa. Usado para definir as bandas do espectro eletromagnético utilizadas em comunicações de voz e dados ou para definir a largura de banda de um meio de transmissão.

ICMP Protocolo de Controle de Mensagem de Internet é um protocolo usado para mensagens de erro, problema e informacionais enviadas entre hosts IP e gateways. As mensagens ICMP são processadas pelo software IP e não são normalmente visíveis para o usuário final.

IEEE The Institute of Electrical and Electronics Engineers, Inc. (<http://www.ieee.org>) é uma organização que prepara normas, estudos técnicos e simpósios para as indústrias elétrica e eletrônica, acreditada pela ANSI.

IEEE 802.11b padrões de rede wireless IEEE

IEEE 802.11g

IEEE 802.3 Ver Ethernet.

IP Protocolo de Internet é um conjunto de padrões que permite que diferentes tipos de computadores se comuniquem uns com os outros e permutem dados por meio da Internet. O IP confere uma aparência de um sistema de comunicação único, contínuo e transforma a Internet em uma rede virtual.

Endereço IP Um único valor de 32 bits que identifica cada host em uma rede TCP/IP. As redes TCP/IP roteiam mensagens com base no endereço IP de destino. Um endereço IP tem duas partes:

- Um endereço de rede designado pela IANA
- O administrador de rede de gateway residencial atribui um endereço de host a cada host conectado no gateway residencial, usando automaticamente seu servidor DHCP como endereço IP estático. Para uma rede Classe C, os primeiros 24 bits são o endereço da rede e os oito bits finais são o endereço do host; em formato decimal pontilhado, o endereço IP aparece como "network.network.network.host." Se você habilitar o cliente de gateway residencial DHCP na Página DHCP Básica, o provedor de Serviços de Internet automaticamente atribui um endereço de rede, uma máscara de sub-rede, um nome de domínio, e o servidor DNS para oferecer uma conexão contínua de Internet.

IPSec Os protocolos de Segurança de Protocolo de Internet são autenticação IETF e padrões de criptografia para permuta segura de pacotes na Internet. O IPSec trabalha na camada OSI 3 e garante que tudo esteja na rede.

IKE Troca de Chave de Internet

ISP Provedor de Serviços de Internet

LAN Uma rede de área local oferece conexão em tempo integral, de banda larga alta, sobre uma área limitada, tal como um prédio ou campus. A Ethernet é o padrão LAN de uso mais difundido.

Endereço MAC O endereço de Controle de Acesso à Mídia é único, com valor de 48 bits permanentemente salvo em ROM na fábrica para identificar o dispositivo de rede Ethernet.

MHz Megahertz — um milhão de ciclos por segundo. Uma medida de radiofrequência.

Multicast Uma transmissão de dados enviada por um emissor a múltiplos destinatários.

NAT Tradução de Endereço de Rede é um padrão de Internet para que uma LAN utilize um conjunto de endereços IP para tráfego interno e um segundo conjunto de endereços IP para tráfego externo.

Rede Dois ou mais computadores conectados para comunicar-se entre si. As redes tradicionalmente vêm sendo conectadas utilizando-se algum tipo de fiação.

NIC Um cartão de interface de rede converte dados de computador a dados seriais em um formato de pacote que envia pela LAN. Um NIC é um slot de expansão ou pode ser embutido. Cada NIC Ethernet tem um endereço MAC permanentemente salvo em seu ROM.

Pacote A unidade de dados que é roteada entre o emissor e o destino na internet ou outra rede de comutação de pacotes. Quando dados, tais como uma mensagem de E-mail, eles são enviados pela Internet, o IP do emissor divide os dados em pacotes de numeração única. O cabeçalho do pacote contém os endereços IP da fonte e do destino. Os pacotes individuais podem percorrer rotas diferentes. Quando todos os pacotes chegam ao destino, o IP no terminal remonta os pacotes.

Passagem Um cliente de passagem no gateway residencial LAN obtém seu endereço IP público do servidor DHCP do provedor de serviços de Internet.

PING Uma ferramenta de rede que testa a possibilidade de alcance do host, enviando um pequeno pacote ao host e aguardando uma resposta. Se você fizer um PING em um endereço IP de computador e receber uma resposta, saberá que o computador está acessível pela rede. A sigla também significa Packet InterNet Groper.

Porta Em um computador ou outro dispositivo eletrônico, uma porta é um soquete ou plugue utilizado para conectá-lo fisicamente à rede ou a outros dispositivos. Em TCP/IP, uma porta é um número de 0 a 65536 usado logicamente por um programa de cliente para especificar um programa do servidor. As portas 0 a 1024 são reservadas.

Ativação de portas Um mecanismo que autoriza a comunicação que entra com aplicações específicas. Essencialmente utilizado para aplicativos de jogos.

PPTP Protocolo Ponto-a-Ponto de Tunelização encapsula outros protocolos. É uma nova tecnologia para criar VPNs desenvolvidos em conjunto por diversos fornecedores.

Protocolo Um conjunto formal de regras e convenções para intercâmbio de dados. Diferentes tipos de computador (por exemplo, PC, UNIX ou mainframe) podem comunicar-se se suportarem protocolos comuns.

Provisionamento O processo de autodescoberta ou configuração manual de um modem a cabo no CMTS.

QoS A qualidade do serviço descreve a prioridade, o atraso, o rendimento e a largura de banda de uma conexão.

RF Radiofrequência — sinais utilizados pelo transmissor e receptor CMTS para enviar dados em HFC. A portadora é modulada para codificar o fluxo de dados digitais para transmissão através da rede de cabos.

Roteador Nas redes IP, um dispositivo que conecta pelo menos duas redes, as quais podem ser similares ou não. Um roteador normalmente é um dispositivo localizado em um gateway entre redes. Um roteador opera em uma rede de camada 3 OSI. Ela filtra pacotes baseados no endereço IP, examinando os endereços IP de origem e destino para determinar a melhor rota pela qual devem enviá-los. Um roteador frequentemente é incluído como parte do computador de rede. Um roteador também pode ser implantado como software em um computador.

Tabela de Roteamento Uma tabela que descreve as rotas disponíveis, as quais são utilizadas por um roteador para determinar a melhor rota para um pacote.

RTS Servidor de solicitação de envio. Em uma arquitetura cliente/servidor, um computador dedicado que alimenta arquivos ou oferece serviços, tais como uma transferência de arquivos, login remoto ou impressão para clientes.

Provedor de Serviços Uma empresa que presta serviços de dados ou telefone a Assinantes.

SMTP Protocolo Simples de Transferência de Mensagem é um protocolo padronizado de Internet para a transferência de mensagens por e-mail.

Splitter Trata-se de um dispositivo que divide o sinal de um cabo de alimentação entre dois ou mais cabos.

SSID O Identificador do Conjunto de Serviços ou nome da rede é um identificador único que os clientes wireless utilizam para associar a um ponto de acesso para diferenciá-lo das WLANs múltiplas na mesma área. Todos os clientes de uma WLAN devem ter o mesmo SSID que o ponto de acesso.

Endereço IP estático Um endereço IP permanentemente atribuído a um host. Normalmente, um endereço IP estático deve ser designado manualmente. O oposto do endereço de IP dinâmico.

Estação IEEE 802.11b Termo para cliente wireless

Assinante Uma residência ou escritório que acesse televisão, dados ou outros serviços por meio de um provedor de Serviços de Internet.

Máscara de Sub-Rede Uma máscara de bits que se conecta por via lógica AND ao endereço IP de destino de um pacote para determinar o endereço de rede. Um roteador roteia os pacotes que utilizam o endereço IP de um pacote para determinar o endereço da rede. Um roteador roteia pacotes utilizando o endereço da rede.

SYSLOG Um padrão UNIX de fato para histórico de eventos do sistema.

TCP Protocolo de Controle de Transmissão na camada quatro OSI de transporte oferece transporte confiável na rede para os dados transmitidos utilizando-se IP (camada três de rede). Trata-se de um protocolo de ponta-a-ponta que define as regras e procedimentos para o intercâmbio de dados entre hosts sobre IP sem conexão. O TCP utiliza um cronômetro para rastrear os pacotes pendentes, verifica erros nos pacotes que chegam e retransmite pacotes, caso solicitado.

TCP/IP Protocolo de Controle de Transmissão/suíte de Protocolo de Internet. Prevê os padrões e regras para a comunicação de dados entre redes na Internet. É o padrão de interconexão mundial em rede e o protocolo de comunicações básicas da Internet.

TFTP Protocolo de Transferência de Arquivo Trivial é um protocolo muito simples utilizado para a transferência de arquivos.

TKIP Protocolo de Integridade de Chave Temporal

Túnel Para colocar pacotes no interior de outros pacotes e enviá-los pela rede. O protocolo do pacote que envolve os demais é entendido pelo nó terminal ou pela interface do túnel, no qual o pacote entra e sai da rede. Os VPNs confiam na tunelização para criar uma rede segura.

A tunelização requer os seguintes tipos de protocolo:

- Um protocolo de portadora, tal como o TCP, utilizado pela rede na qual os dados viajam
- Um protocolo de encapsulamento, tal como IPSec, L2F, L2TP ou PPTP, o qual envolve os dados originais.

- Um protocolo de passageiro, tal como o IP, para os dados originais

Bidirecional Um sistema de cabos que pode transmitir sinais em ambas as direções, de e para a cabeceira de rede e o assinante

UDP Protocolo de Datagrama de Usuário

Unicast Uma transmissão de dados ponto-a-ponto enviada de um emissor para um destinatário. Este é o caminho normal para você acessar websites.

Upstream Em uma rede de dados a cabo, *upstream* descreve o sentido dos dados enviados do computador de um assinante por meio do modem a cabo ao CMTS e à Internet.

VoIP Voz sobre Protocolo de Internet é um método para troca de comunicação de voz, telefax e outras informações pela Internet. Voz e fax vêm sendo transmitidos tradicionalmente por linhas telefônicas de PSTN, utilizando um circuito dedicado para cada linha. VoIP permite que as chamadas trafeguem como pacotes de dados diferenciados nas linhas compartilhadas. VoIP é uma parte importante da convergência de computadores, telefones e televisão em uma rede única de informações integradas.

VPN Uma rede privada virtual é uma rede privada que utiliza conexões “virtuais” (túneis) roteados sobre uma rede pública (normalmente à Internet) para oferecer conexão rápida e segura, normalmente para usuários que trabalham remotamente em casa ou em pequenas filiais de empresas. Uma conexão VPN oferece segurança e desempenho similares a um link dedicado (por exemplo, uma linha concedida), porém a um custo inferior.

WAN Uma rede de área ampla oferece uma conexão sobre uma ampla área geográfica, tal como um país ou todo o mundo. A largura de banda depende da necessidade e dos custos, porém normalmente é muito inferior aos de uma LAN.

WEP A encriptação de Privacidade Equivalente à Com Fio protege a privacidade dos dados transmitidos sobre a WLAN. WEP utiliza chaves para encriptar e desencriptar os dados transmitidos. O ponto de acesso deve autenticar um cliente antes de transferir os dados a um outro cliente. A WEP é parte do IEEE 802.11b. A WEP pode ser difícil de usar e não oferece encriptação resistente.

WiFi Nome da marca - *Wireless fidelity* (pronunciada y-phi [uai-fai]) aplicada aos produtos que suportam IEEE 802.11b.

WLAN wireless LAN

WPA Encriptação Acesso Wi-Fi Protegido (WPA), conforme a descrição na página da web da Wi-Fi Alliance: <http://www.wifialliance.org>. Trata-se de uma forma mais robusta de encriptação que a WEP.

Aviso de Software de Fonte Aberta

Este produto inclui código de software desenvolvido por terceiros, inclusive código de software sujeito à Licença Pública em Geral (GPL) ou Licença Pública Geral Menor (LGPL). Conforme o caso, os termos GPL e LGPL e as informações sobre a obtenção de acesso ao código GPL e ao código LGPL utilizados neste produto estão disponíveis para você em <http://192.168.0.1/GPL/> (inclusive a RG web UI).

O código GPL e o código LGPL utilizados neste produto são distribuídos SEM QUALQUER GARANTIA, além de estar sujeitos a direitos autorais de um ou mais autores. Para detalhes, verificar o Código GPL e o Código LGPL para este produto e os termos do GPL e do LGPL.