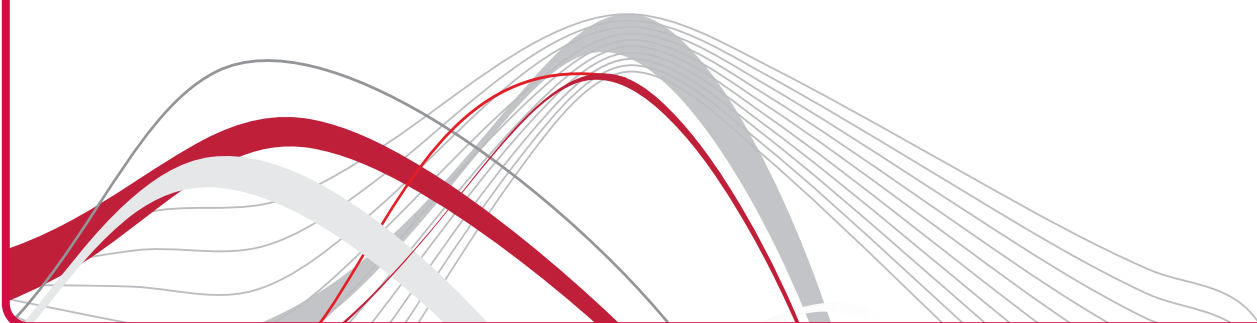




P.DG A1000G

Manual de Utilizador



ÍNDICE

Bem-vindo	1
Sobre este Manual	1
Denominação	1
Convenções	1
Introdução.....	3
Introdução	3
Conteúdos da Embalagem	3
Vantagens do Router.....	5
Aplicações	6
Descrição do Hardware	6
Requisitos Mínimos de Sistema e Componentes	6
Painel Frontal	7
Painel Posterior	9
Instalação do Hardware	10
Definições ISP	10
Posicionamento do Router	11
Instalação dos Microfiltros	11
Alimentação do Router	12
Ligação do Router	12
Ligação Ethernet	14
Configuração TCP/IP	15
Ligação Ethernet >> Instalação do Protocolo TCP/IP	15
Ligação Ethernet >> Configuração do TCP/IP	16
Desactivar o proxy HTTP	21
Obter as Configurações IP do Router	22
Configurações IPv6	24
Ligação Wi-Fi	24
Configuração do Router	27
Interface de Gestão	30
Efectuar Alterações de Configuração	30
Parâmetros de Configuração Avançados	30

Secção do Sistema	33
Sistema >> Definições de Hora	33
Sistema >> Definições de Password	34
Sistema >> DNS	35
Secção WAN	37
WAN >> ATM PVC	37
WAN >> Interface ATM 1483 bridging	39
WAN >> Interface ATM PPPoA	40
WAN >> Interface ATM 1483 routing [roteamento]	43
WAN >> Interface ATM PPPoE	44
WAN >> Interface ATM MAC Encapsulated Routing [roteamento MAC encapsulado]	47
WAN >> Clone MAC Address [Endereço de Clone de MAC]	48
Secção LAN.....	49
LAN >> DHCP Option [opção DHCP]	51
Secção Sem Fios	53
Sem Fios >> Canal e SSID	54
Sem Fios >> Controlo de Acesso	54
Sem Fios >> Segurança	55
Sem Fios >> Segurança >> WEP	56
Sem Fios >> Segurança >> WPA	58
Sem Fios >> Segurança >> 802.1X	60
Sem Fios >> Wi-Fi Protected Setup [Configuração protegida Wi-Fi]	61
Sem Fios >> WDS	63
Sem Fios >> Configuração Avançada	64
Secção NAT	66
NAT >> Mapeamento de Endereços	67
NAT >> Servidor Virtual	68
NAT >> Aplicação Especial	71
NAT >> NAT Mapping Table [Tabela de mapeamento NAT]	73
Secção de Roteamento.....	74
Roteamento >> Roteamento estático	74
Roteamento >> RIP	76
Roteamento >> Tabela de Roteamento	78

Secção Firewall	81
Firewall >> Controlo de Acesso	82
Firewall >> Filtro MAC	84
Firewall >> Bloqueio de URL	86
Firewall >> Regra Programada	87
Firewall >> Detecção de Intrusão	89
Firewall >> DMZ	93
Secção UPnP	95
Secção QoS	97
QoS >> Mapeamento de Tráfego	99
QoS >> Estatísticas de Tráfego	100
Secção ADSL	102
ADSL >> Parâmetros	102
ADSL >> Estado	103
Secção DDNS	106
Secção Ferramentas	108
Ferramentas >> Ferramentas de Configuração	108
Ferramentas >> Actualização de Firmware	109
Ferramentas >> Reiniciar	110
Secção Estado	111
ANEXOS	
A) Informações de segurança	116
B) Endereçamento de IP	118
C) Especificações técnicas	120
D) Glossário	124

Bem-vindo

SOBRE ESTE MANUAL

Este manual descreve a instalação e a configuração do **P.DG A1000G**. Este manual foi concebido para ser utilizado pelos responsáveis pela instalação e configuração do equipamento de rede; por conseguinte, pressupõe-se um conhecimento básico de redes LAN (Redes Locais) e Routers de Internet.

DENOMINAÇÃO

Ao longo deste manual, o **P.DG A1000G** será referido como “Router Wireless”. Os cabos Ethernet de categoria 5 serão referidos como Cabos Ethernet ao longo deste manual.

CONVENÇÕES

A Tabela 1. e a Tabela 2. enumeram as convenções utilizadas ao longo deste manual.

TABELA 1. Símbolos de Aviso

Símbolo	Tipo de Aviso	Descrição
	Nota informativa	Informação que descreve características ou instruções importantes.
	Cuidado	Informação que o alerta para a potencial perda de dados ou potencial dano numa aplicação, sistema ou dispositivo.
	Aviso	Informação que o alerta para potenciais danos corporais.

TABELA 2. Léxico

Convenção	Descrição
As palavras “introduzir” e “digitar”	Neste manual, quando for utilizada a palavra “introduzir” deve inserir algo e, em seguida, premir a tecla Return [voltar] ou Enter. Não prima a tecla Return ou Enter quando a instrução for apenas “digitar”.
Nomes das teclas do teclado	Se for necessário premir simultaneamente duas ou mais teclas, o nomes das teclas aparecerão ligados pelo sinal mais (+). Exemplo: Prima Ctrl+Alt+Del
Palavras em itálico	Os itálicos são utilizados para: • Enfatizar uma afirmação. • Identificar uma voz no menu.
Palavras a negrito	O negrito é utilizado para: • Identificar um botão do menu de comandos (ex.: Prima o botão OK).
Palavras a negrito+itálico	A combinação é utilizada para: • Identificar um caminho que leva a um menu de comandos (Ex.: <i>Statistics->LAN</i> [Estatísticas->LAN]). • Identificar um menu de comandos (ex.: menu <i>Summary</i> [Resumo])

Introdução

INTRODUÇÃO

O **P.DG A1000G** foi criado para fornecer um meio eficaz em termos de custos para a partilha de uma única ligação de Internet de banda larga entre vários computadores com e sem fios. O Router também proporciona protecção sob a forma de uma “firewall”, impedindo que pessoas exteriores à sua rede acessem aos seus ficheiros ou danifiquem os seus computadores.

O **P.DG A1000G** é um router ADSL2+, ideal para ambientes domésticos e clientes SOHO, que oferece serviços de encaminhamento de banda larga a partir de um ponto de acesso único e modular.

O **P.DG A1000G** é a solução ideal para:

1. Ligar vários computadores e consolas de videojogos;
2. Partilhar ligações de Internet de banda larga com todos os computadores domésticos;
3. Partilhar impressoras e periféricos;

CONTEÚDOS DA EMBALAGEM

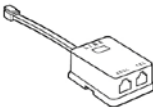
O seu novo kit de router ADSL2+ **P.DG A1000G** contém o respectivo hardware e software. Irá encontrar:

1. Uma unidade **P.DG A1000G**
2. Um adaptador de Comutação da Fonte de Alimentação
3. Um cabo telefónico com ficha RJ-11
4. Um cabo Ethernet de categoria 5 com ficha RJ-45
5. Um microfiltro duplo

6. Um CD-ROM com:
 - a. Manual do Utilizador
 - b. Condições Contratuais de Voz
 - c. Condições Contratuais
 - d. Tarifário Detalhado

7. Guia de Instalação

TABELA 1 Material do Kit

	Quantida de	DESCRIÇÃO
	1	P.DG A1000G
	1	Adaptador de Comutação da Fonte de Alimentação
	1	Microfiltro duplo
	1	Cabo Ethernet
	1	Cabo telefónico
	1	CD-ROM
	1	Guia de instalação

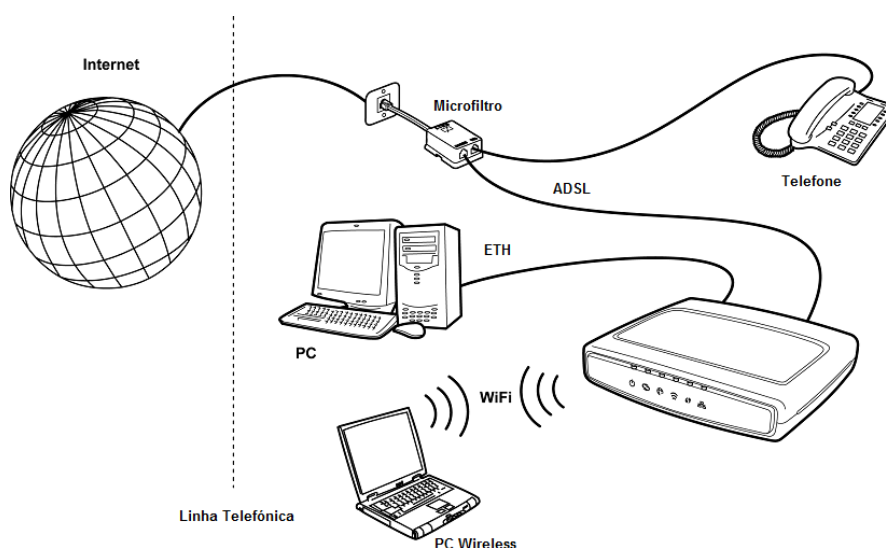
Se algum dos itens incluídos na embalagem estiver danificado, contacte o seu Fornecedor de Serviços.

O Kit funciona com uma ligação de Linha de Subscrição Digital Assimétrica (ADSL2/2+) de alta velocidade à linha telefónica no lado WAN, assim como várias tecnologias de ligação local no lado LAN:

- Uma porta Ethernet 10/100 Base-TX comutada
- Uma ligação Wi-Fi para dispositivos anfitriões

A figura 1 apresenta um exemplo de rede: o seu Router passa a ser a sua ligação à Internet. As ligações podem ser efectuadas directamente ao Router, aumentando o número de computadores que pode ter ligados à sua rede.

FIGURA 1. Exemplo de Rede Doméstica



VANTAGENS DO ROUTER

As vantagens do **P.DG A1000G** incluem:

- Ligação à Internet partilhada para computadores com e sem fios
- Rede sem fios 802.11b/g de alta velocidade
- Funcionamento de plataforma cruzada para ser compatível com computadores Microsoft® Windows, Linux e Apple® MAC
- Fácil utilização, ligação e configuração baseadas na Web
- Centralização de todas as definições do endereço de rede (DHCP)
- Um servidor Virtual para permitir o acesso remoto à Internet, FTP e outros serviços da sua rede
- Uma segurança - protecção por Firewall - contra ataques de piratas informáticos e encriptação para proteger o tráfego da rede sem fios

- GUI (Interface Gráfica do Utilizador) em várias línguas.

APLICAÇÕES

O **P.DG A1000G** inclui várias características de rede vantajosas:

- **LAN com e sem fios:** o router permite a ligação a dispositivos 10/100 Mbps, e a dispositivos IEEE 802.11b/g sem fios compatíveis, facilitando a criação de uma rede doméstica ou em escritórios pequenos.
- **Acesso à Internet:** este dispositivo suporta o acesso à Internet através de uma ligação ADSL. Sendo que muitos fornecedores de DSL utilizam PPPoE ou PPPoA para estabelecer comunicações com os utilizadores finais, o Router inclui clientes incorporados para estes protocolos, eliminando a necessidade de instalação desses serviços no seu computador.

DESCRIÇÃO DO HARDWARE

O Router contém um modem ADSL incorporado e liga-se à Internet ou a um local remoto através da porta ADSL (RJ11). Pode ser ligado directamente através dos seus computadores ou a uma rede local utilizando quatro portas LAN de Ethernet rápida.

A velocidade de acesso à Internet depende do seu tipo de serviço. A velocidade ADSL máxima proporciona uma velocidade de recepção de até 8 Mbps e uma velocidade de transmissão de até 1 Mbps. A ADSL G.lite (ou splitterless) proporciona uma velocidade de recepção de até 1.5 Mbps e uma velocidade de transmissão de até 512 kbps. Contudo, deve ter em consideração que a velocidade real proporcionada pelos respectivos fornecedores de serviços pode divergir drasticamente destes limites máximos.

A transmissão de dados entre dispositivos ligados à sua rede local pode ocorrer a velocidades de até 100 Mbps através das portas de Ethernet rápida e até 54 Mbps através do ponto de acesso sem fios incorporado.

REQUISITOS MÍNIMOS DE SISTEMA E COMPONENTES

O seu Router requer que o(s) computador(es) e componentes na sua rede possuam, pelo menos, as seguintes configurações:

- Um computador com Sistema Operativo que suporte protocolos de rede TCP/IP: Microsoft® Windows 98SE, Windows ME, Windows 2000, Windows XP 32bit, Windows Vista 32bit, Windows 7 ou Apple® MAC 10.x ou Linux
- Conta de acesso à Internet a partir do seu Fornecedor de Serviços de Internet (ISP)
- Um computador que utilize um endereço IP dinâmico atribuído por DHCP, assim como um endereço de servidor gateway e de servidor DNS do seu fornecedor de serviços.
- Um computador equipado com um adaptador de Ethernet rápida de 10/100 Mbps
- Protocolos de rede TCP/IP instalados em todos os computadores que irão aceder à Internet

P.DG A1000G

- Um browser compatível com Java, tal como o Microsoft Internet Explorer 6.0 ou posterior e o Mozilla Firefox 2.0 ou posterior e o Safari, instalado num dos computadores locais para configurar o Router

PAINEL FRONTAL

O painel frontal do Router contém seis luzes indicadoras (LED) que ajudam a descrever o estado das operações de rede e de ligação.

FIGURA 2. Os LED do Painei Frontal

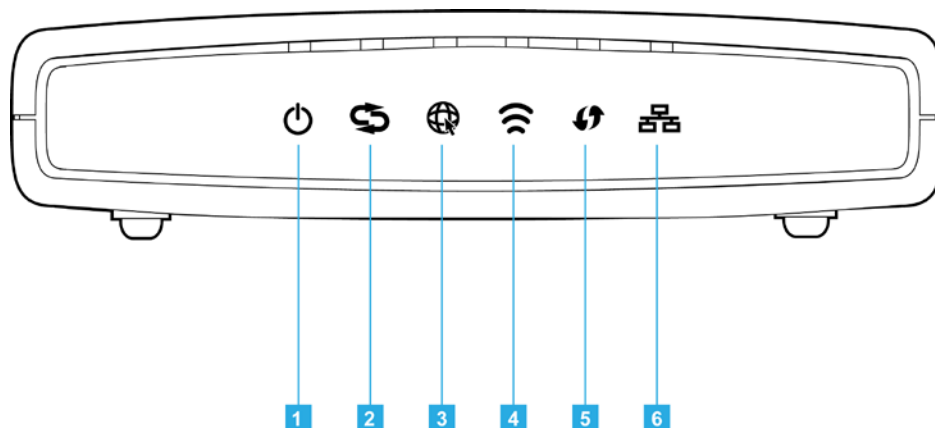


TABELA 2. Descrição do LED

Ref.	LED	Cor do LED	Descrição do LED	
1	Ligar/Desligar	Verde	Ligado	Alimentação ligada
			Desligado	Alimentação desligada ou falha de energia
2	ADSL	Verde	Ligado	A ligação ADSL está a funcionar correctamente
			Intermitente	Inicialização
			Desligado	Sem ligação ADSL
3	Internet	Verde	Intermitente	A porta ADSL está a enviar ou a receber dados
			Desligado	Não estão a ser transferidos dados
4	LAN sem fios	Verde	Intermitente	A ligação sem fios está activa
			Desligado	Sem ligação
5	WPS	Verde	Ligado	Ligação WPS efectuada com sucesso
			Intermitente	O Router está a estabelecer a ligação WPS
			Desligado	Sem ligação WPS
6	LAN	Verde	Ligado	Ligação Ethernet
			Intermitente	A porta LAN está a enviar ou a receber dados
			Desligado	Sem ligação



O botão WPS está localizado na parte superior. Prima este botão durante, pelo menos, 5 segundos para activar a função WPS. Para activar ou desactivar a rede wireless prima o botão durante, pelo menos, 10 segundos.

PAINEL POSTERIOR

O painel posterior do Router contém um botão de reiniciar, uma tomada para o adaptador da alimentação, uma porta LAN e uma porta ADSL.



Não force a antena para além dos seus pontos de paragem mecânica. Rodar excessivamente a antena pode provocar danos.

FIGURA 3. Painel Posterior

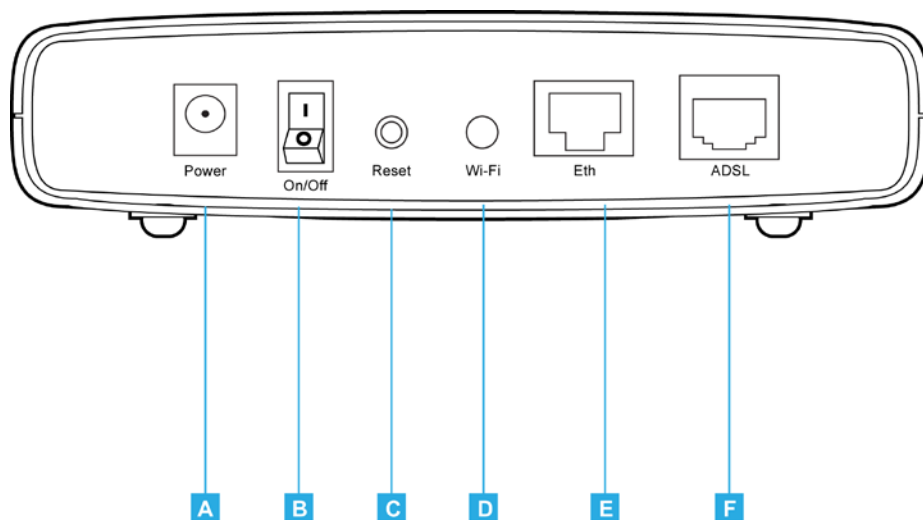


TABELA 3. Descrição dos Elementos do Painel

Ref.	DESCRIÇÃO
<i>a</i>	Entrada da Alimentação
<i>b</i>	Interruptor On/Off [Ligar/Desligar]
<i>c</i>	Botão Reset [Reiniciar]
<i>d</i>	Botão WPS [Activa WPS ou Liga/Desliga a rede Wireless]
<i>e</i>	Porta Ethernet
<i>f</i>	Porta ADSL

Instalação do Hardware

Este capítulo irá guiá-lo através da instalação básica do Router, incluindo:

1. Posicionamento do **P.DG A1000G**
2. Instalação dos Microfiltros
3. Ligação do Router à sua rede
4. Configuração do seu computador para trabalhar em rede com o Router



Leia atentamente a Informação de Segurança no Anexo “A”

DEFINIÇÕES ISP

Reúna as seguintes informações do seu ISP antes de começar a configurar o Router:

- Número de telefone fixo do ISP
- Endereço IP do Servidor Gateway e do Servidor DNS (Nome do Domínio) do seu ISP
- Uma conta ISP que inclua o nome de utilizador e password do ISP
- Endereço de IP e máscara de sub-rede (apenas para utilizadores de IP fixo)

POSICIONAMENTO DO ROUTER

O Router pode ser colocado em qualquer local conveniente no seu escritório ou casa. Não são necessários quaisquer requisitos de ligações eléctricas ou de arrefecimento especiais. No entanto, deve cumprir as seguintes orientações:

- Manter o Router afastado de quaisquer dispositivos de aquecimento
- Não colocar o Router num ambiente com sujidade ou humidade

Deve também lembrar-se de desligar a alimentação, remover o cabo de alimentação da tomada e manter as mãos secas ao instalar o Router.

INSTALAÇÃO DOS MICROFILTROS

Antes de começar a instalação deve localizar os dispositivos domésticos que necessitam de um microfiltro, tais como telefones, faxes, atendedores de chamadas, modems de acesso telefónico, dialers de televisão por satélite ou sistemas de segurança monitorizada, e coloque um microfiltro em todos os que partilharem a mesma linha telefónica do seu modem DSL.

Para instalar os microfiltros efectue os seguintes passos:

1. Desligue o cabo telefónico da tomada telefónica da parede
2. Insira o cabo telefónico na porta do microfiltro identificada com o símbolo do telefone
3. Insira o cabo do microfiltro na tomada telefónica da parede



Não é necessário colocar um microfiltro nas tomadas telefónicas que não são utilizadas.

FIGURA 1. Instalação do Microfiltro



ALIMENTAÇÃO DO ROUTER

Para ligar a alimentação do Router:

1. Ligue a ficha do adaptador de alimentação na porta do adaptador de alimentação situada na parte posterior do Router
2. Ligue a ficha do adaptador de alimentação numa tomada eléctrica normal
3. Prima o botão de Ligar/Desligar situado no painel posterior do Router
4. Aguarde que o LED de alimentação fique verde e estável

Em caso de falha de energia, o Router irá reiniciar-se e começar a funcionar automaticamente assim que a energia for restituída.

Se o router estiver devidamente configurado levará cerca de 30 segundos a estabelecer ligação com o fornecedor de serviços ADSL após ser ligado.

Durante esse tempo, o indicador de ADSL Sync ficará intermitente. Após a ligação ADSL ter sido estabelecida, o indicador ADSL Sync ficará ligado.

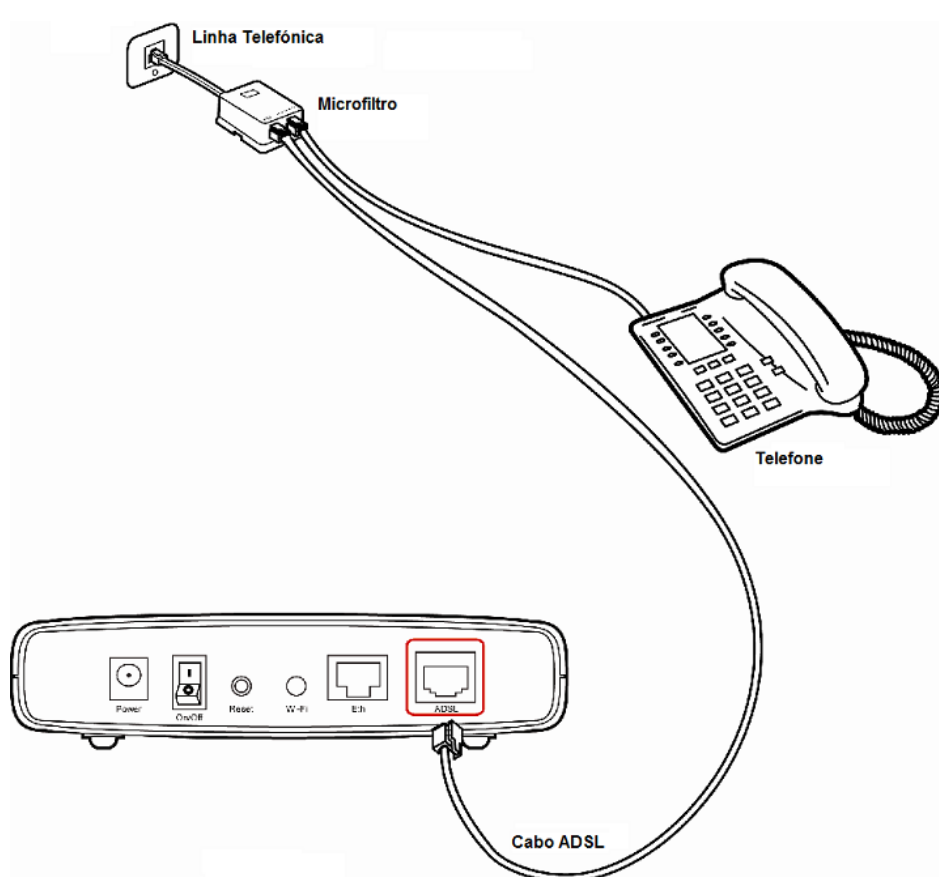
LIGAÇÃO DO ROUTER

O primeiro passo para instalar o router consiste em ligá-lo fisicamente à tomada telefónica e, em seguida, a um computador com ligação Ethernet.

Para ligar o cabo telefónico:

1. Ligue uma das extremidades do cabo telefónico na porta do microfiltro identificada com o símbolo do computador
2. Ligue a outra extremidade do cabo telefónico na porta DSL situada na parte posterior do Router

FIGURA 2. Ligação do Cabo Telefónico



Para ligar o cabo Ethernet:

1. Ligue uma extremidade do cabo Ethernet numa das quatro portas de Ethernet situadas na parte posterior do Router
2. Ligue a outra extremidade do cabo Ethernet na placa de rede Ethernet do seu computador
3. Verifique se a placa de rede Ethernet se encontra configurada como cliente DHCP, caso contrário, configure-a para permanecer na mesma rede local que a interface do router (consulte o capítulo "Configurar o seu Computador")

A porta LAN no router "negocia" automaticamente a velocidade de ligação e o modo duplex com ligação ao dispositivo.

Utilize cabos de par entrançado para ligar o Router a um adaptador Ethernet no seu computador. Ligue qualquer uma das portas LAN do Router em cascata a um hub ou switch Ethernet. Ao inserir a ficha RJ-45, certifique-se de que a mesma fez um "clique", indicando assim que se encontra na posição correcta.

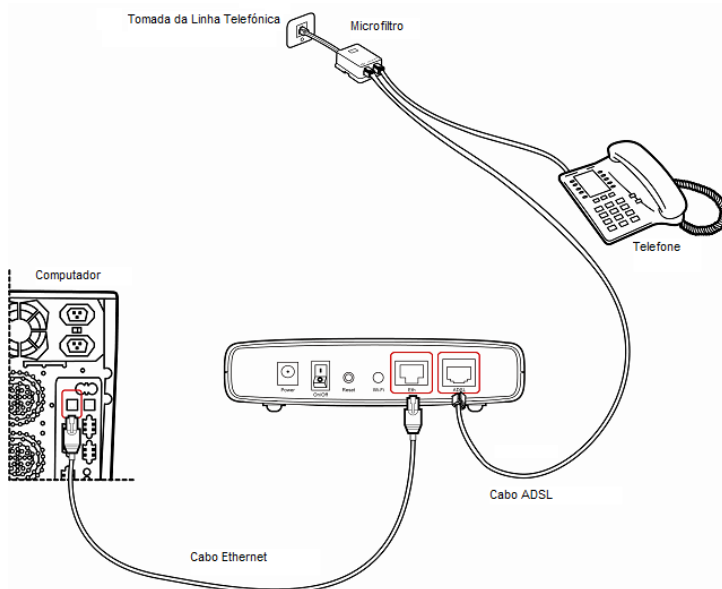


Não ligue uma ficha jack do telefone à tomada RJ-45. Essa acção poderá danificar o Router. Utilize apenas cabos de par entrançado com conectores RJ-45 que cumpram as normas FCC.



Utilize um cabo de par entrançado blindado ou não blindado de 100-ohm com conectores RJ-45 para todas as portas Ethernet. Recomendamos a utilização de cabos de categoria 5 para efectuar ligações ao dispositivo. Certifique-se também de que o comprimento de cada cabo de par entrançado não excede os 100 metros (328 pés).

FIGURA 3. Ligação do Cabo Ethernet



O Router tem a capacidade de alocar dinamicamente os endereços de rede aos computadores da sua rede utilizando DHCP. Contudo, para que isto aconteça, os seus computadores devem estar correctamente configurados. Para alterar a configuração dos seus computadores de forma a permitir a alocação de endereços de rede, siga as instruções deste capítulo.

LIGAÇÃO ETHERNET

Tem de verificar se existe uma pilha de protocolos TCP/IP e, em seguida, dependendo do seu sistema operativo, estabelecer uma ligação Ethernet ao Router. Esta ligação requer a activação da recepção automática do endereço IP do Router, no seu computador: nesse caso, o Router funciona como servidor DHCP na sua rede local.

CONFIGURAÇÃO TCP/IP

Para aceder à Internet através do Router deve configurar as definições de rede dos computadores na sua LAN para que utilizem a mesma sub-rede de IP que o Router. As definições de IP predefinidas do Router são:

ENDEREÇO IP: 192.168.1.1

MÁSCARA DE SUB-REDE: 255.255.255.0

Estas definições podem ser alteradas para se adequarem aos requisitos da sua rede, porém, em primeiro lugar, terá de configurar, pelo menos, um computador para aceder à interface web de configuração do router para poder efectuar as alterações necessárias.

LIGAÇÃO ETHERNET >> INSTALAÇÃO DO PROTOCOLO TCP/IP

Este procedimento requer a instalação do protocolo TCP/IP no seu computador. Consulte os capítulos seguintes e os manuais dos seus sistemas operativos Microsoft® Windows ou Apple® MacOS 10.x.

Microsoft® Windows 98SE, ME, 2000

1. Coloque o CD-ROM de instalação do Windows na unidade de CD-ROM
2. Começando em **Start -> Settings -> Control Panel -> Network Control Panel** [Iniciar -> Definições -> Painel de Controlo -> Painel de Controlo de Rede], faça um duplo clique no ícone **Network** [Rede]
3. Seleccione **Configuration -> TCP/IP** [Configuração -> TCP/IP] e clique no botão **Add** [adicionar]
4. Seleccione os Protocolos, clique no botão **Add** e escolha *Microsoft TCP/IP*. Em seguida, clique no botão **OK**
5. Após o computador ter reiniciado, está pronto para configurar as definições de TCP/IP Configure o adaptador de Rede para obter automaticamente um endereço de IP.

Microsoft® Windows XP

1. Coloque o CD-ROM de instalação do Windows na unidade de CD-ROM
2. Começando em **Start -> Settings -> Control Panel** [Iniciar -> Definições -> Painel de Controlo] faça duplo clique no ícone **Network** [Rede].
3. Seleccione **Protocol** [Protocolo] e clique no botão **Add**. Seleccione *Microsoft* e *TCP/IP* e, em seguida, clique no botão **OK**.
4. Configure o adaptador de Rede para obter automaticamente um endereço de IP.

Microsoft® Windows Vista

5. Começando em Start -> Settings -> Control Panel [Iniciar -> Definições -> Painel de Controlo] faça duplo clique no ícone *Network and Sharing Center* -> *Manage Network Connections* [Centro de Rede e Partilha -> Gerir Ligações de Rede]
6. Seleccione *Protocol* e clique no botão *Add* . Seleccione *Microsoft* e *TCP/IP* e, em seguida, clique no botão *OK*.
7. Configure o adaptador de Rede para obter automaticamente um endereço de IP.

Microsoft Windows 7

O IPv4 já deverá vir pré-instalado com o seu Windows 7. Se necessitar de reinstalar o IPv4, execute uma Linha de Comandos como administrador, escreva “netsh interface ipv4 install” e prima Enter.

Apple® MacOS 10.x

O TCP/IP encontra-se instalado num sistema MacOS como parte do Open Transport.

**LIGAÇÃO ETHERNET >>
CONFIGURAÇÃO DO
TCP/IP****Microsoft® Windows 98SE, ME, 2000**

Para configurar o TCP/IP nestes Sistemas Operativos, efectue os seguintes passos:

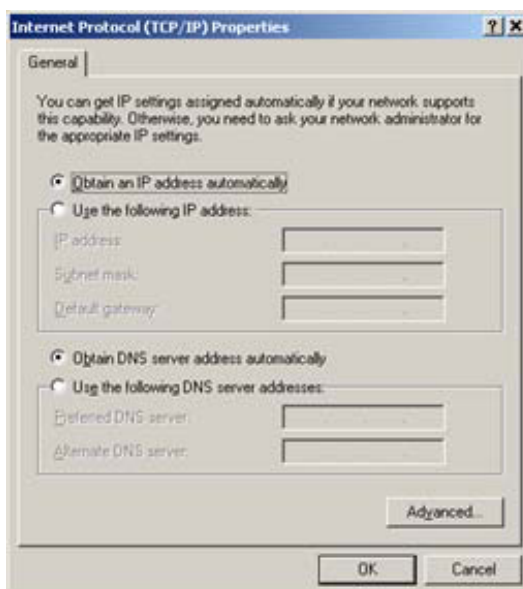
1. Seleccione **Start -> Settings -> Control Panel** [Iniciar -> Definições -> Painel de Controlo] e faça duplo clique no ícone **Network** .
2. Seleccione **Configuration ->TCP/IP** [Configuração -> TCP/IP] e, em seguida, clique no botão **Properties** [Propriedades].

FIGURA 4. Local Area Connection Properties [Propriedades da Ligação de Área Local]



3. Selecione o separador *IP Address* [Endereço de IP] e, em seguida, assinale-o para obter automaticamente um endereço IP. Clique no botão **OK**.

FIGURA 5. Internet Protocol (TCP/IP) Properties [Propriedades do Protocolo de Internet (TCP/IP)]



4. Será necessário reiniciar o sistema para implementar as alterações.
5. Introduza <http://192.168.1.1/> na barra de endereço do seu browser para abrir a Página Inicial do **P.DG A1000G**.

Microsoft® Windows XP

Para configurar o TCP/IP no Sistema Operativo MS Windows XP, efectue os seguintes passos:

1. No ambiente de trabalho do Windows, clique em **Start -> Settings -> Control Panel** [Iniciar -> Definições -> Painel de Controlo] e faça duplo clique no ícone **Network and Dial-Up connections** [Rede e ligações telefónicas].
2. Seleccione **Protocols -> TCP/IP** [Protocolos -> TCP/IP] e, em seguida, clique no botão **Properties** [Propriedades].

FIGURA 6. Local Area Connection Properties [Propriedades da Ligação de Área Local]



3. Se as opções *"Obtain an IP address automatically"* ["Obter automaticamente um endereço IP"] e *"Obtain DNS server address automatically"* ["Obter automaticamente endereço de servidor de DNS"] já estiverem seleccionadas, o seu computador já se encontra configurado para DHCP. Caso contrário, seleccione estas opções.

FIGURA 7. Internet Protocol (TCP/IP) Properties [Propriedades do Protocolo de Internet (TCP/IP)]

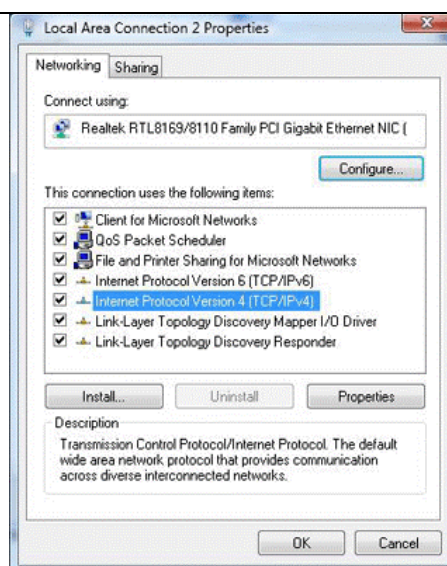


Microsoft® Windows Vista

Para configurar o TCP/IP no Sistema Operativo MS Windows Vista, efectue os seguintes passos:

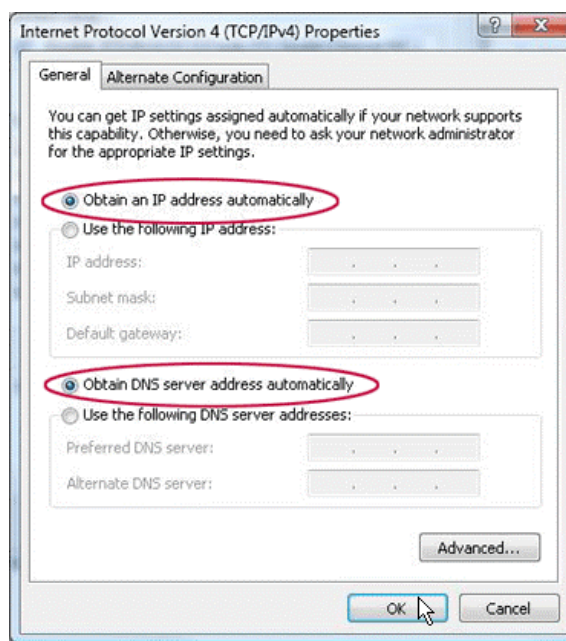
4. Começando em Start -> Settings -> Control Panel -> [Iniciar -> Definições -> Painel de Controlo ->] faça duplo clique no ícone Network and Sharing Center [Centro de Rede e Partilha]
5. Seleccione *Manage Network Connections* [Gerir Ligações de Rede] -> *click in connection -> properties* [ligação -> propriedades]

FIGURA 8. Local Area Connection Properties [Propriedades da Ligação de Área Local] – Windows Vista



6. Seleccione *IPv4* e, em seguida, assinale-o para obter automaticamente um endereço IP. Clique no botão **OK**.

FIGURA 9. Internet Protocol (TCP/IP) Properties [Propriedades do Protocolo de Internet (TCP/IP)]



Microsoft® Windows 7

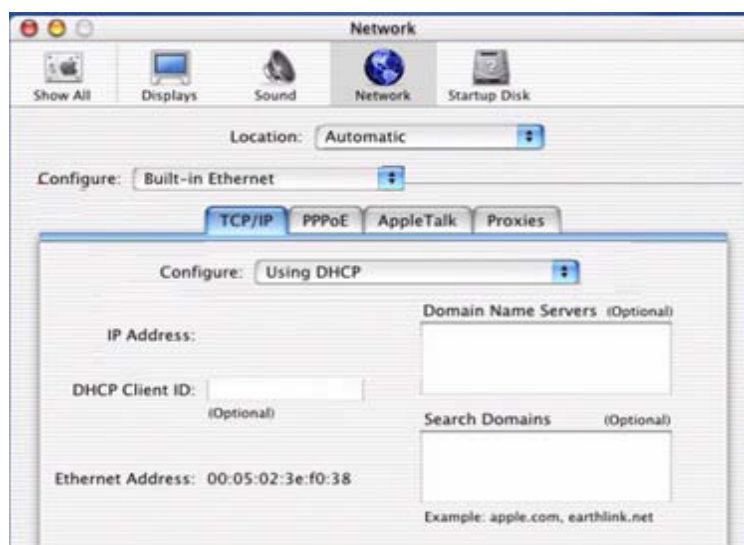
Ir ao menu do Windows e escolher “Ajuda e Suporte”. Pesquisar por “Alterar definições de TCP/IP” e seguir as instruções apresentadas.

Apple® MacOS 10.x

Para configurar o TCP/IP no MAS OS 10.x, efectue os seguintes passos:

1. Abra o **Apple Menu > System Preferences** [Menu Apple > Preferências do Sistema] e seleccione **Network** [Rede].
2. No menu suspenso **Show** [exibir], seleccione **Built-in Ethernet** [Ethernet integrada], conforme o tipo de ligação utilizada.
3. Seleccione o separador **TCP/IP**.
4. Seleccione **DHCP** no menu instantâneo **Configure** [Configurar] para obter um endereço de IP dinâmico.

FIGURA 10. Painel de rede no MAC OS 10.x



5. Clique no botão **Apply Now** [Aplicar Agora].
6. Clique no botão **Register** [Registar] para guardar as alterações efectuadas no Painel de Controlo.
7. Introduza <http://192.168.1.1/> na barra de endereço do seu browser para abrir a Página de Início de Sessão do **P.RG A1000G**.

DESACTIVAR O PROXY HTTP

É necessário verificar se a característica “proxy *HTTP*” do seu browser de Internet se encontra desactivada. Isto é importante para que o seu browser possa apresentar as páginas de configuração HTML do Router.

OBTER AS CONFIGURAÇÕES IP DO ROUTER

Microsoft® Windows 98SE, ME, 2000

Agora que já configurou a ligação do seu computador ao Router, é necessário obter novas definições de rede. Ao substituir as definições de IP DHCP antigas pelas definições do seu Router, pode verificar se configurou o seu computador correctamente.

1. No ambiente de trabalho do Windows, seleccione o item de menu **Start > Programs > Accessories > Command Prompt** [Iniciar > Programas > Acessórios > Linha de comandos]
2. Na janela da Linha de Comandos, digite "*ipconfig/release*" e clique na tecla ENTER

FIGURA 11. Command Prompt (IPCONFIG command) [Linha de Comandos (comando IPCONFIG)]

```

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig/release
Configurazione IP di Windows

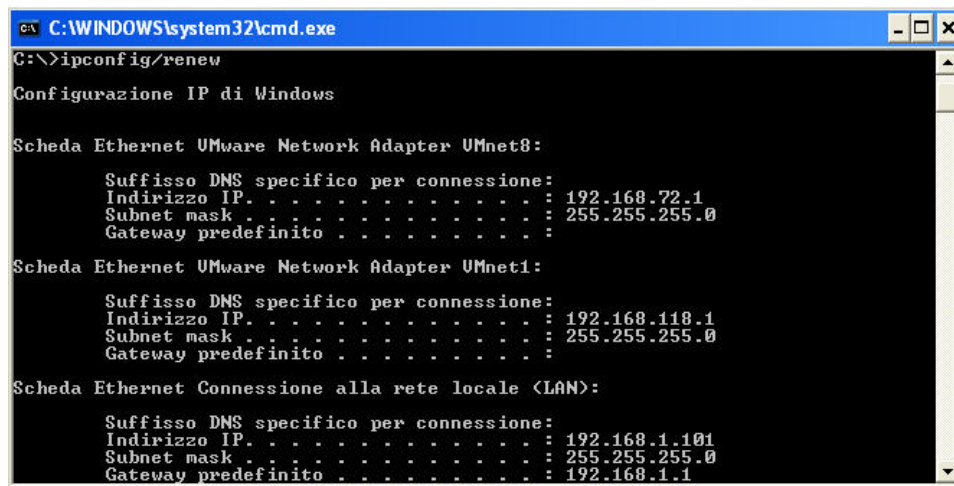
Scheda Ethernet VMware Network Adapter VMnet8:
    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.72.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda Ethernet VMware Network Adapter VMnet1:
    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.118.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda Ethernet Connessione alla rete locale (LAN):
    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 0.0.0.0
    Subnet mask . . . . . : 0.0.0.0
  
```

3. Digite "*ipconfig/renew*" e clique na tecla ENTER. Verifique se o seu Endereço de IP é agora 192.168.1.xxx, a sua Máscara de Sub-rede é 255.255.255.0 e seu Gateway Predefinido é 192.168.1.1. Estes valores confirmam que o seu Router ADSL está a funcionar.

FIGURA 12. Command Prompt (IPCONFIG command) [Linha de Comandos (comando IPCONFIG)]



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig/renew

Configuração IP de Windows

Scheda Ethernet VMware Network Adapter VMnet8:
    Sufisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.72.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda Ethernet VMware Network Adapter VMnet1:
    Sufisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.118.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda Ethernet Connessione alla rete locale (LAN):
    Sufisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.1.101
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1
```

4. Feche a janela da Linha de Comandos

Microsoft® Windows XP, Vista e 7

Agora que já configurou a ligação do seu computador ao Router, é necessário obter novas definições de rede. Ao substituir as definições de IP DHCP antigas pelas definições do seu Router, pode verificar se configurou o seu computador correctamente.

1. No ambiente de trabalho do Windows, clique no item de menu **Start > Programas > Accessories > Command Prompt** [Iniciar > Programas > Acessórios > Linha de Comandos]
2. Na janela da Linha de Comandos, digite "*ipconfig/release*" e clique na tecla ENTER
3. Digite "*ipconfig/renew*" e clique na tecla ENTER. Verifique se o seu Endereço de IP é agora 192.168.1.xxx, a sua Máscara de Sub-rede é 255.255.255.0 e seu Gateway Predefinido é 192.168.1.1. Estes valores confirmam que o seu Router ADSL está a funcionar.
4. Feche a janela da Linha de Comandos

CONFIGURAÇÕES IPV6

Para as configurações em IPV6, deve seguir o seguinte procedimento:
 Seleccionar Iniciar [Start] e depois Ajuda [Help and Support].
 Pesquisar na Ajuda [Help and Support] por “Alterar definições de TCP/IP [Change TCP/IP settings]”.
 Escolher a opção “Alterar definições de TCP/IP [Change TCP/IP settings]” e seguir os passos aí definidos.

LIGAÇÃO WI-FI



É necessário um computador com um adaptador sem fios 802.11b/g (com certificação Wi-Fi) instalado.

1. Instale o seu adaptador sem fios seguindo as instruções do fabricante e verifique se o seu computador se encontra definido para obter automaticamente um endereço de IP (modo DHCP).



*Será necessário configurar correctamente o seu adaptador para que este estabeleça comunicação com o **P.RG A1000G** segundo as normas de configuração.*

2. Na janela de configuração do seu adaptador sem fios, verifique a rede sem fios (marcada com o nome SSID relevante) presente no seu ambiente físico.
3. Seleccione o SSID do **P.DG A1000G**
4. Complete a configuração do adaptador sem fios seguindo os mesmos parâmetros do **P.DG A1000G**

Para verificar a ligação, entre na Página de Início de Sessão do **P.RG A1000G** (consulte a Figura 13), introduzindo o endereço <http://192.168.1.1> ou <http://sapoadsl.setup>

P.DG A1000G

FIGURA 13. P.DG A1000GLogin Page [Página de Início de Sessão do P.DG A1000G]

ADB

Login Screen

Username:

Password:

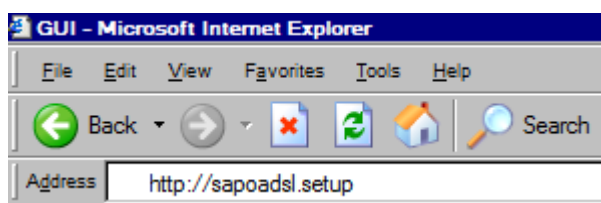
Please enter correct password for Administrator Access. Thank you.
We suggest that you use Internet Explorer 5.5 or above at a minimum of 1024x768 resolution.

Firmware version:

Configuração do Router

1. Aceda ao seu browser (aconselhamos o internet explorer 5.5 ou superior) e acesse ao endereço <http://192.168.1.1>. Poderá utilizar o alias <http://sapo.adsl.setup>

FIGURA 1. Endereço de acesso ao router



No caso de estar a efectuar o acesso sem Fios, encontrará a seguinte secção:

FIGURA 2. Tela de Login

A screenshot of a web-based login interface. At the top, the title 'Tela de Login' is displayed. Below the title, there are two input fields. The first is labeled 'Nome de usuário:' and contains the text 'admin'. The second is labeled 'Senha:' and contains five dots, indicating a masked password. Below these fields are two buttons: 'LOGIN' and 'CANCELAR'.

Insira admin no campo Nome de Utilizador e admin no campo Senha e clique em Login.

2. De seguida deverá encontrar a página de Configuração Rápida:

FIGURA 3. Painel de Configuração Rápida

3. Preencha os campos referentes à conta ADSL com a informação contida no envelope sigilo, inserindo o seu Username e Password respectivamente:

FIGURA 4. Secção da Conta SAPO ADSL

CONTA SAPO ADSL
Introduza o username e password que constam no seu envelope sigilo

Username [envelope sigilo] @

Password [envelope sigilo]

Ligação à Internet : ☒ Desligado

Clique em Ligar, o estado da ligação à internet passará a Ligado com o respectivo indicador a verde.

Caso o estado da ligação à Internet já se encontre ligado, após a inserção dos dados contidos no envelope sigilo, clique em Guardar.

Após estas instruções, caso o seu acesso já se encontre activo será redireccionado para a página <http://www.sapo.pt>.

4. Configuração da Rede sem Fios:

FIGURA 5. Secção de configuração da Rede sem Fios

REDE SEM FIOS
Altere ou mantenha as configurações actuais. Para estabelecer uma ligação sem fios com o seu PC, consulte o Guia de Instalação Rápida

Nome da rede sem fios

Nível de Segurança ☒ Alta (WPA) ☐ Média (WEP) ☐ Nenhuma

Chave

Rede sem fios : ☒ Activada

Na secção Rede sem Fios, introduza o nome pretendido para a sua rede sem fios e insira a palavra-chave de acesso à rede no campo Chave e clique em Guardar. É recomendada a utilização do nível de segurança mais alto (WPA).

Clique em activar, a rede passará a activa e passará a ser anunciada, conforme a figura seguinte:

FIGURA 6. Introdução de password da Rede sem Fios

Após estas instruções basta procurar a rede sem fios no seu computador e ligar-se a esta.

NOTA: A p palavra-chave WPA deve conter entre 8 a 63 caracteres, enquanto a password WEP deve conter exactamente 13.

5. Configurações Avançadas:

FIGURA 7. Configurações avançadas, Reiniciar e Reverter

Poderá seleccionar os botões:

“Ir para configuração avançada” – Para aceder ao menu de configurações avançadas (Apenas para utilizadores Experientes).

“Reiniciar” - Reiniciar o seu Router.

“Reverter” - Reverter para as definições originais do Router.

INTERFACE DE CONFIGURAÇÕES AVANÇADAS

INTERFACE DE GESTÃO

O Assistente de Configuração encontra-se no canto superior esquerdo. Utilize o Assistente de Configuração para uma configuração rápida e simples da sua ligação de Internet e das definições sem fios básicas.

EFFECTUAR ALTERAÇÕES DE CONFIGURAÇÃO

Os parâmetros configuráveis possuem uma caixa de diálogo ou um menu suspenso. Após ter sido efectuada uma alteração de configuração num ecrã, clique nos botões **APPLY > SAVE SETTINGS** [Aplicar > Guardar definições] ou **NEXT** [Seguinte] no ecrã para activar as novas definições.

PARÂMETROS DE CONFIGURAÇÃO AVANÇADOS

No lado esquerdo é apresentado o menu principal e no lado direito é exibida a informação descritiva do Estado (consulte a Figura 8). Os itens do menu principal estão descritos na Tabela 1 que apresenta a lista de itens do menu de comando para a Gestão do Router.

FIGURA 8. Menu das Configurações avançadas do Router

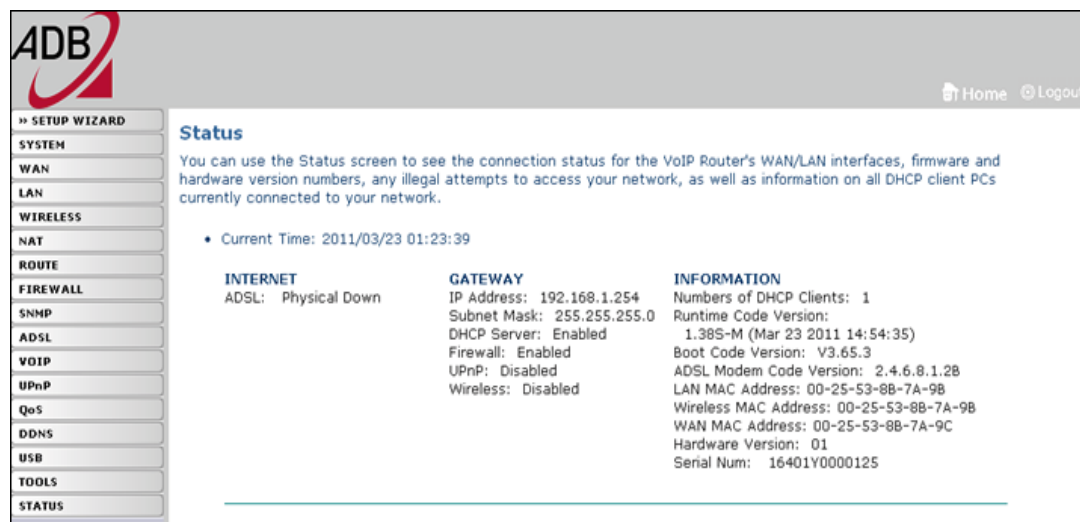


TABELA 1. Itens do menu de comando

PARÂMETRO	DESCRIÇÃO
QUICK SETUP [Configuração rápida]	Permite configurar rapidamente as configurações sem fios básicas e
SYSTEM [Sistema]	Define o fuso horário local, a password de acesso do administrador e o endereço de IP de um computador que poderá fazer a gestão remota do Router. Também permite definir a função DNS (consulte o capítulo 5)
WAN	Especifica as definições de ligação à Internet (consulte o capítulo 6)
LAN	Define a configuração de TCP/IP para os clientes DHCP da interface LAN do Router. Para além disso, configura a função UPnP (consulte o capítulo 7)
WIRELESS [Sem fios]	Configura a radiofrequência, o SSID e a segurança das comunicações Sem Fios (consulte o capítulo 8)
NAT	Configura o Mapeamento de Endereços, o servidor virtual e as aplicações especiais (consulte o capítulo 9)
ROUTING [Roteamento]	Define os parâmetros de roteamento e apresenta a tabela de roteamento actual (consulte o capítulo 10)
FIREWALL	Configura várias funções de segurança e funções especializadas, incluindo: Controlo de Acesso, Bloqueio de URL, programação do controlo de Acesso à Internet, detecção de intrusos e DMZ (consulte o capítulo 11)
UPnP	Permite activar/desactivar as definições Universal Plug and Play (consulte o capítulo 13)
QoS [Qualidade de serviço]	Configura as definições de Qualidade de Serviço (consulte o capítulo 14)
ADSL	Define o tipo de funcionamento ADSL e apresenta o estado ADSL (consulte o capítulo 15)
DDNS	Configura a função DNS Dinâmico (consulte o capítulo 16)
TOOLS [Ferramentas]	Contém opções para usar o ping na ligação de rede, identificar rotas, fazer cópias de segurança e restaurar a configuração actual, restaurar todas as definições de configuração para as predefinições de fábrica, actualizar o firmware do sistema ou reiniciar o sistema (consulte o capítulo 17)
STATUS [Estado]	Identifica o estado e tipo de ligação WAN, os números de versão de firmware e hardware, as definições de IP do sistema, assim como as informações de DHCP, NAT e firewall. Indica o número de clientes ligados, a versão de firmware, o endereço MAC físico para cada interface de multimédia, a versão de hardware e o número de série. Apresenta o registo de segurança e DHCP do cliente (consulte o capítulo 18)

TABELA 2. Outros Itens do menu de comando

PARÂMETRO	DESCRIÇÃO
HOME	<i>Volta à página inicial das configurações avançadas.</i>
LOGOUT	<i>Volta à página inicial de configuração.</i>

Secção do Sistema

Esta secção deve ser utilizada para configurar correctamente as definições básicas do Router, tais como o *fuso horário*, a *password*, a *gestão remota* e o *DNS*

SISTEMA >> DEFINIÇÕES DE HORA

Selecione o seu *fuso horário local* no menu suspenso (consulte a Figura 1). Esta informação é utilizada para entradas no registo e filtragem de clientes

FIGURA 1. Menu de comando TIME ZONE SETTINGS [Definições do fuso horário] da secção do SISTEMA

Time Settings

Set Time Zone:

Use this setting to insure the time-based client filtering feature and system log entries are based on the correct localized time.

(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Configure Time Server (NTP):

You can automatically maintain the system time on your ADSL router by synchronizing with a public time server over the Internet.

☒ Enable Automatic Time Server Maintenance

When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area:

Primary Server:	129.132.2.21 - Europe
Secondary Server:	130.149.17.8 - Europe
Tertiary Server:	132.163.4.102 - North America

Se pretender sincronizar automaticamente o Router ADSL com o fuso horário de um servidor público, assinale a caixa *Enable Automatic Server Maintenance* [Activar Manutenção Automática do Servidor]. Seleccione os servidores pretendidos nos menus suspensos.

SISTEMA >> DEFINIÇÕES DE PASSWORD

Utilize este ecrã para alterar a password de acesso à interface de gestão.

FIGURA 2. Comando PASSWORD SETTINGS [Definições de password] da secção do SISTEMA

Password Settings

Set a password to restrict management access to the router.

- Current Password :
- New Password:
- Re-Enter Password for Verification:

- Idle Time Out: Min
(Idle Time =0 : NO Time Out)

[HELP](#) [SAVE SETTINGS](#) [CANCEL](#)

A password pode conter entre 3-12 caracteres alfanuméricos e é sensível a maiúsculas e minúsculas.



Se perdeu a password, ou se não consegue aceder à interface de utilizador, prima o botão reiniciar no painel posterior, mantendo-o premido durante, pelo menos, cinco segundos para restaurar as predefinições de fábrica. A password predefinida é "admin".

Introduza um valor máximo para *Idle Time Out* [Tempo de Inactividade] (em minutos) para definir um período de tempo máximo durante o qual a sessão iniciada é mantida durante a inactividade. Se a ligação estiver inactiva durante um tempo superior ao tempo de inactividade máximo, a sessão será terminada e terá de iniciar novamente sessão para aceder à interface de gestão (Predefinição: 5 minutos).

SISTEMA >> DNS

Os **Servidores de Nome do Domínio (DNS)** são utilizados para mapear o nome do domínio (por exemplo, www.somecompany.com) com o endereço de IP (por exemplo, 64.147.25.20). O seu ISP deverá fornecer o endereço de IP de um ou mais Servidores de Nome de Domínio. Introduza esses endereços neste ecrã e clique no botão **SAVE SETTINGS** [Guardar definições] (consulte a Figura 3)

FIGURA 3. Comando definição de DNS da secção do SISTEMA

DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as , a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

Domain Name Server (DNS) Address	0	.	0	.	0	.	0
Secondary DNS Address (optional)	0	.	0	.	0	.	0

HELP SAVE SETTINGS CANCEL

Secção WAN

Esta secção permite especificar os parâmetros da ligação WAN e as definições ATM PVC disponibilizadas pelo seu Fornecedor de Serviços de Internet (ISP).

A Figura 1 apresenta diferentes tipos de ligações utilizadas pelo Router para se ligar à rede.

FIGURA 1. Ecrã principal WAN

WAN Settings

The router can be connected to your service provider in any of the following ways:

[ATM PVC](#)
[Clone MAC](#)

To configure ATM VC parameters
To configure WAN Interface MAC Address

O Router suporta os seguintes dois modos:

- **ATM PVC**
- **Clone de MAC**

WAN >> ATM PVC

Ao seleccionar o primeiro modo (**ATM PVC**), é necessário introduzir os parâmetros de ligação virtual (consulte a Figura 2).

FIGURA 2. Lista de ligações virtuais ATM configuradas

ATM PVC

ADSL router uses ATM as its layer 2 protocol. ATM PVC is a virtual connection which acts as a WAN interface. The Gateway supports up to 8 ATM PVCs.

Description	VPI/VCI	Encapsulation	Protocol
VC1	8/35	LLC	PPPoE
VC2	-/-	---	---
VC3	-/-	---	---
VC4	-/-	---	---
VC5	-/-	---	---
VC6	-/-	---	---
VC7	-/-	---	---
VC8	-/-	---	---

[HELP](#)

TABELA 1. Parâmetros de ligação virtual ATM

PARÂMETRO	DESCRIÇÃO
VC1-VC8	Clique no VC pretendido para definir os valores para a ligação. Na maioria das situações será fornecido um VC único. Para um VC único utilize VC1
VPI/VCI	Apresenta o Virtual Path Identifier [Identificador de Caminho Virtual] (VPI) e o Virtual Circuit Identifier [Identificador de Circuito Virtual] (VCI) configurados para o VC correspondente
Encapsulation [Encapsulamento]	Apresenta o Encapsulamento configurado para o VC correspondente - VC-MUX: O Point-to-Point Protocol [Protocolo Ponto a Ponto] sobre o ATM Virtual Circuit Multiplexer [Multiplexador de Circuito Virtual] (sem encapsulamento) apenas permite a execução de um protocolo em cada circuito virtual com menos sobrecarga. - LLC: O Point-to-Point Protocol [Protocolo Ponto a Ponto] sobre o ATM Logical Link Control [Controlo da Ligação Lógica] (LLC) permite a execução de vários protocolos num circuito virtual (utilizando uma sobrecarga ligeiramente superior)
Protocol [Protocolo]	Apresenta os protocolos configurados para o VC correspondente. Os protocolos configurados podem ser: 1483 Bridging [ligação], PPPoA, 1483 Routing [Roteamento], PPPoE, MAC Encapsulated Routing [Roteamento MAC Encapsulado].

WAN >> INTERFACE ATM 1483 BRIDGING

Quando for seleccionado *1483 Bridging* na interface ATM, terá de preencher uma lista de parâmetros (consulte a Figura 3). Consulte a Tabela 2 para obter mais informações sobre o significado e os valores do parâmetro. Quando todos os campos estiverem correctamente preenchidos, prima o botão **SAVE SETTINGS** [Guardar definições].

FIGURA 3. Definições da interface ATM (1483 Bridging) da secção WAN

ATM Interface

ATM1	
Protocol	1483 Bridging
VPI/VCI	8 / 35
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10

HELP SAVE SETTINGS CANCEL

TABELA 2. Lista de parâmetros da Interface ATM 1483 Bridging

PARÂMETRO	DESCRIÇÃO
Protocol [Protocolo]	<i>1483 Bridging</i>
VLAN	<i>Selecione a VLAN a utilizar</i>
VPI/VCI	<i>Introduza o Identificador de Caminho Virtual (VPI) e o Identificador de Circuito Virtual (VCI) fornecidos pelo seu ISP</i>
Encapsulation [Encapsulamento]	<i>Selecione o encapsulamento utilizado pelo seu ISP no menu suspenso</i>
QoS Class [Classe de Qualidade de Serviço]	<i>Classes QoS ATM incluindo CBR, UBR e VBR</i>

TABELA 2. Lista de parâmetros da Interface ATM 1483 Bridging

PARÂMETRO	DESCRIÇÃO
PCR/SCR/MBS	<i>Os Parâmetros QoS – PCR (Peak Cell Rate) [Taxa Máxima de Células], SCR (Sustainable Cell Rate) [Taxa Sustentável de Células] e MBS (Maximum Burst Size) [Tamanho Máximo da Rajada] são configuráveis.</i>

**WAN >> INTERFACE ATM
PPPoA**

Quando for seleccionado *PPPoA* na interface ATM, terá de preencher uma lista de parâmetros (consulte Figura 4). Consulte a Tabela 3 para obter mais informações sobre o significado e os valores do parâmetro. Quando todos os campos estiverem correctamente preenchidos, prima o botão **SAVE SETTINGS** [Guardar definições].

FIGURA 4. Definições da interface ATM (PPPoA) da secção WAN

ATM Interface

ATM1	
Protocol	PPPoA
VPI/VCI	8 / 35
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connection Type	Always Connected
Idle Time	20 (minutes)
Authentication Protocol	AUTO
Connection Retry Timer	3 (seconds)
Keepalive Timer	15 (seconds)
Username	
Password	
Confirm Password	
MTU	1492

[HELP](#)
[SAVE SETTINGS](#)
[CANCEL](#)

TABELA 3. Lista de parâmetros da Interface ATM PPPoA

PARÂMETRO	DESCRIÇÃO
Protocol [Protocolo]	PPPoA
VPI/VCI	Introduza o Identificador de Caminho Virtual (VPI) e o Identificador de Circuito Virtual (VCI) fornecidos pelo seu ISP
Encapsulation	Selecione o encapsulamento utilizado pelo seu ISP no menu suspen-

TABELA 3. Lista de parâmetros da Interface ATM PPPoA

PARÂMETRO	DESCRIÇÃO
[Encapsulamento]	so
QoS Class [Classe de Qualidade de Serviço]	Classes QoS ATM incluindo CBR, UBR e VBR
PCR/SCR/MBS	Os Parâmetros QoS – PCR (Peak Cell Rate) [Taxa Máxima de Células], SCR (Sustainable Cell Rate) [Taxa Sustentável de Células] e MBS (Maximum Burst Size) [Tamanho Máximo da Rajada] são configuráveis.
IP assigned by ISP [IP atribuído pelo ISP]	Selecione Yes [Sim] se tiver um endereço de IP dinâmico. Selecione No [Não] se tiver um endereço de IP estático.
IP address [Endereço de IP]	Introduza o endereço de IP fornecido pelo seu ISP. Para IP dinâmico deixe este campo em branco
Connection type [Tipo de ligação]	Define o modo de ligação para Always connected [Sempre ligado], Auto triggering by traffic [Ligação automática desencadeada pelo tráfego] ou Manual connection [Ligação manual]. Para serviços de taxa fixa utilize Always connected
Idle time [Tempo de inatividade]	Introduza o tempo máximo de inatividade para a ligação de Internet. Quando este tempo for excedido, a ligação será terminada. Esta definição só é aplicável quando o tipo de ligação for definido para Auto-triggering by traffic
Authentication protocol [Protocolo de autenticação]	Selecione o protocolo no menu suspenso
Connection retry timer [temporizador de nova tentativa de ligação]	Este temporizador controla o período de tempo entre duas ligações PPP que procuram estabelecer nova ligação. O Connection retry timer só funciona quando a ligação PPP se encontra no estado disconnected [desligada]
Keep alive timer [temporizador de tempo de actividade]	O PPP possui o seu próprio protocolo (LCP echo) para verificar periodicamente o estado da ligação PPP, o temporizador keep alive timer controla o período de tempo entre duas verificações. O Keep alive timer funciona quando a ligação PPP se encontra no estado connected [ligada]
Username [Nome de utilizador]	Introduza o nome de utilizador
Password	Introduza a password
Confirm Password [Confirmação da Password]	Confirme a password
MTU	Deixe a Maximum Transmission Unit [Unidade Máxima de Transmissão] (MTU) com o valor predefinido, a menos que o seu ISP lhe tenha

TABELA 3. Lista de parâmetros da Interface ATM PPPoA

PARÂMETRO	DESCRIÇÃO
-----------	-----------

dado instruções diferentes

WAN >> INTERFACE ATM
1483 ROUTING
[ROTEAMENTO]

Quando for seleccionado o 1483 Routing na interface ATM, terá de preencher uma lista de parâmetros (consulte a Figura 5). Consulte a Tabela 4 para obter mais informações sobre o significado e os valores do parâmetro. Quando todos os campos estiverem correctamente preenchidos, prima o botão **SAVE SETTINGS** [Guardar definições].

FIGURA 5. Definições da interface ATM (1483 Routing) da secção WAN

ATM Interface

ATM1	
Protocol	1483 Routing
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
VPI/VCI	8 / 35
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
DHCP Client	☐

TABELA 4. Lista de parâmetros da Interface ATM 1483 Routing

PARÂMETRO	DESCRIÇÃO
-----------	-----------

Protocol [Protocolo]	1483 routing [roteamento]
-----------------------------	---------------------------

IP address [Endereço de IP]	Introduza o endereço de IP fornecido pelo seu ISP
------------------------------------	---

TABELA 4. Lista de parâmetros da Interface ATM 1483 Routing

PARÂMETRO	DESCRIÇÃO
Subnet Mask [Máscara de Sub-rede]	<i>Introduza o endereço da máscara de sub-rede fornecido pelo seu ISP</i>
Default Gateway [Gateway Predefinido]	<i>Introduza o endereço gateway fornecido pelo seu ISP</i>
VPI/VCI	<i>Introduza o Identificador de Caminho Virtual (VPI) e o Identificador de Circuito Virtual (VCI) fornecidos pelo seu ISP</i>
Encapsulation [Encapsulamento]	<i>Selecione o encapsulamento utilizado pelo seu ISP no menu suspenso</i>
QoS Class [Classe de Qualidade de Serviço]	<i>Classes QoS ATM incluindo CBR, UBR e VBR</i>
PCR/SCR/MBS	<i>Os Parâmetros QoS – PCR (Peak Cell Rate) [Taxa Máxima de Células], SCR (Sustainable Cell Rate) [Taxa Sustentável de Células] e MBS (Maximum Burst Size) [Tamanho Máximo da Rajada] são configuráveis.</i>

WAN >> INTERFACE ATM PPPoE

Quando for seleccionado *PPPoE* na interface ATM, terá de preencher uma lista de parâmetros (consulte a Figura 6). Consulte a Tabela 5 para obter mais informações sobre o significado e os valores do parâmetro. Quando todos os campos estiverem correctamente preenchidos, prima o botão **SAVE SETTINGS** [Guardar definições].

FIGURA 6. Definições da interface ATM (PPPoE) da secção WAN

ATM Interface

ATM1	
Protocol	PPPoE
VPI/VCI	8 / 35
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connection Type	Always Connected
Idle Time	20 (minutes)
Authentication Protocol	AUTO
Connection Retry Timer	3 (seconds)
Keepalive Timer	15 (seconds)
Username	tele2
Password	•••••
Confirm Password	•••••
MTU	1492

[HELP](#)
[SAVE SETTINGS](#)
[CANCEL](#)

TABELA 5. Lista de parâmetros da Interface ATM PPPoE

PARÂMETRO	DESCRIÇÃO
Protocol [Protocolo]	PPPoE
VPI/VCI	Introduza o Identificador de Caminho Virtual (VPI) e o Identificador de Circuito Virtual (VCI) fornecidos pelo seu ISP
Encapsulation [Encapsulamento]	Selecione o encapsulamento utilizado pelo seu ISP no menu suspenso
QoS Class [Classe de Qualidade de Serviço]	Classes QoS ATM incluindo CBR, UBR e VBR

TABELA 5. Lista de parâmetros da Interface ATM PPPoE

PARÂMETRO	DESCRIÇÃO
PCR/SCR/MBS	Os Parâmetros QoS – PCR (Peak Cell Rate) [Taxa Máxima de Células], SCR (Sustainable Cell Rate) [Taxa Sustentável de células] e MBS (Maximum Burst Size) [Tamanho Máximo da Rajada] são configuráveis.
IP assigned by ISP [IP atribuído pelo ISP]	<i>Seleccione Yes [Sim] se tiver um endereço de IP dinâmico. Seleccione No [Não] se tiver um endereço de IP estático.</i>
IP address [Endereço de IP]	<i>Introduza o endereço de IP fornecido pelo seu ISP. Para IP dinâmico deixe este campo em branco</i>
Connection type [Tipo de ligação]	<i>Define o modo de ligação para Always connected [Sempre ligado], Auto triggering by traffic [Ligação automática desencadeada pelo tráfego] ou Manual connection [Ligação manual]. Para serviços de taxa fixa utilize Always connected</i>
Idle time [Tempo de inatividade]	<i>Introduza o tempo máximo de inatividade para a ligação de Internet. Quando este tempo for excedido, a ligação será terminada. Esta definição só é aplicável quando o tipo de ligação for definido para Auto-triggering by traffic</i>
Authentication protocol [Protocolo de autenticação]	<i>Seleccione o protocolo no menu suspenso</i>
Connection retry timer [temporizador de nova tentativa de ligação]	<i>Este temporizador controla o período de tempo entre duas ligações PPP que procuram estabelecer nova ligação. O Connection retry timer só funciona quando a ligação PPP se encontra no estado disconnected [desligada]</i>
Keep alive timer [temporizador de tempo de actividade]	<i>O PPP possui o seu próprio protocolo (LCP echo) para verificar periodicamente o estado da ligação PPP, o temporizador keep alive timer controla o período de tempo entre duas verificações. O Keep alive timer funciona quando a ligação PPP se encontra no estado connected [ligada]</i>
Username [Nome de utilizador]	<i>Introduza o nome de utilizador</i>
Password	<i>Introduza a password</i>
Confirm Password [Confirmação da Password]	<i>Confirme a password</i>
MTU	<i>Deixe a Maximum Transmission Unit [Unidade Máxima de Transmissão] (MTU) com o valor predefinido, a menos que o seu ISP lhe tenha dado instruções diferentes</i>

WAN >> INTERFACE ATM
MAC ENCAPSULATED
ROUTING [ROTEAMENTO
MAC ENCAPSULADO]

Quando for seleccionado o *Mac Encapsulated routing* na interface ATM, terá de preencher uma lista de parâmetros (consulte a Figura 7). Consulte a Tabela 6 para obter mais informações sobre o significado e os valores do parâmetro. Quando todos os campos estiverem correctamente preenchidos, prima o botão **SAVE SETTINGS** [Guardar definições].

FIGURA 7. Definições da interface ATM (MAC Encapsulated Routing) da secção WAN

ATM Interface

ATM1	
Protocol	MAC Encapsulated Routing
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
VPI/VCI	8 / 35
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
DHCP Client	☐

TABELA 6. Lista de parâmetros da Interface ATM MAC Encapsulated Routing

PARÂMETRO	DESCRIÇÃO
Protocol [Protocolo]	<i>MAC Encapsulated Routing</i>
IP address [Endereço de IP]	<i>Introduza o endereço de IP fornecido pelo seu ISP</i>
Subnet Mask [Máscara de Sub-rede]	<i>Introduza o endereço da máscara de sub-rede fornecido pelo seu ISP</i>
Default Gateway [Gateway Predefinido]	<i>Introduza o endereço gateway fornecido pelo seu ISP</i>

TABELA 6. Lista de parâmetros da Interface ATM MAC Encapsulated Routing

PARÂMETRO	DESCRIÇÃO
VPI/VCI	Introduza o Identificador de Caminho Virtual (VPI) e o Identificador de Circuito Virtual (VCI) fornecidos pelo seu ISP
Encapsulation [Encapsulamento]	Selecione o encapsulamento utilizado pelo seu ISP no menu suspenso
QoS Class [Classe de Qualidade de Serviço]	Classes QoS ATM incluindo CBR, UBR e VBR
PCR/SCR/MBS	Os Parâmetros QoS – PCR (Peak Cell Rate) [Taxa Máxima de Células], SCR (Sustainable Cell Rate) [Taxa Sustentável de Células] e MBS (Maximum Burst Size) [Tamanho Máximo da Rajada] são configuráveis.
DHCP Client [Cliente DHCP]	Assinale a caixa se o seu ISP atribui um endereço IP de forma dinâmica.

WAN >> CLONE MAC ADDRESS [ENDEREÇO DE CLONE DE MAC]

Alguns ISP pedem-lhe que registre o seu *endereço MAC*. Se for esse o seu caso, e se tiver registado anteriormente o endereço MAC de outro dispositivo, deverá alterar o endereço MAC do Router para o endereço MAC que registou com o seu ISP (consulte a Figura 8).

Após ter inserido o endereço MAC, prima o botão **SAVE SETTINGS** [Guardar definições].

FIGURA 8. Painel de Endereço de Clone de MAC secção WAN

Clone MAC Address

Some ISPs require you to register your MAC address with them. If you have done this, the MAC address of the Gateway must be changed to the MAC address that you supplied to your ISP.

■ WAN Interface MAC Address:

☒ Use the Gateway's default MAC address **00:1C:A2:E0:0C:69**

☐ Use this PC's MAC address **00:1A:6B:66:A0:71**

☐ Enter a new MAC address manually:

: : : : :

HELP SAVE SETTINGS CANCEL

Secção LAN

O menu **LAN** permite configurar o *endereço IP da LAN*, permitindo que o servidor DHCP faça a alocação dinâmica de endereços de cliente e defina o intervalo de endereços IP dentro de um domínio. Na Figura 1 é apresentada a primeira parte do ecrã principal da secção **LAN**, com os parâmetros disponíveis.

FIGURA 1. Painei principal da LAN

LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The router must have an IP address for the local network.

LAN IP

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255.255.255. 0
DHCP Server	☒ Enabled ☐ Disabled

DHCP Server

DHCP Server ID	
Lease Time	Two Days

IP Address Pool

Start IP	192 . 168 . 1 . 2
End IP	192 . 168 . 1 . 254
Domain Name	

HELP SAVE SETTINGS CANCEL

No painel apresentado é possível configurar vários parâmetros, tal como é descrito na Tabela 1

TABELA 1. Lista de parâmetros da secção LAN

PARÂMETRO	DESCRIÇÃO
LAN IP [IP da LAN]	
IP Address [Endereço de IP]	O endereço de IP do Router
IP Subnet mask [IP da máscara de sub-rede]	A máscara de sub-rede da rede
DHCP server [Servidor DHCP]	Para activar ou desactivar a função de servidor DHCP. O servidor DHCP encontra-se predefinido para a atribuição automática de endereço de IP a dispositivos clientes

TABELA 1. Lista de parâmetros da secção LAN

PARÂMETRO	DESCRIÇÃO
Parâmetros do servidor DHCP	
DHCP Server ID [Identificação do Servidor DHCP]	<i>Introduza aqui a ID</i>
Lease Time [Tempo de Concessão]	<i>Selecione o período de tempo entre a atribuição de dois endereços de IP</i>
IP Address Pool [Intervalo de Endereços de IP]	<i>Especifique o IP inicial / IP final do intervalo DHCP. Não inclua o endereço de IP do Router no intervalo de endereços de cliente. Se alterar o intervalo de IP, certifique-se de que os primeiros três octetos correspondem ao endereço de IP do gateway, por exemplo, 192.168.1.xxx</i>
Start IP / End IP [IP inicial / IP final]	
Domain Name [Nome do Domínio]	<i>Se a sua rede utilizar um nome de domínio, introduza-o aqui. Caso contrário, deixe este campo em branco</i>

LAN >> DHCP OPTION
[OPÇÃO DHCP]

FIGURA 2. DHCP Option [opção DHCP]

DHCP Option

Enable or disable DHCP Option function : ☒ Disable ☐ Enable

No.	Vendor Class ID
1	
2	
3	
4	

[HELP](#)

[SAVE SETTINGS](#)

[CANCEL](#)

Secção Sem Fios

O Router também funciona como um Ponto de Acesso sem fios (AP), permitindo que os computadores comuniquem entre si sem fios. Para configurar esta função, apenas necessita de activar a função sem fios, definir o *radio channel* [canal de rádio], o *SSID* e as *opções de segurança*.

Clique no botão *Enable* radio [activar rádio] e, em seguida, seleccione o país no menu suspenso e clique no botão **SAVE SETTINGS** [Guardar definições]. Na Figura 1 é apresentado o ecrã principal da secção **SEM FIOS**: do lado esquerdo surge uma lista de comandos desta secção.

FIGURA 1. PAINEL PRINCIPAL DA SECÇÃO SEM FIOS

Configurações de Rede sem Fio

O router pode rapidamente ser configurado como um ponto de acesso sem fio para o acesso de clientes através da configuração do Service Set Identifier (SSID) e do número do canal. Também suporta a criptografia dos dados e filtragem de clientes.

Ligar ou desligar o funcionamento do módulo Wireless: ☒ Ligar ☐ Desligar

Seleção de País :

SALVA AS CONFIGURAÇÕES

SEM FIOS >> CANAL E SSID

É necessário especificar o *common radio channel* [canal de rádio comum] e *ESSID* que serão utilizados pelo Router e por todos os seus clientes sem fios (consulte a Figura 2). Certifique-se de que configura os mesmos valores para todos os clientes ligados.

FIGURA 2. CONFIGURAÇÃO DO CANAL E SSID

Canal e SSID

Esta página permite-lhe definir o SSID e o Canal para conexão wireless. No ambiente wireless, o router pode também actuar como um ponto de acesso sem fio. Estes parâmetros são usados para que as estações móveis se conectem a este ponto de acesso.

Modo Wireless	[Misto (11b+11g)]
Canal	[Auto]

SSID

Número.	Nome da Rede Wireless (SSID)	Broadcast do SSID
WLAN	SAPO-PIEDD9E	☒ Ligar

[AJUDA](#) [SALVA AS CONFIGURAÇÕES](#) [CANCELAR](#)

SEM FIOS >> CONTROLO DE ACESSO

Ao utilizar a funcionalidade de Controlo de Acesso, é possível restringir o acesso com base no endereço MAC. Cada computador possui um identificador único conhecido como *Medium Access Control (MAC) address* [Endereço de Controlo de Acesso ao Meio]. Com a activação da filtragem MAC, os computadores cujos endereços MAC estejam na tabela de filtragem poderão ligar-se (ou ser-lhes-á negado o acesso) ao Router. Na Figura 3 é apresentada a **Tabela de Filtragem de Acesso à WLAN**.

FIGURA 3. WLAN MAC FILTERING TABLE [TABELA DE FILTRAGEM MAC WLAN]

WLAN MAC Filtering Table

For a more secure Wireless network you can specify that only certain Wireless PCs can connect to the Access Point. Up to 32 MAC addresses can be added to the MAC Filtering Table. When enabled, all registered MAC addresses are controlled by the Access Rule.

• Enable MAC Filtering : ☐ Yes ☒ No

• Access Rule for registered MAC address : ☐ Allow ☒ Deny

• MAC Filtering Table (up to 32 stations)

ID	MAC Address								
1	00	:	00	:	00	:	00	:	00
2	00	:	00	:	00	:	00	:	00
3	00	:	00	:	00	:	00	:	00
4	00	:	00	:	00	:	00	:	00
5	00	:	00	:	00	:	00	:	00
6	00	:	00	:	00	:	00	:	00
7	00	:	00	:	00	:	00	:	00

TABELA 1. Lista de campos da Tabela de Filtragem MAC WLAN

PARÂMETRO	DESCRIÇÃO
Enable MAC filtering [Activar filtragem MAC]	<i>Selecione para activar esta característica</i>
Access Rule for registered MAC address [Regra de Acesso para endereços MAC registados]	<i>Selecione Allow / Deny [Permitir / Negar] acesso aos endereços MAC registados. Ao seleccionar Allow apenas os endereços MAC aqui registados poderão ligar-se ao Router. Ao seleccionar Deny apenas os endereços MAC aqui registados terão acesso negado ao Router negado.</i>
MAC Filtering Table (up to 32 stations) [Tabela de Filtragem MAC (até 32 estações)]	<i>Pode introduzir até 32 endereços nesta tabela. Clique no botão Add currently MAC stations [Adicionar estações MAC actuais] para copiar rapidamente a entrada para a Tabela de Filtragem MAC.</i>

SEM FIOS >> SEGURANÇA

A função de segurança deve estar activada para tornar as redes sem fios mais seguras. Na Figura 4 é apresentado o painel onde é possível definir a segurança. O Router suporta mecanismos de segurança **WEP (Wired Equivalent Privacy)** [Privacidade Equivalente a Rede] e **WPA (Wi-Fi Protected)** [Acesso Protegido Wi-Fi].

FIGURA 4. DEFINIÇÕES DE SEGURANÇA SEM FIOS

Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages.

SSID	Allowed Client Type
tele2_001CA2E00C68	WPA Only

[HELP](#)
[SAVE SETTINGS](#)
[CANCEL](#)

Encontram-se disponíveis as seguintes opções:

- No WEP, No WPA [Sem WEP, Sem WPA]
- WEP only [Apenas WEP]
- WPA only [Apenas WPA]



Ao seleccionar a opção "No WEP, no WPA" qualquer cliente com o SSID correcto poderá ligar-se a este Router. Sugerimos a activação da função de segurança para proteger a comunicação sem fios.

SEM FIOS >> SEGURANÇA >> WEP

A Figura 5 apresenta o painel de configuração **WEP**. Para utilizar a WEP para proteger a rede sem fios, é necessário definir os mesmos parâmetros para o Router e para todos os clientes sem fios.

FIGURA 5. PAINEL DE CONFIGURAÇÃO WEP

WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your router and wireless client devices to use WEP.

WEP Mode

☒ 64-bit
 ☐ 128-bit

Key Entry Method

☒ Hex
 ☐ ASCII

Static WEP Key Setting

10/26 hex digits for 64-WEP/128-WEP

Passphrase

☐

(1~32 characters)

Key 1

0101010101

Key 2

0202020202

Key 3

0303030303

Key 4

0404040404

Clear

Generate Key

SSID

SSID

Using Key ID

No.1

1

HELP

SAVE SETTINGS

CANCEL

TABELA 2. Lista de parâmetros da configuração WEP

PARÂMETRO	DESCRIÇÃO
WEP Mode [Modo WEP]	Selecione uma chave de 64 bits ou de 128 bits para encriptação
Key Entry Method [Método de Entrada de chave]	Selecione Hex ou ASCII. Se for seleccionado ASCII, a caixa de selecção Passphrase [frase-passe] não estará disponível
Key Provisioning [Fornecimento da Chave]	Selecione Static [estático] ou Dynamic [Dinâmico]. Se seleccionar Dinâmico, deve igualmente definir a função 802.1X
Static WEP Key Settings [Definições de C haves WEP Estáticas]	Entre 1-4 caracteres
ID da Chave Predefinida	
Passphrase [Frase-passe]	Existem duas formas de criar chaves de encriptação, com ou sem a função de frase-passe.

TABELA 2. Lista de parâmetros da configuração WEP

PARÂMETRO	DESCRIÇÃO
	Para criar chaves de encriptação utilizando a função de frase-passe, assinala a caixa <i>Passphrase</i> e introduza a cadeia de caracteres. Lembre-se de que a frase-passe só pode conter até 32 caracteres alfanuméricos. Para criar chaves de encriptação sem utilizar a função de frase-passe, efectue as suas selecções em <i>WEP Mode</i> [Modo WEP] e em <i>Key Entry Method</i> [Método de Entrada de Chave] e as chaves de encriptação serão criadas automaticamente. É igualmente possível introduzir manualmente as chaves de encriptação. Introduza cinco pares hexadecimais de dígitos para o modo WEP de 64 bits, ou introduza 13 pares para o modo WEP de 128 bits. Lembre-se de que o dígito hexadecimal consiste num número ou numa letra entre 0-9 e entre A-F



Antes de guardar as definições, a chave é apresentada em linguagem clara. Caso o seu cliente sem fios não possua um utilitário de frase-passe, anote a chave predefinida antes de guardar as definições. Assim, poderá configurar o seu cliente sem fios com o SSID adequado para se poder ligar a este Router.

Sugerimos a activação da função de segurança para proteger a sua comunicação sem fios.

SEM FIOS >> SEGURANÇA

>> WPA

A Figura 6 apresenta as definições **WPA**. O *Acesso Protegido Wi-Fi (WPA)* combina o *temporal key integrity protocol* [Protocolo de Integridade de Chave Temporária] (TKIP) e mecanismos 802.1X. Proporciona uma encriptação dinâmica de chaves e um serviço de autenticação 802.1X. O Router suporta WPA e WPA2.

FIGURA 6. PAINEL DE DEFINIÇÕES WPA

WPA

WPA is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your router and wireless client devices to use WPA.

WPA mode	WPA
Cipher suite	TKIP
Authentication	☒ Pre-shared Key ☐ 802.1X
Pre-shared key type	☒ Passphrase (8~63 characters) ☐ Hex (64 digits)
Pre-shared Key	••••••••••

[HELP](#)
[SAVE SETTINGS](#)
[CANCEL](#)

TABELA 3. Lista de parâmetros do menu de definições WPA

PARÂMETRO	DESCRIÇÃO
WPA Mode [Modo WPA]	<i>Seleccione WPA, WPA2 ou mixed [misto]</i>
Cipher suite [Pacote de Criptografia]	<i>Seleccione TKIP + AES, ou AES</i>
Authentication [Autenticação]	<i>Seleccione 802.1X ou Pre-shared Key [Chave pré-partilhada]</i> 802.1X: para um ambiente de rede com servidor RADIUS. - Pre-shared Key: para ambiente de rede SOHO sem servidor de autenticação
Pre-shared Key type [Tipo de chave pré-partilhada]	<i>Seleccione Passphrase [frase-passe] ou Hex</i>
Pre-shared Key [Chave pré-partilhada]	<i>Introduza a chave neste campo</i>
Group Key Re_Keying [Alteração de Chave de Grupo]	<i>O período de renovação de chaves broadcast / multicast</i>

SEM FIOS >> SEGURANÇA
>> 802.1X

A figura 7 apresenta as definições **802.1X**. Se o **802.1X** for utilizado na rede, esta funcionalidade do Router poderá ser activada.

FIGURA 7. PAINEL DE DEFINIÇÕES 802.1X

802.1X

This page allows you to set the 802.1X, a method for performing authentication to wireless connection. These parameters are used for this access point to connect to the Authentication Server.

802.1X Authentication	☐ Enable ☒ Disable
Session Idle Timeout	300 Seconds (0 for no timeout checking)
Re-Authentication Period	3600 Seconds (0 for no re-authentication)
Quiet Period	60 Seconds after authentication failed
Server Type	RADIUS

RADIUS Server Parameters							
Server IP	192	.	168	.	1	.	1
Server Port	1812						
Secret Key							
NAS-ID							

[HELP](#)
[SAVE SETTINGS](#)
[CANCEL](#)

TABELA 4. Lista de parâmetros do menu de definições 802.1X

PARÂMETRO	DESCRIÇÃO
802.1X Authentication [Autenticação 802.1X]	Seleccione a opção enable [activar] ou disable [desactivar] para esta função
Session Idle Timeout [Tempo de Inactividade da Sessão]	Define um período de tempo máximo durante o qual a ligação é mantida em caso de inactividade
Re-Authentication Period [Período de Reautenticação]	Define um período de tempo máximo durante o qual o servidor de autenticação irá reatribuir, de forma dinâmica, uma chave de sessão a um cliente ligado.

TABELA 4. Lista de parâmetros do menu de definições 802.1X

PARÂMETRO	DESCRIÇÃO
Quiet Period [Período de paragem]	<i>Define um período de tempo máximo durante o qual o Router irá aguardar entre falhas de autenticação</i>
Server Type [Tipo de servidor]	<i>Encontra-se definido para RADIUS</i>
Server IP [IP do servidor]	<i>O endereço de IP do nosso servidor de autenticação</i>
Server Port [Porta do Servidor]	<i>A porta utilizada para o serviço de autenticação</i>
Secret Key [Chave secreta]	<i>A chave secreta partilhada entre o servidor de autenticação e os seus clientes</i>
NAS-ID [Identificação do NAS]	<i>Define o identificador de pedido do Servidor de Acesso à Rede (NAS)</i>

SEM FIOS >> WI-FI PROTECTED SETUP [CONFIGURAÇÃO PROTEGIDA DE WI-FI]

O **Wi-Fi Protected Setup (WPS)** é o método padrão da indústria para simplificar a configuração da segurança e a gestão das redes Wi-Fi. É possível configurar e ligar-se a uma rede *WPA-enabled 802.11* através de dispositivos com certificação WPS que utilizem um *Número de Identificação Pessoal (PIN)* ou o método *Push Button Configuration* [Configuração do Botão de Pressão] (*PBC*). Os dispositivos legados sem WPS podem ser adicionados à rede utilizando o método de configuração manual tradicional (consulte a Figura 8).

FIGURA 8. WI-FI PROTECTED SETUP PANEL [PAINEL DE CONFIGURAÇÃO PROTEGIDA DE WI-FI]

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) Enabled

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of the Wi-Fi networks. You now can easily setup and connect to a WPA-enabled 802.11 network with WPS-certificated devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

[Apply Changes](#)

1) Personal Information Number (PIN) Method
Enter the PIN from the client device and click "Enroll". Then start WPS on the client device from it's wireless utility or WPS application within 2 minutes.

Enter Client Device PIN [Enroll](#)

If an external registrar is available, you can also enter Router's PIN at the external registrar. To change Router's PIN, click "Generate New PIN" or click "Restore Default PIN" to reset the PIN to factory default.

Router PIN : 12345670

[Generate New PIN](#)

[Restore Default PIN](#)

2) Push Button Configuration (PBC) Method
Push and hold PBC button on your router for 3 seconds or click "Start PBC". Then start PBC on the device you want to connect to the router within 2 minutes.

[Start PBC](#)

3) Manual Configuration Method
For client devices without WPS, manually configure the device with the following settings.

Network Name (SSID) : tele2_001CA2E00C68
Wireless security : Configured
Network Authentication : WPA+PSK
Data Encryption : TKIP
Network Key (PSK) : 99201Y0001677

SEM FIOS >> WDS

O **Wireless Distribution System** [Sistema de Distribuição Sem Fios] (WDS) permite aumentar o alcance da Rede de Área Local Sem Fios (WLAN). O WDS permite que um Access Point [Ponto de Acesso] (AP) estabeleça uma ligação directa a outros AP e permita que as estações sejam deslocadas livremente na área coberta pelo WDS (consulte a Figura 9).

FIGURA 9. CONFIGURAÇÕES WDS DA SECÇÃO SEGURANÇA SEM FIOS

WDS

The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows an Access Point (AP) to establish a direct link to other APs and to allows stations to roam freely within the area covered by the WDS.

Enable or disable WDS features : ☐ Enable ☒ Disable

AP MAC Address Table (up to 4 APs)			
	SSID	MAC Address	Mode
☐	PBSWiFiHotSpot	00 : 08 : 27 : 99 : 6F : 3D	11g
☐	PBSWiFiHotSpot	00 : 08 : 27 : 99 : 68 : 5A	11g
☐	PirelliBS1	00 : 22 : 69 : 06 : F0 : 50	11g
☐	PBSWiFiHotSpot	00 : 08 : 27 : 99 : EA : F7	11g
☐	PBSWiFiHotSpot	00 : 08 : 27 : 99 : 6B : D0	11g
☐	PBSWiFiHotSpot	00 : 08 : 27 : 9A : 07 : 0B	11g
☐	PBSWiFiHotSpot	00 : 08 : 27 : 9A : 07 : 06	11g
☐	PBSWiFiHotSpot	00 : 08 : 27 : 99 : 6B : E5	11g

TABELA 5. Lista de campos de definição do menu de definições WDS

PARÂMETRO	DESCRIÇÃO
Enable or disable WDS features [Activar ou desactivar características WDS]	<i>Selecione turn on [activar] / turn off [desactivar] para esta função</i>
Rescan [Novo scan]	<i>Clique aqui para actualizar a lista de pontos de acesso disponíveis</i>

Os pontos de acesso disponíveis irão surgir na *AP MAC Address Table* [Tabela de Endereços MAC de AP]; assinale a caixa correspondente para adicionar esse ponto de acesso específico ao WDS.

SEM FIOS >> CONFIGURAÇÃO AVANÇADA

Podem ser configurados cinco parâmetros adicionais na função Sem Fios. Para obter o máximo de desempenho da sua rede sem fios, sugerimos que mantenha os valores deste ecrã com as definições predefinidas (consulte a Figura 10).

FIGURA 10. PAINEL ADVANCED SETTINGS [CONFIGURAÇÃO AVANÇADA]

Advanced Setting

This page allows you to config advanced settings in the wireless driver.

Beacon Interval	100	(Default: 100, Range: 1-65535)
DTIM Interval	1	(Default: 1, Range: 1-255)
Fragmentation Threshold	2346	(Default: 2346, Range: 256-2346)
RTS Threshold	2347	(Default: 2347, Range: 0-2347)
WMM Mode	Disable	(Default: Disable)

TABELA 6. Parâmetros do painel de Configuração Avançada

PARÂMETRO	DESCRIÇÃO
Beacon Interval [Intervalo de Marcação]	<i>Representa o tempo existente entre transmissões de sinais de marcação. Antes de uma estação entrar no modo de economia de energia, a estação necessita do intervalo de marcação para saber quando deve voltar a ficar activa para receber o sinal de marcação (e para saber se existem limites de memória intermédia no ponto de acesso)</i>
DTIM Interval [Intervalo DTIM]	<i>A Delivery Traffic Indication Message [Mensagem de indicação de tráfego de entrega] indica a ocorrência de uma DTIM. Um intervalo DTIM consiste numa contagem do número de sinais de marcação que devem ocorrer antes de o ponto de acesso enviar pacotes multicast de memória intermédia. Por exemplo, Um intervalo DTIM igual a um significa que os multicast são enviados após cada sinal de marcação. Um intervalo DTIM igual a dois indica que os pacotes multicast são enviados a cada dois sinais de marcação, sucessivamente. Sendo que cada sinal de marcação inclui um campo que identifica o intervalo DTIM, todas as estações sabem quando devem ficar activas e receber os pacotes multicast caso estejam em modo de economia de energia.</i>
Fragmentation Threshold [Limite de fragmentação]	<i>Consiste no tamanho máximo para os pacotes de dados transmitidos. Os pacotes maiores são fragmentados em vários pacotes deste tamanho ou de tamanhos mais pequenos antes da transmissão. A estação receptora junta os fragmentos transmitidos.</i>
RTS Threshold [Limite de RTS] (Request to Send) [Pedido de Transmissão]	<i>Este parâmetro controla o tamanho do pacote de dados que o protocolo RF de nível mais baixo envia para um pacote RTS. A utilização de um valor pequeno leva a que os pacotes RTS sejam enviados com maior frequência, ocupando assim mais largura de banda disponível do que anteriormente, o que reduz a produtividade aparente do pacote de rede. Contudo, quantos mais pacotes RTS forem enviados, mais rapidamente o sistema consegue recuperar de uma interferência ou colisão.</i>
WMM Mode [Modo WMM]	<i>Suporte multimédia sem fios. O WMM organiza o tráfego segundo diferentes prioridades, de acordo com 4 AC (Access Categories [Categorias de Acesso]) - voz, vídeo, melhor desempenho e contexto. Contudo, não garante produtividade. É ideal para aplicações simples que requeiram QoS.</i>

Secção NAT

A secção NAT (*Network Address Translation*) [Tradução de Endereços de Rede] permite que vários utilizadores acessem à Internet partilhando um IP público. A Figura 1 apresenta o ecrã principal NAT.

FIGURA 1. Ecrã principal NAT

NAT Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

Enable or disable NAT module function :
 ☒ Enable
 ☐ Disable

SAVE SETTINGS

TABELA 1. Definições NAT

PARÂMETRO	DESCRIÇÃO
Enable or disable NAT module function [Activar ou	Activar / desactivar a função NAT

TABELA 1. Definições NAT

PARÂMETRO	DESCRIÇÃO
desactivar a função módulo NAT]	

NAT >> MAPEAMENTO DE ENDEREÇOS

Permite que um ou mais endereços de IP públicos sejam partilhados por vários utilizadores internos. Esta função também permite esconder a rede interna, aumentando a privacidade e a segurança. Introduza o *endereço de IP público* que pretende partilhar no campo Global IP [IP Global]. Introduza um intervalo de IP internos que irão partilhar o IP global no campo “from” [de].

A Figura 2 representa a configuração do Endereço que será partilhado na Internet pública ou global.

FIGURA 2. Address Mapping configuration [Configuração do Mapeamento de Endereços]

Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.

Address Mapping	
1. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
2. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
3. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
4. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
5. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
6. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
7. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
8. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
9. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	
10. Global IP: 0 . 0 . 0 . 0	is transformed as multiple virtual IPs
from 192.168.1.0 to 192.168.1.0	

HELP SAVE SETTINGS CANCEL

NAT >> SERVIDOR VIRTUAL

Se configurar o Router como servidor virtual, os utilizadores remotos que acederem a serviços como a Web ou FTP no seu site local, através de endereços de IP públicos, podem ser dirigidos automaticamente para os servidores locais configurados com endereços de IP privados. Por outras palavras, dependendo

do serviço pedido (número de porta TCP / UDP), o Router redirige o pedido de serviço externo para o servidor adequado (localizado noutra endereço de IP interno).

Na Figura 3 é apresentada a configuração do Router como **Servidor Virtual**.

FIGURA 3. Configuração do Router do Servidor Virtual

Virtual Server

You can configure the router as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:

- Port Ranges: ex. 100-150
- Multiple Ports: ex. 25,110,80
- Combination: ex. 25-100,80

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.1. 	TCP v			☐	Add Clean
2	192.168.1. 	TCP v			☐	Add Clean
3	192.168.1. 	TCP v			☐	Add Clean
4	192.168.1. 	TCP v			☐	Add Clean
5	192.168.1. 	TCP v			☐	Add Clean
6	192.168.1. 	TCP v			☐	Add Clean
7	192.168.1. 	TCP v			☐	Add Clean
8	192.168.1. 	TCP v			☐	Add Clean
9	192.168.1. 	TCP v			☐	Add Clean
10	192.168.1. 	TCP v			☐	Add Clean
11	192.168.1. 	TCP v			☐	Add Clean
12	192.168.1. 	TCP v			☐	Add Clean
13	192.168.1. 	TCP v			☐	Add Clean
14	192.168.1. 	TCP v			☐	Add Clean
15	192.168.1. 	TCP v			☐	Add Clean
16	192.168.1. 	TCP v			☐	Add Clean
17	192.168.1. 	TCP v			☐	Add Clean
18	192.168.1. 	TCP v			☐	Add Clean
19	192.168.1. 	TCP v			☐	Add Clean
20	192.168.1. 	TCP v			☐	Add Clean

Por exemplo, se definir o *Type/Public Port* [Tipo/Porta Pública] para TCP/80 (http ou web) e o *Private IP/Port* [IP Privado/Porta] para 192.168.1.40/80, todos os pedidos HTTP de utilizadores externos serão transferidos para 192.168.1.40 na porta 80. Assim sendo, ao introduzir simplesmente o endereço de IP fornecido pelo ISP, os utilizadores da Internet podem aceder ao serviço de que necessitam no endereço local para o qual os dirigiu.

As portas de serviço TCP mais comuns são: HTTP:80, FTP:21, Telnet:23 e POP3:110.

Poderá encontrar uma lista exaustiva das portas na hiperligação que se segue:

<http://www.iana.org/assignments/port-numbers>.

NAT >> APLICAÇÃO ESPECIAL

Algumas aplicações necessitam de várias ligações, tais como os jogos na Internet, Videoconferências e telefonemas pela Internet. Estas aplicações poderão não funcionar quando a função **Networks Address Translation** [Tradução de Endereços de Rede] (**NAT**) se encontra activada. Caso pretenda executar aplicações que requerem várias ligações, utilize estes ecrãs para especificar as portas públicas adicionais que devem ser abertas para cada aplicação.

A Figura 4 apresenta a introdução de uma porta (Trigger port) para abrir o tráfego de entrada para aplicações especiais.

FIGURA 4. Configuração da trigger port [porta de activação] para o tráfego de entrada de aplicações especiais

Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Note: The range of the Trigger Ports is from 1 to 65535.

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
2.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
3.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
4.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
5.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
6.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
7.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
8.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
9.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐
10.		☒ TCP ☐ UDP		☒ TCP ☐ UDP	☐

Popular applications

TABELA 2. Lista de campos no menu de Aplicações Especiais

PARÂMETRO	DESCRIÇÃO
Trigger Port [porta de activação]	Permite abrir o tráfego de entrada para aplicações especiais, tais como os jogos de Internet, videoconferências, telefonemas pela Internet e outras.
Trigger Type [tipo de porta de activação]	Selecione o protocolo TCP ou UDP.

TABELA 2. Lista de campos no menu de Aplicações Especiais

PARÂMETRO	DESCRIÇÃO
Public port [Porta Pública]	Porta em direcção à rede.
Public Type [Tipo Público]	Selecione o protocolo TCP ou UDP.
Enabled [Activada]	Activar / Desactivar a porta.
Popular applications [aplicações populares]	Para copiar rapidamente a entrada para a tabela.

NAT >> NAT MAPPING TABLE [TABELA DE MAPEAMENTO NAT]

Esta secção apresenta o mapeamento de endereços **NAPT (Network Address Port Translation)** [Tradução de Portas de Endereços de Rede] actuais (consulte aFigura 5).

FIGURA 5. Network Address Port Translation Table [Tabela de Tradução de Portas de Endereços de rede]

NAT Mapping Table

NAT Mapping Table displays the current NAPT address mappings.

Index	Protocol	Local IP	Local Port	Pseudo IP	Pseudo Port	Peer IP	Peer Port
-------	----------	----------	------------	-----------	-------------	---------	-----------

REFRESH

HELP

Secção Roteamento

Este item de menu define os parâmetros relativos ao roteamento, incluindo o roteamento estático e os parâmetros RIP. A Figura 1 apresenta o ecrã principal **Routing** [Roteamento].

FIGURA 1. **Routing main screen** [Ecrã principal de roteamento]

Routing Settings

This page defines the routing related parameters including static routes and RIP parameters.

ROTEAMENTO >> ROTEAMENTO ESTÁTICO

O painel de Roteamento Estático serve para configurar os roteamentos estáticos (consulte a Figura 2).

FIGURA 2. Static Route Parameter configuration [Configuração dos Parâmetros de Roteamento Estático]

Static Route Parameter

Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure

Clique no botão **Add route** [Adicionar rota] para definir uma nova entrada de roteamento estático.

FIGURA 3. Static Route Parameter configuration (add new route) [Configuração de Parâmetro de Roteamento Estático (adicionar nova rota)]

Static Route Parameter

Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure
1				N/A

TABELA 1. Lista de campos do menu de Mapeamento de endereços

PARÂMETRO	DESCRIÇÃO
Network Address [Endere-	<i>Introduza o endereço de IP do computador remoto para o qual</i>

TABELA 1. Lista de campos do menu de Mapeamento de endereços

PARÂMETRO	DESCRIÇÃO
ço de Rede]	<i>pretende definir o roteamento estático</i>
Subnet Mask [Máscara de Sub-rede]	<i>A máscara de sub-rede da rede de destino</i>
Gateway [Porta de Ligação]	<i>Introduza o endereço de IP WAN do gateway para a rede remota</i>
Configure [Configurar]	<i>Clique no botão Edit [Editar] para alterar parâmetros de roteamento estático existentes. Ao clicar no botão Delete [Eliminar], a entrada correspondente será removida</i>

ROUTING >> RIP

O RIP (Routing Information Protocol) [Protocolo de Informação de Rotas] envia mensagens de actualização de roteamento em intervalos regulares e quando a topologia da rede é alterada. Quando um router recebe uma actualização de roteamento que inclui alterações numa entrada, este actualiza a sua tabela de roteamento para incluir o novo roteamento. Os routers RIP mantêm apenas o melhor roteamento para um destino. Após ter actualizado a sua tabela de roteamento, o router começa imediatamente a transmitir actualizações de roteamento para informar outros routers da rede sobre a alteração efectuada.

FIGURA 4. RIP parameter configuration [Configuração do parâmetro RIP]

RIP Parameter

Please Enter the following Configuration Parameters:

■ General RIP parameter:

RIP Mode: ☒ Disable ☐ Enable

Auto Summary: ☒ Disable ☐ Enable

■ Table of current interface RIP parameter:

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
VLAN1(Default)	Disable	1	Disable	None	
ATM1	Disable	1	Disable	None	
ATM2	Disable	1	Disable	None	
ATM3	Disable	1	Disable	None	
ATM4	Disable	1	Disable	None	
ATM5	Disable	1	Disable	None	
ATM6	Disable	1	Disable	None	
ATM7	Disable	1	Disable	None	
ATM8	Disable	1	Disable	None	
PPPoE1	Disable	1	Disable	None	
PPPoE2	Disable	1	Disable	None	
PPPoE3	Disable	1	Disable	None	
PPPoE4	Disable	1	Disable	None	
PPPoE5	Disable	1	Disable	None	
PPPoE6	Disable	1	Disable	None	
PPPoE7	Disable	1	Disable	None	
PPPoE8	Disable	1	Disable	None	

O significado dos parâmetros RIP é explicado na Tabela 2

TABELA 2. Lista do parâmetro RIP

PARÂMETRO	DESCRIÇÃO
General RIP parameter [Parâmetro RIP geral]	<i>Selecione enables [activar] ou disables [desactivar] RIP</i>
<i>RIP Mode</i> [Modo RIP]	
<i>Auto Summary</i> [Resumo automático]	<i>Se o Resumo Automático estiver desactivado, os pacotes RIP irão incluir a informação de sub-rede de todas as sub-redes ligadas ao router. Se estiver activado, a informação de sub-rede será resumida a uma informação que abranja todas as sub-redes.</i>
Table of current interface RIP parameter [Tabela da interface actual do parâmetro RIP]	
<i>Interface</i>	<i>Identifique a interface WAN a ser configurada</i>
<i>Operation Mode</i> [Modo de funcionamento]	É possível definir: • <i>Disable</i> [Desactivar]: <i>RIP desactivado nesta interface</i> • <i>Enable</i> [Activar]: <i>RIP activado nesta interface</i> • <i>Silent</i> [Silencioso]: <i>recebe as emissões de roteamento e actualiza a tabela de roteamento. Não participa na emissão de roteamento</i>
<i>Version</i> [Versão]	<i>Define a versão RIP a utilizar nesta interface</i>
<i>Poison Reverse</i> [Envenenamento Inverso]	<i>Um método que impede situações nas quais os dados de tráfego poderiam ser retransmitidos num ciclo interminável</i> • <i>None</i> [Nenhum]: <i>SEM autenticação</i> • <i>Password</i>: <i>É incluída no pacote uma chave de autenticação da password. Se esta não coincidir com o que é esperado, o pacote será rejeitado. Este método proporciona muito pouca segurança, uma vez que é possível conhecer a chave de autenticação através da observação dos pacotes RIP.</i>
<i>Authentication Required</i> [Autenticação Necessária]	<i>Password ou chave de Autenticação MD5</i>

ROTEAMENTO >> TABELA DE ROTEAMENTO

Este menu apresenta a lista de rotas configuradas (consulte a Figura 5).

FIGURA 5. Routing Table [Tabela de Roteamento]

Routing Table

List Routing Table:

Flags	Network Address	Netmask	Gateway	Interface
C	192.168.1.0	255.255.255.0	Directly	VLAN1
C	127.0.0.1	255.255.255.255	Directly	Loopback

Flags : C - directly connected, S - static, R - RIP, I - ICMP Redirect

HELP

TABELA 3. Lista de campos da Tabela de Roteamento da secção Roteamento

PARÂMETRO	DESCRIÇÃO
Flags [Indicadores]	C= Ligação directa à mesma sub-rede S= Roteamento estático R= Rota RIP atribuída I= Rota redireccionada ICMP (Internet Control Message Protocol) [Protocolo de Mensagens de Controlo da Internet]
Network Address [Endereço de Rede]	Endereço de IP de destino
Netmask [Máscara de rede]	A sub-rede associada ao destino. Este modelo identifica os bits de endereço num endereço de destino utilizado para roteamento de sub-redes específicas. Cada bit correspondente a "1" faz parte do número de máscara de sub-rede; cada bit correspondente a "0" faz parte do número anfitrião
Gateway [Porta de Ligação]	O endereço de IP do router na paragem seguinte para a qual são encaminhados dados
Interface	A interface local através da qual é alcançada a próxima paragem desta rota
Metric [Métrica]	Quando um router recebe uma actualização de roteamento que contém uma entrada de rede de destino nova ou alterada, o router adiciona 1 ao valor métrico indicado na actualização e introduz a rede na tabela de roteamento.

Secção firewall

A firewall do Router examina pacotes na camada da aplicação, conserva informações de sessão de TCP e UDT, incluindo interrupções e o número de sessões activas, e fornece a capacidade de detectar e prevenir certos tipos de ataques de rede.

Os ataques de rede que negam o acesso a um dispositivo de rede são denominados por ataques de *Denial of Service* [Negação de serviço] (*DoS*). Os ataques DoS atingem os dispositivos e redes com uma ligação à Internet. O seu objectivo não consiste em roubar informação, mas sim desactivar um dispositivo ou rede para que os utilizadores deixem de ter acesso aos recursos da rede.

O router protege contra os seguintes ataques DoS: *IP Spoofing*, *Land Attack*, *Ping of Death*, *IP with zero length*, *Smurf attack*, *UDP port loopback*, *Snork Attack*, *TCP null scan* e *TCP SYN flooding*.

A firewall não afecta o desempenho do sistema de forma significativa, por isso, aconselhamos que a deixe activa para proteger a sua rede.

Selecione *Enable* [Activar] e clique no botão **SAVE SETTINGS** [Guardar Definições] para abrir os submenus da firewall (consulte a Figura 1).

FIGURA 1. Enabling Firewall screen [Ativação do ecrã firewall]

Security Settings (Firewall)

The Device provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

Enable or disable Firewall features :
 ☐ Enable
 ☒ Disable

SAVE SETTINGS

FIREWALL >> CONTROLO DE ACESSO

O item do menu **ACCESS CONTROL** [Controlo de Acesso] permite que os utilizadores definam o tráfego de saída permitido ou não permitido através da interface WAN. A predefinição consiste em permitir todo o tráfego de saída.

FIGURA 2. Access Control configuration on Firewall section [Configuração do Controlo de acesso na Secção firewall]

Access Control

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

• Enable Filtering Function :
 ☒ Yes
 ☐ No

• Normal Filtering Table (up to 10 computers)

Rule Description	Client PC IP Address	Client Service	Schedule Rule	Configure
Add PC				

HELP
 SAVE SETTINGS
 CANCEL

TABELA 1. Lista de campos no menu de comandos do Controlo de acesso

PARÂMETRO	DESCRIÇÃO
Enable Filtering Function [Activar Função de Filtra-]	Clique em Yes [sim] para ligar a função de filtragem

TABELA 1. Lista de campos no menu de comandos do Controlo de acesso

PARÂMETRO	DESCRIÇÃO
gem]	
<i>Normal Filtering Table</i>	<i>Apresenta um resumo das regras de filtragem configuradas</i>
[Tabela de filtragem normal]	

Para adicionar um computador à tabela de filtragem:

- Clique no botão **Add PC** [Adicionar Computador] no ecrã Access Control [Controlo de acesso]
- Defina as definições adequadas para os serviços do computador cliente
- Clique no botão **OK** e, em seguida, clique no botão **SAVE SETTINGS** [guardar definições] para guardar as suas definições.

FIGURA 3. Insertion of new access limitation on Access Control [Introdução de uma nova limitação de acesso no Controlo de Acesso]

Access Control Add PC

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

- Rule Description:
- Client PC IP Address: 192.168.1. ~
- Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	☐
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
Telnet Service	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☐
NetMeeting	H.323, TCP Port 1720, 1503	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐
VPN-PPTP	TCP Port 1723	☐
VPN-L2TP	UDP Port 1701	☐
TCP	All TCP Port	☐
UDP	All UDP Port	☐

User Define Service
Protocol: ☐ TCP ☐ UDP
Port Range: ~ , ~ , ~ , ~ ,
 ~
- Scheduling Rule (Ref. Schedule Rule Page):

FIREWALL >> FILTRO MAC

O Router também pode limitar o acesso de anfitriões dentro da rede de área local (LAN). **A Tabela de filtragem MAC** permite ao Router introduzir até 32 endereços MAC aos quais não seja permitido aceder à porta WAN. Tenha em atenção que este filtro aplica-se apenas a clientes Ethernet.

FIGURA 4. MAC Filter configuration on MAC Filter Table Command
[Configuração do filtro MAC no comando da Tabela de filtragem MAC]

MAC Filtering Table

This section helps provides MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.

• MAC Address Control : ☐ Yes ☒ No

• MAC Filtering Table (up to 32 computers)

ID	MAC Address					
1		:		:		:
2		:		:		:
3		:		:		:
4		:		:		:
5		:		:		:
6		:		:		:
7		:		:		:
8		:		:		:
9		:		:		:
10		:		:		:
11		:		:		:
12		:		:		:
13		:		:		:
14		:		:		:
15		:		:		:
16		:		:		:
17		:		:		:
18		:		:		:
19		:		:		:
20		:		:		:
21		:		:		:
22		:		:		:
23		:		:		:
24		:		:		:
25		:		:		:
26		:		:		:
27		:		:		:
28		:		:		:
29		:		:		:
30		:		:		:
31		:		:		:
32		:		:		:

DHCP Client List: ip=192.168.1.2 name=SCOUTING-WIFI
COPY TO 1

HELP SAVE SETTINGS CANCEL

O significado dos campos é apresentado na Tabela 2

TABELA 2. Lista de campos na Tabela de filtragem MAC

PARÂMETRO	DESCRIÇÃO
<i>MAC Address Control</i> [Controlo de Acesso MAC]	<i>Selecione enable [activar] ou disable [desactivar] para esta função</i>
<i>MAC Filtering Table</i> [Tabela de Filtragem MAC]	<i>Introduza o endereço MAC no campo fornecido</i>
<i>DHCP Client List</i> [lista de clientes DHCP]	<i>Utilize este menu suspenso para copiar, de forma rápida, os clientes actualmente associados para a tabela</i>

FIREWALL >> BLOQUEIO DE URL

O Router permite que o utilizador bloqueie o acesso a websites através da introdução do endereço de URL completo ou de apenas uma palavra-chave. Esta funcionalidade pode ser utilizada para proteger as crianças do acesso a websites violentos ou de pornografia.

FIGURA 5. URL Blocking menu [Menu de bloqueio de URL]

URL Blocking

Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	
Site 13		Site 28	
Site 14		Site 29	
Site 15		Site 30	

CLEAR ALL

HELP SAVE SETTINGS CANCEL

Poderá definir até 30 sites.

FIREWALL >> REGRA PROGRAMADA

É possível filtrar o acesso à Internet dos clientes locais com base em regras. Cada regra de controlo de acesso pode ser activada num momento agendado.

Defina a agenda no ecrã **Schedule Rule** [Regra Programada] e aplique a regra no ecrã Access Control [Controlo de Acesso].

FIGURA 6. Schedule Rule [Regra programada]

Schedule Rule

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

• Schedule Rule Table (up to 10 rules)

Rule Name	Rule Comment	Configure
No Valid Schedule Rule !!!		

[Add Schedule Rule](#)

HELP SAVE SETTINGS CANCEL

Siga estes passos para adicionar uma regra programada:

- Seleccione o item *Add Schedule Rule* [Adicionar Regra Programada] no ecrã Schedule Rule [Regra Programada]
- Defina as definições adequadas para a regra programada
- Clique no botão **OK** e, em seguida, clique no botão **SAVE SETTINGS** [guardar definições] para guardar as suas definições.

FIGURA 7. Editing of Schedule Rule [Edição da regra programada]

Edit Schedule Rule

Name:

Comment:

Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	:	:
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:

FIREWALL >> DETECÇÃO DE INTRUSÃO

É utilizado para detectar e bloquear ataques comuns de piratas informáticos. A funcionalidade principal da firewall é o *SPI (Stateful Packet Inspection)* que suporta várias aplicações que utilizam números de porta. No menu desta secção existem diversos campos:

- Intrusion Detection Feature [Funcionalidade de Detecção de Intrusão]**

Intrusion Detection Stateful Packet Inspection (SPI) and Anti-DoS firewall protection [Detecção de Intrusão com Stateful Packet Inspection (SPI) e Anti-DoS para a protecção da firewall] (Predefinição: Activado)

A funcionalidade de Detecção de Intrusão do Router limita o acesso para tráfego de entrada na porta WAN. Quando a funcionalidade SPI está ligada, todo o tráfego de entrada na porta WAN será bloqueado, excepto os tipos definidos na secção Stateful Packet Inspection

RIP Defect (Predefinição: Desactivado)

Se um pedido de pacote RIP não for reconhecido pelo router, o mesmo irá permanecer na fila de espera de entrada e não será transferido. Os pacotes acumulados podem fazer com que as filas de espera de entrada fiquem cheias, provocando graves problemas para todos os

protocolos. A activação desta funcionalidade previne a acumulação de pacotes.

Discard Ping to WAN (Predefinição: Activado)

Previne o encaminhamento de um ping na porta WAN do Router para a rede.

• Stateful Packet Inspection

É denominado por pacote de inspecção “completa” porque examina os conteúdos do pacote para determinar o estado das comunicações; isto é, assegura-se de que o computador de destino pediu previamente a comunicação actual. Esta é uma forma de assegurar que todas as comunicações são iniciadas pelo computador receptor e que ocorrem apenas com fontes conhecidas e de confiança a julgar por interações anteriores. Para além de ser mais rigoroso na inspecção dos pacotes, as firewalls de inspecção completa também fecham portas até que seja pedida uma ligação a uma porta específica.

Quando são verificados determinados tipos de tráfego, só serão permitidos os tipos de tráfego especificamente iniciados pela LAN interna. Por exemplo, se o utilizador assinalar apenas “serviço FTP” na secção Stateful Packet Inspection, todo o tráfego de entrada será bloqueado excepto as ligações FTP iniciadas a partir da LAN local.

A Stateful Packet Inspection permite-lhe seleccionar diferentes tipos de aplicações que estejam a utilizar números de portas dinâmicas. Se pretender utilizar a Stateful Packet Inspection (SPI) para bloquear pacotes, clique no botão Yes [sim] no tipo de inspecção de que necessita, tal como Packet Fragmentation [Fragmentação de Pacotes], TCP connection [Ligação TCP], UDP Session [Sessão UDP], FTP Service [Serviço FTP], H.323 Service [Serviço H.323], ou TFTP Service [Serviço TFTP].

FIGURA 8. Intrusion detection panel [Painel de Detecção de Intrusão]

Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Device will support full operation as initiated from the local LAN.

The Device firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

Intrusion Detection Feature

SPI and Anti-DoS firewall protection	☒
RIP defect	☐
Discard Ping To WAN Interface	☒

Stateful Packet Inspection

Packet Fragmentation	☒
TCP Connection	☒
UDP Session	☒
FTP Service	☒
H.323 Service	☒
TFTP Service	☒

When hackers attempt to enter your network, we can alert you by e-mail

Your E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :

Connection Policy

Fragmentation half-open wait: secs

TCP SYN wait: sec.

TCP FIN wait: sec.

TCP connection idle timeout: sec.

UDP session idle timeout: sec.

H.323 data channel idle timeout: sec.

DoS Detect Criteria:

Total incomplete TCP/UDP sessions HIGH: session

Total incomplete TCP/UDP sessions LOW: session

Incomplete TCP/UDP sessions (per min) HIGH: session

Incomplete TCP/UDP sessions (per min) LOW: session

Maximum incomplete TCP/UDP sessions number from same host:

Incomplete TCP/UDP sessions detect sensitive time period: msec.

Maximum half-open fragmentation packet number from same host:

Half-open fragmentation detect sensitive time period: msec.

Flooding cracker block time: sec.

[HELP](#) [SAVE SETTINGS](#) [CANCEL](#)

Desloque-se para baixo para consultar mais informações.

- **When hackers attempt to enter your network, we can alert you by e-mail.** [Quando piratas informáticos tentarem aceder à sua rede, podemos alertá-lo por e-mail.]

Introduza o seu endereço de e-mail. Especifique os seus servidores STMP e POP3, nome de utilizador e password.

- **Connection Policy** [Política de Ligação]

Introduza os valores para sessões TCP / UDP adequados, tal como é descrito na seguinte tabela.

TABELA 3. Lista de valores para sessões TCP/UDP

PARÂMETRO	PREDEFINIÇÕES	DESCRIÇÃO
<i>Fragmentation half-open wait</i> [tempo de espera de fragmentação meio aberta]	10 s	<i>Configura o número de segundos que a estrutura de estado de um pacote permanece activa. Quando o valor do tempo de espera expira, o router larga o pacote não recebido, libertando a estrutura para ser utilizada por outro pacote.</i>
<i>TCP SYN wait</i> [tempo de espera TCP SYN]	30 s	<i>Define o período de tempo durante o qual o software espera que uma sessão TCP sincronize antes de a largar.</i>
<i>TCP FIN wait</i> [tempo de espera TCP FIN]	5 s	<i>Especifica o período de tempo durante o qual uma sessão TCP será mantida depois de a firewall detectar um pacote FIN</i>
<i>TCP connection idle timeout</i> [tempo de espera de inactividade da ligação TCP]	3 600 s	<i>O período de tempo durante o qual uma sessão TDP será gerida se não existir actividade</i>
<i>UDP session idle timeout</i> [tempo de espera de inactividade da sessão UDP]	30 s	<i>O período de tempo durante o qual uma sessão UDP será gerida se não existir actividade</i>
<i>H.323 data channel idle timeout</i> [tempo de espera de inactividade do canal de dados H.323]	180 s	<i>O período de tempo durante o qual uma sessão H.323 será gerida se não existir actividade</i>

- **DoS criteria and port scan criteria** [Critérios DoS e critérios de procura de portas]

Defina os critérios DoS e de procura de portas nos espaços fornecidos (tal como é demonstrado na Tabela 4)

TABELA 4. Lista de valores dos parâmetros DoS

PARÂMETRO	PREDEFINIÇÕES	DESCRIÇÃO
<i>Total incomplete TCP / UDP session HIGH</i> [Sessão TCP / UDP incompleta total ELEVADO]	300 sessões	<i>Define a quantidade de sessões novas não estabelecidas que irá fazer com que o software comece a eliminar as sessões meio abertas</i>
<i>Total incomplete TCP / UDP session LOW</i> [Sessão TCP / UDP incompleta total BAIXO]	250 sessões	<i>Define a quantidade de sessões novas não estabelecidas que irá fazer com que o software pare de eliminar as sessões meio abertas</i>
<i>Total incomplete TCP / UDP session (per min) HIGH</i> [Sessão TCP / UDP incompleta total (por minuto) ELEVADO]	250 sessões	<i>Número máximo de sessões TCP / UDP incompletas permitidas por minuto</i>
<i>Total incomplete TCP / UDP session (per min) LOW</i> [Sessão TCP / UDP incompleta total (por minuto) BAIXO]	200 sessões	<i>Número mínimo de sessões TCP / UDP incompletas permitidas por minuto</i>
<i>Incomplete TCP / UDP sessions detect sensitive time period</i> [Sessões TCP / UDP incompletas detecção de período de tempo]	300 msec	<i>Período de tempo que antecede uma sessão TCP / UDP incompleta do mesmo anfitrião</i>
<i>Maximum half-open fragmentation packet number from same host</i> [Número máximo de pacotes de fragmentação meio abertos do mesmo anfitrião]	30	<i>Número máximo de pacotes de fragmentação meio abertos do mesmo anfitrião.</i>
<i>Half-open fragmentation detect sensitive time period</i> [Fragmentação meio aberta detecção de período de tempo]	10 000 msec	<i>Período de tempo que antecede a detecção de uma sessão de fragmentação meio aberta</i>
<i>Flooding cracker block time</i> [tempo de bloqueio de um flooding cracker]	300 s	<i>Período de tempo decorrido entre a detecção de um flood attack e o bloqueio do mesmo.</i>



A firewall não afecta o desempenho do sistema de forma significativa, por isso, aconselhamos que active as funcionalidades de prevenção e que as mantenha nas suas predefinições para proteger a sua rede

FIREWALL >> DMZ

Se tiver um computador cliente que não consiga correr devidamente uma aplicação de Internet por trás da firewall, pode permitir que o cliente tenha um acesso à Internet de duas vias não restrito. Introduza o endereço de IP de um

anfitrião **DMZ (zona desmilitarizada)** neste ecrã. A adição de um cliente à DMZ pode expor a sua rede local a vários riscos de segurança, por isso, utilize esta opção apenas como último recurso.

FIGURA 9. DMZ settings [Definições DMZ]

DMZ(Demilitarized Zone)

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

Enable DMZ: ☐ Yes ☒ No

Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

Public IP Address					Client PC IP Address	
1.	0	0	0	0	192.168.1.	0
2.	0	0	0	0	192.168.1.	0
3.	0	0	0	0	192.168.1.	0
4.	0	0	0	0	192.168.1.	0
5.	0	0	0	0	192.168.1.	0
6.	0	0	0	0	192.168.1.	0
7.	0	0	0	0	192.168.1.	0
8.	0	0	0	0	192.168.1.	0

[HELP](#) [SAVE SETTINGS](#) [CANCEL](#)

Secção UPnP

A arquitectura *Universal Plug and Play* [“Usar e Ligar” Universal] fornece uma conectividade de rede posto-a-posto generalizada nos computadores de todos os factores de forma, aparelhos inteligentes e dispositivos sem fios. O **UPnP** possibilita uma rede de proximidade sem interrupções, para além de controlo e transferência de dados entre os dispositivos da rede no escritório, em casa e em qualquer local dentro da sua rede.

A Figura 1 apresenta o item do menu **UPnP**.

FIGURA 1. Universal Plug and Play (UPnP) menu [Menu “Usar e Ligar” Universal]

UPnP(Universal Plug and Play) Setting

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the home, office and everywhere in between.

Enable or disable UPnP module function : ☐ Enable ☒ Disable

O UPnP permite que o dispositivo automaticamente:

- adira a uma rede
- obtenha endereços de IP
- transmita as suas capacidades e reconheça a presença e as capacidades de outros dispositivos

Selecione a opção *Enable* [Activar] e, em seguida, clique no botão **SAVE SETTINGS** [guardar definições] para activar esta função.

Secção QoS

A função **QoS (Quality of Service)** [Qualidade de Serviço] permite-lhe diferenciar entre os tipos de tráfego e fornecer um serviço de reencaminhamento de prioridade elevada para aplicações tais como VOIP ou jogos.

Através deste item do menu, poderá classificar o tráfego de aplicações e oferecer-lhes serviços diferenciados (consulte a Figura 1).

FIGURA 1. QoS Settings Main panel [Painel principal de Definições QoS]

QoS Settings

The bandwidth gap between LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming, and VPN. This QoS function allows users to classify traffic of applications and provides them with differentiated services (Diffserv).

Enable or disable QoS module function : ☐ Enable ☒ Disable

Diffserv Forwarding Groups :

Below shows the Diffserv forwarding behaviors this router supports. User can further configure the bandwidth allocation of each forwarding behavior.

Name	Description	Priority	Bandwidth Allocation	
			Minimum	Allow More
BE	Best Effort forwarding	Lowest	0 %	☒
AF1x	Assured Forwarding, provides delivery of packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence.	Low ↑ ↓ High	0 %	☒
AF2x			0 %	☒
AF3x			0 %	☒
AF4x			0 %	☒
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.	Highest	0 %	☒

HELP

SAVE SETTINGS

CANCEL

Na Tabela 1 é apresentada uma lista dos parâmetros presentes no painel de Definições QoS.

TABELA 1. Lista de parâmetros do menu de Definições QoS

PARÂMETRO	DESCRIÇÃO
Enable or disable QoS module function [Activar ou desactivar a função do módulo QoS]	<i>Seleccione enable [activar] ou disable [desactivar] para esta função</i>
BE	<i>Encaminhamento Best Effort [melhor esforço], defina a percentagem</i>

TABELA 1. Lista de parâmetros do menu de Definições QoS

PARÂMETRO	DESCRIÇÃO
	<i>para este tipo de QoS.</i>
AF1x	<i>Defina a percentagem para quatro tipos diferentes de Assured Forwarding [Encaminhamento Garantido].</i>
AF2x	
AF3x	
AF4x	
EF	<i>Expedited Forwarding [Encaminhamento Expedito], tem como objetivo fornecer um atraso reduzido, uma variação de atraso reduzida e uma baixa perda de pacotes</i>

QoS >> MAPEAMENTO DE TRÁFEGO

Este painel serve para classificar o tráfego em grupos de encaminhamento Diffserv e VC de saída. A Figura 2 apresenta o painel Traffic Mapping [Mapeamento de Tráfego] no qual é referido um conjunto de regras aplicadas.

FIGURA 2. Traffic Mapping Menu [Menu de Mapeamento de Tráfego]

Traffic Mapping

Up to 16 rules can be defined to classify traffic into Diffserv forwarding groups and outgoing VCs.

Rule Name	Traffic Description	Map to Diffserv	Outgoing VC	Configure
No Traffic Mapping was defined, all traffic is mapped to BE				
Add traffic class				

Clique no botão **Add traffic class** [Adicionar Classe de Tráfego] para adicionar uma nova classe de tráfego. A Figura 3 apresenta a introdução de uma nova classe de tráfego.

FIGURA 3. Editing / insertion of Traffic Class [Edição / introdução de uma Classe de tráfego]

Edit Traffic Class

This page is for user to specify a classify rule. First, define the class by the traffic type and the local and remote addresses. Then set the Diffserv forwarding group this class is mapped to. Finally, select the outgoing VC that traffic of this class would be routed to.

Rule Name		
Traffic Type	Any v	ADVANCED CONFIG
Map to Forwarding Group	BE v	Remark DSCP as BE (000000 00) v
Direct to VC	By Routing v	

QoS >> ESTATÍSTICAS DE TRÁFEGO

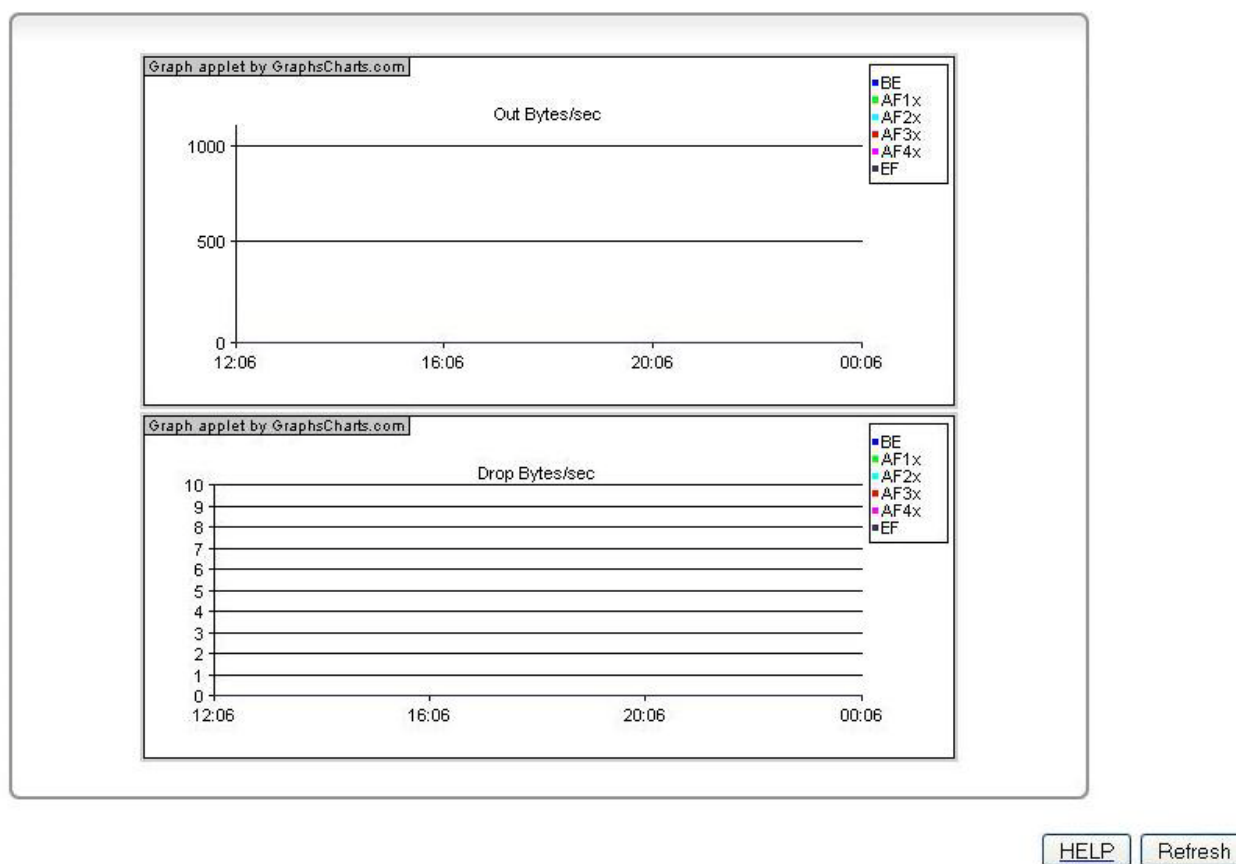
Este ecrã apresenta as estatísticas do tráfego de saída WAN de todos os grupos de reencaminhamento Diffserv nas últimas 12 horas.

A Figura 4 apresenta as estatísticas de tráfego através de gráficos.

FIGURA 4. Traffic Statistics graphic report menu [Menu de relatório gráfico de Estatísticas de tráfego]

Traffic Statistics

This page shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours (automatically update every 5 mins).



Clique no botão **Refresh** [actualizar] para actualizar os gráficos.

Secção ADSL

A **ADSL (Asymmetric Digital Subscriber Line)** [Linha de Subscrição Digital e Assimétrica] foi criada para proporcionar uma maior largura de banda para o downstream (do escritório central até ao local do cliente) do que para o upstream. Esta secção (consulte a Figura 1) é utilizada para configurar o tipo de funcionamento ADSL e apresenta o estado da ADSL.

FIGURA 1. ADSL Parameter panel [Painel de Parâmetros ADSL]

ADSL Parameters and Status

This page displays ADSL-related parameters and status.

ADSL >> PARÂMETROS

Este item de menu permite-lhe especificar os standards de funcionamento ADSL que pretende utilizar. Pode definir explicitamente um standard específico, ou seleccionar “Automatic” [Automático] para negociar automaticamente com DSLAM remoto.

A Figura 2 apresenta a selecção de standards ADSL no menu **ADSL Parameter** [Parâmetro ADSL].

FIGURA2. ADSL Parameter panel [Painel de Parâmetros ADSL]

ADSL Parameter

This page allows you to specify the ADSL standards to operate with. You may explicitly set a specific standard, or choose "Automatic" to automatically negotiate with remote DSLAM.

Operation Mode:

Automatic

HELP

SAVE SETTINGS

RETRAIN

A Tabela 1 explica o significado dos valores do menu de parâmetros ADSL.

TABELA 1. Modos de funcionamento (ADSL)

PARÂMETRO	DESCRIÇÃO
Operation Mode [Modo de Funcionamento]	• <i>Automático</i> • <i>G.992.1 (G.DMT)</i> • <i>G.992.3 (ADSL2)</i> • <i>G.992.5 (ADSL2+)</i> • <i>G.992.3 Annex-M</i> • <i>G.992.5 Annex-M</i>

ADSL >> ESTADO

O ecrã Status [Estado] apresenta informação sobre o estado da linha de ligação, a velocidade de transmissão dos dados, dados de funcionamento, indicação de defeitos e estatísticas.

FIGURA 3. ADSL Status panel [Painel de Estado ADSL]

Monitoring Index:

• ADSL Status Information:

- [Status](#)
- [Data Rate Information](#)
- [Defect/Failure Indication](#)
- [Statistics](#)

• Status:

	Configured	Current
Line Status	---	IDLE
Link Type	---	---

• [\[Go Top\]](#)

• Data Rate:

Stream Type	Actual Data Rate
Upstream	0 (Kbps.)
Downstream	0 (Kbps.)

[\[Go Top\]](#)

• Operation Data / Defect Indication:

Operation Data	Upstream	Downstream
Noise Margin	0.0 dB	0.0 dB
Attenuation	0.0 dB	0.0 dB

Indicator Name	Near End Indicator	Far End Indicator
Output Power	0 dBm	0 dBm
Fast Path FEC Correction	NA	NA
Interleaved Path FEC Correction	0	0
Fast Path CRC Error	NA	NA
Interleaved Path CRC Error	0	0
Loss of Signal Defect	0	0
Fast Path HEC Error STR	NA	NA
Interleaved Path HEC Error	0	0
Error Per Sec.	0	0

• [\[Go Top\]](#)

• Statistics:

Received Cells	0
Transmitted Cells	0

• [\[Go Top\]](#)

REFRESH

Para mais informações, consulte a parte inferior da página.

TABELA 2. Lista de parâmetros do menu de estado ADSL

PARÂMETRO	DESCRIÇÃO
Status [Estado]	
<i>Line status</i> [Estado da linha]	<i>Apresenta o estado actual da ligação da linha ADSL</i>
<i>Link type</i> [Tipo de ligação]	<i>Indica o tipo de ligação</i>
Data Rate [Velocidade de transmissão dos Dados]	
<i>Upstream</i> [Transmissão]	<i>Velocidade máxima de transmissão de dados</i>
<i>Downstream</i> [Recepção]	<i>Velocidade mínima de transmissão de dados</i>
Operation Data / Defect Indication [Dados de Funcionamento / Indicação de Defeitos]	
<i>Noise Margin</i> [Margem de Ruído]	<i>Margem de ruído máxima de upstream e downstream</i>
<i>Attenuation</i> [Atenuação]	<i>Redução máxima na potência do sinal de upstream e downstream</i>
<i>Fast Path FEC Correction</i> [Acesso Rápido à Correção FEC]	<i>Podem ser utilizados dois caminhos de latência: rápido e entrelaçado. Para ambos os caminhos, é aplicado um esquema de correção antecipada de erros (FEC) para garantir uma maior integridade dos dados. Para uma maior imunidade ao ruído, pode ser utilizado um dispositivo de intercalação para auxiliar a FEC</i>
<i>Fast Path CRC Error</i> [Erro CRC de Acesso Rápido]	<i>O número de erros de Controlo de Redundância Cíclica de Acesso Rápido</i>
<i>Interleaved Path CRC Error</i> [Erro CRC de Caminho Entrelaçado]	<i>O número de erros de Controlo de Redundância Cíclica de Caminho Entrelaçado</i>
<i>Loss of Signal Defect</i> [Defeito de Perda de Sinal]	<i>Descontinuidades de sinal momentâneas</i>
<i>Fast Path HEC Error</i> [Erro HEC de Acesso Rápido]	<i>Fast Path Header Error Concealment errors [Erro de Ocultação de Erros no Cabeçalho]</i>
<i>Interleaved Path HEC Error</i> [Erro HEC de Caminho Entrelaçado]	<i>Interleaved Path Header Error Concealment errors [Erros de Ocultação de Erros no Cabeçalho de Caminho Entrelaçado]</i>
Statistics [Estatísticas]	
<i>Received Cells</i> [Células Recebidas]	<i>Número de células recebidas</i>
<i>Transmitted Cells</i> [Células Enviadas]	<i>Número de células enviadas</i>

Secção DDNS

Nesta secção, pretende-se descrever a utilização e as definições da funcionalidade DDNS: A funcionalidade *DDNS* permite efectuar uma actualização externa e dinâmica de uma zona específica por outros anfitriões ou processos. O router pode enviar uma actualização de registo para o servidor DNS apropriado com base no nome NetBIOS DHCP do cliente. A actualização ocorre após a negociação da alocação do endereço de IP e é removida quando essa alocação expira.

Ao seleccionar o item do menu **DDNS** (consulte a Figura 1), será possível ligar Nome de Domínio estático a um endereço de IP dinâmico. Para tirar proveito desta característica, é necessário obter uma conta, uma password e um nome de domínio estático de um Fornecedor de Serviços DDNS (este router suporta serviços DDNS de www.dyndns.org e www.tzo.com).

FIGURA 1. DDNS Panel [Painel DDNS]

DDNS (Dynamic DNS) Settings

DDNS allows users to map a static Domain Name to a dynamic IP address. However, You must get an account, password, and your static Domain Name from a DDNS service provider. This router supports DDNS services from www.dyndns.org and www.tzo.com.

Dynamic DNS	☐ Enable ☒ Disable
Provider	DynDNS.org ▼
Domain Name	
Account / E-mail	admin
Password / Key	•••••

[HELP](#)
[SAVE SETTINGS](#)
[CANCEL](#)

Após a criação da conta do Fornecedor de Serviços DDNS, clique no botão *Enable* [Activar], seleccione o nome do Fornecedor na lista suspensa *Provider* [Fornecedor] e preencha correctamente os campos *Domain Name* [Nome de Domínio], *Account / E-mail* [Conta/E-mail] e *Password / Key* [Password/Chave].

A funcionalidade DDNS ficará activa depois de clicar no botão **SAVE SETTINGS** [Guardar Definições] e depois da autenticação do Fornecedor de Serviços.

Secção Ferramentas

Nesta secção, pretende-se descrever a utilização de um conjunto de ferramentas criadas para gerir as cópias de segurança, a restauração, a reiniciação e a actualização do firmware do router através dos submenus **Configuration Tools** [Ferramentas de Configuração], **Firmware Upgrade** [Actualização de Firmware] e **Reset** [Reiniciação].

FIGURA 1. Tools Main panel [Painel principal de Ferramentas]

Tools Settings

This page allows you to backup, restore, reset, and upgrade the router's firmware.

FERRAMENTAS >> FERRAMENTAS DE CONFIGURAÇÃO

Ao seleccionar o item do menu **Tools >> Configuration Tools** [Ferramentas >> Ferramentas de Configuração] (consulte a Figura 1), poderá fazer cópias de segurança e restaurar tarefas, clicando no botão correspondente:

- “**Backup Router Configuration**” [Configuração das Cópias de Segurança do Router]: ao clicar neste botão, poderá fazer uma cópia de segurança da configuração actual do router num ficheiro com o nome “*backup.bin*” no seu computador. Para tal, clique primeiro no botão **Next>>** [Seguinte] e, em

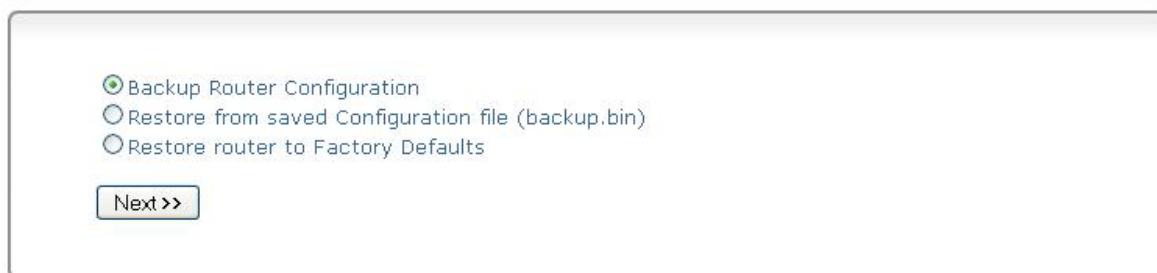
seguida, no botão **Save** [Guardar] para guardar, numa pasta do computador à sua escolha, o ficheiro backup.bin.

- “**Restore from saved Configuration file (backup.bin)**” [Restaurar a partir de um ficheiro de Configuração guardado (backup.bin)]: ao clicar neste botão, poderá restaurar uma configuração do router guardada anteriormente (a partir de um ficheiro backup.bin). Clique no botão **Next>>** [Seguinte] e introduza o caminho e o nome do ficheiro backup.bin, ou clique no botão **Browse...** [Procurar...] para procurar nas pastas do seu computador. Após seleccionar o ficheiro backup.bin correcto, clique no botão **APPLY** [Aplicar]: uma mensagem instantânea pedir-lhe-á para confirmar a restauração.
- “**Restore router to Factory Defaults**” [Restaurar as predefinições do router]: ao clicar neste botão, poderá forçar o router a fazer uma reiniciação e a restaurar as definições originais de fábrica. Clique no botão **APPLY** [Aplicar]: uma mensagem instantânea pedir-lhe-á para confirmar a restauração das predefinições.

FIGURA 2. Configuration Tools panel [Painel das Ferramentas de Configuração]

Configuration Tools

Use the "Backup" tool to save the router's current configuration to a file named backup.bin" on your PC. You can then use the "Restore" tool to restore the saved configuration to the router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the router to perform a power reset and restore the original factory settings.



FERRAMENTAS >> ACTUALIZAÇÃO DE FIRMWARE

Ao seleccionar o item do menu **Tools >> Firmware Upgrade**[Ferramentas >> Actualização de Firmware] (consulte a Figura 3), poderá efectuar o upgrade do firmware do router utilizando um ficheiro fornecido pelo fabricante.

Introduza o caminho e o nome do ficheiro de firmware, ou clique no botão **Browse...** [Procurar...] para procurar nas pastas do seu computador; em seguida, clique no botão **BEGIN UPGRADE** [Iniciar Upgrade]. Uma mensagem instantânea pedir-lhe-á para confirmar o processo de upgrade.

FIGURA 3. Firmware Upgrade panel [Painel de Upgrade de Firmware]

Firmware Upgrade

This tool allows you to upgrade the router firmware using a file provided by us. You can download the latest firmware from the related web site

Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process.

FERRAMENTAS >> REINICIAR

Ao seleccionar o item do menu **Tools >> Reset** [Ferramentas >> Reiniciar] (consulte a Figura 4), poderá efectuar uma reiniciação caso o router deixe de responder correctamente ou, por algum motivo, deixe de funcionar correctamente. As definições do router não serão alteradas.

Para efectuar uma reiniciação, clique no botão **REBOOT ROUTER** [Reiniciar Router] abaixo. Ser-lhe-á pedido para confirmar a sua decisão. A reiniciação estará terminada quando a luz da alimentação deixar de estar intermitente.

FIGURE 1 Reset panel [Painel de Reiniciação]

Reset

In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking.

Secção Estado

Nesta secção, pretende-se apresentar o estado de ligação das interfaces WAN/LAN do Dispositivo, os números da versão de firmware e de hardware, quaisquer tentativas de aceder ilegalmente à sua rede, assim como informações sobre todos os computadores cliente DHCP ligados à sua rede.

Nesta página, uma primeira área de **Status** [Estado] (consulte a Figura 1) contém informação sobre:

- *Current Time* [Hora Actual]: indica a hora e data da página apresentada;
- *INTERNET*: indica o tipo e o estado da ligação WAN e se o uplink IPv6 se encontrar estabelecido, apresenta ainda o endereço e Prefixo IPv6 correspondentes;
- *GATEWAY* [Porta de Ligação]: apresenta as definições de IP do sistema, assim como o estado de DHCP, NAT e Firewall;
- *INFORMATION* [INFORMAÇÃO]: apresenta o número de clientes ligados, assim como os números da versão de hardware e de firmware do Dispositivo.

FIGURA 1. Status Panel [Painel de Estado]

Status

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 08/01/2003 00:02:19 am

INTERNET

ADSL: CONNECTED
WAN IP: 10.0.0.20
Subnet Mask: 255.0.0.0
Gateway: 10.0.0.1
IPv6 Address:
2001:05c0:1502:ca20:0223:8eff:feeb:295b
Prefix: 2001:05c0:1502:ca20::/64
Primary DNS: 10.0.0.1
Secondary DNS: 0.0.0.0

GATEWAY

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled
FIREWALL: Disabled
UPnP: Disabled
WIRELESS: Enabled

INFORMATION

Numbers of DHCP Clients: 1
Runtime Code Version:
0.99.13b1-PT_TR069_AnnexM (Jan 25 2010
10:00:28)
Boot Code Version: V0.02.06
ADSL Modem Code Version: 3.4.3.13.0.1A
LAN MAC Address: 00-23-8E-EB-29-5A
WAN MAC Address: 00-23-8E-EB-29-5B
Wireless MAC Address: 00-23-8E-EB-29-5A
Hardware Version: R0B
Serial Num: J939000064

Disconnect

A área **WLAN Status** [Estado da WLAN] (consulte a Figura 2) é utilizada para apresentar a Configuração e o Estado da WLAN.

FIGURA 2. WLAN Status Panel [Painel de Estado da WLAN]

WLAN Status

SSID	Wireless Module function	Channel	SSID Broadcast	Encryption Type
PBS-EB295A	Enable	AUTO	Enable	WPA Only

- A área **ATM PVC** (consulte a Figura 3) apresenta, para cada VC activado, a sua configuração: *VPI/VCI*, *Encapsulation* [Encapsulamento], *Protocol* [Protocolo], *IP Address* [Endereço de IP] (se o uplink IPv6 for estabelecido, também é apresentado o endereço e Prefixo correspondentes ao IPv6), *Subnet Mask* [Máscara de Sub-rede], *Gateway* [Porta de Ligação], *Primary DNS* [DNS Principal] e *Secondary DNS* [DNS Secundário].

FIGURA 3. ATM PVC Panel [Painel ATM PVC]

VC1	
VPI/VCI	8/35
Encapsulation	LLC
Protocol	PPPoE
IP Address	Down
Subnet Mask	---
Gateway	---
Primary DNS	---
Secondary DNS	---
Disconnect Connect	

VC2
Disabled

VC3
Disabled

VC4
Disabled

A área inferior da parte superior (consulte a Figura 4) apresenta informação sobre:

- *Security Log* [Registo de Segurança]: lista de tentativas de acesso à sua rede local. O registo de dados apresentado pode ser guardado, eliminado ou actualizado através dos botões correspondentes.
- *DHCP Client Log* [Registo do Cliente DHCP]: Lista de clientes DHCP da LAN actualmente ligados ao router. Para cada cliente DHCP é apresentado o endereço IP atribuído, o endereço MAC e o seu nome de utilizador.

FIGURA 4. Security and DHCP Client Log Panel [Painel de segurança e de Registo do Cliente DHCP]

Security Log

View any attempts that have been made to gain access to your network.

08/01/2003	04:37:28	192.168.1.101
08/01/2003	02:50:21	192.168.1.101
08/01/2003	02:06:47	sending ACK to
08/01/2003	02:06:46	sending OFFER
08/01/2003	02:06:42	sending OFFER
08/01/2003	00:02:37	192.168.1.101
08/01/2003	00:01:13	sending ACK to
08/01/2003	00:01:09	sending ACK to
08/01/2003	00:01:09	sending OFFER

Save Clear Refresh

DHCP Client Log

View information on LAN DHCP clients currently linked to the router.

ip=192.168.1.100	mac=00-15-00-1D-EC
ip=192.168.1.101	mac=00-1A-6B-66-A0

HELP

P.DG A1000G

Esta Página foi intencionalmente deixada em branco

Endereçamento de IP

Internet Control Suite [Conjunto de Protocolos de Internet]

O conjunto de protocolos de Internet consiste num grupo bem definido de protocolos de comunicação e em diversos protocolos de aplicação standard. O Protocolo de Controlo de Transmissão/Protocolo Internet (TCP/IP) é, provavelmente, o protocolo mais conhecido e consiste numa combinação de dois dos protocolos (IP e TCP) a trabalhar em conjunto. O TCP/IP é um standard de rede adoptado e suportado internacionalmente que oferece conectividade entre equipamentos de diversos fornecedores, suportando uma grande variedade de tecnologias de rede.

Gestão do Router através da rede

Para gerir um dispositivo através da rede, o Router deve estar correctamente configurado com a seguinte informação de IP:

- Um endereço de IP
- Uma máscara de sub-rede

Endereços de IP e Máscaras de Sub-rede

Cada dispositivo da sua rede tem de ter um endereço de IP único para funcionar correctamente. Um endereço de IP identifica o endereço do dispositivo para o qual estão a ser enviados os dados e o endereço da rede de destino. Os endereços de IP têm o formato n.n.n.x, no qual “n” é um número decimal entre 0 e 255 e “x” é um número entre 1 e 254, inclusive.

Contudo, um endereço de IP não é suficiente para fazer com que o seu dispositivo funcione. Para além do endereço de IP, irá ter de definir uma máscara de sub-rede. Todas as redes estão divididas em sub-redes mais pequenas, sendo que uma máscara de sub-rede é um número que permite ao dispositivo identificar a sub-rede à qual se encontra ligado.

Para que a sua rede funcione correctamente, todos os dispositivos da rede têm de ter:

- O mesmo endereço de sub-rede.
- A mesma máscara de sub-rede.

O único valor que será diferente é o número específico do dispositivo anfitrião. Este valor tem de ser sempre único.

Um exemplo de um endereço de IP é ‘192.168.1.8’. Contudo, o tamanho da rede determina a estrutura deste endereço de IP. Ao utilizar o Router irá, provavelmente, encontrar apenas dois tipos de endereços de IP e estruturas de máscara de sub-rede.

Primeiro Tipo

Numa rede de pequenas dimensões, o endereço de IP de ‘192.168.1.8’ é dividido em duas partes:

- A primeira parte (‘192.168.1’) identifica a rede na qual reside o dispositivo.
- A segunda parte (‘.8’) identifica o dispositivo dentro da rede.

Este tipo de Endereço de IP funciona numa máscara de sub-rede de '255.255.255.0'.

Segundo Tipo

Em redes de maiores dimensões, nas quais existem mais dispositivos, o endereço de IP de '192.168.1.8' está, novamente, dividido em duas partes, mas encontra-se estruturado de forma diferente:

- A primeira parte ('192.168') identifica a rede na qual reside o dispositivo.
- A segunda parte ('.1.8') identifica o dispositivo dentro da rede.

Este tipo de Endereço de IP funciona numa máscara de sub-rede de '255.255.0.0'.

Como é que um Dispositivo Obtém um Endereço de IP e a Máscara de Sub-rede?

Existem três formas diferentes de obter um endereço de IP e a máscara de sub-rede. Que são:

- Endereçamento Dynamic Host Configuration Protocol [Protocolo de Configuração de Anfitrião Dinâmico] (DHCP)
- Endereçamento Estático
- Endereçamento Automático (Endereçamento de IP automático)

Endereçamento DHCP

O Router contém um servidor DHCP, o qual permite aos computadores da sua rede obterem automaticamente um endereço de IP e uma máscara de sub-rede. O DHCP atribui um endereço de IP e uma máscara de sub-rede temporários, os quais são reatribuídos assim que os desligue da rede.

O DHCP funciona em qualquer Sistema Operativo cliente. Para além disso, a utilização de um DHCP significa que o mesmo endereço de IP e máscara de sub-rede nunca serão duplicados para os dispositivos da rede. O DHCP é particularmente útil para redes com um vasto número de utilizadores.

Endereçamento Estático

Tem de introduzir um endereço de IP e a máscara de sub-rede manualmente em todos os dispositivos. A utilização de um IP e de uma máscara de sub-rede estáticos significa que o endereço é atribuído de forma permanente.

Endereçamento de IP Automático

Os dispositivos de rede utilizam o endereçamento de IP automático se estiverem configurados para adquirir um endereço através do DHCP, mas não conseguirem estabelecer contacto com o servidor DHCP. O Endereçamento de IP Automático consiste num esquema no qual os dispositivos atribuem a si mesmos um endereço de IP aleatório da sub-rede standard da indústria de 169.254.x.x (com uma máscara de sub-rede de 255.255.0.0). Se dois dispositivos atribuírem a si mesmos endereços iguais, o conflito é detectado e um dos dispositivos irá atribuir a si mesmo um novo endereço. O suporte de Endereçamento de IP Automático foi introduzido pela Microsoft no sistema operativo Windows 98, sendo também suportado pelo Windows 2000, Windows XP, Vista e Windows 7.

Especificações Técnicas

Esta secção apresenta as especificações técnicas para o **ADB P.DG A1000G**.

Interfaces/Standard

Interface WAN

Porta Nº1 (conector RJ-11, par interno) suporta os seguintes standards:

- ADSL (G.992.1, G992.2, T1.413, G994.1, G.997.1)
- ADSL2 (G.992.3)
- ADSL2+ (G992.5)

O Anexos A/Anexo B estão disponíveis em versões do produto diferentes

Interface LAN

- Portas Ethernet Nº 1 10/100BASE-T (conector RJ-45), em conformidade com a norma IEEE 802.3, com auto MDIX e auto-negociação
- A porta pode ser configurada para ser dedicada ao tráfego de vídeo de/para um STB

Interface LAN Sem Fios

A solução de ponto de acesso Wi-Fi encontra-se em conformidade com os seguintes standards:

- IEEE 802.11b/g
- Segurança: WPA/WPA2 (IEEE 802.11i)
- SSID único
- QoS: WMM (IEEE 802.11e)



Características DSL (ATM)

- ATM (AAL5) formato de carga útil
- Classes de tráfego UBR, VBR-nrt, VBR-rt, CBR
- Até 8 PVC
- HW SAR
- Possibilidade de múltiplas filas de espera físicas (até 8) por classe de tráfego, com suporte para o agendamento com base em prioridades

Protocolo de Encapsulamento WAN

- Bridged/Routed Ethernet sob ATM (RFC 2684 / RFC 1483)
- PPP sobre Ethernet (RFC 2516)
- PPP sobre ATM (RFC 2364)
- IP sobre ATM (RFC 1577)
- MTU configurável - bridging transparente entre dispositivos LAN

Roteamento / Bridging	- NAT/NAPT (com ALG) - QoS de IP - Servidor/Cliente DHCP - Passagem por VPN - IPv4 - DNS relay - NTP - IGMPv2/3 proxy
IPv6	- Double Stack IPv4/IPv6 (PPP RFC suporta: RFC2865, RFC2868, RFC3575)
QoS	- Traffic shaping (camada ATM) - Agendamento com base em prioridade (até 16 filas de espera) - Remarcação DSCP/TOS
Gestão Remota	- DSL Fórum TR-069 - HTTP para o upgrade remoto do firmware - Diagnósticos e LOG - Telnet com CLI - Servidor WEB com páginas de configuração de Admin/Utilizador
Segurança	- Firewall Stateful Packet Inspection (SPI) - Controlo parental
Especificações Ambientais	Temperatura (ETS 300-019-1-3): - Em funcionamento: +0° a 40° C - Desligado: -20° a 65° C Humidade relativa (ETS 300-019-1-3): - Em funcionamento: 10% a 85% sem condensação - Desligado: 5% a 95% sem condensação
Adaptador de Alimentação	- Ficha Europeia - Primária: tensão nominal 100V-240V, 50 Hz; - Secundária: 12Vdc, 0.5A, 6W

Glossário

802.11b

A especificação IEEE para Ethernet sem fios que permite uma velocidade de até 11 Mbps. A norma prevê velocidades de transmissão de dados de 1, 2, 5.5 e 11 Mbps. A velocidade alterna automaticamente consoante o alcance e o ambiente.

802.11g

A especificação IEEE para Ethernet sem fios que permite uma velocidade de até 54 Mbps. A norma prevê velocidades de transmissão de dados de 6, 12, 24, 36, 48 e 54 Mbps. A velocidade alterna automaticamente consoante o alcance e o ambiente.

10BASE-T

A especificação IEEE para Ethernet de 10 Mbps através de cabo de par entrançado de Categoria 3, 4, ou 5.

100BASE-TX

A especificação IEEE para Ethernet de 100 Mbps através de cabo de par entrançado de Categoria 5.

Ponto de Acesso

Um Ponto de Acesso consiste num dispositivo através do qual os clientes sem fios se ligam a outros clientes sem fios, e o qual funciona como uma ponte entre clientes sem fios e uma rede com fios, tal como a Ethernet. Os clientes sem fios podem deslocar-se para qualquer lugar dentro da área de cobertura do ponto de acesso e permanecer ligados uns aos outros. Se estiver ligado a uma rede Ethernet, o ponto de acesso monitoriza o tráfego Ethernet e encaminha mensagens Ethernet adequadas para a rede sem fios, enquanto monitoriza igualmente o tráfego rádio do cliente sem fios e encaminha mensagens do cliente sem fios para a Ethernet LAN.

Modo Ad Hoc

O modo Ad Hoc consiste numa configuração suportada pela maioria dos clientes sem fios. É utilizado para ligar uma rede posto-a-posto sem utilizar um ponto de acesso. Fornece um desempenho inferior ao do modo infra-estrutura, o qual é utilizado pelo router. (consulte também o Modo infra-estrutura).

Auto-negociação

Alguns dispositivos da gama suportam auto-negociação. A auto-negociação sucede quando dois dispositivos que partilham uma ligação se configuram automaticamente para a utilização da melhor velocidade comum. A ordem de preferência (o melhor primeiro) é: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, e 10BASE-T half duplex. A auto-negociação é definida na norma IEEE 802.3 para Ethernet e consiste numa operação que acontece em poucos milissegundos.

Largura de Banda

A quantidade de informação, medida em bits por segundo, que um canal consegue transmitir. A largura de banda de Ethernet é de 10 Mbps, a largura de banda de Ethernet Rápida é de 100 Mbps. A largura de banda para 802.11b sem fios é de 11Mbps.

Cabos de Categoria 5

Uma das cinco categorias de cablagem de Par Entrançado (TP) definidas pela norma EIA/TIA-586. A categoria 5 pode ser utilizada em redes de Ethernet (10BASE-T) e Ethernet Rápida (100BASE-TX) e pode transmitir dados a velocidades de até 100 Mbps. Os cabos de categoria 5 são melhores para uma utilização em cablagem de rede do que os de categoria 3, uma vez que suportam tanto velocidades de Ethernet (10 Mbps) como de Ethernet Rápida (100 Mbps).

Canal

Tal como sucede nos dispositivos de rádio, o router Sem Fios/DSL permite-lhe escolher diferentes canais de rádio no espectro sem fios. Um canal é uma frequência específica dentro do conjunto de 2.4GHz no qual o Router funciona.

Cliente

O termo utilizado para descrever o computador que está ligado à sua rede.

DHCP

Dynamic Host Configuration Protocol [Protocolo de Configuração de Anfitrião Dinâmico] Este protocolo atribui automaticamente um endereço de IP a todos os computadores da sua rede. O Windows 95, Windows 98 e Windows NT 4.0 contêm um software que atribui endereços de IP a estações de trabalho numa rede. Estas atribuições são efectuadas pelo software de servidor DHCP que corre no Windows NT Server, sendo que o Windows 95 e o Windows 98 irão pedir ao servidor que obtenha o endereço. O Windows 98 irá atribuir a si mesmo um endereço caso não seja encontrado um servidor DHCP.

DMZ

DMZ (Zona Desmilitarizada) consiste numa área fora da firewall, a qual permite aos utilizadores remotos acederem a itens na sua rede (websites, download FTP e zona de actualizações, etc.).

Endereço do Servidor DNS

DNS significa Domain Name System [Sistema de Nomes de Domínio], permite aos computadores anfitriões da Internet terem um nome de domínio (tal como adbglobal.com) e um ou mais endereços de IP (tal como 192.168.10.8). Um servidor DNS mantém uma base de dados dos computadores anfitriões e dos respectivos nomes de domínio e endereços de IP, para que quando é pedido um nome de domínio (por exemplo, quando digita "adbglobal.com" no browser de Internet) o utilizador seja enviado para o devido endereço de IP. O endereço do servidor DNS utilizado pelos computadores na sua rede doméstica consiste na localização do servidor DNS que o seu ISP atribuiu.

DSL

Abreviatura de digital subscriber line [linha de assinante digital], mas é vulgarmente utilizada em referências à versão assimétrica da tecnologia (ADSL) que permite o envio de dados através de linhas telefónicas de cobre existentes a velocidade de transferência de 1,5 a 9 Mbps quando são recebidos dados (conhecida por velocidade de downstream) e de 16 a 640 Kbps quando são enviados dados (conhecida por velocidade de upstream). A ADSL necessita de um modem ADSL especial. A popularidade da ADSL está a crescer à medida que mais áreas em todo o mundo obtêm acesso.

Modem DSL

DSL significa digital subscriber line [linha de assinante digital]. Um modem DSL utiliza as linhas telefónicas existentes para enviar e receber dados a altas velocidades.

Encriptação

Trata-se de um método que permite fornecer um maior nível de segurança às transmissões de dados sem fios. O Router utiliza dois níveis de encriptação; 40/64 bits e 128 bits. O nível de encriptação de 128 bits é superior ao de 40/64 bit.

Ethernet

Uma especificação LAN desenvolvida em conjunto pela Xerox, Intel e Digital Equipment Corporation. As redes Ethernet utilizam CSMA/CD para transmitir pacotes a uma velocidade de 10 Mbps através de diversos cabos.

Endereço Ethernet

Consulte o endereço MAC.

Ethernet Rápida

Um sistema de Ethernet concebido para funcionar em velocidades de 100 Mbps.

Firewall

Protecção electrónica que impede que qualquer pessoa fora da sua rede possa ver os seus ficheiros ou danificar os seus computadores.

Full Duplex

Um sistema que permite a transmissão e recepção de pacotes ao mesmo tempo e que duplica, efectivamente, o potencial de produtividade de uma ligação.

IEEE

Institute of Electrical and Electronics Engineers [Instituto dos Engenheiros de Electricidade e de Electrónica]. Esta organização americana foi fundada em 1963 e define normas para computadores e comunicações.

IETF

Internet Engineering Task Force [Grupo da missão de engenharia da Internet]. Trata-se de uma organização responsável pelo fornecimento de soluções de engenharia para redes TCP/IP. Na área da gestão de redes, este grupo é responsável pelo desenvolvimento do protocolo SNMP.

IGMP

O Internet Group Management Protocol [Protocolo de gestão de Grupos] (IGMP) consiste num protocolo de Internet que fornece ao computador com Internet uma forma de comunicar aos routers adjacentes a respectiva filiação ao grupo multicast. O Multicasting permite que um computador com Internet envie conteúdos a múltiplos computadores que se tenham identificado como tendo interesse em receber o conteúdo desse computador. O Multicasting pode ser utilizado para aplicações como a actualização de livros de endereços dos utilizadores de computadores portáteis, o envio de boletins informativos de empresas para uma lista de distribuição, e a "transmissão" de programas de fluxo de media com elevada largura de banda a uma audiência que se tenha "sintonizado" ao definir uma afiliação com um grupo multicast.

Modo infra-estrutura

O modo infra-estrutura consiste numa configuração sem fios suportada pelo Router. Terá de se assegurar de que todos os seus clientes estão definidos para utilizar o modo infra-estrutura, para que possam comunicar com o Ponto de Acesso incorporado no Router. (consulte também o Modo Ad Hoc)

IP

Internet Protocol [Protocolo Internet]. O IP é um protocolo de rede de 3 camadas, tratando-se do protocolo standard para o envio de dados através da rede. O IP faz parte do conjunto de protocolos TCP/IP, os quais descrevem o roteamento de pacotes para dispositivos endereçados. Um endereço de IP consiste em 32 bits (128 bits em IPV6) divididos em dois ou três campos: um número de rede e um número de anfitrião ou um número de rede, um número de sub-rede e um número de anfitrião.

Endereço de IP

Endereço do Protocolo Internet Um identificador único para um dispositivo ligado a uma rede que utiliza TCP/IP. O endereço é escrito em quatro octetos separados por pontos (pontos finais) e é constituído por uma secção de rede, uma secção de sub-rede opcional e uma secção de anfitrião.

IPV6

O Protocolo de comunicação IPV6 visa substituir o IPV4 que só suporta cerca de 4 bilhões (4×10^9) de endereços IP, contra cerca de $3,4 \times 10^{38}$ endereços do novo protocolo. O protocolo está a ser implementado gradualmente e funcionará em simultâneo com o IPV4 sobre *dual stack* para permitir a interoperabilidade destes.

ISP

Internet Service Provider [Fornecedor de Serviço Internet]. Um ISP é uma empresa que fornece ligação à Internet para uso privado ou para empresas ou organizações.

LAN

Local Area Network [Rede de área local]. Trata-se de uma rede de terminais (tais como computadores, impressoras, servidores) e de dispositivos de rede (hubs e switches) que cobre uma área geográfica relativamente pequena (normalmente não é maior do que um piso ou edifício). As LAN são caracterizadas por velocidades de transmissão elevadas em pequenas distâncias (até 1 000 metros).

MAC

Media Access Control [Controlo de Acesso ao Meio]. Consiste num protocolo especificado pelo IEEE para determinar quais são os dispositivos que têm acesso a uma rede a qualquer momento.

Endereço MAC

Endereço do Controlo de Acesso ao Meio. Também denominado por hardware ou endereço físico. Um endereço de camada 2 associado a um dispositivo de rede específico. A maioria dos dispositivos ligados a uma LAN recebe um endereço MAC, uma vez que são utilizados para identificar outros dispositivos numa rede. Os endereços MAC são compostos por 6 bytes.

Mbps

Megabits por segundo.

MDI/MDIX

Em termos de cablagem, os conceitos de recepção e transmissão são vistos do ponto de vista do computador, o qual se encontra ligado como uma Media Dependant Interface [Interface Dependente do Meio] (MDI). Na cablagem MDI, um computador transmite nos pinos 1 e 2. No hub, switch, router ou ponto de acesso, a perspectiva encontra-se revertida e o hub recebe nos pinos 1 e 2. Esta cablagem é referida como um Media Dependant Interface - Crossover [Interface Dependente do Meio - Cruzada] (MDI-X).

NAT

Networks Address Translation [Tradução de Endereços de Rede]. A NAT possibilita que todos os computadores da sua rede partilhem um endereço de IP. A capacidade de NAT do Router permite-lhe aceder à Internet a partir de qualquer computador na sua rede doméstica sem ter de adquirir mais endereços de IP ao seu ISP.

Rede

Uma Rede consiste num conjunto de computadores e outros equipamentos informáticos que se encontram ligados com a finalidade de trocar informações ou partilhar recursos. As redes variam em tamanho, algumas existem dentro de uma única sala, outras estendem-se a vários continentes.

Network Interface Card [Controlador de Interface de Rede] (NIC)

Trata-se de uma placa de circuito instalada numa peça de equipamento informático, por exemplo, um computador, que lhe permite ligá-lo à mesma rede. Um NIC também é conhecido como um adaptador ou placa de rede.

Protocolo

Consiste num conjunto de normas de comunicação entre dispositivos numa rede. As normas ditam a formação, temporização, sequenciação e controlo de erros.

PSTN

Public Switched Telephone Network [Rede Telefónica Pública Comutada].

PPPoA

Point-to-Point Protocol over ATM [Protocolo Ponto-a-Ponto sobre ATM]. O PPP sobre ATM consiste num protocolo para a ligação à Internet de anfitriões remotos através de uma ligação sempre ligada, efectuando a simulação de uma ligação telefónica.

PPPoE

Point-to-Point Protocol over Ethernet [Protocolo Ponto-a-Ponto sobre Ethernet]. O Protocolo Ponto-a-Ponto consiste num método de transmissão de dados originalmente criado para ligações telefónicas; o PPPoE destina-se a ligações Ethernet.

RJ-45

Um conector standard utilizado para ligar redes Ethernet. A sigla “RJ” significa “registered jack”.

Router

Trata-se de um dispositivo que funciona como um hub central ao ligar-se ao controlador de interface de rede de cada computador e gerir o tráfego de dados entre a rede local e a Internet.

Servidor

Trata-se de um computador numa rede que é partilhado por múltiplos terminais. Os servidores fornecem aos terminais acesso a serviços de rede partilhados, tais como ficheiros de computador e filas de espera para impressoras.

SSID

Service Set Identifier [Identificador do Conjunto de Serviços]. Alguns fornecedores de produtos sem fios utilizam SSID de forma intercambiável com ESSID.

Endereço de Sub-rede

Consiste numa extensão do esquema de endereçamento de IP que permite a um site a utilização de um endereço de rede IP único para múltiplas redes físicas.

Máscara de Sub-rede

Uma máscara de sub-rede, que pode fazer parte da informação TCP/IP fornecida pelo seu ISP, é um conjunto de quatro números configurados como um endereço de IP. É utilizada para criar números de endereço de IP que são utilizados apenas dentro de uma rede particular (em oposição aos números de endereço de IP válidos reconhecidos pela Internet, que têm de ser atribuídos pela InterNIC).

Sub-redes

Trata-se de uma rede que é um componente de outra rede de maiores dimensões.

Switch

Consiste num dispositivo que interliga várias LAN para formar uma LAN lógica única que abrange vários segmentos de LAN. Os switches são semelhantes às pontes, na medida em que ligam diferentes tipos de LAN; contudo, ligam um maior número de LAN do que uma ponte e, geralmente, são mais sofisticados.

TCP/IP

Transmission Control Protocol/Internet Protocol [Protocolo de Controlo de Transmissão/Protocolo Internet]. Esta é a de nominação dada aos dois protocolos mais conhecidos desenvolvidos para a interligação de redes. Começou por ser uma norma UNIX, mas o TCP/IP é actualmente suportado por quase todas as plataformas e é o protocolo da Internet.

TCP

Está relacionado com o conteúdo dos dados que circulam pela rede — assegura que toda a informação enviada chega inteira ao respectivo destino. O IP está relacionado com o endereço do terminal para o qual os dados são enviados, assim como com o endereço da rede de destino.

Tráfego

O movimento de pacotes de dados numa rede.

Universal plug and play

O Universal plug and play [“Ligar e usar” universal] é um sistema que permite a aplicações compatíveis ler algumas das definições do Router. Este sistema permite-lhes configurar algumas, ou todas, as definições automaticamente, precisando assim de menos configurações efectuadas pelo utilizador.

Filtro URL

Um filtro URL consiste numa funcionalidade da firewall que lhe permite impedir os seus clientes de navegar para websites inapropriados.

UTP

O Unshielded twisted pair [par entrançado não blindado] é o cabo utilizado pelas redes Ethernet 10BASE-T e 100BASE-Tx.

VCI

VCI - Virtual Channel Identifier [Identificador de Canal Virtual]. O identificador no cabeçalho da célula do ATM (Modo de transferência assíncrono) que identifica a qual canal virtual pertence a célula.

VPI

VPI - Virtual Path Identifier [Identificador de Caminho Virtual]. O identificador no cabeçalho da célula do ATM (Modo de transferência assíncrono) que identifica a qual VP (caminho virtual) pertence a célula.

WAN

Wide Area Network [Rede de Área Alargada]. Trata-se de uma rede que liga computadores localizados em áreas geográficas separadas (por exemplo, edifícios, cidades ou países diferentes). A Internet é um exemplo de uma rede de área alargada.

WEP

Wired Equivalent Privacy [Privacidade Equivalente com Fios]. Trata-se de um mecanismo de chave de encriptação partilhada para redes sem fios. A encriptação é de 40/64 bits ou de 128 bits.

Wi-Fi

Wireless Fidelity [fidelidade sem fios]. Trata-se da certificação concedida pela WECA a produtos que obedecem aos seus critérios de interoperabilidade. (consulte também 802.11b, WECA)

Wi-Fi Alliance

A Wi-Fi Alliance é um grupo comercial que detém a marca registada Wi-Fi, e que tem como objectivo o desempenho de testes, certificações de interoperabilidade de produtos e a promoção da tecnologia.

Cliente sem fios

O termo utilizado para descrever um computador de secretária ou um portátil que se encontra ligado sem fios à rede sem fios.

Área de Serviço Sem Fios LAN

Outro termo para ESSID (Extended Service Set Identifier [identificador do conjunto de serviços alargado])

Assistente

Uma aplicação do Windows que automatiza procedimentos tais como instalações ou configurações.

WLAN

Wireless Local Area Network [Rede de Área Local Sem Fios]. Uma WLAN consiste num conjunto de computadores e dispositivos ligados por uma rede sem fios numa área relativamente pequena (como, por exemplo, uma casa ou escritório).

WPA

Wi-Fi Protected Access [Acesso Protegido Wi-Fi]. Consiste num mecanismo de encriptação com variação dinâmica para redes sem fios. A encriptação é de 256 bits.



■ ADB Broadband S.p.A
Viale Sarca 222
20126 Milano

■ <http://broadband.adbglobal.com>

