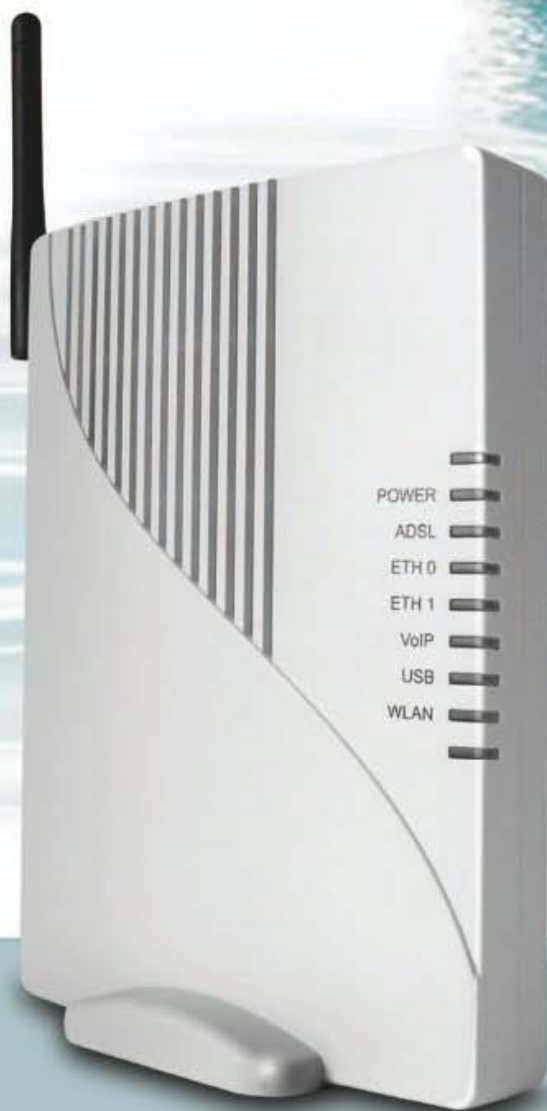


IRELLI

BROADBAND
SOLUTIONS

 **access**



Discus™ DRG A223G

 **discus™**

ÍNDICE

Configuração do Router 1

Introdução 1

Secção sobre Configuração Rápida 6

Ligação de Internet 7

Conta SIP 7

Secção sobre as Ligações de Rede 8

Ponte LAN 9

Ponte LAN >> Geral 9

Ponto de Acesso 802.11g da LAN sem fios 10

Ponto de Acesso 802.11g da LAN sem fios>> Geral 10

Ponto de Acesso 802.11g da LAN sem fios >> Definições 11

Ponto de Acesso 802.11g da LAN sem fios >> Sem fios 12

Ponto de Acesso 802.11g da LAN sem fios >> Avançadas 17

WAN PPOE 19

WAN PPOE >> GERAL 19

Secção sobre Segurança 20

Geral 21

Controlo dos Acessos 23

Reencaminhamento de Portas 25

Anfitrião DMZ 28

Restrições a *websites* 29

NAT 30

Filtragem Avançada 31

Secção sobre VoIP 33

Definições da Linha 33

Marcação Rápida 34

Monitorização 35

Secção sobre as Definições Avançadas 37

Acerca do DRG A223G 38

Ficheiro de Configuração 39
DDNS 40
Servidor DNS 41
Actualização do *Firmware* do DRg A223G 42
Data e Hora 44
Diagnósticos 45
Distribuição de Endereços de IP 48
Protocolos 49
Reiniciação 50
Restaurar as Predefinições 51
Roteamento 52
SSH 53
Regras Programadas 54
Universal Plug and Play 56

Secção de Monitorização do Sistema 57

Ligações de Rede 57
Registo de Sistema 58
CPU 59

Configuração do Router

INTRODUÇÃO

O programa de configuração do Router é baseado na *web*, o que significa que o acesso é feito através do seu *browser da web*.

Para aceder ao servidor *web* do Router:

1. Inicie o seu *browser* no computador
2. Introduza o seguinte URL no campo de localização ou de endereço do seu *browser*: `http://192.168.1.1`



O Router vem com um endereço de IP predefinido (192.168.1.1). Se mudar o endereço, por favor tome nota do novo endereço de IP do Router, caso contrário deve ser feita uma operação de "Reset to Factory Default" (Restaurar os Padrões de Fábrica) para poder voltar a ter acesso ao Router.

O acesso às páginas de configuração do router ADSL é controlado através de contas de utilizador. A conta predefinida é a do utilizador *admin*, o qual pode alterar e visualizar a configuração do Router ADSL sem restrições.



Tanto o nome de utilizador como a palavra-passe predefinidos são "admin". Recomenda-se que altere estes valores predefinidos. Certifique-se de que se lembra do seu nome de utilizador e palavra-passe, pois esta é a única forma através da qual vai ser capaz de gerir o seu Router.

Vai ser-lhe pedido que escolha o idioma da interface do Router entre *inglês, francês, russo, espanhol, coreano, chinês tradicional, japonês, alemão, italiano e chinês simplificado*, e que introduza um *User Name* (nome de utilizador) e uma *Password* (palavra-passe): insira-os para aceder aos painéis de configuração.

No primeiro início de sessão, se os parâmetros de ligação ainda não tiverem sido configurados, é apresentado o painel *Installation Wizard* (assistente de instalação) para que possa configurar estes parâmetros. Se já tiverem sido configurados, é aberta a *Home page* (página principal) tal como mostra a Figura 1.

A *Home page* possui um menu à esquerda, sempre disponível em todas as páginas *web*, que é o ponto de partida para a configuração de qualquer Router.

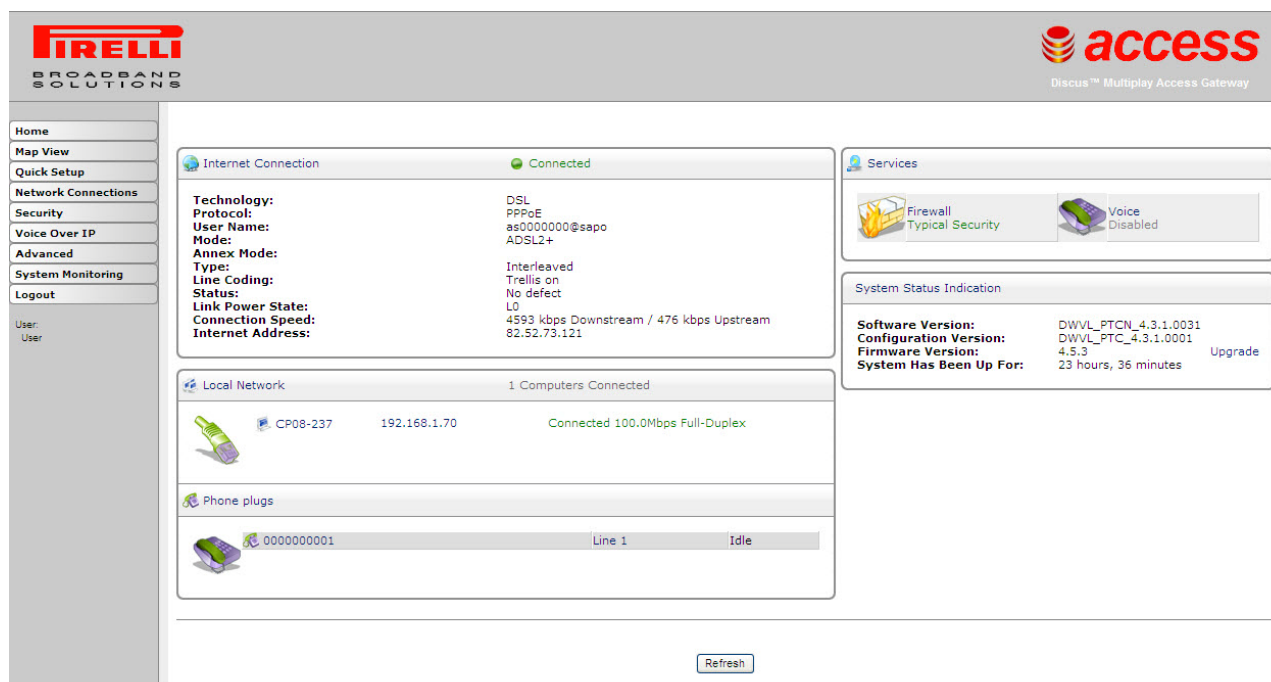
O menu completo tem os seguintes itens principais:

1. **Home (página principal):** mostra uma representação gráfica da sua rede.
2. **Map View (visualização do mapa):** apresenta o mapa de rede dos dispositivos anexados ou configurados. Figura 2, em baixo.
3. **Quick Setup (configuração rápida):** permite configurar a ligação do Router com rapidez.
4. **Network Connections (ligações de rede):** mostra o estado das ligações de rede, permitindo modificá-las ou criar novas ligações.
5. **Security (segurança):** permite configurar as definições de segurança.
6. **Voice over IP (voz sobre IP):** permite configurar contas VoIP.
7. **Advanced (avançadas):** permite o acesso aos painéis de configuração avançados e permite definir parâmetros do Router dedicados ao acesso dos utilizadores, gestão do registo, hora do Router, *backup* da configuração do Router, etc.
8. **System Monitoring (monitorização do sistema):** menu que mostra e permite executar testes de diagnóstico para fins de resolução de problemas ou de análise de comportamento do sistema, e para ter acesso a informações sobre o dispositivo e estatísticas.
9. **Logout (terminar sessão):** terminar a sessão do Router.



*Para submeter as alterações efectuadas à maior parte dos parâmetros do dispositivo, é necessário clicar no botão **Apply** (aplicar) para que as alterações sejam guardadas permanentemente. Em alguns casos, é necessário reiniciar o Router.*

FIGURA 1.



A tabela que se segue apresenta uma lista de todos os objectos de rede disponíveis com a sua respectiva descrição.

TABELA 1. Objectos de Rede Disponíveis




Mapa de Símbolos	Descrição
	Representa a Internet.
	Representa a sua ligação ADSL de Rede de Área Alargada (WAN). Clique neste ícone para configurar a interface WAN.
	Representa a sua ligação Ethernet de Rede de Área Alargada (WAN) ou uma ligação Ethernet de Rede Local (LAN). Clique neste ícone para configurar a interface WAN ou o dispositivo Ethernet LAN.

TABELA 1. Objectos de Rede Disponíveis

Mapa de Símbolos

Descrição



Representa o Firewall (parede corta-fogo) da porta de ligação. A altura da parede corresponde ao nível de segurança definido no momento em questão: Mínimo, Típico ou Máximo. Clique neste ícone para configurar as definições de segurança.



Representa uma ligação USB LAN. Clique neste ícone para configurar os parâmetros de rede do dispositivo USB LAN.



Representa uma ligação LAN sem fios. Clique neste ícone para configurar os parâmetros de rede do dispositivo LAN sem fios.



Representa uma ponte (bridge) ligada na rede doméstica. Clique neste ícone para ver os dispositivos subjacentes da ponte.



Representa um computador (sistema anfitrião) ligado na rede doméstica. Cada um dos computadores ligados à rede aparece por baixo do símbolo de rede correspondente à rede através da qual esse computador está ligado. Clique num dos ícones para ver informação sobre o computador correspondente.

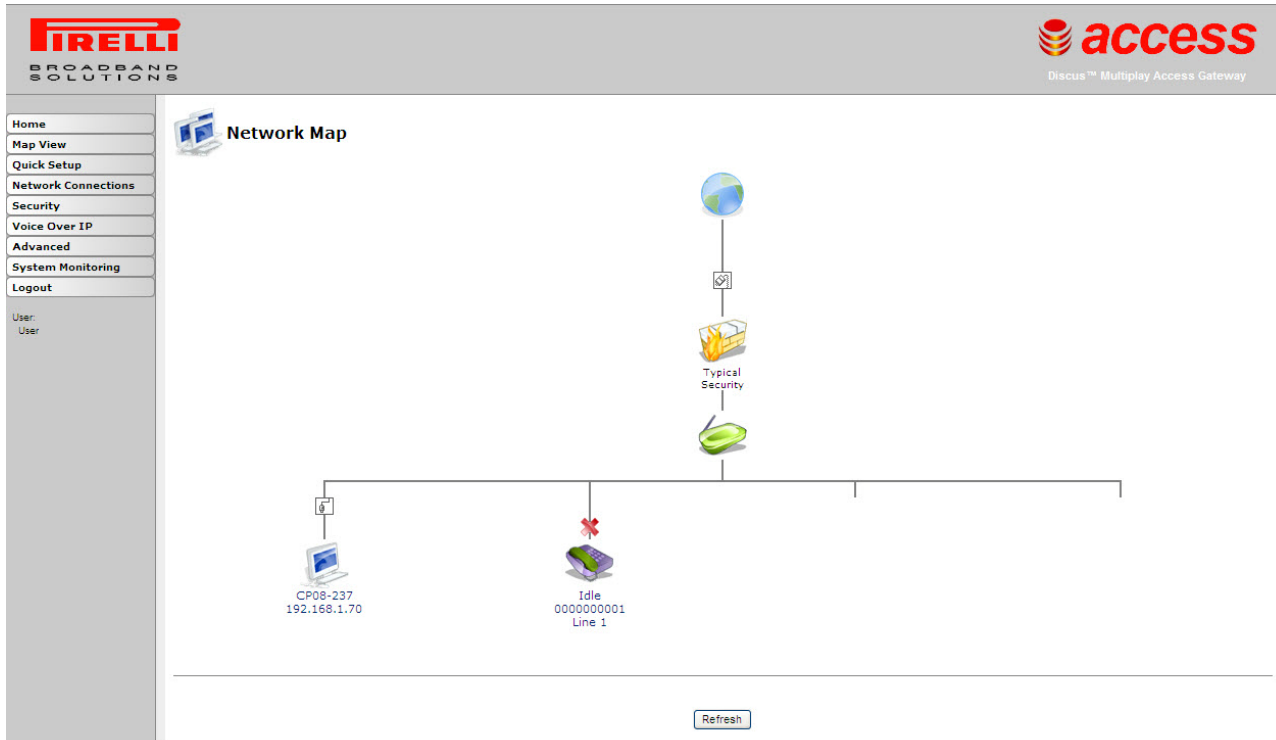


Representa uma impressora que está ligada ao Router e que é partilhada pelos utilizadores da rede. Clique no ícone para ver as definições da impressora.



Representa um servidor de ficheiros que está ligado ao Router e que é partilhado pelos utilizadores da rede. Clique no ícone para ver a configuração do servidor de ficheiros.

FIGURA 2 Map View (visualização do mapa):



Secção sobre Configuração Rápida

Este capítulo irá descrever a **Secção sobre Configuração Rápida** (Quick Setup Section), a qual pode ser acedida através da *home page* do **DISCUS™ DRG A223G**, mediante a autenticação do utilizador do Router.



Esteja ciente de que quaisquer alterações à configuração podem comprometer a sua conectividade.

Quando estiver a subscrever um serviço de banda larga, deve estar ciente do método através do qual se liga à Internet. O seu dispositivo WAN físico pode ser Ethernet, ADSL ou ambos. Qualquer informação técnica acerca das propriedades da sua ligação de Internet deve ser providenciada pelo seu Fornecedor de Serviços Internet (ISP). Por exemplo, o seu ISP deve informá-lo se a sua ligação à Internet é feita através de um endereço de IP estático ou dinâmico, ou dos protocolos, tais como o PPTP ou o PPPoE, que irá utilizar para comunicar através da Internet.

O Router vai reconhecer automaticamente se há mais de um dispositivo WAN físico na sua porta de ligação e vai definir automaticamente os parâmetros necessários para configurar a ligação WAN.

O utilizador deve apenas fazer a sua autenticação através da secção de Configuração Rápida.

FIGURA 1 Painel de Configuração Rápida

PIRELLI
BROADBAND
SOLUTIONS

access
Discus™ Multiplay Access Gateway

Quick Setup

Internet Connections

WAN DSL

Login User Name (case sensitive): as000000@sapo

Login Password: *****

SIP Account

Enabled

Authentication User Name:

Authentication Password:

OK Cancel

INTERNET CONNECTION (LIGAÇÃO DE INTERNET)

A(s) sua(s) ligação(ões) WAN é/são configurada(s) automaticamente pelo Router.

Deve introduzir as informações da conta:

- Nome de utilizador
- Palavra-passe

SIP ACCOUNT (CONTA SIP)

1. Para activar a conta SIP precisa apenas de seleccionar *Enabled* (funcionalidade activa) e introduzir o nome de utilizador e a palavra-passe para a autenticação da SIP.

Secção sobre as Ligações de Rede

Este capítulo irá descrever a **Secção sobre as Ligações de Rede**, a qual pode ser acedida através da *home page* do **DISCUS™ DRG A223G**.



Esteja ciente de que quaisquer alterações à configuração podem comprometer a sua conectividade.

Pretende-se que esta secção (ver Figura 1) apresente um resumo das ligações do Router, tais como as interfaces WAN e LAN (i.e. Ethernet, USB, sem fios).

O **DISCUS™ DRG A223G** suporta várias ligações de rede, tanto físicas como lógicas. O ecrã *Network Connections* (ligações de rede) permite-lhe configurar os vários parâmetros das suas ligações físicas – a LAN e a WAN – e criar novas ligações utilizando protocolos de túnel sobre as ligações existentes, tais como o PPP ou o VPN.

Clique no botão *Advanced* (avançadas) para expandir o ecrã e exibir todas as entradas de ligação.

FIGURA 1 *Network Connections Panel* (painel das ligações de rede)



LAN BRIDGE (PONTE LAN)

A ligação em ponte LAN é usada para combinar vários dispositivos LAN numa única rede virtual. Por exemplo, pode criar uma rede para dispositivos LAN Ethernet e LAN sem fios.

Repare que, quando uma ponte é removida, os anteriores dispositivos subjacentes da ponte herdam as definições DHCP desta. Por exemplo, a remoção de uma ponte configurada como cliente DHCP configura automaticamente os anteriores dispositivos LAN que constituíam a ponte como clientes DHCP, com a configuração de cliente DHCP exacta.

LAN BRIDGE >> GENERAL (PONTE LAN >> GERAL)

Para visualizar e alterar as definições de ligação da ponte LAN clique no *link LAN Bridge*, no ecrã *Network Connections*. Vai, então, aparecer o ecrã *LAN Bridge Properties* (propriedades da ponte LAN), o qual apresenta um resumo detalhado dos parâmetros de ligação, por baixo do separador *General* (geral). Estes parâmetros podem ser alterados nos restantes separadores do ecrã, tal como vai ser descrito nas secções seguintes.

FIGURA 2 LAN Bridge >> General Panel (Ponte LAN >> Painel Geral)

LAN Bridge Properties
General

Name:	LAN Bridge
Device Name:	br0
Status:	Connected
Network:	LAN
Underlying Device:	LAN Ethernet LAN Ethernet 2 LAN Wireless 802.11g Access Point LAN USB
Connection Type:	Bridge
MAC Address:	00:22:33:e5:e5:e5
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Received Packets:	11086
Sent Packets:	19563
Time Span:	23:41:55

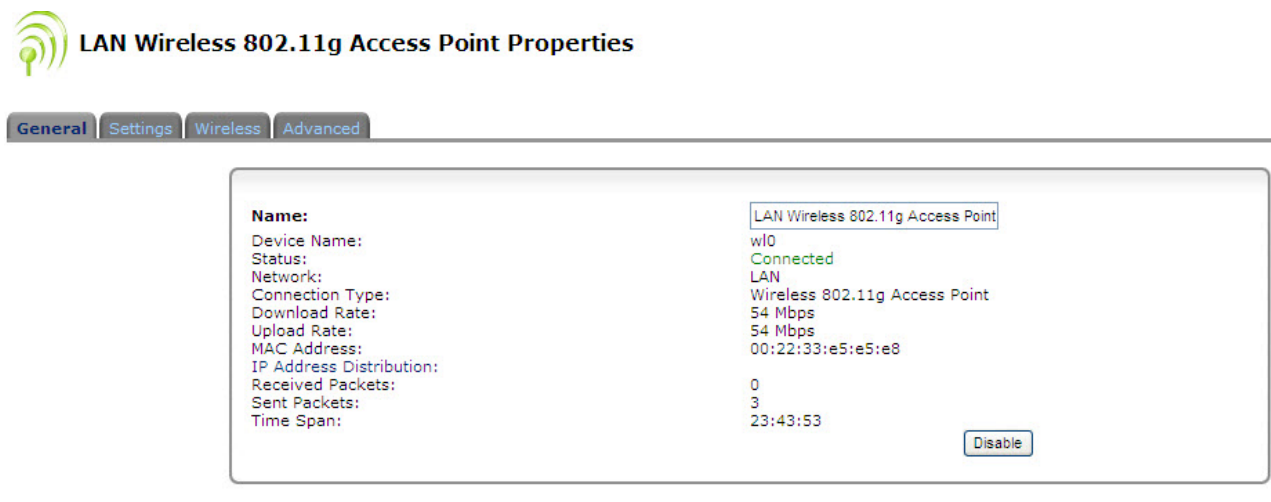
**LAN WIRELESS 802.11g
ACCESS POINT (PONTO DE
ACESSO DA LAN SEM FIOS
802.11G)**

O **DISCUS™ DRG A223G** integra múltiplas camadas de segurança sem fios. Estas incluem o protocolo de autenticação baseada em portas IEEE 802.1x, o cliente RADIUS, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Acesso Protegido Wi-Fi (WPA), WPA2, WPA e WPA2 (modo misto) e o *Firewall* Discus e as aplicações VPN, líderes no sector. Além disso, o servidor de autenticação incorporado do Router permite aos utilizadores home/SOHO definir utilizadores sem fios autorizados sem que seja preciso um servidor RADIUS externo.

**LAN WIRELESS 802.11g
ACCESS POINT >>
GENERAL (PONTO DE
ACESSO DA LAN SEM FIOS
802.11G >> GERAL)**

Para visualizar e alterar as definições de ligação da LAN sem fios clique no *link LAN Wireless 802.11g Acess Point*, no ecrã *Network Connections*. Vai, então, aparecer o ecrã *LAN Wireless 802.11g Acess Point* (ponto de acesso da LAN sem fios 802.11g), o qual apresenta um resumo detalhado dos parâmetros de ligação, por baixo do separador *General* (geral). Estes parâmetros podem ser alterados nos restantes separadores do ecrã, tal como vai ser descrito nas secções seguintes.

FIGURA 3 LAN Wireless 802.11g Access Point >> General Panel (Ponto de Acesso da LAN sem fios 802.11g >> Paineil Geral)



LAN Wireless 802.11g Access Point Properties

General Settings Wireless Advanced


Name:	LAN Wireless 802.11g Access Point
Device Name:	wl0
Status:	Connected
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Download Rate:	54 Mbps
Upload Rate:	54 Mbps
MAC Address:	00:22:33:e5:e5:e8
IP Address Distribution:	
Received Packets:	0
Sent Packets:	3
Time Span:	23:43:53

Disable

**LAN WIRELESS 802.11g
ACCESS POINT >>
SETTINGS (PONTO DE
ACESSO DA LAN SEM FIOS
802.11G >> DEFINIÇÕES)**

General (geral): Esta secção apresenta os parâmetros gerais da ligação. Recomenda-se que não altere os valores predefinidos, a não ser que esteja familiarizado com os conceitos de rede que estes representam. Visto que a sua porta de ligação está configurada para operar com os valores predefinidos, não é necessária qualquer modificação de parâmetros.

FIGURA 4 LAN Wireless 802.11g Access Point >> Settings Panel (Ponto de Acesso da LAN sem fios 802.11g >> Paineil Definições)



LAN Wireless 802.11g Access Point Properties

General Settings Wireless Advanced

Device Name:	wl0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Physical Address:	00:22:33:e5:e5:e8
MTU:	Automatic 1500

Schedule (agenda): Por predefinição, a ligação estará sempre activa. No entanto, pode configurar regras programadas para definir segmentos de tempo

durante os quais a ligação pode estar activa. Assim que for(em) definida(s) (uma) regra(s) programada(s), o campo transforma-se numa caixa de combinação (combo-box) permitindo-lhe escolher entre as regras disponíveis.

Network (rede): Escolha se os parâmetros que está a configurar dizem respeito a uma ligação WAN, LAN ou DMZ escolhendo o tipo de ligação na caixa de combinação.

Physical Address (endereço físico): Consiste no endereço físico da placa de rede usada pela sua rede. Algumas placas permitem-lhe alterar este endereço.

MTU: A MTU é a Unidade Máxima de Transmissão. Esta especifica qual o maior pacote permitido para a transmissão Internet. Na definição predefinida – Automatic (automático) – a porta de ligação selecciona a melhor MTU para a sua ligação de Internet. Seleccione *Automatic by DHCP* (automático por DHCP) para que seja o DHCP a determinar a MTU. Caso seleccione *Manual*, recomenda-se que introduza um valor entre 1200 e 1500.


**LAN WIRELESS 802.11g
ACCESS POINT >>
WIRELESS (PONTO DE
ACESSO DA LAN SEM FIOS
802.11G >> SEM FIOS)**

Wireless Access Point (Ponto de Acesso Sem Fios)

Sirva-se desta secção para definir as definições básicas do ponto de acesso sem fios.

SSID: O SSID é o nome da rede partilhado por todos os pontos numa rede sem fios. O SSID deve ser idêntico para todos os pontos da rede sem fios. É sensível a maiúsculas e minúsculas e não deve exceder 32 caracteres (use qualquer um dos caracteres no teclado). Certifique-se de que esta definição é igual para todos os pontos da sua rede sem fios. Para ter segurança adicional deve mudar o SSID predefinido (openrg) para um nome especial.


FIGURA 5 LAN Wireless 802.11g Access Point >> Wireless Panel (Ponto de Acesso da LAN sem fios 802.11g >> Pannel sem fios)

 LAN Wireless 802.11g Access Point Properties

General Settings **Wireless** Advanced

Wireless Network (SSID):
 SSID Broadcast
802.11 Mode: 802.11b/g Mixed
Country: Portugal
Channel: Automatic (2.412)
Network Authentication: Open System Authentication
HAC Filtering Mode: Disable




HAC Filtering Table

New MAC Address	HAC Address	Action
		

Security: WPA
Authentication Method: Pre-Shared Key
Pre-Shared Key:
Encryption Algorithm: TKIP
 Group Key Update Interval: 300 Seconds
 Inter-Client Privacy

Transmission Rate: Auto
CTS Protection Mode: None
CTS Protection Type: cts-only
Frame Burst - Max Number: 3
Frame Burst - Burst Time: 2
Beacon Interval: 100 ms
DTIM Interval: 1 ms
Fragmentation Threshold: 2348
RTS Threshold: 2347

Virtual APs

Name	BSSID	SSID	Status	Action
 LAN Wireless 802.11g Access Point	00:22:33:e5:e5:e8	PBS-E5E5E5	Connected	
New Virtual AP 				

Wireless WDS: Enabled

SSID Broadcast (difusão do SSID): Seleccione esta caixa para activar a difusão do SSID. Usa-se a difusão do SSID para ocultar o nome do AP (SSID) para que clientes que não devam ter conhecimento da sua existência não o possam ver.

802.11 Mode (modo 802.11): Selecciono o padrão de comunicação sem fios que é compatível com a placa sem fios do seu PC. Pode trabalhar no modo 802.11g, 802.11b ou no modo misto.

Country (país): Selecciono o país em questão entre as opções da lista.

Channel (canal): Selecciono o canal adequado da lista de forma a corresponder às definições da sua rede. Cada um dos dispositivos na sua rede sem fios deve ser difundido num canal diferente para que todos possam funcionar correctamente. Os canais disponíveis dependem da Autoridade Reguladora (entre parêntesis) à qual a sua porta de ligação se conforma.

Network Authentication (autenticação da rede): O método de autenticação da rede WPA é *Open System Authentication* (autenticação de sistema aberto), o que significa que a autenticação não é feita através de uma chave de rede. Quando usar os protocolos de segurança 802.1X WEP ou Non-802.1X WEP, este campo transforma-se numa caixa de combinação, oferecendo o método *Shared Key Authentication* (autenticação com chave partilhada), o qual usa uma chave de rede para fazer a autenticação, ou ambos os métodos em conjunto.

MAC Filtering Mode (modo de filtragem MAC): Pode filtrar os utilizadores sem fios de acordo com o seu endereço MAC, autorizando ou negando o acesso aos mesmos. Escolha a acção a executar entre as opções oferecidas no menu pendente.

MAC Filtering Table (tabela de filtragem MAC)

Sirva-se desta secção para configurar as definições avançadas do ponto de acesso sem fios.

New MAC Address (novo endereço MAC): Clique neste *link* para definir a filtragem de endereços MAC. Introduza o endereço MAC a ser filtrado e clique no botão *OK*. Irá, então, aparecer uma lista dos endereços MAC nos quais será executada a acção de filtragem seleccionada.

Security (segurança):

Para configurar a segurança da sua ligação sem fios, pode escolher entre WPA, WPA2, WPA e WPA2, 802.1x WEP, e Non-802.1x WEP. O ecrã irá ser actualizado para apresentar a configuração de cada protocolo, respectivamente.

WPA: O WPA é um método de encriptação de dados para LANs sem fios 802.11.

Authentication Method (método de autenticação): Selecciono o método de autenticação que gostaria de usar. Pode escolher entre *Pre-Shared Key* (chave pré-partilhada) e 802.1x.

Pre-Shared Key (chave pré-partilhada): Esta entrada só aparece se tiver seleccionado este método de autenticação. Introduza a sua chave de encriptação no campo *Pre-Shared Key*. Pode usar tanto um valor ASCII como um valor Hex, seleccionando o tipo de valor na caixa de combinação que é fornecida.

Encryption Algorithm (algoritmo de encriptação): Selecciona entre *Temporal Key Integrity Protocol* (protocolo de integridade de chave temporária) ou TKIP, e *Advanced Encryption Standard* (padrão de encriptação avançado) ou AES, para o algoritmo de encriptação.

Group Key Update Interval (intervalo de actualização de chave de grupo)
Define o intervalo de tempo em segundos que uma chave de grupo demora a ser actualizada.

WPA2: O WPA2 é uma versão melhorada do WPA e define o protocolo 802.11i.

Authentication Method (método de autenticação): Selecciona o método de autenticação que gostaria de usar. Pode escolher entre *Pre-Shared Key* (chave pré-partilhada) e 802.1x.

Pre-Shared Key (chave pré-partilhada): Esta entrada só aparece se tiver seleccionado este método de autenticação. Introduza a sua chave de encriptação no campo *Pre-Shared Key*. Pode usar tanto um valor ASCII como um valor Hex, seleccionando o tipo de valor na caixa de combinação que é fornecida.

Encryption Algorithm (algoritmo de encriptação): O algoritmo de encriptação usado para o WPA2 é o *Advanced Encryption Standard* (padrão de encriptação avançado) ou AES.

Group Key Update Interval (intervalo de actualização de chave de grupo)
Define o intervalo de tempo em segundos que uma chave de grupo demora a ser actualizada.

WPA e WPA2 em Modo Misto: O WPA e WPA2 é um método misto de encriptação de dados.

Authentication Method (método de autenticação): Selecciona o método de autenticação que gostaria de usar. Pode escolher entre *Pre-Shared Key* (chave pré-partilhada) e 802.1x.

Pre-Shared Key (chave pré-partilhada): Esta entrada só aparece se tiver seleccionado este método de autenticação. Introduza a sua chave de encriptação no campo *Pre-Shared Key*. Pode usar tanto um valor ASCII como um valor Hex, seleccionando o tipo de valor na caixa de combinação que é fornecida.

Encryption Algorithm (algoritmo de encriptação): O algoritmo de encriptação usado para o WPA e WPA2 é ou o *Temporal Key Integrity Protocol* (protocolo de integridade de chave temporária) ou TKIP, ou o *Advanced Encryption Standard* (padrão de encriptação avançado) ou AES.

Group Key Update Interval (intervalo de actualização de chave de grupo): Define o intervalo de tempo em segundos que uma chave de grupo demora a ser actualizada.

802.1x WEP: O 802.1x WEP é um método de encriptação de dados que usa uma chave definida estaticamente ou automaticamente, para clientes sem fios que usam 802.1x para fins de autenticação e WEP para fins de encriptação. Pode definir até quatro chaves, mas pode usar apenas uma de cada vez.

Generate Keys Automatically (gerar chaves automaticamente): Selecione esta opção para gerar as chaves de encriptação automaticamente, em vez de as introduzir manualmente. O ecrã vai ser actualizado, escondendo a tabela de chaves descrita em baixo.

Group Key Update Interval (intervalo de actualização de chave de grupo): Define o intervalo de tempo em segundos que uma chave de grupo demora a ser actualizada. Active *Select the Encryption Key* (seleccionar a chave de encriptação) para fazer a activação.

Encryption Key (chave de encriptação): Comece a introduzir a chave de encriptação até o campo inteiro estar preenchido. A chave não pode ser mais curta do que a extensão do campo.

Entry Method (método de entrada): Selecione o tipo de caracteres da chave: Hex ou ASCII. Selecione o comprimento da chave em bits: 40 ou 104 bits.

Key Length (comprimento da chave): Selecione o comprimento da chave em bits: 40 ou 104 bits.

Non-802.1x WEP: O Non-802.1xWEP WEP é um método de encriptação de dados que usa uma chave definida estaticamente para clientes sem fios que não usam 802.1x para fins de autenticação e WEP para fins de encriptação. A configuração deste método é virtualmente idêntica à do método 802.1x WEP, descrito em cima, com excepção da geração automática da chave e da especificação do intervalo de actualização de chave de grupo. Por favor, consulte a secção anterior sobre o 802.1x WEP quando estiver a configurar este método. Lembre-se que a chave estática também tem de ser definida no cliente Windows sem fios.

Wireless QoS (WMM) (QoS sem fios)

O *Wi-Fi* Multimédia (WMM) oferece funcionalidades básicas de Qualidade de Serviço (QoS) para redes IEEE 802.11. Se a sua placa sem fios suporta WMM,

active esta funcionalidade seleccionando a caixa de verificação *Enabled* (activa).

Quando o WMM está activo, é dada a mais elevada prioridade aos pacotes de Voz, sendo que os pacotes de Fundo recebem a prioridade mais baixa.

Além disso, pode controlar a fiabilidade do fluxo de tráfego. Por predefinição, a *Ack Policy* (política de confirmação) para cada categoria de acesso está definida como *Normal* o que significa que, por cada pacote recebido, é devolvido um pacote de confirmação. Isto proporciona uma transmissão mais fiável mas também aumenta a carga de tráfego, o que diminui o desempenho. Pode escolher cancelar o pacote de confirmação seleccionando *No Ack* (sem confirmação) na caixa de combinação de cada uma das categorias de acesso mudando, assim, a política de confirmação. Isto pode ser útil nos pacotes de Voz, por exemplo, nos quais a rapidez de transmissão é importante e nos quais se pode tolerar um certo grau de perda do pacote.

Virtual APs (APs virtuais)

Pode activar múltiplas LANs sem fios no **DISCUS™ DRG A223G**, estando apenas limitado pelo número de LANs suportado pela sua placa sem fios. Cada uma das LANs sem fios é definida como um ponto de acesso.

A secção *Virtual APs* apresenta os pontos de acesso sem fios físicos do Router sobre os quais podem ser criadas ligações virtuais. Para criar uma ligação virtual, clique no *link New Virtual AP* (novo AP virtual).

A nova ligação também vai ser adicionada à lista de ligações da rede, e vai ser configurável tal como qualquer outra ligação. Pode alterar o nome predefinido da ligação clicando no ícone *Edit action* (alterar a acção) e alterando o valor SSID no ecrã *Configure LAN Wireless 802.11g Access Point – Virtual AP* (configurar o ponto de acesso da LAN sem fios 802.11g - AP virtual).

Wireless WDS (WDS sem fios)

Permite estabelecer pontes sem fios entre pontos de acesso dentro do seu alcance. São usados pontos de acesso virtuais para interagir com pontos WDS do router, dando aos utilizadores LAN acesso a redes sem fios remotas.

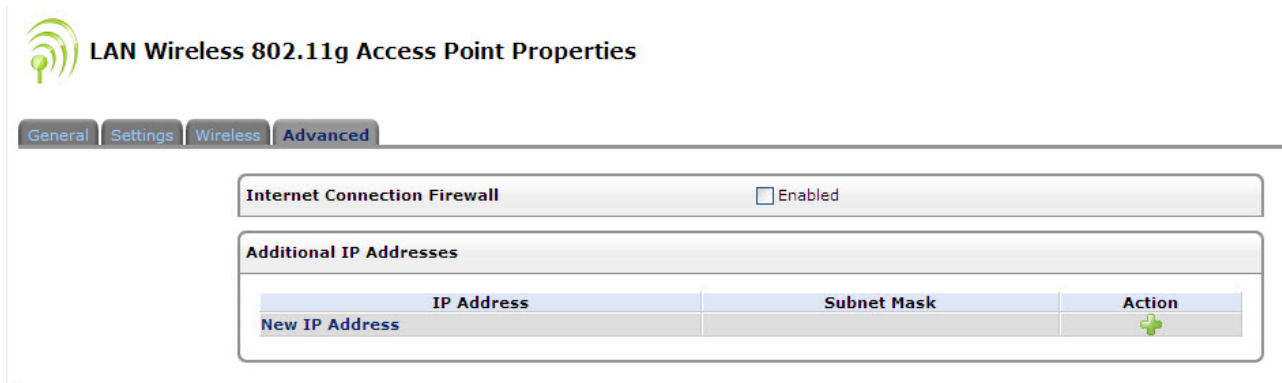
Quando a funcionalidade está activa, é apresentada uma caixa de listagem.

**LAN WIRELESS 802.11g
ACCESS POINT >>
ADVANCED (PONTO DE
ACESSO DA LAN SEM FIOS
802.11G >> AVANÇADAS)**

Internet Connection Firewall (firewall da ligação de Internet): O *firewall* da sua porta de ligação ajuda a proteger o seu computador, impedindo utilizadores não-autorizados de aceder ao seu computador através de uma rede como a

Internet. Pode ser activado um *firewall* para cada ligação de rede. Para activar o *firewall* nesta ligação da rede seleccione a caixa *Enabled* (activo).

FIGURA 6 LAN Wireless 802.11g Access Point >> Advanced Panel (Ponto de Acesso da LAN sem fios 802.11g >> Painel Avançadas)

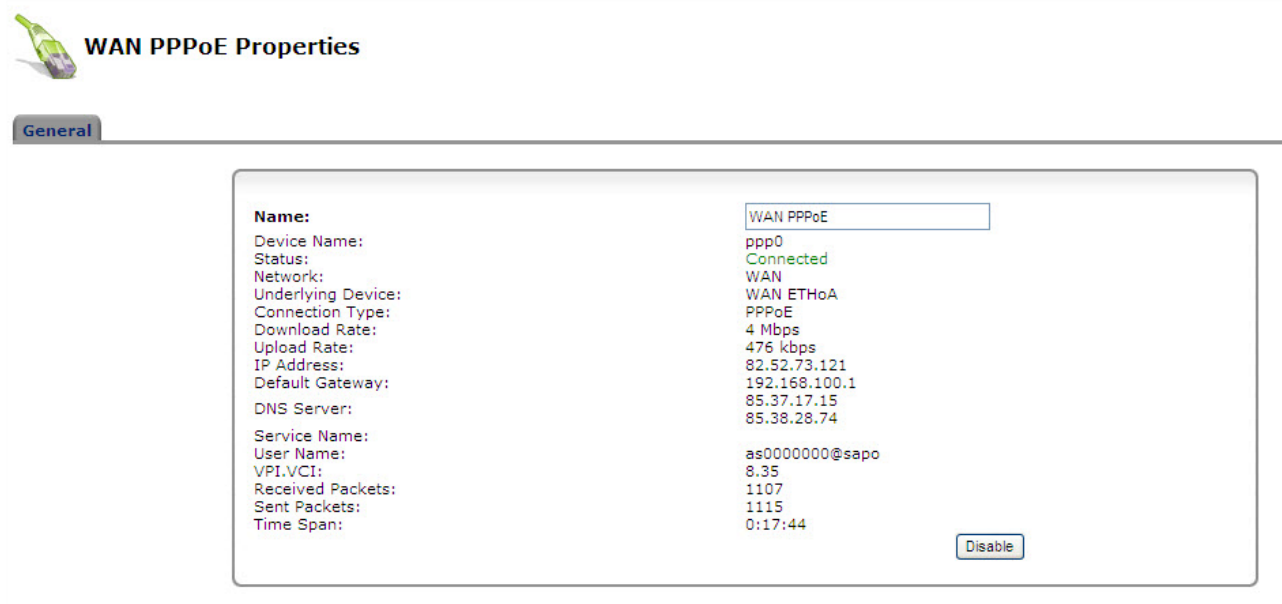


The screenshot shows the 'Advanced' tab of the LAN Wireless 802.11g Access Point Properties. It features a section for 'Internet Connection Firewall' with an 'Enabled' checkbox. Below it is a table for 'Additional IP Addresses' with columns for 'IP Address', 'Subnet Mask', and 'Action'. A 'New IP Address' link is present in the 'Action' column.

IP Address	Subnet Mask	Action
New IP Address		+

Additional IP Addresses (endereços de IP adicionais): Pode adicionar nomes alternativos (endereços de IP adicionais) à porta de ligação clicando no *link* "New IP Address" (novo endereço de IP). Isto permite-lhe aceder à porta de ligação usando estes nomes alternativos, além do nome 192.168.1.1.

FIGURA 7 WAN PpOE >> General (WAN PpOE >> geral)



The screenshot shows the 'General' tab of the WAN PPPoE Properties. It displays various configuration details for the WAN PPPoE connection, including device name, status, network, and service name.

Name:	WAN PPPoE
Device Name:	ppp0
Status:	Connected
Network:	WAN
Underlying Device:	WAN ETHoA
Connection Type:	PPPoE
Download Rate:	4 Mbps
Upload Rate:	476 kbps
IP Address:	82,52,73,121
Default Gateway:	192,168,100,1
DNS Server:	85,37,17,15 85,38,28,74
Service Name:	
User Name:	as0000000@sapo
VPI,VCI:	8,35
Received Packets:	1107
Sent Packets:	1115
Time Span:	0:17:44

Disable

WAN PPOE

Os painéis WAN PPOE permitem-lhe verificar e configurar a interface WAN de linha DSL.

WAN PPOE >> GENERAL (WAN PPOE >> GERAL)

No painel WAN PPOe *General* é possível activar/desactivar a interface WAN PPOE e definir um nome amigável para o WAN PPOE.

Secção sobre Segurança

Este capítulo irá descrever a **Secção de Segurança**, a qual pode ser acedida através da *Home Page* do **DISCUS™ DRG A223G**.



Esteja ciente de que quaisquer alterações à configuração podem comprometer a sua conectividade.

O conjunto de segurança da porta de ligação do Router inclui um leque abrangente e robusto de serviços: Um *Stateful Packet Inspection Firewall* (*firewall* de inspecção de pacotes com informações de estado), protocolos de autenticação do utilizador e mecanismos de protecção da palavra-passe. Este conjunto de funcionalidades permite aos utilizadores ter os seus computadores ligados à Internet estando, ao mesmo tempo, protegidos das ameaças à segurança existentes na Internet.

O *firewall* foi criado para se adaptar exclusivamente às necessidades do utilizador doméstico/de escritório e foi pré-configurado para oferecer uma segurança otimizada.

O *firewall* do Router providencia a segurança e a flexibilidade que um utilizador doméstico ou de escritório procuram. Providencia um nível profissional e administrado de segurança de rede, permitindo ao mesmo tempo uma utilização segura de aplicações interactivas, tais como jogos na Internet ou videoconferências.

Funcionalidades adicionais, tais como restrições de navegação e controlo de acesso, podem ser facilmente configuradas pelo utilizador localmente, através

de uma interface de fácil utilização com base na *web*, ou remotamente através de um fornecedor de serviços.

O *firewall* do Router suporta uma filtragem avançada, criada para permitir um controlo abrangente sobre o comportamento do *firewall*. Pode definir regras específicas de entrada e saída, controlar a ordem dos conjuntos de regras logicamente semelhantes e fazer distinções entre as regras que se aplicam aos dispositivos de rede WAN e aos de rede LAN.

GERAL:

Sirva-se do ecrã *General* para configurar as definições básicas de segurança da porta de ligação.

O *firewall* regula o fluxo de dados entre a rede doméstica e a Internet. Tanto os dados recebidos como os enviados são inspeccionados e, de seguida, ou são aceites (é-lhes permitido passar pelo Router), ou são rejeitados (é-lhes impedida a passagem pelo Router), de acordo com um conjunto de regras que é flexível e configurável. Estas regras são criadas como forma de prevenção contra intrusos do exterior, permitindo aos utilizadores domésticos aceder aos serviços de Internet que desejam.

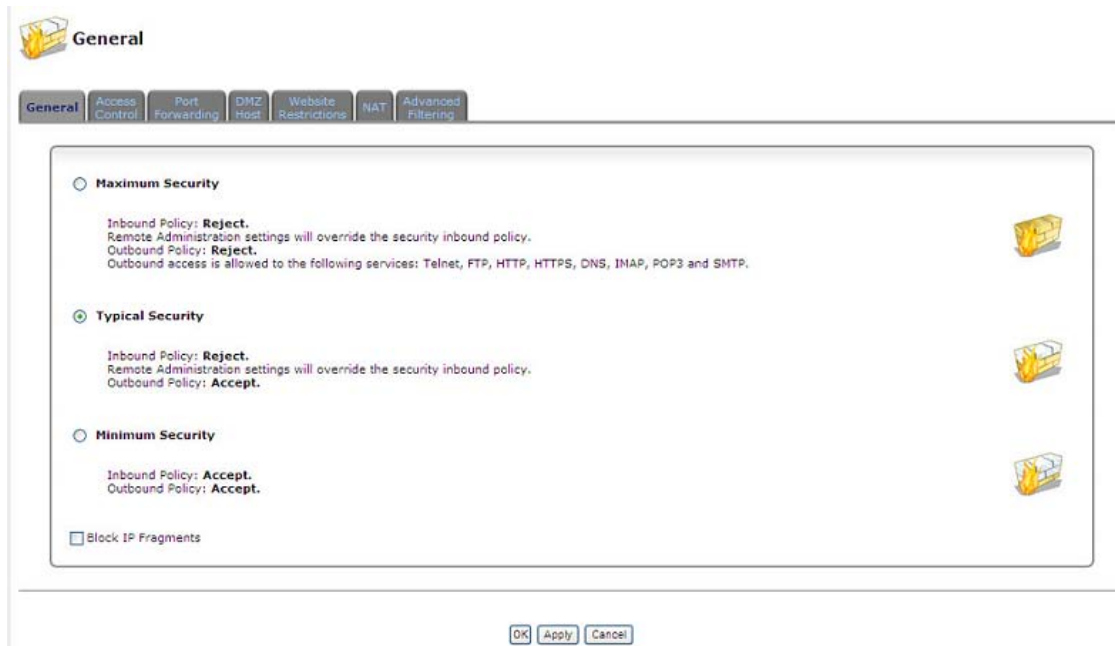
As regras do *firewall* especificam quais os tipos de serviços disponíveis na Internet a que pode aceder a partir da rede doméstica, e quais os tipos de serviços disponíveis na rede doméstica que podem ser acedidos a partir da Internet. Cada pedido de serviço que o *firewall* recebe, quer venha da Internet ou de um computador da rede doméstica, é verificado tendo em conta o conjunto de regras do *firewall*, para determinar se esse pedido deve ou não ser autorizado a passar pelo *firewall*. Se o pedido receber autorização para passar, quaisquer dados subsequentes associados ao pedido em questão (uma “sessão”) também estarão autorizados a passar, independentemente da sua direcção.

Por exemplo, quando tenta aceder a uma página *web* através do seu *browser*, é enviado um pedido à Internet para aceder à página. Quando o pedido chega ao Router, o *firewall* identifica o tipo e a origem do pedido – HTTP e um PC específico na sua rede doméstica, neste caso. A menos que tenha configurado o controlo de acessos para bloquear pedidos deste tipo vindos deste computador, o *firewall* vai permitir que o pedido passe para a Internet. Quando o servidor devolver a página *web*, o *firewall* vai associar a página com esta sessão e vai deixá-la passar, independentemente do acesso HTTP da Internet estar bloqueado ou autorizado.

O que é importante reter é que é a origem do pedido, e não as reacções subjacentes a este pedido, que determina se uma sessão pode ou não ser estabelecida. Pode escolher entre três níveis de segurança predefinidos para o Router. *Minimum* (mínimo), *Typical* (típico – o valor predefinido) e *Maximum* (máximo). A tabela em baixo oferece um sumário do comportamento que pode ser esperado do Router para cada um dos níveis de segurança.

TABELA 1 - Security Levels (níveis de segurança)

Nível de Segurança	Pedidos Originados na WAN (tráfego recebido)	Pedidos Originados na LAN (tráfego enviado)
<i>Segurança Máxima (Predefinição)</i>	<i>Bloqueado: sem acesso à rede doméstica através da Internet, com exceção para o que foi configurado nos ecrãs de reencaminhamento de portas, DMZ, sistema anti-triã e acesso remoto.</i>	<i>Limitado: por predefinição, apenas são permitidos serviços utilizados frequentemente, tais como navegação na web e e-mail.</i>
<i>Segurança Típica</i>	<i>Bloqueado: sem acesso à rede doméstica através da Internet, com exceção para o que foi configurado nos ecrãs de reencaminhamento de portas, DMZ, sistema anti-triã e acesso remoto.</i>	<i>Sem restrições: são permitidos todos os serviços, com exceção para o que foi configurado no ecrã de controlo dos acessos.</i>
<i>Segurança Mínima</i>	<i>Sem restrições: permite total acesso à rede doméstica a partir da Internet; todos os pedidos de ligação são permitidos.</i>	<i>Sem restrições: são permitidos todos os serviços, com exceção para o que foi configurado no ecrã de controlo dos acessos.</i>

FIGURA 1 Security General panel (painel geral de segurança)

ACCESS CONTROL (CONTROLO DE ACESSOS)

Pode querer impedir que computadores específicos na rede doméstica (ou mesmo a rede inteira) consigam aceder a determinados serviços na Internet. Por exemplo, pode querer proibir um computador de navegar na *web*, outro computador de transferir ficheiros por FTP, e a rede inteira de receber correio electrónico.

O Controlo de Acessos define restrições ao nível do tipo de pedidos que podem passar da rede doméstica para a Internet e, assim sendo, pode bloquear os fluxos de tráfego de ambas as direcções. Também pode ser usado para autorizar serviços específicos quando está configurada a segurança máxima. No exemplo do correio electrónico dado em cima, pode impedir computadores da rede doméstica de receber e-mail, bloqueando o envio de pedidos a servidores POP3 na Internet.

Há vários serviços que deve considerar bloquear, tais como servidores populares de jogos e de partilha de ficheiros. Por exemplo, se quiser ter a certeza de que os seus funcionários não põem o seu negócio em risco devido ao uso de ficheiros com direitos de autor, pode decidir bloquear várias aplicações populares P2P e de partilha de ficheiros.

FIGURA 2 Access Control panel (painel de controlo dos acessos)



Para permitir ou restringir serviços:

1. *Selecione o separador “Access Control” (controlo dos acessos) no ecrã “Security management” (gestão da segurança). Vai aparecer o ecrã “Access Control”.*
2. *Clique no link “New Entry” (nova entrada). Vai aparecer o ecrã “Add Access Control Rule” (adicionar regra de controlo dos acessos).*
3. *A caixa de combinação “Address” (endereço) permite-lhe especificar o computador ou grupo de computadores aos quais deseja aplicar a regra de controlo dos acessos. Pode escolher um computador específico na sua LAN ou um “User Defined” (utilizador definido). Se escolher a opção “User Defined”, vai aparecer o ecrã “Edit Network Object” (alterar objecto de rede). A especificação de um endereço é feita através da criação de um “Network Object” (objecto de rede).*
4. *A caixa de combinação “Protocol” (protocolo) permite-lhe seleccionar ou especificar o tipo de protocolo que vai ser usado. Seleccionar a opção “Show All Services” (mostrar todos os serviços) expande a lista dos protocolos disponíveis. Selecione um dos protocolos existentes ou crie um novo protocolo usando a opção “User Defined” (utilizador definido). Isto vai começar uma sequência que irá criar um novo serviço, representando o protocolo.*
5. *Selecione a caixa de verificação “Reply an HTML page to the blocked client” (devolver uma página HTML ao cliente bloqueado) para mostrar a seguinte mensagem ao cliente: “Access Denied - this computer is not allowed to surf the WAN. Please contact your admin.” (Acesso Negado – este computador não tem autorização para navegar na WAN. Por favor contacte o seu administrador.). Quando esta caixa não está seleccionada, os pacotes do cliente vão simplesmente ser ignorados e este não receberá qualquer notificação.*
6. *A caixa de combinação “Schedule” (agenda) permite-lhe definir o período de tempo durante o qual a regra terá efeito. Por predefinição, a regra estará sempre activa. No entanto, pode configurar regras de agenda seleccionando “User Defined”.*

7. Clique no botão "OK" para guardar as suas alterações. O ecrã "Access Control" (controlo dos acessos) vai mostrar um resumo da regra que acabou de criar.

PORT FORWARDING (REENCAMINHAMENTO DE PORTAS)

No seu estado predefinido, o DISCUS™ DRG A223G impede todos os utilizadores exteriores de se ligarem à ou comunicarem com a sua rede.

Assim, o sistema está protegido contra *hackers* que possam penetrar a rede e danificá-la. No entanto, pode desejar expor a sua rede na Internet de forma limitada e controlada de forma a permitir que algumas aplicações funcionem a partir da LAN (aplicações de jogos, voz e chat, por exemplo), e para permitir que os servidores da rede doméstica tenham acesso à Internet. A funcionalidade *Port Forwarding* (reencaminhamento de portas) suporta estas duas funcionalidades. Se está familiarizado com a terminologia e conceitos do funcionamento em rede, pode ter encontrado uma referência a este tópico sob o nome *Local Servers* (servidores locais).

O ecrã de *Port Forwarding* (reencaminhamento de portas) permite-lhe definir as aplicações que precisam de ser geridas de forma especial pelo Router.

Tudo o que precisa de fazer é seleccionar o protocolo da aplicação e o endereço de IP local do computador que vai usar ou providenciar o serviço. Se necessário, pode criar novos protocolos, para além dos protocolos mais comuns que o Router oferece.

Por exemplo, se desejasse usar uma aplicação *File Transfer Protocol* (protocolo de transferência de ficheiros), ou FTP, num dos seus PC, apenas teria de seleccionar a opção "FTP" da lista e introduzir o endereço de IP local ou o nome do administrador do computador em questão.

A partir desse momento, todos os dados relacionados com o FTP que chegam até ao Router vindos da Internet vão ser reenviados para o computador determinado. De forma semelhante, pode autorizar os utilizadores da Internet a aceder aos servidores da sua rede doméstica identificando cada um dos serviços e o PC que o executa. Isto é útil, por exemplo, se quiser ter um servidor *web* na sua rede doméstica. Quando um utilizador da Internet aponta o seu *browser* para o endereço de IP exterior do Router, a porta de ligação irá reencaminhar o pedido de HTTP para o seu servidor *web*.

Com um endereço de IP exterior (o endereço de IP principal do Router), podem ser atribuídas diferentes aplicações aos computadores da sua LAN. No entanto, cada tipo de aplicação está limitado ao uso de um só computador. Por exemplo, pode estabelecer que o FTP vai usar o endereço X para entrar em contacto com o computador A, e que a Telnet também vai usar o endereço X para entrar em contacto com o computador A. No entanto, se tentar estabelecer que o FTP vai usar o endereço X para entrar em contacto não só com o computador A, mas também com o computador B, a operação vai falhar.

Assim, o Router permite acrescentar endereços de IP públicos adicionais às regras de reencaminhamento de portas, os quais precisa de obter primeiro através do seu ISP e introduzir no *NAT IP Addresses Pool* (pool de endereços de IP NAT). De seguida, vai poder determinar que o FTP vai usar o endereço X para entrar em contacto com o computador A, e o endereço Y para entrar em contacto com o computador B. Além disso, o reencaminhamento de portas permite-lhe redireccionar o tráfego para uma porta diferente, em vez de para a porta designada.

Imaginemos que tem um servidor *web* em execução no seu PC na porta 8080 e quer que todos os utilizadores que acedam ao Router via HTTP possam aceder a este servidor. Para concretizar esta situação, faça o seguinte:

- Defina uma regra de reencaminhamento de portas para o serviço HTTP, com o IP do PC ou o nome do sistema anfitrião.
- Especifique 8080 no campo *Forward to Port* (reencaminhar para a porta).

Todo o tráfego HTTP recebido será, a partir de agora, reencaminhado para o PC que tem o servidor *web* em execução na porta 8080.

Quando estiver a definir um serviço de reencaminhamento de portas, deve certificar-se de que a porta não está a ser utilizada por outra aplicação, pois esta pode deixar de funcionar. Um exemplo comum é quando se usa a sinalização SIP em Voz sobre IP – a porta usada pela aplicação VoIP da porta de ligação (5060) é a mesma porta na qual o reencaminhamento de portas está definido para agentes SIP da LAN.

FIGURA 3. *Port Forwarding panel (painel de reencaminhamento de portas)*



Para adicionar um novo serviço de reencaminhamento de portas:

1. *Selecione o separador "Port Forwarding" no ecrã de gestão da segurança ("Security"). Vai aparecer o ecrã "Port Forwarding".*
2. *Clique no link "New Entry" (nova entrada). Vai aparecer o ecrã "Add Port Forwarding Rule" (adicionar uma regra de reencaminhamento de portas).*
3. *Selecione a caixa de verificação "Specify Public IP Address" (especifique o endereço de IP público) se quiser aplicar esta regra a um endereço de IP exterior específico. O ecrã vai ser actualizado.*
4. *Introduza o endereço de IP externo adicional no campo "Public IP Address" (endereço de IP público).*
5. *Introduza o nome do sistema anfitrião, ou o endereço de IP do computador que vai fornecer o serviço (o "server" (servidor)) no campo "Local Host" (sistema anfitrião local). Repare que, a menos que tenha sido adicionado um endereço de IP externo adicional, apenas um computador da LAN pode ser designado para fornecer um serviço ou aplicação específicos.*
6. *A caixa de combinação "Protocol" (protocolo) permite-lhe seleccionar ou especificar o tipo de protocolo que vai ser usado. Seleccionar a opção "Show All Services" (mostrar todos os serviços) expande a lista dos protocolos disponíveis. Selecione um dos protocolos existentes ou crie um novo protocolo usando a opção "User Defined" (utilizador definido). Isto vai começar uma sequência que irá criar um novo serviço, representando o protocolo.*
7. *Por predefinição, o Router irá reencaminhar o tráfego para a mesma porta que a porta de recepção. Se deseja redireccionar o tráfego para uma porta diferente, selecione a opção "Specify" (especificar). O ecrã vai ser actualizado e vai aparecer um campo adicional que lhe permitirá introduzir o número da porta.*
8. *A caixa de combinação "Schedule" (agenda) permite-lhe definir o período de tempo durante o qual a regra terá efeito. Por predefinição, a regra estará sempre activa. No entanto, pode configurar regras de agenda seleccionando "User Defined".*

9. Clique no botão “OK” para guardar as suas alterações. O ecrã “Port Forwarding” (reencaminhamento de portas) vai mostrar um resumo da regra que acabou de criar.

“DMZ HOST” (ANFITRIÃO DMZ)

A funcionalidade *DMZ Host* (anfitrião desmilitarizado) permite a um computador local estar exposto na Internet.

Designe um anfitrião DMZ quando:

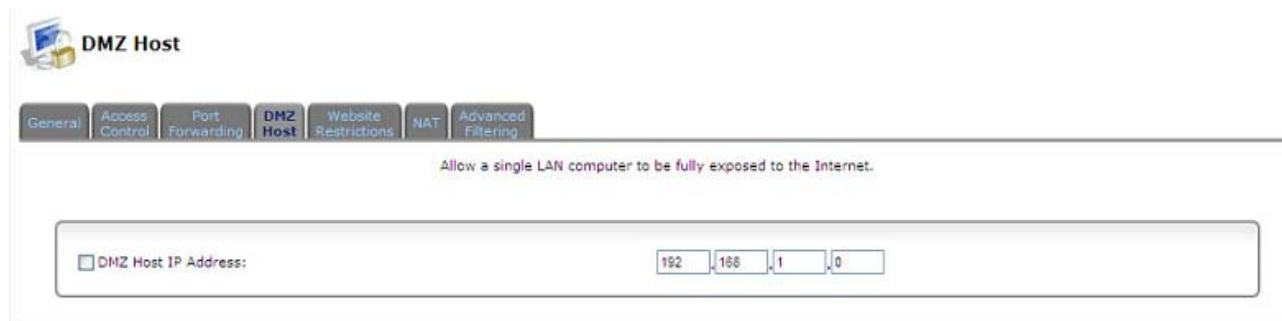
- Desejar usar um serviço de Internet com um propósito especial, tal como um jogo *online* ou um programa de videoconferência, que não esteja presente na lista de *Port Forwarding* (reencaminhamento de portas), e para o qual não existe informação disponível acerca da extensão da porta.
- Não tiver preocupações de segurança e desejar expor um computador a todos os serviços, sem restrições.



Um anfitrião DMZ não está protegido pelo firewall e pode ser vulnerável a ataques. A designação de um anfitrião DMZ também pode por os outros computadores da rede doméstica em risco. Quando estiver a designar um anfitrião DMZ, deve considerar as implicações de segurança e protegê-lo se necessário.

A recepção de pedidos de acesso a um serviço da rede doméstica, tal com um servidor *web*, é gerida pelo Router. O DISCUS™ DRG A223G irá reencaminhar este pedido para o anfitrião DMZ (se houver um designado), a não ser que o serviço esteja a ser fornecido por outro PC da rede doméstica (atribuído no *Port Forwarding*). Nesse caso, será esse PC a receber o pedido.

FIGURA 4 *DMZ Host panel* (painel do anfitrião DMZ).



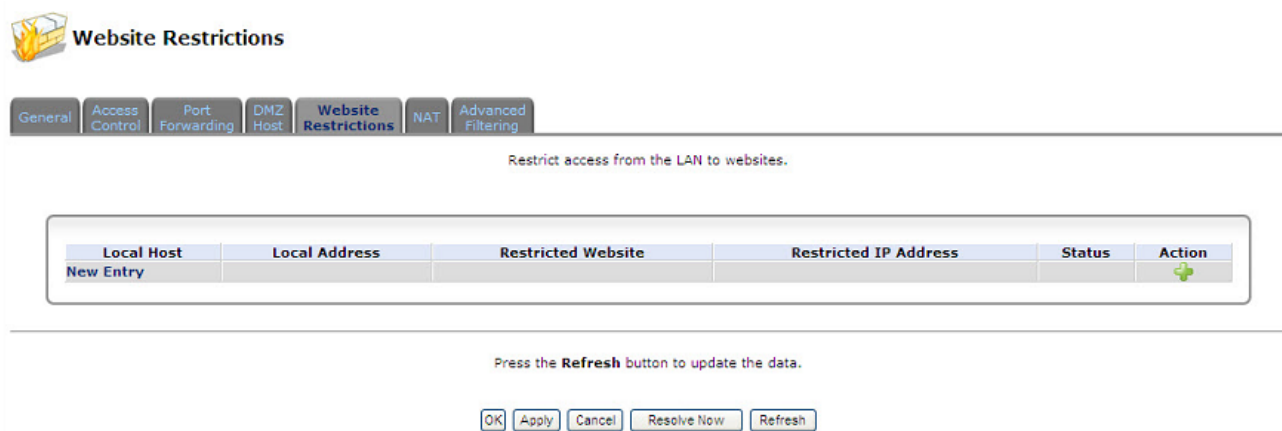
Para designar um computador local como anfitrião DMZ:

1. Seleccione o separador *DMZ Host* (anfitrião DMZ) no ecrã *Security management* (gestão da segurança). Vai aparecer o ecrã *DMZ Host*.
2. Introduza o endereço de IP local do computador que deseja designar como anfitrião DMZ, e seleccione a caixa de verificação. Repare que apenas um computador da LAN de cada vez pode ser um anfitrião DMZ.
3. Clique “OK” para guardar as alterações.

WEBSITE RESTRICTIONS (RESTRICÇÕES A WEBSITES)

Pode configurar o Router para bloquear *websites* específicos da Internet, para que estes não possam ser acedidos através dos computadores da rede doméstica. Além disso, podem ser aplicadas restrições a uma ampla tabela de actualização automática, de *websites* de acesso não-recomendado.

FIGURA 5 *Website restrictions panel* (painel de restrições a *websites*)



Para bloquear o acesso a um *website*:

1. Clique no separador *Website Restrictions* (restrições a *websites*) no ecrã *Security management* (gestão da segurança).
2. Clique no *link New Entry* (nova entrada). Vai aparecer o ecrã *Restricted website* (*website* restrito).
3. Introduza o endereço do *website* (endereço de IP ou URL) que deseja tornar inacessível a partir da sua rede doméstica (todas as páginas *web* dentro desse site também serão bloqueadas). Se o endereço do *website* tiver múltiplos endereços de IP, o Router irá resolver todos os endereços adicionais e irá adicioná-los automaticamente à tabela de restrições.
4. A caixa de combinação *Local Host* (anfitrião local) permite-lhe especificar o computador ou grupo de computadores aos quais deseja aplicar a restrição de *websites*. Pode escolher um computador específico na sua LAN ou um *User Defined* (utilizador definido). Se escolher a opção *User Defined*, vai aparecer o ecrã *Edit Network Object* (alterar objecto de rede). A especificação de um endereço é feita através da criação de um *Network Object* (objecto de rede).
5. A caixa de combinação *Schedule* (agenda) permite-lhe definir o período de tempo durante o qual a regra terá efeito. Por predefinição, a regra estará

DISCUS™ DRG A223G

sempre activa. No entanto, pode configurar regras de agenda seleccionando *User Defined*.

6. Clique “OK” para guardar as alterações. Enquanto o Router estiver a tentar encontrar o *website*, será levado de volta ao ecrã anterior. Na coluna *Status* (estado) vai aparecer “*Resolving ...*” (a resolver...), enquanto o sítio está a ser localizado (o URL é “resolvido” em um ou mais endereço de IP).

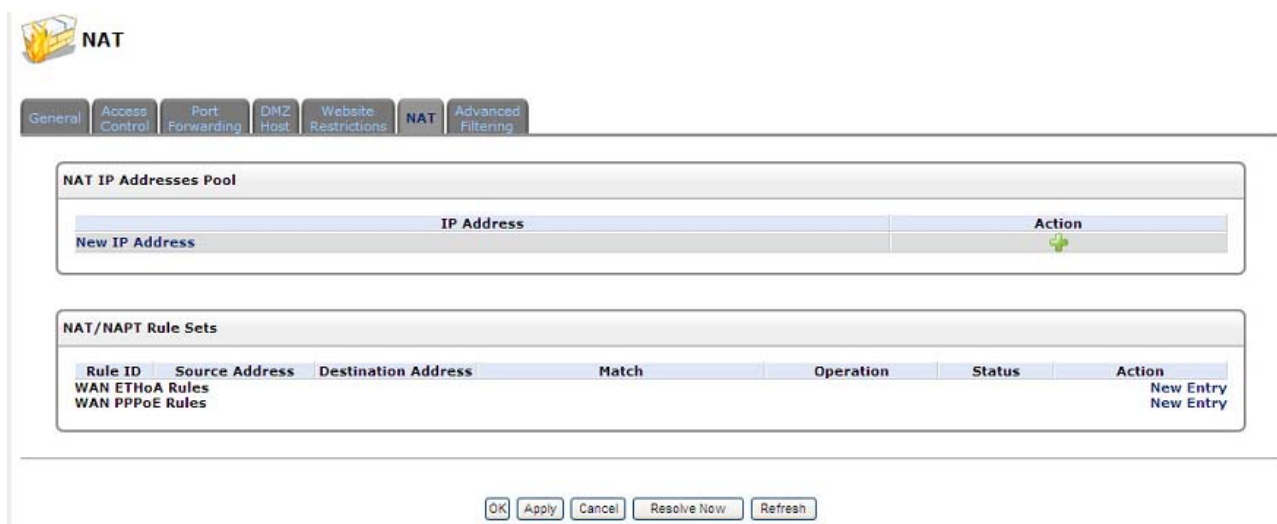
NAT

O DISCUS™ DRG A223G inclui um mecanismo de *Network Address Translation* (tradução do endereço da rede) ou NAT, e de *Network Address Port Translation* (tradução da porta do endereço da rede) ou NAPT, que lhe permite controlar os endereços e portas de rede dos pacotes encaminhados através da sua porta de ligação. Quando autorizar vários computadores da sua rede a aceder à Internet utilizando um número fixo de endereços de IP públicos, pode definir estaticamente qual o endereço de IP LAN que vai ser traduzido para que endereço de IP NAT e/ou portas.

Por predefinição, o Router opera em modo de encaminhamento NAPT. No entanto, pode controlar a tradução da sua rede através da definição de regras estáticas de NAT/NAPT. Este tipo de regras mapeiam os computadores LAN até endereços de IP NAT.

O mecanismo NAT/NAPT é útil para gerir os consumos de Internet na sua LAN ou para cumprir as exigências de várias aplicações. Por exemplo, pode atribuir um só endereço de IP NAT ao seu computador principal da LAN, de forma a assegurar a sua ligação permanente à Internet. Outro exemplo é quando o servidor de uma aplicação ao qual se deseja ligar, tal como um servidor de segurança, exige que os pacotes tenham um endereço de IP específico – pode definir uma regra NAT para esse endereço.

FIGURA 6 NAT panel (painel NAT)



ADVANCED FILTERING (FILTRAGEM AVANÇADA)

A filtragem avançada é criada para permitir um controlo abrangente sobre o comportamento do *firewall*. Pode definir regras específicas de entrada e saída, controlar a ordem dos conjuntos de regras logicamente semelhantes e fazer distinções entre as regras que se aplicam aos dispositivos de rede WAN e aos de rede LAN.

Para ver as opções avançadas de filtragem do Router clique em *Advanced Filtering* (filtragem avançada), por baixo do separador *Firewall* no ecrã *Services* (serviços). Vai aparecer o ecrã *Advanced Filtering*.

Este ecrã está dividido em duas secções idênticas, uma para *Input Rule Sets* (grupo de regras de recepção) e outra para *Output Rule Sets* (grupo de regras de envio), as quais servem para configurar o tráfego recebido e enviado, respectivamente. Cada secção é composta por subgrupos, os quais podem ser agrupados em três assuntos principais:

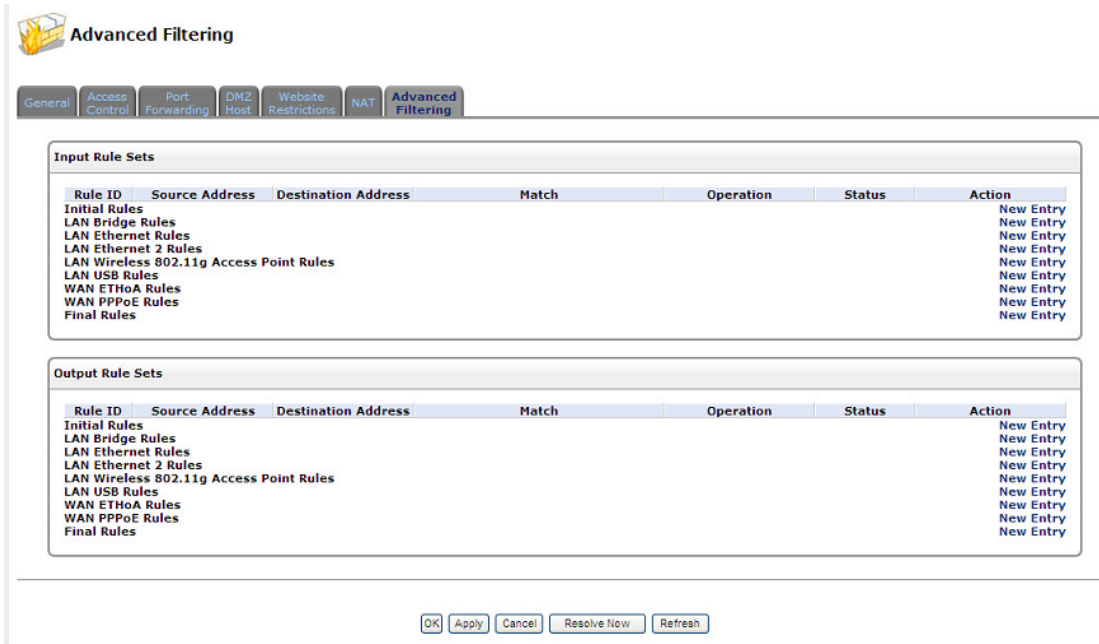
- Regras iniciais – as regras aqui definidas vão ser aplicadas em primeiro lugar a todos os dispositivos da porta de ligação.
- Regras dos dispositivos da rede – podem ser definidas regras por cada dispositivo da porta de ligação.
- Regras finais – as regras aqui definidas vão ser aplicadas em último lugar a todos os dispositivos da porta de ligação.

A ordem de aparição das regras representa não só a ordem em que foram definidas, mas também a sequência em que vão ser aplicadas. Pode alterar esta ordem depois das suas regras já estarem definidas (sem ter de as apagar ou de voltar a adicioná-las), servindo-se dos ícones de acção *Move Up* (mover para cima) e *Move Down* (mover para baixo).

Existem várias regras introduzidas automaticamente pelo *firewall* para fornecer uma segurança optimizada e para bloquear ataques nocivos.

Para acrescentar uma regra de filtragem avançada, escolha primeiro a direcção de tráfego e o dispositivo ao qual quer aplicar a regra. De seguida, clique no *link New Entry* (nova entrada). Vai aparecer o ecrã *Add Advanced Filter* (adicionar filtro avançado). Este ecrã está dividido em duas secções principais, *Matching* (correspondência) e *Operation* (operação), os quais servem para definir a operação que deve ser executada quando se aplicam as condições correspondentes.

FIGURA 7 *Advanced Filtering panel (painel de filtragem avançada)*



Advanced Filtering

General Access Control Port Forwarding DMZ Host Website Restrictions NAT **Advanced Filtering**

Input Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Ethernet 2 Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN USB Rules						New Entry
WAN ETHoA Rules						New Entry
WAN PPPoE Rules						New Entry
Final Rules						New Entry

Output Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Ethernet 2 Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN USB Rules						New Entry
WAN ETHoA Rules						New Entry
WAN PPPoE Rules						New Entry
Final Rules						New Entry

OK Apply Cancel Resolve Now Refresh

Secção sobre VoIP

Este capítulo irá descrever a **Secção sobre VoIP** (Voz sobre IP), a qual pode ser acedida através da *Home Page* do **DISCUS™ DRG A223G**.



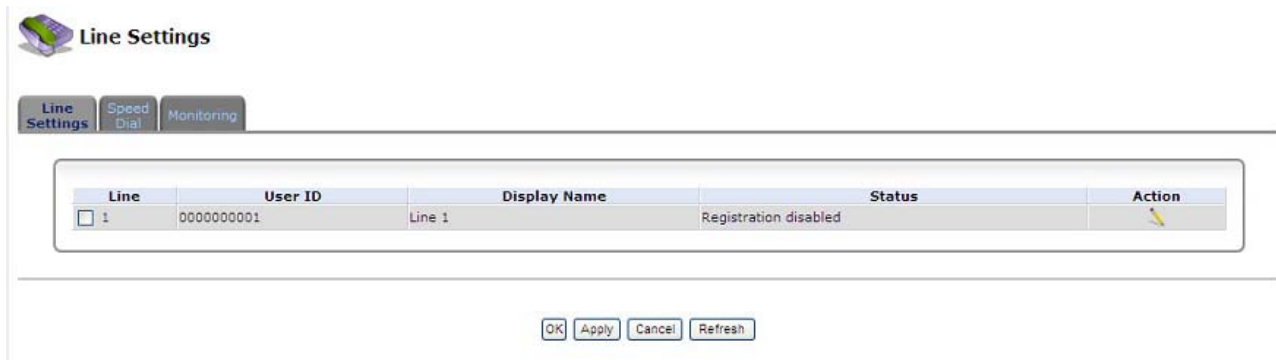
Esteja ciente de que quaisquer alterações à configuração podem comprometer a sua conectividade.

LINE SETTINGS (DEFINIÇÕES DA LINHA)

O separador *Line Settings* (definições da linha) do ecrã VoIP (voz sobre IP) define as portas telefónicas do Router e permite-lhe configurá-las.

1. Clique no ícone *Voice Over IP* da barra lateral.
2. Clique no separador *Line Settings* e aparecer-lhe-á o ecrã seguinte. Antes de começar a efectuar chamadas telefónicas, é necessário configurar os parâmetros de cada uma das linhas. Pode escolher qual o telefone que vai estar operacional seleccionando a caixa de verificação ao seu lado.

FIGURA 1 *Line Settings Panel* (painel de definições da linha)

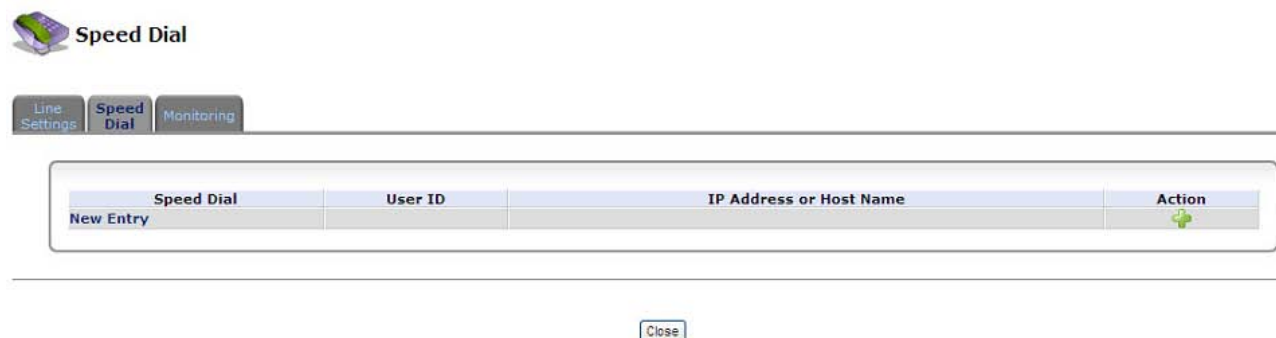


3. Clique no ícone *edit action* (alterar acção) em cada uma das linhas para configurar os diferentes parâmetros.

SPEED DIAL (MARCAÇÃO RÁPIDA)

Pode atribuir números de marcação rápida aos utilizadores a quem liga frequentemente. Uma entrada de marcação rápida deve especificar um destino a partir de 3 tipos: *proxy*, linha local ou chamada directa.

FIGURA 2 *Speed Dial Panel* (painel de marcação rápida)



Marcação Rápida via Proxy Para adicionar uma nova entrada de marcação rápida via *proxy*:

1. Clique no separador *Speed Dial*.
2. Clique no *link New Entry* para adicionar uma nova entrada de marcação rápida. Vai aparecer o ecrã *Speed Dial Settings* (definições da marcação rápida).
3. Introduza os parâmetros seguintes:
Speed Dial: Um número de atalho que irá usar para ligar a este utilizador.
Destination (destino): O destino da entrada, neste caso é um servidor *proxy*.

User ID (identificação do utilizador): Especifique a identificação do utilizador remoto.

4. Clique “OK” para guardar as alterações.

Marcação Rápida via Linha Local Para adicionar uma nova entrada de marcação rápida via linha local:

1. Clique no *link New Entry* no separador *Speed Dial* e seleccione a opção *Local Line* (linha local) da caixa de combinação.
2. Introduza os parâmetros seguintes:
Speed Dial: Um número de atalho que irá usar para ligar a este contacto.

Destination (destino): O destino da entrada, neste caso é uma linha local.

Line (linha): Uma caixa de combinação irá mostrar as suas linhas locais predefinidas. Seleccione a linha de destino.

3. Clique “OK” para guardar as alterações.

Speed Dial via Chamada Directa Para adicionar uma nova entrada de marcação rápida via chamada directa:

1. Clique no *link New Entry* no separador *Speed Dial* e seleccione a opção *Direct Call* (chamada directa) da caixa de combinação.
2. Introduza os parâmetros seguintes:
Speed Dial: Um número de atalho que irá usar para ligar a este contacto.

Destination (destino): O destino da entrada, neste caso é uma chamada directa.

User ID (identificação do utilizador): Especifique a identificação do utilizador remoto.

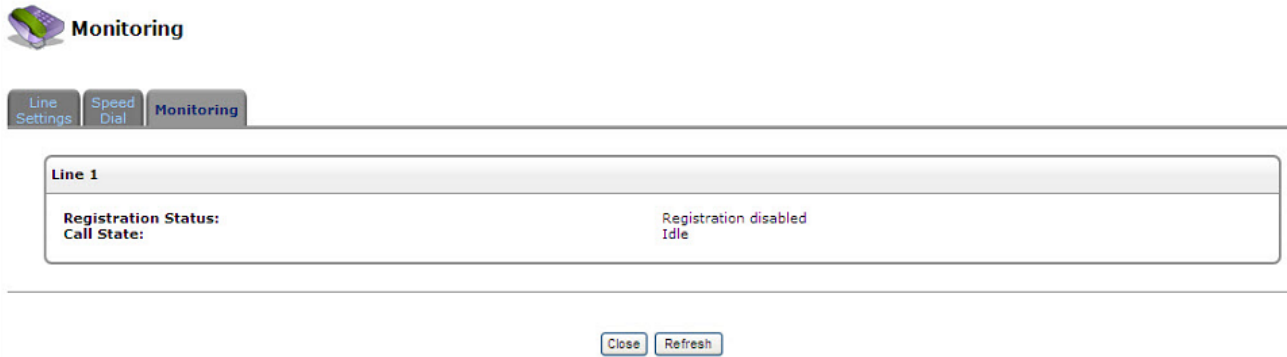
IP Address (endereço de IP) ou *Host name* (nome do anfitrião): Especifique o endereço de IP ou o nome de anfitrião do utilizador remoto.

3. Clique “OK” para guardar as alterações.

MONITORING (MONITORIZAÇÃO)

É possível aceder à página de monitorização da linha seleccionando o painel do separador *Monitoring*: são apresentados o *Registration Status* (estado do registo) e o *Call State* (estado da chamada) para cada uma das linhas.

FIGURA 3 *Monitoring Panel* (painel de monitorização)



Secção sobre as Definições Avançadas

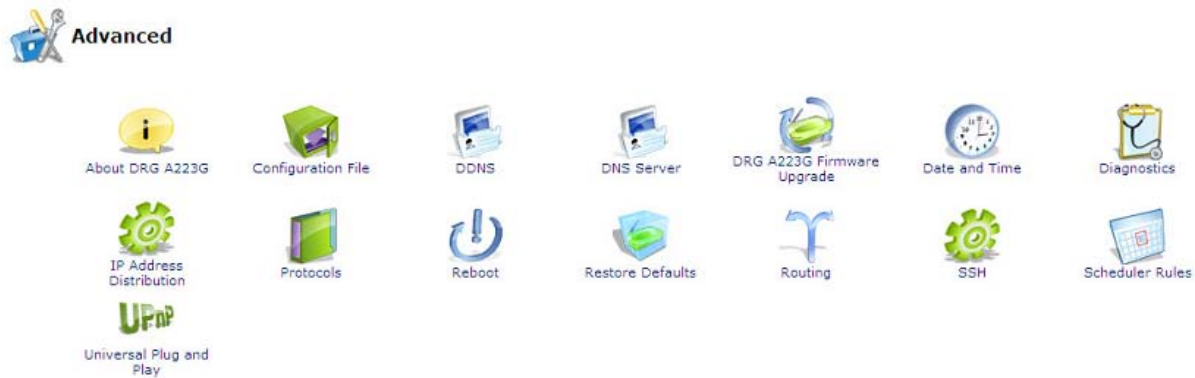
Este capítulo irá descrever a **Secção sobre Definições Avançadas**, a qual pode ser acedida através da *Home Page* do **DISCUS™ DRG A223G**.



Esteja ciente de que quaisquer alterações à configuração podem comprometer a sua conectividade.

O painel de Definições Avançadas agrupa várias funcionalidades do ponto de vista operacional e configurativo. Este capítulo vai descrever cada um dos ícones, um por um, e as suas respectivas funcionalidades, tal como pode ver na captura de ecrã que se segue.

FIGURA 1. Advanced Panel (painel das definições avançadas)

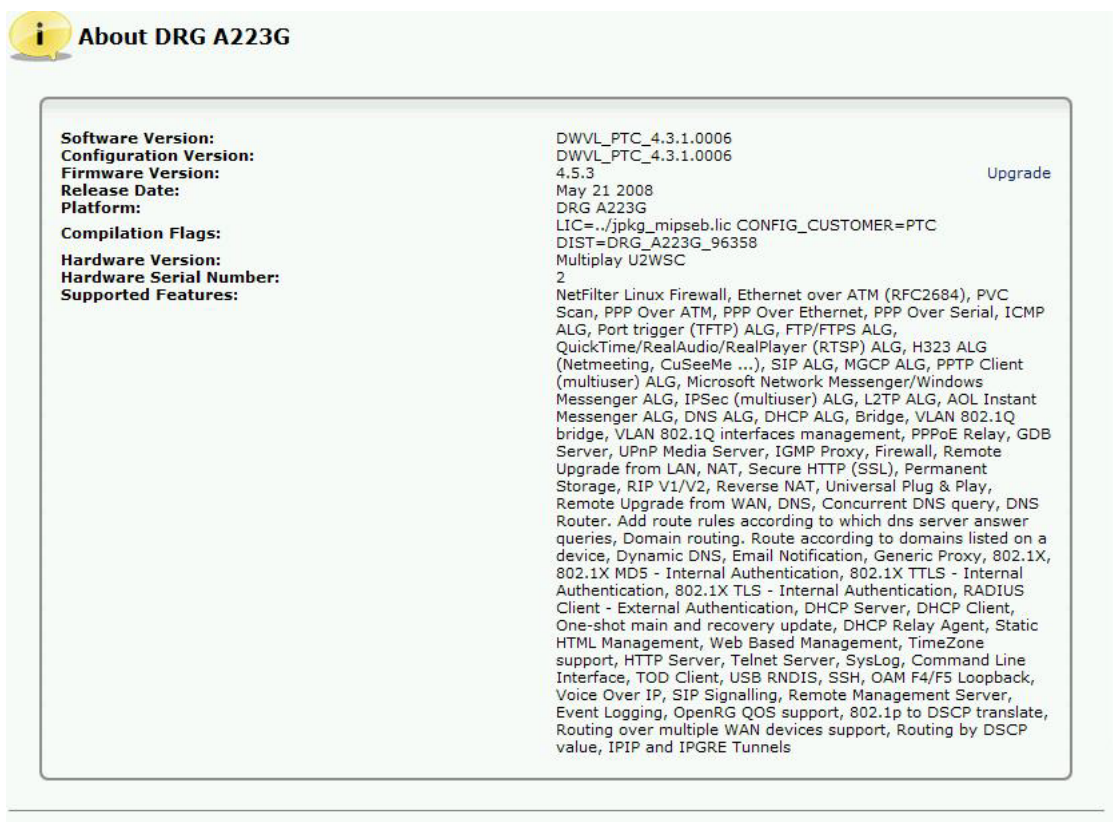


**ABOUT THE DRG A223G
(ACERCA DO DRG A223G)**

O ecrã *About DRG A223G* apresenta vários detalhes acerca da versão do *software* do Router, tais como o número da versão, o tipo de plataforma e uma lista das funcionalidades.

DISCUS™ DRG A223G

FIGURA 2. *About DRG A223G Panel* (painel acerca do DRG A223G)

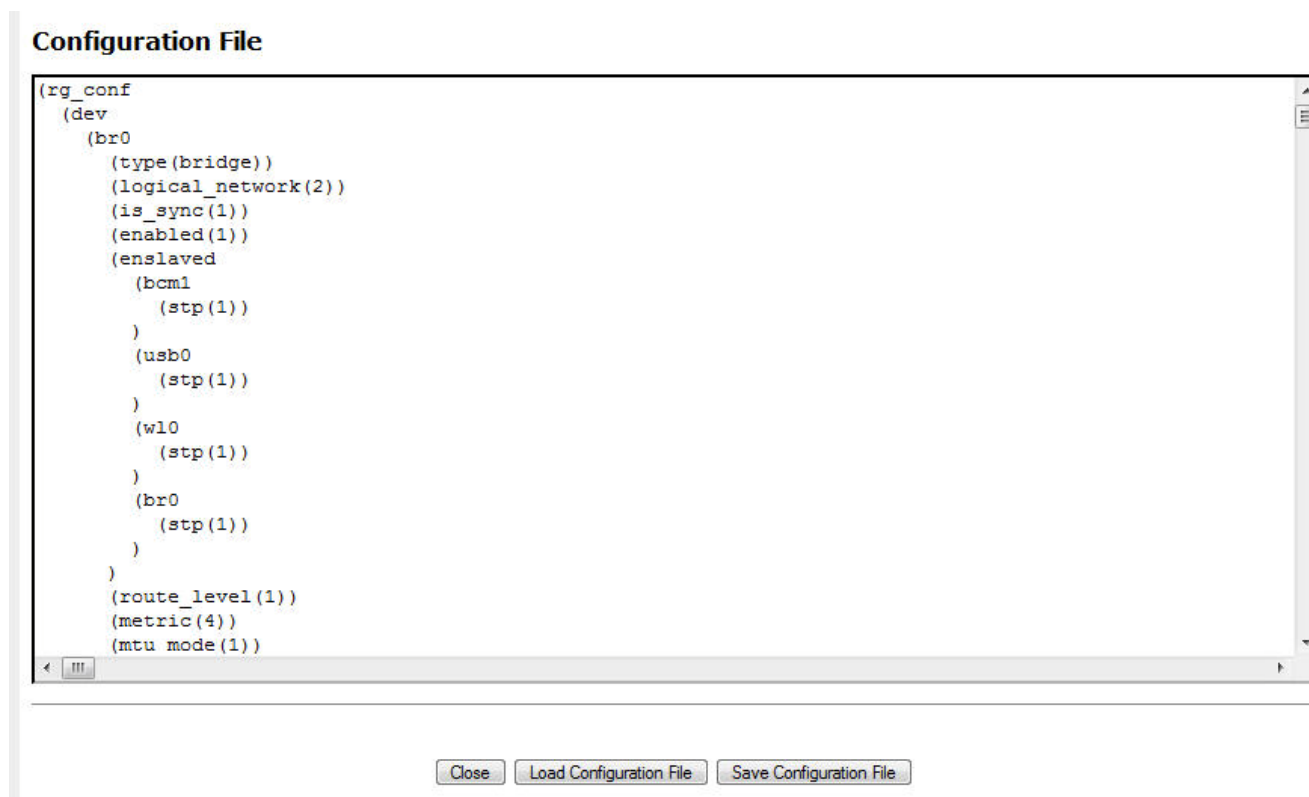


About DRG A223G

Software Version:	DWVL_PTC_4.3.1.0006	
Configuration Version:	DWVL_PTC_4.3.1.0006	
Firmware Version:	4.5.3	Upgrade
Release Date:	May 21 2008	
Platform:	DRG A223G	
Compilation Flags:	LIC=../pkg_mipseb.lic CONFIG_CUSTOMER=PTC DIST=DRG_A223G_96358	
Hardware Version:	Multiplay U2WSC	
Hardware Serial Number:	2	
Supported Features:	NetFilter Linux Firewall, Ethernet over ATM (RFC2684), PVC Scan, PPP Over ATM, PPP Over Ethernet, PPP Over Serial, ICMP ALG, Port trigger (TFTP) ALG, FTP/FTPS ALG, QuickTime/RealAudio/RealPlayer (RTSP) ALG, H323 ALG (Netmeeting, CuSeeMe ...), SIP ALG, MGCP ALG, PPTP Client (multiuser) ALG, Microsoft Network Messenger/Windows Messenger ALG, IPSec (multiuser) ALG, L2TP ALG, AOL Instant Messenger ALG, DNS ALG, DHCP ALG, Bridge, VLAN 802.1Q bridge, VLAN 802.1Q interfaces management, PPPoE Relay, GDB Server, UPnP Media Server, IGMP Proxy, Firewall, Remote Upgrade from LAN, NAT, Secure HTTP (SSL), Permanent Storage, RIP V1/V2, Reverse NAT, Universal Plug & Play, Remote Upgrade from WAN, DNS, Concurrent DNS query, DNS Router. Add route rules according to which dns server answer queries, Domain routing. Route according to domains listed on a device, Dynamic DNS, Email Notification, Generic Proxy, 802.1X, 802.1X MD5 - Internal Authentication, 802.1X TTLS - Internal Authentication, 802.1X TLS - Internal Authentication, RADIUS Client - External Authentication, DHCP Server, DHCP Client, One-shot main and recovery update, DHCP Relay Agent, Static HTML Management, Web Based Management, TimeZone support, HTTP Server, Telnet Server, SysLog, Command Line Interface, TOD Client, USB RNDIS, SSH, OAM F4/F5 Loopback, Voice Over IP, SIP Signalling, Remote Management Server, Event Logging, OpenRG QOS support, 802.1p to DSCP translate, Routing over multiple WAN devices support, Routing by DSCP value, IPIP and IPGRE Tunnels	

**CONFIGURATION FILE
(FICHEIRO DE
CONFIGURAÇÃO)**

Esta funcionalidade pretende tratar da configuração inteira do DISCUS™ DRG A223G num só passo. Só lhe é pedido que localize o ficheiro e inicie o processo de carregamento do ficheiro de configuração. O ficheiro de configuração é um *script* que contém todos os parâmetros que deseja alterar, e é uma alternativa à alteração manual, passo a passo, dos mesmos parâmetros, executada através de capturas de ecrã da *web*.

FIGURA 3. *Configuration File* (ficheiro de configuração)

DDNS

O serviço *Dynamics DNS* (DDNS) permite-lhe replicar um endereço de IP dinâmico num nome de anfitrião estático, tornando possível aceder ao seu computador com maior facilidade através de várias localizações na Internet. Tipicamente, quando se liga à Internet, o seu fornecedor de serviços escolhe um endereço de IP não-utilizado, de um grupo de endereços de IP, e este endereço é apenas usado durante uma ligação específica. A atribuição dinâmica de endereços aumenta o grupo de endereços de IP disponíveis, mantendo um nome de domínio constante.

Quando usar o serviço DDNS, cada vez que o endereço de IP fornecido pelo seu IP for alterado, a base de dados DNS irá também mudar, de maneira a reflectir esta alteração. Desta forma, apesar do seu endereço de IP mudar com frequência, o seu nome de domínio continuará constante e acessível.

FIGURA 4. DDNS

Personal Domain Name (Dynamic DNS)

Host Name	Status	Provider	User Name	Action
New Dynamic DNS Entry				

Press the **Refresh** button to update the status.

Para poder usar a funcionalidade DDNS, precisa de obter uma conta DDNS primeiro. Por exemplo, pode abrir uma conta gratuita no *website* <http://www.dyndns.org/account/create.html>. Quando solicitar uma conta, vai ter de especificar um nome de utilizador e uma palavra-passe.

DNS SERVER (SERVIDOR DNS)

O *Domain Name System* (sistema de nomes de domínio) ou DNS, fornece um serviço que traduz nomes de domínio em endereços de IP e vice versa. O servidor DNS da porta de ligação é um DNS de aprendizagem automática o que significa que, quando um novo computador é ligado à rede, o servidor DNS aprende o seu nome e adiciona-o automaticamente à tabela DNS. Outros utilizadores da rede podem comunicar de forma imediata com este computador, usando ou o seu nome ou o seu endereço de IP.




Além disso, o DNS da sua porta de ligação:

- Partilha uma base de dados comum de nomes de domínio e de endereço de IP com o servidor DHCP.
- Suporta múltiplas sub-redes dentro da LAN em simultâneo.
- Anexa automaticamente um nome de domínio a nomes não-qualificados.
- Permite adicionar novos nomes de domínio à base de dados usando o WBM do Router.
- Permite ao computador ter múltiplos nomes de anfitrião.
- Permite a um nome de anfitrião ter múltiplos IPs (o que é necessário quando um anfitrião tem várias placas de rede).

O servidor DNS não necessita de ser configurado. No entanto, pode desejar ver a lista de computadores de que o DNS tem conhecimento, alterar o nome de anfitrião ou o endereço de IP de um computador da lista, ou adicionar manualmente um novo computador à lista.

FIGURA 5. DNS Server Panel (painel do servidor DNS)

DNS Server

Host Name	IP Address	Source	Action
iway32	192.168.1.1	DHCP	 
New DNS Entry			

Para adicionar uma nova entrada à lista:

1. Clique no botão *New DNS Entry* (nova entrada DNS). Vai aparecer o ecrã *DNS Entry*.
2. Introduza o nome de anfitrião e o endereço de IP do computador.
3. Clique “OK” para guardar as alterações.

**DRG A223G FIRMWARE
UPGRADE
(ACTUALIZAÇÃO DO
FIRMWARE DO DGR
A223G)**

O DISCUS™ DRG A223G oferece um mecanismo incorporado para fazer actualizações da imagem do seu *software* sem perder nenhuma das suas configurações e definições personalizadas. Existem dois métodos de actualização da imagem do *software*:

1. Fazer a actualização através de um computador local: use um ficheiro de imagem de *software* cujo *download* foi feito previamente para a unidade de disco do seu PC, ou localizado no CD de avaliação que veio com ele.
2. Fazer a actualização através da Internet: também se pode chamar *Remote Update* (actualização remota), use este método para actualizar o seu *Firmware* através do *download* remoto de um ficheiro de imagem de *software* actualizado.

Fazer a actualização através de um computador local:

Para fazer a actualização da imagem de *software* do router usando um ficheiro *rmt.* disponível localmente: aceda a esta funcionalidade através do separador *Maintenance* (manutenção), no ecrã *System* (sistema), ou clicando no seu ícone no ecrã *Advanced* (avançadas). Vai aparecer o ecrã *Firmware Upgrade*.

Actualização Remota:

Ajuda-o a manter a sua imagem de *software* em dia, fazendo verificações diárias de rotina de novas versões do *software*, permitindo-lhe também executar verificações manuais.

Para ver as definições de verificação automática da utilidade e os resultados da última verificação, clique no ícone *Firmware Upgrade* no ecrã *Advanced*. Vai aparecer o ecrã *Firmware Upgrade*. Na secção *Upgrade from the Internet* (actualizar a partir da Internet) pode seleccionar o método de actualização da utilidade e o intervalo de tempo. O resultado da última verificação é apresentado na linha perto dos botões *Check Now* (verificar agora) e *Force Upgrade* (forçar a actualização), indicando se há ou não uma nova versão disponível.

Se houver uma nova versão disponível:

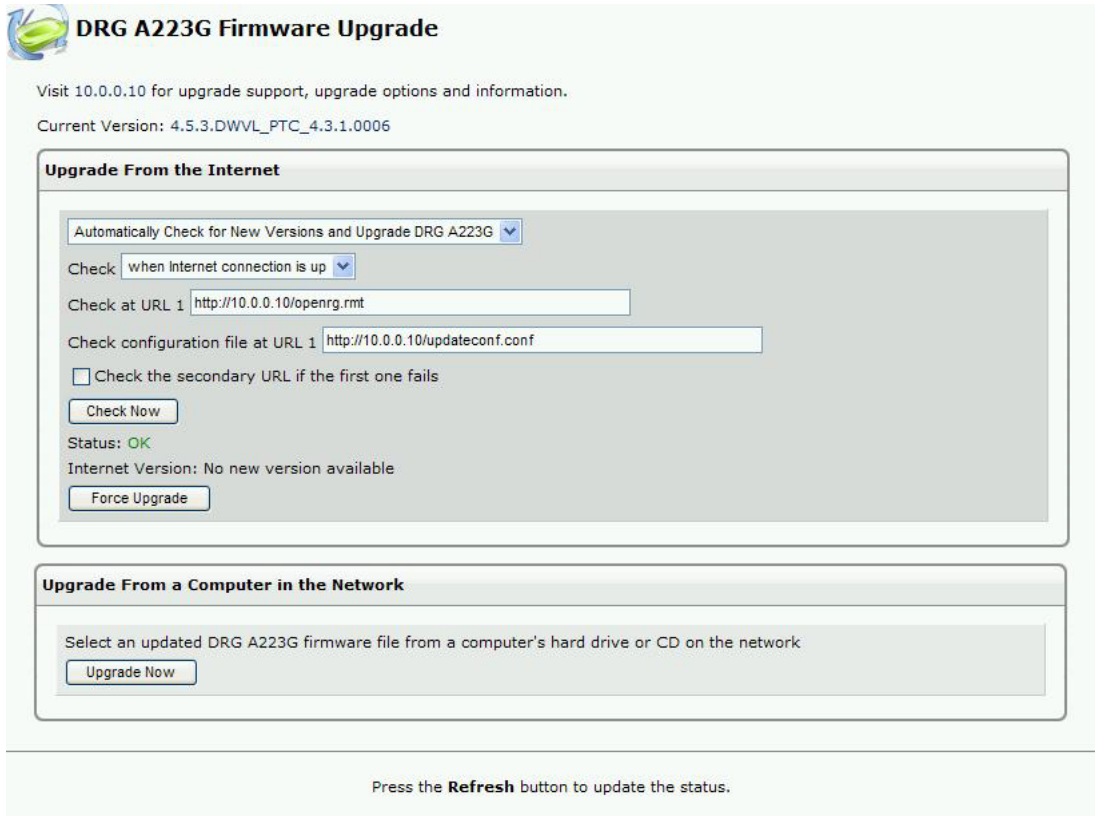
- Clique no botão *Force Upgrade*. Vai ser iniciado um processo de *download*. Quando o *download* estiver completo, vai aparecer um ecrã de confirmação que lhe vai perguntar se quer actualizar para a nova versão.

- Clique *OK* para confirmar. Vai então começar o processo de actualização, o qual não deve demorar mais de um minuto.

Quando o processo de actualização terminar, o Router irá reiniciar-se automaticamente. A nova versão do *software* vai ser executada, mantendo as suas configurações e definições personalizadas.

Se não houver uma nova versão disponível, clique no botão *Check Now* (verificar agora) para executar uma verificação imediata (em vez de aguardar pela próxima verificação agendada). O ecrã vai mostrar a seguinte mensagem em verde: "*Check in progress...*" (verificação em progresso).

FIGURA 6. DRG A223G Firmware Upgrade Panel (painel de actualização do firmware do DGR A223G)



DRG A223G Firmware Upgrade

Visit 10.0.0.10 for upgrade support, upgrade options and information.

Current Version: 4.5.3.DWVL_PTC_4.3.1.0006

Upgrade From the Internet

Automatically Check for New Versions and Upgrade DRG A223G

Check: when Internet connection is up

Check at URL 1: http://10.0.0.10/openrg.rmt

Check configuration file at URL 1: http://10.0.0.10/updateconf.conf

Check the secondary URL if the first one fails

Check Now

Status: OK

Internet Version: No new version available

Force Upgrade

Upgrade From a Computer in the Network

Select an updated DRG A223G firmware file from a computer's hard drive or CD on the network

Upgrade Now

Press the **Refresh** button to update the status.

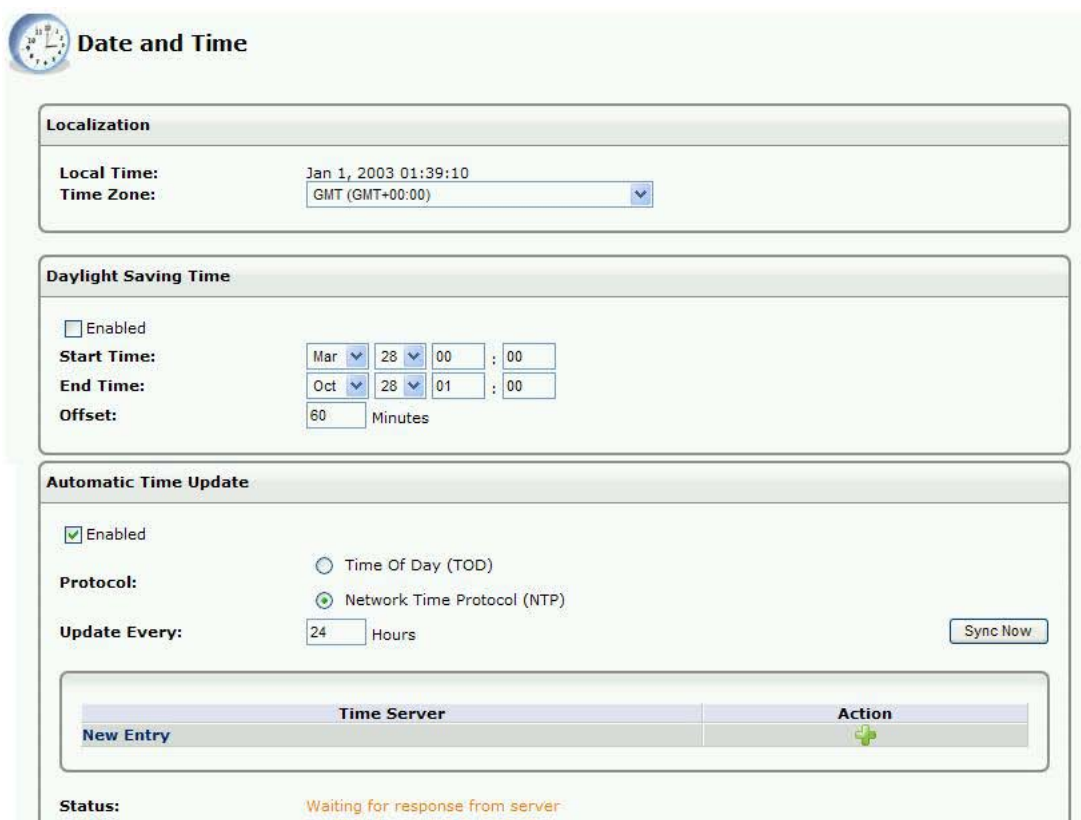
DATE AND TIME (DATA E HORA)

Para configurar as definições de data, hora e mudança da hora, siga os seguintes passos:

1. Clique no ícone *Date and Time* (data e hora) no ecrã *Advanced* da gestão pela Internet. Vai ser mostrado o ecrã das definições *Date and Time*.
2. Selecciono o fuso horário local do menu pendente. O Router é capaz de detectar as definições de mudança da hora automaticamente para os fusos horários seleccionados. Se as definições da mudança de hora para o seu fuso horário não forem detectadas automaticamente, são apresentados os campos seguintes:
 - *Enabled* (activo). Selecciono esta caixa de verificação para activar a mudança da hora.
 - *Start* (início). Data e hora do início da mudança de hora.
 - *End* (fim). Data e hora do fim da mudança de hora.
 - *Offset* (desactivar). Desactivar mudança de hora.

3. Se deseja que a porta de ligação execute uma actualização da hora automática, siga os seguintes passos:
 - Seleccione a caixa de verificação *Enabled* (activo), por baixo da secção *Automatic Time Update* (actualização automática da hora).
 - Seleccione o protocolo a ser usado para executar a actualização da hora, seleccionando o botão de opção *Time of Day* (hora do dia) ou o botão de opção *Network Time Protocol* (protocolo de hora da rede).
 - Especifique a frequência de execução da actualização no campo *Update Every* (actualize a cada...).
 - Pode definir endereços do servidor de hora clicando no link *New Entry* (nova entrada) no fim da secção *Automatic Time Update* (actualização automática da hora).

FIGURA 7. Date and Time Panel (painel da data e hora)



Date and Time

Localization

Local Time: Jan 1, 2003 01:39:10
 Time Zone: GMT (GMT+00:00)

Daylight Saving Time

Enabled


Start Time: Mar 28 00 : 00
 End Time: Oct 28 01 : 00
 Offset: 60 Minutes

Automatic Time Update

Enabled

Protocol: Time Of Day (TOD) Network Time Protocol (NTP)

Update Every: 24 Hours

Time Server	Action
New Entry	

Status: Waiting for response from server

**DIAGNOSTICS
(DIAGNÓSTICO)**

O ecrã *Diagnostics* (diagnóstico) pode ajudá-lo a testar a conectividade da rede e a ver estatísticas, tal como o número de pacotes transmitidos e recebidos, o tempo de transmissão e o estado de sucesso.

FIGURA 8. *Diagnostics Panel* (painel de diagnóstico)

Diagnostics

Ping (ICMP Echo)

Destination: Go

Number of pings:

Status: Test Failed

Packets: 4/4 transmitted, 0/4 received, 100% loss

ARP

Destination: Go

Status:

Traceroute

Destination: Cancel

Status: Testing

Hops: 10

```

tracert to www.pirelli.com (80.241.235.23), 30 hops max
1 192.168.100.1 (192.168.100.1) 58.436 ms 54.671 ms 55.718 ms
2 * * *
3 r-mi224-vl19.opb.interbusiness.it (80.20.6.31) 57.661 ms 54.623 ms 55.843 ms
4 r-rm199-ca29-a.opb.interbusiness.it (151.99.99.161) 59.754 ms * 107.388 ms
5 151.99.75.163 (151.99.75.163) 55.560 ms 58.726 ms 55.541 ms
    
```

PVC Scan

Status: Done Go

Results:

OAM Ping

Type: Go

VPI:

VCI:

Count:

Status:

Ping (Eco ICMP) Para diagnosticar a conectividade da rede siga os passos seguintes:

1. Clique no ícone *Diagnostics* (diagnóstico) no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã *Diagnostics*.

2. Na secção *Ping* (Eco ICMP), introduza o endereço de IP ou URL a ser testado no campo *Destination* (destino).
3. Introduza o número de *pings* que gostaria de executar.
4. Clique no botão *Go* (ir).
5. No espaço de poucos segundos são apresentadas as estatísticas de diagnóstico. Se não lhe for apresentada informação nova, clique no botão *Refresh* (actualizar).

ARP: Executar um teste a um pacote ARP.

Executar um *Traceroute* (rastreo de rota): Para executar um *traceroute* siga os seguintes passos:

1. Clique no ícone *Diagnostics* (diagnóstico) no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã *Diagnostics*.
2. Na secção *Traceroute*, introduza o endereço de IP ou URL a ser testado no campo *Destination* (destino).
3. Clique no botão *Go* (ir). Vai começar a ser executado um *traceroute*, com o ecrã a ser constantemente actualizado.
4. Para parar o *traceroute* e ver os resultados, clique em *Cancel* (cancelar).

Executar um *PVC Scan* (rastreo do PVC): Para executar um *PVC Scan* siga os passos seguintes:

1. Clique no ícone *Diagnostics* (diagnóstico) no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã *Diagnostics*.
2. Por baixo da secção *PVC Scan* clique no botão *Go* (ir).
3. No espaço de poucos segundos são apresentadas as estatísticas de diagnóstico. Se não lhe for apresentada informação nova, clique no botão *Refresh* (actualizar).

Executar um *OAM Ping*: Para executar um *OAM Ping* siga os seguintes passos:

1. Clique no ícone *Diagnostics* (diagnóstico) no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã *Diagnostics*.
2. Por baixo da secção *OAM Ping* seleccione o tipo de *OAM Ping* que deseja executar. *F4 End-to-End* (extremo-a-extremo), *F4 Segment* (segmento), *F5 End-to-End*, *F5 Segment*.
3. Clique no botão *Go* (ir).
4. No espaço de poucos segundos são apresentadas as estatísticas de diagnóstico. Se não lhe for apresentada informação nova, clique no botão *Refresh* (actualizar).

**IP ADDRESS
DISTRIBUTION
(DISTRIBUIÇÃO DE
ENDEREÇOS DE IP)**

O servidor Protocolo de Configuração de Anfitrião Dinâmico (DHCP) da sua porta de ligação permite-lhe adicionar facilmente computadores que estão configurados como clientes DHCP da rede doméstica. Fornece um mecanismo para atribuir endereços de IP e para entregar os parâmetros de configuração da rede a tais anfitriões. O servidor DHCP predefinido do Router é a ponte LAN.

Um cliente (anfitrião) envia uma mensagem de difusão pela LAN, a pedir um endereço de IP para si. Então, o servidor DHCP verifica a sua lista de endereços disponíveis e aluga um endereço de IP local ao anfitrião durante um período de tempo específico e, em simultâneo, designa esse endereço de IP como "usado". Nesse momento, o anfitrião está configurado com um endereço de IP durante o período de tempo do aluguer.

O anfitrião pode escolher entre renovar um aluguer prestes a expirar ou deixá-lo expirar. Se escolher renovar um aluguer, vai também receber informações actuais acerca dos serviços da rede, tal como no caso do aluguer original, permitindo-lhe actualizar as suas configurações de rede de forma a reflectirem quaisquer alterações que possam ter ocorrido desde a sua primeira ligação à rede. Se um anfitrião desejar terminar o aluguer antes de expirar, pode enviar uma mensagem de libertação ao servidor DHCP, a qual irá tornar o endereço de IP disponível para ser usado por outros.

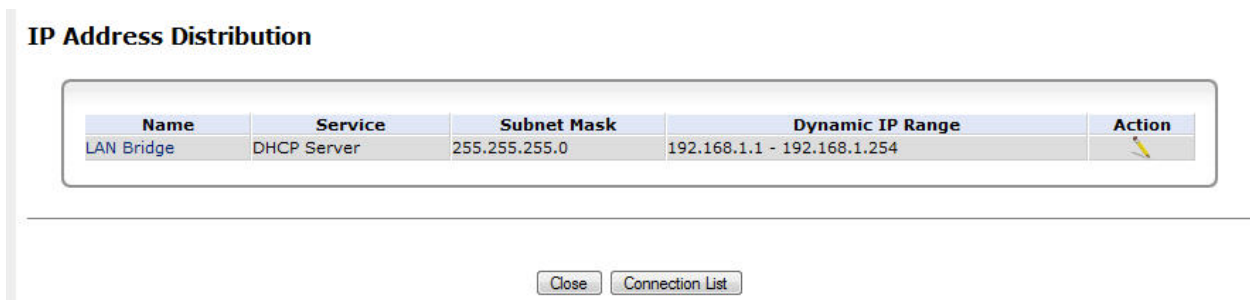
O servidor DHCP da sua porta de ligação:

- Apresenta uma lista de todos os dispositivos com anfitriões DHCP ligados ao Router.
- Define a extensão de endereços de IP que podem ser atribuídos na LAN.
- Define o período de tempo durante o qual os endereços de IP dinâmicos estão atribuídos.
- Fornece as configurações em cima para cada dispositivo LAN e pode ser configurado ou activado/desactivado em separado para cada dispositivo LAN.
- Pode atribuir um aluguer estático a um PC LAN, para que este possa receber o mesmo endereço de IP de cada vez que se ligar à rede, mesmo se esse endereço de IP estiver entre o grupo de endereços que o servidor DHCP pode atribuir a outros computadores.
- Fornece o servidor DNS com o nome de anfitrião e endereço de IP de cada um dos PC ligados à LAN.

Além disso, o Router pode agir como um agente de reencaminhamento de DHCP, escalando as responsabilidades de DHCP para um servidor DHCP WAN. Neste caso, o DISCUS™ DRG A223G irá apenas agir como router, enquanto que os seus anfitriões LAN irão receber os seus endereços de IP de um servidor DHCP na WAN.

Com a funcionalidade *Zero Configuration Technology* (tecnologia de configuração zero) do Router, que é opcional, o método *IP Auto Detection* (detecção automática de IPs) detecta endereços de IP definidos estaticamente, para além dos clientes DHCP do Router. Aprende todos os endereços de IP da LAN, e integra a informação recolhida na base de dados do servidor DHCP. Isto permite ao servidor DHCP emitir alugueres válidos evitando, assim, endereços de IP em conflito usados por outros computadores da rede.

FIGURA 9. IP Address Distribution Panel (painel de distribuição de endereços de IP)



PROTOCOLS (PROTOCOLOS)

A funcionalidade *Protocols* (protocolos) incorpora uma lista de aplicações predefinidas e definidas pelo utilizador, e definições comuns às portas. Pode usar protocolos em várias funcionalidades de segurança, tais como *Access Control* (controlo dos acessos) e *Port Forwarding* (reencaminhamento de portas). Pode adicionar novos protocolos para suportar novas aplicações ou alterar os protocolos existentes de acordo com as suas necessidades.

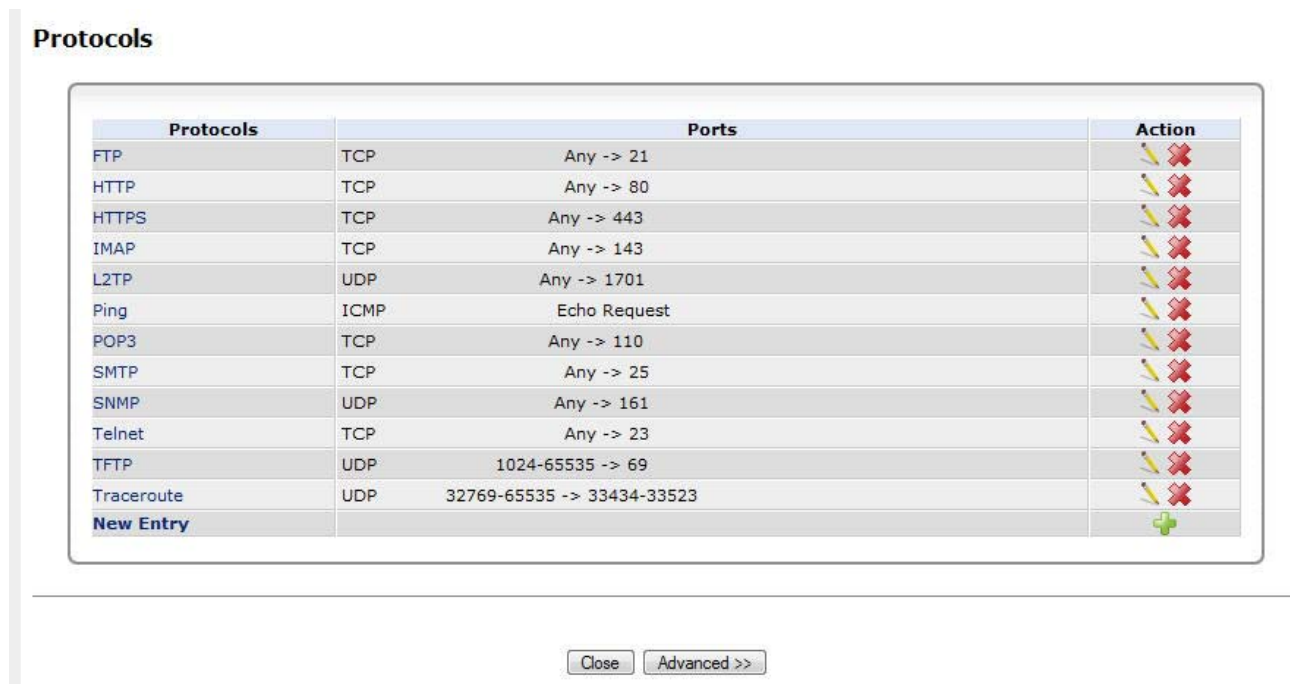
Para ver a lista de protocolos básicos clique no ícone *Protocols* no ecrã *Advanced*. Clique no botão *Advanced* no fim deste ecrã para ter acesso à lista completa dos protocolos suportados pelo Router.

Para definir um protocolo:

1. Clique no ícone *Protocols* no ecrã *Advanced*. Vai aparecer o ecrã *Protocols*.
2. Clique no *link New Entry* (nova entrada). Vai aparecer o ecrã *Edit Service* (editar o serviço).
3. Dê um nome ao serviço no campo *Service Name* e clique no *link New Service Ports* (novas portas de serviço). Vai aparecer o ecrã *Edit Service Server Ports* (alterar as portas de serviço do servidor). Pode escolher qualquer um dos protocolos disponíveis na caixa de combinação, ou adicionar um novo protocolo clicando em *Other* (outro). Quando estiver a seleccionar um protocolo da caixa de combinação, o ecrã vai ser actualizado, apresentando os respectivos campos nos quais deve introduzir a informação relevante.

4. Seleccione um protocolo e introduza a informação relevante.
5. Clique *OK* para guardar as alterações.

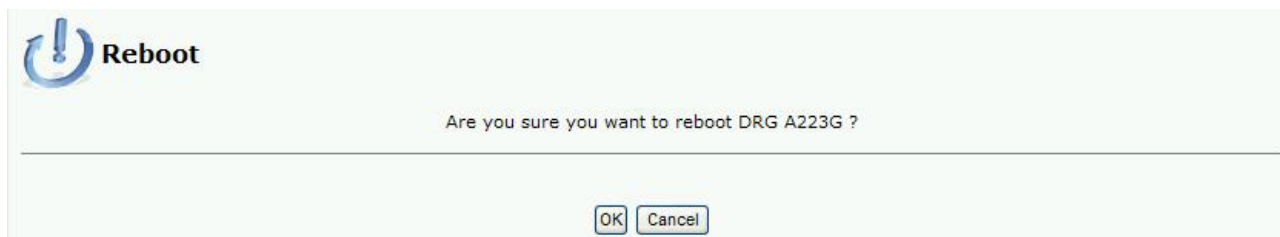
FIGURA 10. Protocols Panel (painel dos protocolos)



REBOOT (REINICIAR)

Para reiniciar o DISCUS™ DRG **A223G**:

1. Clique no ícone *Reboot* (reiniciar) no ecrã *Advanced* do WBM. Vai aparecer o ecrã *Reboot*.
2. Clique *OK* para reiniciar o Router. Isto pode demorar até um minuto. Para reintroduzir o WBM após reiniciar a porta de ligação, clique no botão de *Refresh* (actualizar) do *browser*.

FIGURA 11. *Reboot Panel* (painel de reiniciação)

RESTORE DEFAULTS (RESTAURAR PREDEFINIÇÕES)

Às vezes, pode querer restaurar as predefinições de fábrica do Router. Isto pode acontecer, por exemplo, quando desejar começar uma nova rede do princípio, ou quando não se lembrar das alterações feitas à rede e desejar voltar à configuração predefinida.

Para restaurar as definições predefinidas:

1. Clique no ícone *Defaults* (predefinições) no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã *Restore Defaults* (restaurar predefinições).
2. Clique *OK* para restaurar as predefinições de fábrica do Discus.

FIGURA 12. *Restore Defaults Panel* (painel de restauração das predefinições)

ROUTING (ROTEAMENTO)

Aceda às definições de roteamento do Router clicando no ícone *Routing* no ecrã *Advanced*. Vai aparecer o ecrã básico de *Routing*. Clique no botão *Advanced* para ver as definições completas de roteamento.

Routing Table (tabela de roteamento):

Pode adicionar, alterar ou eliminar as regras de roteamento da tabela de roteamento. Clique no *link New Route* (nova rota). Vai aparecer o ecrã *Route Settings* (definições da rota). Quando estiver a adicionar uma regra de roteamento, precisa de especificar o seguinte:

Name (nome): Seleccionar o dispositivo da rede.

Destination (destino): O destino é o anfitrião do destino, endereço da sub-rede, endereço da rede ou a rota predefinida, O destino para uma rota predefinida é 0.0.0.0.

Netmask (máscara de rede): A máscara de rede é usada em conjunto com o destino para determinar quando é que uma rota está a ser usada.

Gateway (porta de ligação): Introduza o endereço de IP da porta de ligação.

Metric (métrica): Medida da preferência de uma rota. Tipicamente, a medida mais baixa é a rota preferida. Se existem várias rotas com o mesmo valor de medida, a rota predefinida vai ser a primeira a aparecer.

Routing Protocols (protocolos de roteamento)

Routing Information Protocol (protocolo de informação de rota) ou RIP: Seleccionar esta caixa de verificação para permitir que as ligações previamente definidas usem o RIP. Se esta caixa de verificação não estiver seleccionada, o RIP vai ser desactivado para todas as ligações, incluindo as ligações definidas para usar o RIP.

- *Poison Reverse* (envenenamento inverso): O Discus irá apresentar a informação adquirida sobre a rota com uma medida alta, para que os outros routers a ignorem.

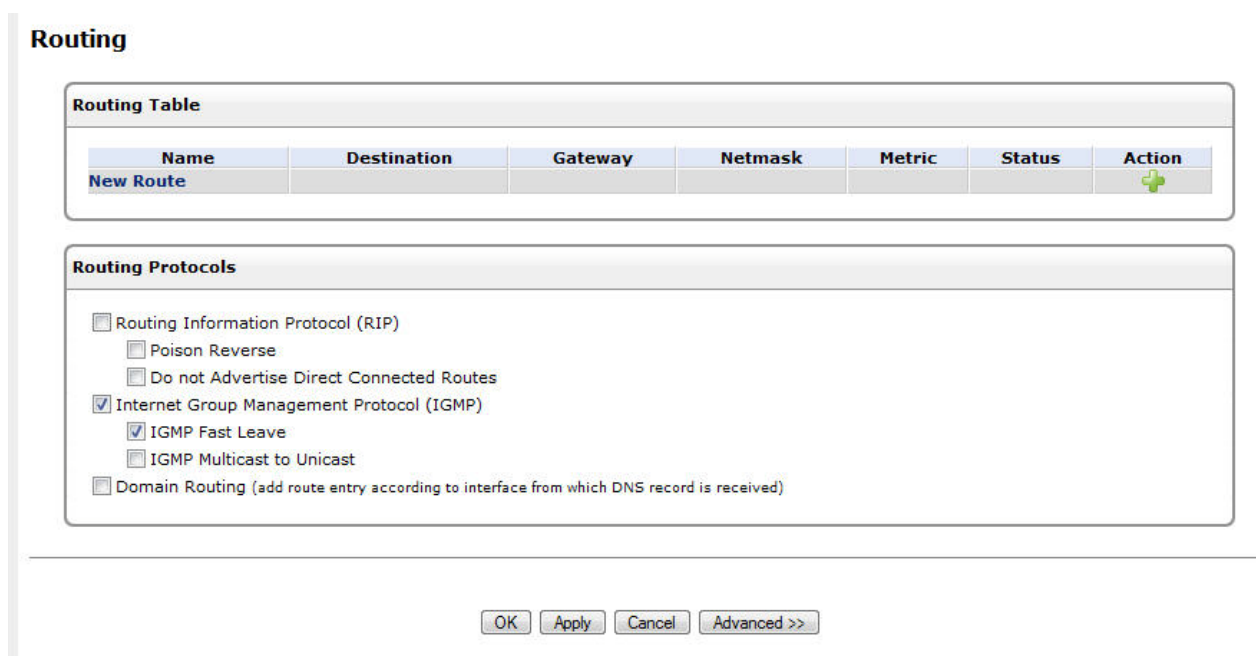
- *Do not Advertise Direct Connected Routes* (não anunciar rotas ligadas directamente): O Router não vai anunciar a informação da rota ao mesmo dispositivo da sub-rede que emitiu esta informação.

Internet Group Management Protocol (protocolo de gestão de grupo de Internet) ou IGMP: O Router dá suporte à transmissão múltipla (*multicasting*) do IGMP, a qual permite que anfitriões ligados a uma rede sejam actualizados sempre que for feita uma alteração importante à rede. Uma transmissão múltipla (*multicast*) é simplesmente uma mensagem que é enviada em simultâneo para um grupo predefinido de receptores. Quando aderir a um grupo de transmissão múltipla (*multicast group*), vai receber todas as mensagens endereçadas para esse grupo, de forma semelhante ao que acontece quando uma men-

sagem de correio electrónico é enviada para uma lista de correio (*mailing list*). A transmissão múltipla de IGMP pode ter utilidade quando estiver ligado à Internet a partir de um router. Quando uma aplicação em execução num computador LAN envia um pedido de adesão a um grupo de transmissão múltipla, o Router ouve e intercepta as mensagens deste grupo, enviando-as para a aplicação que aderiu ao grupo.

Domain Routing (roteamento de domínios): Quando o servidor DNS do Router receber uma resposta de um servidor DNS exterior, vai ser adicionada uma entrada de roteamento para o endereço de IP da resposta, através do dispositivo de onde veio a resposta. Isto significa que os pacotes vindos deste endereço de IP no futuro vão ser encaminhados através do dispositivo de onde veio a resposta.

FIGURA 13. Routing Panel (painel de roteamento)



SSH

O protocolo *Secure Shell* (SSH) fornece ligações encriptadas a anfitriões ou servidores remotos. O DISCUS™ DRG A223G suporta pedidos de ligação SSH de clientes LAN com permissões de administração. Quando está ligada, uma sessão segura da linha de comandos irá conceder acesso a todos parâmetros e definições do sistema. Este serviço também pode ser aberto a clientes WAN.

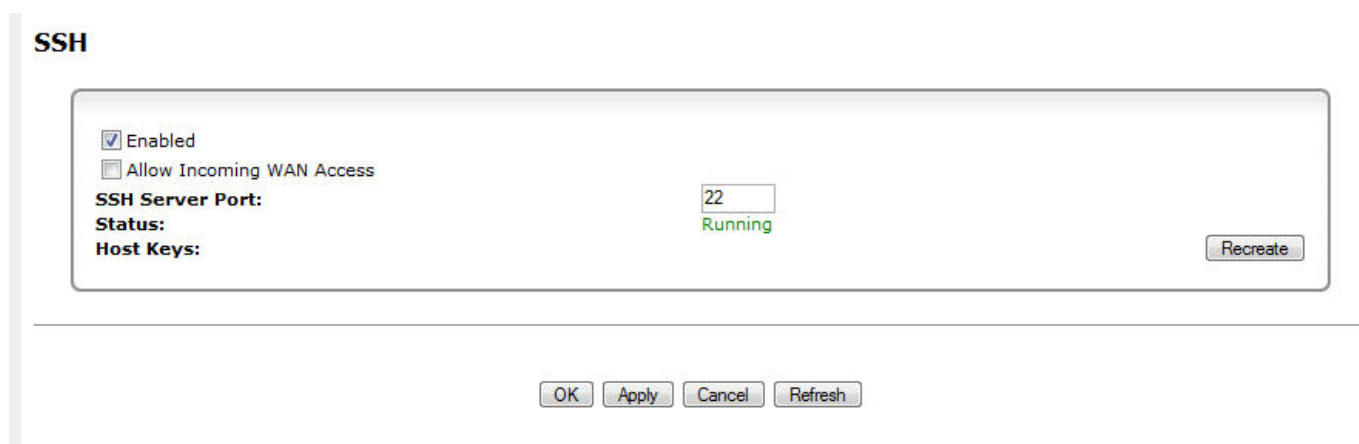
Clique no ícone SSH no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã SSH.

Enabled (activo). Seleccione ou desseleccione esta caixa para activar ou desactivar esta funcionalidade.

Status (estado): Por predefinição, esta funcionalidade está activa e o seu estado aparece como *Running* (em execução). Este estado irá mudar de forma a reflectir as acções executadas.

Host Keys (chaves de anfitrião): As *host keys* (chaves de anfitrião) são usadas para indicar o Router para os pedidos de ligação SSH recebidos. Pode desejar usar chaves novas em vez das chaves antigas. Para tal, clique no botão *Recreate* (recriar). O estado vai mudar para *Generating Host Keys* (a gerar chaves de anfitrião), enquanto as chaves estão a ser criadas e guardadas no ficheiro de configuração do Router.

FIGURA 14. *SSH Panel* (painel da SSH)



SCHEDULER RULES (REGRAS PROGRAMADAS)

As regras programadas são usadas para limitar a activação das regras de *fire-wall* a determinados períodos, especificados em termos de dias da semana e horas.




Para definir uma regra:

1. Clique no ícone *Scheduler Rules* (regras programadas) no ecrã *Advanced* da gestão pela Internet. Vai aparecer o ecrã *Scheduler Rules*.
2. Clique no *link New Scheduler Entry* (nova entrada de agenda). Vai aparecer o ecrã *Scheduler Rule Edit* (alteração da regra agendada).
3. Especifique um nome para a regra no campo *Name* (nome).
4. Especifique se a regra vai estar activa/inactiva durante o período de tempo designado, seleccionando a caixa de verificação *Rule Activity Settings* (definições da actividade das regras) adequada.
5. Clique no *link New Time Segment Entry* (nova entrada de segmento temporal) para definir o segmento temporal durante o qual a regra vai ser aplica-

- da. Vai aparecer o ecrã *Time Segment Edit* (alterar o segmento temporal).
- (a) Seleccione os dias da semana em que deve desejar que esteja activo/inactivo.
 - (b) Clique em *New Time Segment Entry* (nova entrada de segmento temporal) para definir um período de tempo durante o qual deseja que esteja activo/inactivo).
6. Clique OK para guardar as alterações.

FIGURA 15. Scheduler Rules Panel (painel das regras programadas)

Scheduler Rules

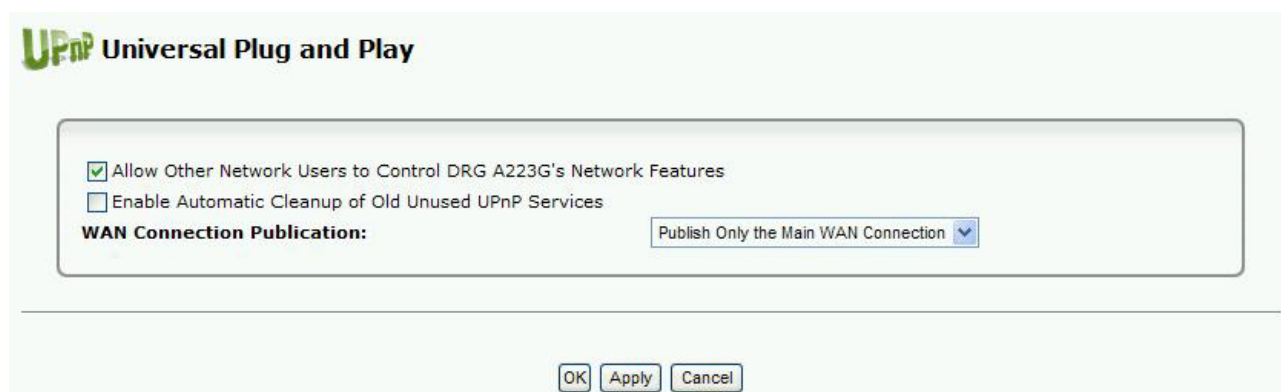
Name	Settings	Status	Action
new Rule	Mon between 00:00-02:00	Inactive	 
New Entry			

**UNIVERSAL PLUG AND
PLAY (“USAR E LIGAR”
UNIVERSAL)**

O *Universal Plug-and-Play* é uma arquitectura de funcionamento em rede que proporciona compatibilidade entre equipamento de funcionamento em rede, *software*, e periféricos. Os produtos com UPnP podem ligar-se e comunicar com outros dispositivos com *Universal Plug-and-Play*, sem o utilizador precisar de o configurar, sem servidores centralizados ou sem *drivers* de dispositivos específicos para determinados produtos.

Se o seu computador estiver a executar um sistema operativo que suporta UPnP, tal como o Windows XP, pode adicionar o computador à sua rede doméstica e aceder à gestão pela Internet directamente a partir do Windows.

FIGURA 16. *Universal Plug and Play Panel* (painel Universal Plug and Play)



Secção sobre Monitorização do Sistema

Este capítulo irá descrever a Secção de Monitorização do Sistema, a qual pode ser acedida através da *Home Page* do DISCUS™ DRG A223G, mediante a autenticação do utilizador do Router.



Esteja ciente de que quaisquer alterações à configuração podem comprometer a sua conectividade.

NETWORK CONNECTIONS (LIGAÇÕES DE REDE):

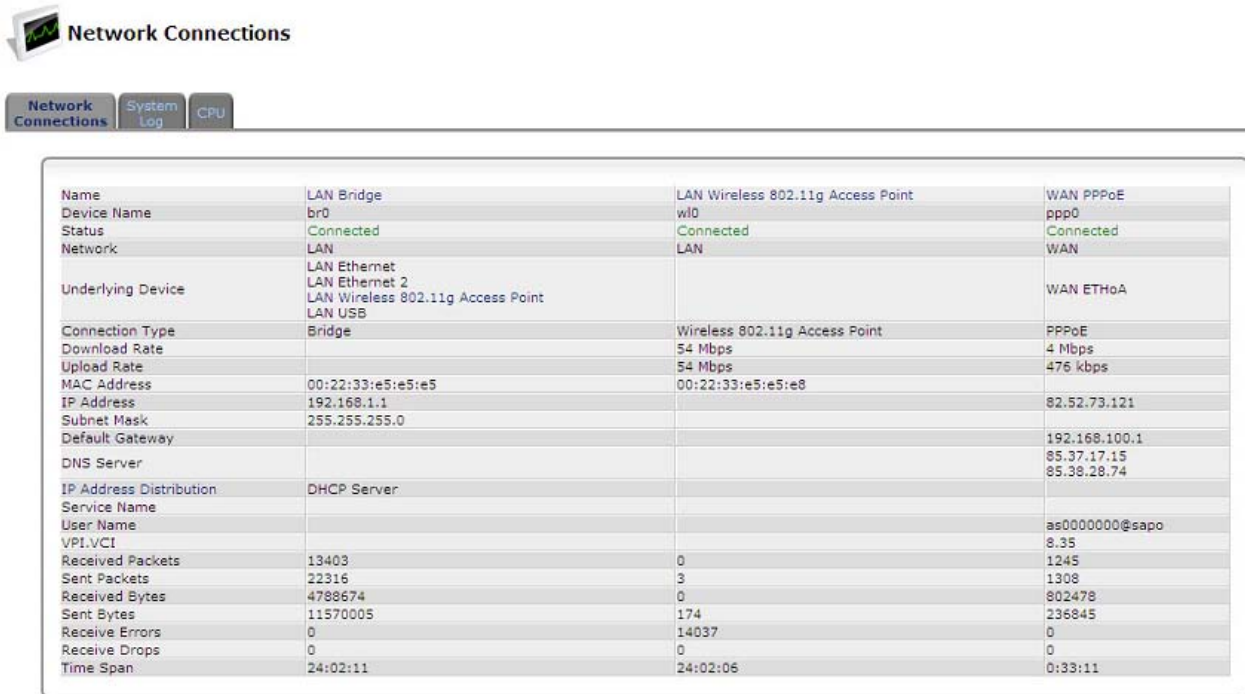
O ecrã de *Monitoring* (monitorização) apresenta uma tabela que faz um resumo dos dados de ligação monitorizados.

O DISCUS DRG A223G monitoriza constantemente o tráfego que ocorre na rede local e entre a rede local e a Internet.

Pode ver informação estatística acerca dos dados recebidos da e transmitidos para a Internet (WAN) e para computadores na rede local (LAN).

Clique no botão *Refresh* para actualizar o ecrã, ou clique no botão *Automatic Refresh On* para actualizar constantemente os parâmetros apresentados no ecrã.

FIGURA 1. Network ConnectionsPanel (painel de ligações de rede)



Network Connections

Network Connections | System Log | CPU

Name	LAN Bridge	LAN Wireless 802.11g Access Point	WAN PPPoE
Device Name	br0	wl0	ppp0
Status	Connected	Connected	Connected
Network	LAN	LAN	WAN
Underlying Device	LAN Ethernet LAN Ethernet 2 LAN Wireless 802.11g Access Point LAN USB		WAN ETHoA
Connection Type	Bridge	Wireless 802.11g Access Point	PPPoE
Download Rate		54 Mbps	4 Mbps
Upload Rate		54 Mbps	476 kbps
MAC Address	00:22:33:e5:e5:e5	00:22:33:e5:e5:e8	
IP Address	192.168.1.1		82.52.73.121
Subnet Mask	255.255.255.0		
Default Gateway			192.168.100.1
DNS Server			85.37.17.15 85.38.28.74
IP Address Distribution	DHCP Server		
Service Name			
User Name			as0000000@sapo
VPI.VCI			8.35
Received Packets	13403	0	1245
Sent Packets	22316	3	1308
Received Bytes	4788674	0	802478
Sent Bytes	11570005	174	236845
Receive Errors	0	14037	0
Receive Drops	0	0	0
Time Span	24:02:11	24:02:06	0:33:11

SYSTEM LOG (REGISTO DO SISTEMA)

O ecrã de registo do sistema apresenta uma lista das actividades mais recentes que aconteceram no Router.

FIGURA 2. System Log Panel (painel de registo do sistema)



System Log

Network Connections | System Log | CPU

Close Clear Log Save Log Refresh

Press the **Refresh** button to update the data.

Time	Event	Event-Type	Details
------	-------	------------	---------

CPU

O ecrã CPU mostra quanto tempo passou desde que o sistema foi iniciado pela última vez, e a média de carga. Além disso, o ecrã também apresenta uma lista de todos os processos em execução no Router nesse momento e o seu consumo de memória virtual. Por predefinição, o ecrã é actualizado automaticamente, mas isto pode ser alterado clicando no botão *Automatic Refresh Off* (actualização automática desligada).

FIGURA 3. CPU Panel (painel CPU)

