

Secção A

Modem Router DR814Q ADSL2+ de Banda Larga da Aolynk

Índice

1 Visão Geral do Produto	1
1.1 Introdução.....	1
1.2 Aparência.....	1
1.2.1 Painel Frontal	1
1.2.2 Painel Traseiro	2
1.3 Características.....	3
2 Instalação	5
2.1 Conteúdo do Pacote.....	5
2.2 Precauções.....	5
2.3 Ligação do Dispositivo	6
3 Antes de Começar	8
3.1 Tarefas Pré-requisito para Configuração.....	8
3.2 Login.....	8
3.3 Descrição das Configurações Padrões de Fábrica.....	10
4 Configuração Básica Baseada em Web	12
4.1 Instalação Rápida	12
4.2 Configuração da WAN	13
4.2.1 WAN.....	13
4.2.2 Conversão de Protocolo DNS	21
4.2.3 DDNS.....	22
4.3 Configuração LAN	24
4.3.1 LAN.....	24
4.3.2 Servidor DHCP	27
4.3.3 Conversão de Protocolo DHCP	28
4.4 Dispositivo.....	32
4.4.1 Senha.....	32
4.4.2 Acesso Remoto.....	33
4.4.3 Reiniciar/Restaurar as Configurações Padrões de Fábrica.....	35
4.4.4 Fazer Cópia de Reserva/Restaurar Configuração.....	36
4.4.5 Actualização.....	38
4.5 Estado.....	39
4.5.1 Estado.....	40
4.5.2 Registro.....	41
4.5.3 Procura do PVC	42
4.6 Salvar a Configuração.....	43
5 Configuração Avançada	45
5.1 Ligar as Portas LAN aos PVCs.....	45
5.2 Segurança.....	52

5.2.1 Interface.....	52
5.2.2 Política.....	61
5.2.3 Trigger (exceção de segurança).....	69
5.2.4 IDS.....	73
5.3 Configuração de DMZ	76
5.4 Configuração de rota.....	79
5.5 Serviço.....	83
5.5.1 SNTP.....	83
5.5.2 ZIPB.....	85
5.5.3 SNMP.....	86
6 Localização de Defeitos.....	88
6.1 Localização de Defeitos do DR814Q	88
6.2 Ferramentas de Diagnóstico.....	91
6.2.1 Ping.....	91
6.2.2 Nslookup.....	92
7 Apêndice - Protocolo TCP/IP.....	94
7.1 Instalar o TCP/IP.....	94
7.2 Configurar o TCP/IP.....	97
7.2.1 Especificar para Obter um Endereço IP Automaticamente.....	97
7.2.2 Especificar um Endereço IP Fixado.....	100
8 Apêndice - Configuração USB	102
8.1 Instalar o Driver USB.....	102
8.2 Configurar as Propriedades IP.....	105
9 Apêndice – Endereço IP e Máscara de Sub-rede.....	106
9.1 Endereço IP	106
9.1.1 Estrutura do Endereço IP.....	106
9.1.2 Classes dos Endereços IP.....	107
9.2 Máscara de Sub-rede	108
10 Apêndice – Especificações Técnicas.....	110
11 Apêndice - Glossário.....	1

1 Visão Geral do Produto

Este capítulo focaliza-se na aparência e na funcionalidade do Router DR814Q ADSL2+ de Banda Larga da Aolynk, para que se possa familiarizar com este produto.

1.1 Introdução

O Router DR814Q ADSL2+ de Banda Larga da Aolynk (a partir deste ponto referido como DR814Q), apresentando a tecnologia ADSL2+ embutida, acesso de alta velocidade à Internet e ligação remota, é uma ferramenta ideal para os utilizadores SOHO. Possibilita aos utilizadores da LAN partilhar a ligação de banda larga de alta velocidade através do NAT e do servidor DHCP embutidos e fornece soluções completas de segurança de rede para evitar hackers e invasões vindas de fora. Para além disso, satisfaz os requisitos de rede, pois suporta múltiplas ligações, tais como PPPoE, PPPoA, IpoA e ligação em ponte.

Com o DR814Q, poderá ligar as portas de Rede aos PVCs (circuitos virtuais permanentes) e estabelecer os parâmetros QoS correspondentes para ter múltiplos serviços fornecidos por meio de diferentes PVCs através de uma única ligação ADSL.

O DR814Q oferece as páginas de configuração da Web como uma forma de configurá-lo através de browsers comuns da Web. O interface gráfico de utilizador facilita a configuração e a gestão.

Este guia do utilizador apresenta a instalação e configuração do DR814Q. Depois de o orientar através da ligação do dispositivo e da configuração básica, focaliza-se na configuração avançada para que possa operar o DR814Q de forma ideal.

1.2 Aparência

1.2.1 Painel Frontal

Os LEDs do painel frontal indicam o estado do DR814Q.



Figura 1 Vista frontal

Tabela 1 Descrições dos estados dos LEDs no DR814Q

LED	Estado	Descrição
-----	--------	-----------

Power	aceso	A energia está ligada e a operação está normal.
	apagado	A energia está desligada ou ocorreu uma falha.
Link	aceso	A ligação ADSL está activa.
	Intermitente	A ligação ADSL está a iniciar.
	apagado	A ligação ADSL está desactivada.
Act	Intermitente	Os dados estão a ser transmitidos e recebidos na ligação ADSL.
	apagado	Nenhuma transmissão de dados está presente na ligação.
USB	aceso	A ligação USB está estabelecida.
	apagado	Nenhuma ligação USB está presente.
LAN1/2/3/4	aceso	A ligação Rede está estabelecida.
	Intermitente	Os dados estão a ser transmitidos e recebidos na porta de Rede.
	apagado	Nenhuma ligação está presente.
Diag	—	Somente para teste em fábrica.

1.2.2 Painel Traseiro

Todas as portas do DR814Q, uma porta de energia e um botão de reset encontram-se localizados no painel traseiro.

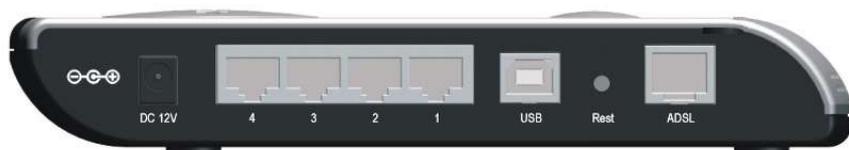


Figura 2 Painel traseiro

Tabela 1 Descrição das portas e do botão de reset

Item	Quantidade	Porta	Descrição	Uso
Porta Rede	4	RJ45	10/100Base-TX negociação automática 10/100 Mbps MDI/MDIX automática IEEE802.3/802.3u	Ligar à porta de Rede de um PC, Hub ou comutador.
Porta USB	1	Soquete da Série-B	USB 1.1	Ligar à porta USB de um PC.

Item	Quantidade	Porta	Descrição	Uso
Porta ADSL	1	RJ11	ANSI T1.413 Emissão 2 ITU G.992.1 Anexo A G.dmt ITU G.992.2 G.lite ITU G.992.3 ADSL2 ITU G.992.5 ADSL2+	Ligar à ficha de telefone na parede ou à porta ADSL de um micro-filtro.
Porta de energia	1	—	—	Ligar ao transformador de energia.
Botão de reset	1	—	—	Restaurar as configurações padrões de fábrica (manter o botão pressionado por pelo menos cinco segundos).

1.3 Características

O DR814Q possibilita uma excelente ligação de rede apresentando:

- Tecnologia de transmissão de dados assimétrica com velocidade de fluxo descendente de 20 Mbps e velocidade de fluxo ascendente de 1 Mbps.
- Ligação de uma porta de Rede a um PVC, que lhe permite aceder aos serviços de Internet através de diferentes portas LAN.
- A tecnologia NAT (tradução de endereço de rede) que permite que todos os PCs de uma rede acessem à Internet compartilhando um único endereço IP.
- Ligação por linha discada PPPoE ao ISP.
- Capacidade de um cliente do DHCP (protocolo de configuração de host dinâmico) obter um endereço IP fixado a partir de um ISP ou de um endereço IP atribuído dinamicamente.
- Capacidade de um servidor DHCP atribuir endereços IP aos hosts numa LAN ou configurar clientes através do servidor DHCP.
- A conversão de protocolo DNS permite-lhe especificar o endereço IP de uma porta de Rede no DR814Q como um endereço IP do servidor DNS de um PC.

- A conversão de protocolo DHCP permite um servidor DHCP disponível para múltiplos clientes DHCP em segmentos de rede diferentes.
- ZIPB (ponte PPP de instalação de zero), NAT, firewall e filtragem IP que protege a sua LAN.
- UPnP (plug-and-play universal) para utilizadores LAN para usar todas as funções fornecidas pelo software suportado por UPnP (tal como MSN) sem nenhuma configuração adicional.
- Redireccionamento IP, configuração DNS (sistema de nomes de domínio) e os serviços tais como a monitoração de desempenho do IP e do DSL.
- Interface gráfico de utilizador baseado em Web para facilitar a configuração e a gestão através de browsers de Web comuns.

2 Instalação

Assumindo que adquiriu os serviços DSL do seu ISP, as seguintes secções descrevem como deverá instalar o DR814Q e configurar o seu PC.

2.1 Conteúdo do Pacote

Desempacotar cuidadosamente a caixa de papelão de transporte e verificar se contém os seguintes itens listados na 2.1.

Tabela 2 Conteúdo do pacote

Item	Quantidade
Router DR814Q ADSL2+ de Banda Larga da Aolynk	1
Transformador de energia	1
Cabo de telefone	1
Cabo de Rede	1
Cabo USB	1
Conjunto de parafuso e apoio	2
Inicialização Rápida do Router DR814Q ADSL2+ de Banda Larga da Aolynk	1
CD que inclui o guia do utilizador e o driver	1
Cartão de Garantia	1
Certificado de Qualidade	1

Se algo faltar ou estiver danificado, contacte o seu representante para o ajudar.

2.2 Precauções

Para garantir a operação normal e a longevidade do DR814Q, o seu local de instalação deverá satisfazer os requisitos descritos abaixo:

- Usar o DR814Q em recinto coberto e mantê-lo afastado de fontes de calor e de água/líquido.
- Manter o gabinete ou a mesa estável o suficiente para suportar o DR814Q. Fixar bem o DR814Q e o transformador de energia na parede, quando for de montagem em parede.
- Reservar pelo menos 10 cm de distância em torno do chassi do DR814Q para dissipação de calor.
- Manter o ambiente de operação limpo. A formação de poeira sobre o chassi pode resultar em absorção estática, reduzindo o tempo de vida do equipamento e podendo provocar falhas na comunicação.
- Usar um sistema de ligação à terra ou proteção contra raios diferente daquele para o equipamento da fonte de alimentação e mantê-los o mais afastados possível.

- Manter o DR814Q longe de emissores de radiofrequência de alta potência, emissores de radar e equipamentos com alta frequência e alta corrente.
- A instalação de cabos ao ar livre é proibida, para evitar danos à porta de sinais, que possam ser causados por sobretensão e sobrecorrente provocada por raios.

2.3 Ligação do Dispositivo

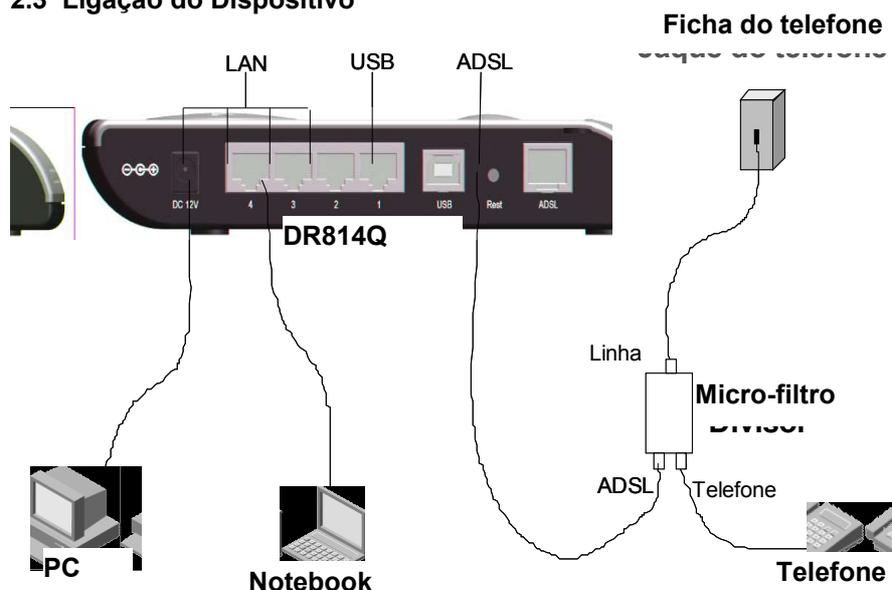


Figura 3 Ligar o DR814Q

I. Ligar a uma linha ADSL

Para ligar o DR814Q a uma linha ADSL, estão disponíveis duas opções:

- Ligar uma extremidade do cabo do telefone à porta ADSL (similar a uma porta de telefone comum) no painel traseiro do DR814Q e a outra extremidade à ficha do telefone na parede.
- Como ilustrado na 2.3, ligar a porta ADSL ao DR814Q e o telefone a um micro-filtro e, depois, ligar o micro-filtro à ficha do telefone na parede. Esta opção permite-lhe usar o telefone quando estiver a aceder à rede.

I. Ligar a um PC ou à Rede

Para ligar o DR814Q a um PC ou à Rede, existem duas opções disponíveis:

•As portas de Rede do DR814Q são MDI/MDIX automáticos, permitindo-lhe usar o cabo de cruzamento ou em linha recta para ligar o seu PC, Hub ou comutador à porta de Rede (um entre LAN1 a LAN4) do DR814Q.

•Ligar o seu PC ao DR814Q através das portas USB com um cabo USB. É conveniente para o PC sem NIC para aceder à Internet.



Aviso:

Para usar a porta USB do DR814Q, deverá instalar o driver USB e configurar o seu PC (consultar a secção 8“Apêndice - Configuração USB ” para obter informações detalhadas).

II. Ligar ao adaptador de potência

Fixe uma extremidade do transformador de energia ao DR814Q e a outra extremidade à tomada de força. O DR814Q não tem interruptor de energia, de forma que fica ligado assim que ligar o transformador de energia à tomada de força.

Aproximadamente um minuto após a ligação do DR814Q, os estados dos LEDs do painel frontal deverão ser os listados na II.

Tabela 1 Descrições dos estados dos LEDs

LED	Estado	Descrição
Power	Verde	—
Link	Verde	—
Act	Intermitente	Os dados estão a ser transmitidos e recebidos.
	Apagado	Nenhuma transmissão de dados está presente.
LAN	Verde	A ligação de Rede está estabelecida.
	Intermitente	Os dados estão a ser transmitidos e recebidos na porta de Rede.

3 Antes de Começar

O DR814Q oferece uma série de páginas de configuração de Web que auxiliam na sua gestão. Poderá configurar o DR814Q, conforme necessário. Este capítulo orienta-o de forma a familiarizar-se com as páginas de configuração de Web.

3.1 Tarefas Pré-requisito para Configuração

Para configurar o DR814Q através das páginas da Web embutidas, deverá configurar o seu PC como se segue:

I. Requisitos de Sistema

- Um NIC de Rede (10Base-T ou 10/100Base-T/TX) ou uma porta USB
- Um browser de Web (Microsoft Internet Explorer 5.5, Netscape 6.0 ou mais recente)
- Protocolo TCP/IP utilizado

II. Endereço IP do seu PC

O utilizador deverá atribuir um endereço IP ao seu PC para fazê-lo no mesmo segmento de rede do DR814Q, antes de aceder à página de configuração. O endereço IP padrão da porta de Rede do DR814Q é 192.168.1.1. Consulte a secção 7“Apêndice - Protocolo TCP/IP”.

III. Nenhum servidor proxy

Se o seu PC utilizar o servidor proxy para aceder à Internet, deverá desligar o serviço proxy.

Escolha [*Tool/Internet options*] (ferramenta/opções de internet) para abrir a janela [*Internet options*].

Seleccione o separador [*Connections*] (ligações) e clique em <*LAN settings...*> (configurações da LAN...).

Certifique-se de que a opção *Use a proxy server* (usar um servidor proxy) não está seleccionada.

3.2 Login

Execute o seu browser de Web e entre em **http://192.168.1.1** na barra de endereço. A caixa de diálogo de login aparecerá, como ilustrado na 3.2.



Figura 4 Caixa de diálogo de login

Se este for o seu primeiro login, digite o nome do utilizador padrão e a senha **admin** e clique em <OK> para entrar na página [Welcome] (bem-vindo), reproduzida na 3.2.

Port	Type	Connected	Line State
DSL	atm	×	N/A
Ethernet0	ethernet		N/A
Usb-ethernet	ethernet	×	N/A

Figura 5 Página de Boas Vindas

A secção à esquerda da página de configuração da Web é a barra de navegação e a secção à direita é a de configuração de parâmetros; quando clicar num botão de navegação na barra de navegação, aparecerão as configurações dos parâmetros correspondentes.

 **Nota:**

- Para alterar a senha de login, consulte a secção "" para obter informações detalhadas.
 - Se receber uma mensagem de erro ou a página de configuração não puder ser exibida, consulte a secção 6.1“Localização de Defeitos do DR814Q ” para obter instruções detalhadas.
-

3.3 Descrição das Configurações Padrões de Fábrica

O DR814Q é ajustado com as configurações padrões de fábrica pelos utilizadores SOHO.

A tabela abaixo lista algumas das configurações padrões mais importantes e os capítulos subsequentes irão abranger todas as características em detalhe. Se estiver familiarizado com configuração de rede, reveja estas configurações para verificar se satisfazem os requisitos da sua rede e siga as instruções para alterá-las, se necessário. Caso contrário, utilize o DR814Q com as configurações padrões.

Tabela 1 Descrição das configurações padrões de fábrica

Item	Configurações padrões	Descrição
Nome do utilizador padrão/senha	Administrador: admin/admin Utilizador comum: user/user	Poderá executar o login na página de configuração da Web como um administrador ou um utilizador comum. Diferentes direitos de operação estarão disponíveis para diferentes utilizadores de login. Consulte o item "" para obter informações detalhadas.
Endereço IP da porta LAN	Endereço IP estático atribuído: 192.168.1.1 Máscara de sub-rede: 255.255.255.0	Este é o endereço IP da porta LAN do DR814Q que liga o DR814Q à sua Rede. Geralmente, não há necessidade de alterar este endereço.

Item	Configurações padrões	Descrição
DHCP (protocolo de configuração de host dinâmico)	Servidor DHCP ligado com o seguinte conjunto de endereços: 192.168.1.2 a 192.168.1.51	O DR814Q fornece um conjunto de endereços IP privados para atribuição dinâmica aos PCs na LAN. Para usar este serviço, deverá configurar o seu PC para obter um endereço IP dinamicamente. Consulte a secção 7.2.1“Especificar para Obter um Endereço IP Automaticamente”.
NAT (tradução de endereço de rede)	NAT ligado	O endereço IP privado do seu PC é traduzido para o endereço IP público sempre que aceder à Internet. Consulte a secção III“Configuração NAT ” para obter informações detalhadas.
Modo DSL	Multimodo	Aplicável a múltiplos modos de linha DSL padrões.

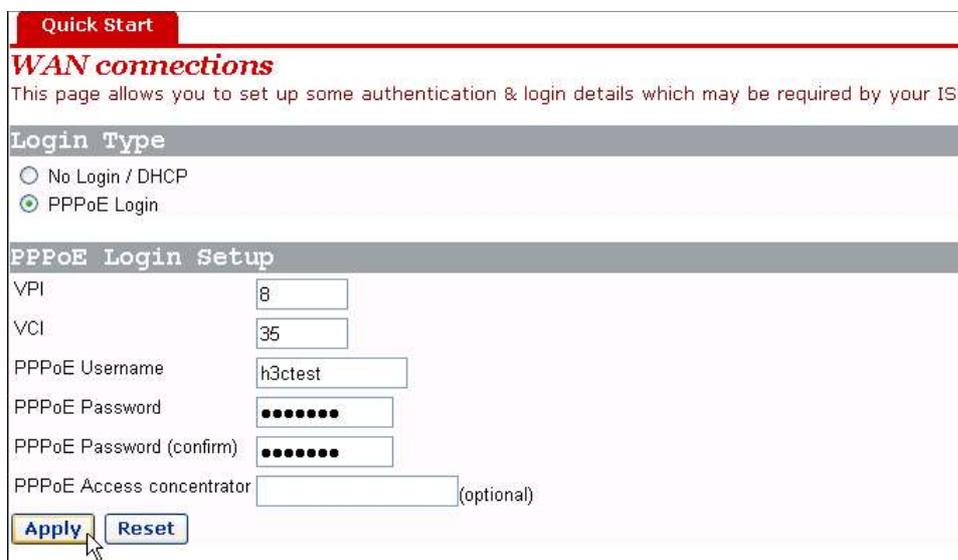
4 Configuração Básica Baseada em Web

Este capítulo descreve as páginas de configurações básicas do DR814Q para utilizadores SOHO para implementar as suas funções básicas. Para obter detalhes da configuração avançada, consulte a secção 5 “Configuração Avançada”.

4.1 Instalação Rápida

Clique em [*Quick Setup*] (instalação rápida) na barra de navegação para entrar na página [*Quick Start*], na qual poderá realizar alguns ajustes simples para aceder à Internet rapidamente. Aqui, dois tipos de login comuns estão disponíveis: PPPoE e DHCP.

I. PPPoE



The screenshot shows a web interface for configuring WAN connections. At the top, there is a red header with the text "Quick Start". Below this, the section is titled "WAN connections" in red, followed by a subtitle: "This page allows you to set up some authentication & login details which may be required by your ISP". Under the heading "Login Type", there are two radio button options: "No Login / DHCP" (which is unselected) and "PPPoE Login" (which is selected). Below this is the "PPPoE Login Setup" section, which contains several input fields: "VPI" with the value "8", "VCI" with the value "35", "PPPoE Username" with the value "h3ctest", "PPPoE Password" (masked with dots), "PPPoE Password (confirm)" (masked with dots), and "PPPoE Access concentrator" (empty) with "(optional)" text to its right. At the bottom left of this section are two buttons: "Apply" and "Reset".

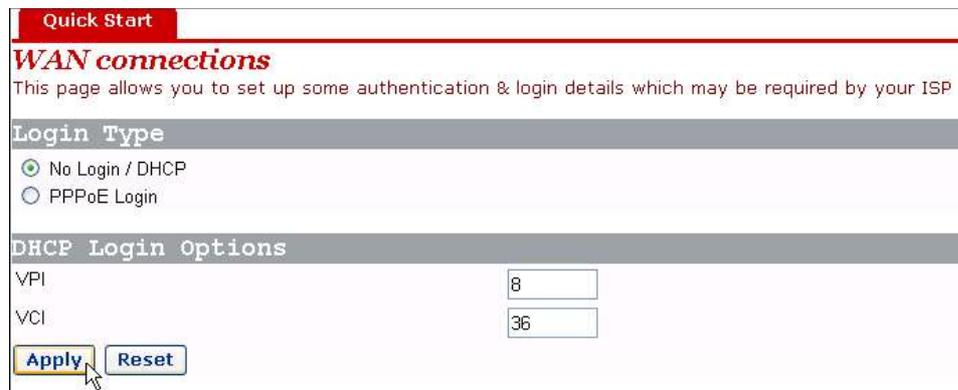
Figura 6 Instalação Rápida – Login do PPPoE

O tipo de login padrão na página é o PPPoE. Este tipo solicita-lhe que digite os valores VPI e VCI, o nome do utilizador PPPoE e a senha PPPoE especificados pelo seu ISP e repita a senha para confirmação na caixa de texto [*PPPoE Password (confirm)*] (senha PPPoE (confirmar)).

Quando houver múltiplos servidores PPPoE na rede, poderá especificar o identificador do servidor PPPoE através do qual o cliente PPPoE acede à caixa de texto [*PPPoE Access concentrator*] (concentrador de acesso PPPoE).

Clique em <Apply> quando a configuração estiver completa.

II. DHCP



Quick Start

WAN connections

This page allows you to set up some authentication & login details which may be required by your ISP

Login Type

No Login / DHCP
 PPPoE Login

DHCP Login Options

VPI

VCI

Figura 7 Instalação Rápida – Nenhum Login/DHCP

Se puder obter os endereços IP do servidor DHCP do seu ISP automaticamente, seleccione a opção **No Login/DHCP** (nenhum login/DHCP) na página [*Quick Start*] (iniciação rápida) (ver I) e digite os valores VPI e VCI especificados pelo seu ISP na página (ver II).

Clique em <Apply> quando a configuração estiver completa.



Aviso:

Não configure os mesmos valores VPI e VCI para tipos de DHCP e login do PPPoE.

4.2 Configuração da WAN

Clique em [*WAN Setup*] (configuração da WAN) na barra de navegação para entrar na página correspondente, onde poderá encontrar três separadores disponíveis: WAN, Conversão de Protocolo DNS e DDNS. Clique no separador desejado para entrar na sua página de configuração.

4.2.1 WAN

Esta página permite-lhe configurar as ligações WAN em detalhe ou modificar os atributos do serviço. Poderá aceder à Internet normalmente apenas quando estes atributos estiverem configurados correctamente.

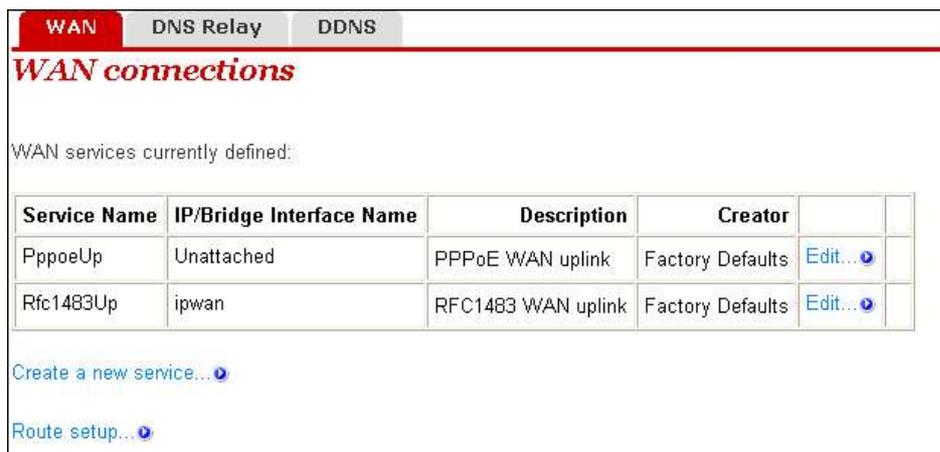


Figura 8 WAN

I. Criar um novo serviço

Para criar um novo serviço, clique em <Create a new service...> (criar um novo serviço...) para entrar na página [WAN connection: create service] (ligação WAN: criar serviço) (ver I).



Figura 9 Criar um serviço WAN

Esta página fornece quatro modos para ligação WAN: DHCP/IP Estático, IPoA, PPPoA e PPPoE. O que segue apresenta as suas configurações respectivamente.

1) DHCP/IP Estático

O endereço IP neste modo pode ser manualmente especificado ou automaticamente atribuído pelo seu ISP. O formulário solicita-lhe a especificação manual do endereço do servidor DNS na

página [DNS Relay] (conversão de protocolo DNS). Para obter detalhes, consulte a secção 4.2.2“Conversão de Protocolo DNS ”.

Para criar uma ligação WAN DHCP/IP Estático, seleccione a opção **DHCP/StaticIP** da lista de modo ATM (ver I) e clique em <Configure> (configurar) para entrar na página (ver I).

Figura 10 DHCP/IP Estático

Tabela 1 Descrições dos itens DHCP/IP Estático

Item	Descrição
<i>Description</i> (descrição)	Digite a descrição característica sobre este serviço.
VPI	Digite o valor VPI fornecido pelo seu ISP.
VCI	Digite o valor VCI fornecido pelo seu ISP.
<i>Encapsulation method</i> (método de encapsulamento)	Selecione o método de encapsulamento de pacote de acordo com o seu ISP, LLC/SNAP ou VcMux, do último drop-down/SNAP que estiver normalmente seleccionado.
<i>Obtain an IP Address Automatically</i> (obter um endereço IP automaticamente)	Selecione esta opção para obter um endereço IP do servidor DHCP do seu ISP automaticamente.
<i>Use the following IP Address</i> (usar o seguinte endereço IP)	Selecione esta opção se tiver o endereço IP estático fornecido pelo seu ISP. Precisarás também de fornecer o endereço IP e a máscara de sub-rede.
<i>WAN IP Address</i> (endereço IP da WAN)	Digite o endereço IP estático fornecido pelo seu ISP.

Item	Descrição
<i>Subnet Mask</i> (máscara de sub-rede)	Digite a máscara de sub-rede fornecida pelo seu ISP.
<i>Enable NAT on this interface</i> (ligar NAT nesta interface)	Selecione esta caixa de verificação para ligar o NAT. Com isso, os utilizadores SOHO poderão fazer múltiplos hosts acederem à rede através de um endereço IP público.

Clique em <Apply> quando a configuração estiver completa.

2) IPoA

O IPoA permite pacotes de IP directamente sobre a ligação física ADSL em altas taxas de transmissão.

Para criar uma ligação WAN do IPoA, seleccione a opção **IPoA** da lista de modo ATM (ver I) e clique em <Configure> para entrar na seguinte página:

WAN connection: IPoA

Description:

VPI:

VCI:

Encapsulation method: ▼

WAN IP address:

Subnet Mask:

Enable NAT on this interface

Figura 11 IPoA

Tabela 1 Descrição dos itens do IPoA

Item	Descrição
<i>Description</i> (descrição)	Digite a descrição característica sobre este serviço.
VPI	Digite o valor VPI fornecido pelo seu ISP.
VCI	Digite o valor VCI fornecido pelo seu ISP.
<i>Encapsulation method</i> (método de encapsulamento)	Selecione o método de encapsulamento de pacote de acordo com o seu ISP, LLC/SNAP ou VcMux, do último drop-down/SNAP que estiver normalmente seleccionado.
<i>WAN IP Address</i> (endereço IP da WAN)	Digite o endereço IP estático fornecido pelo seu ISP.
<i>Subnet Mask</i> (máscara de sub-rede)	Digite a máscara de sub-rede fornecida pelo seu ISP.
<i>Enable NAT on this interface</i> (ligar NAT nesta interface)	Selecione esta caixa de verificação para ligar o NAT. Com isso, os utilizadores SOHO podem fazer múltiplos hosts acederem à rede através de um endereço IP público.

Clique em <Apply> quando a configuração estiver completa.

3) PPPoA

Para criar uma ligação WAN do PPPoA, seleccione a opção **PPPoA** da lista de modo ATM (ver I) e clique em <Configure> (configurar) para entrar na seguinte página:

WAN connection: PPPoA

Description:

VPI:

VCI:

User name:

Password:

Auto Connect:

User Idle Timeout (in minutes):

Enable NAT on this interface

Figura 12 PPPoA

Tabela 1 Descrições dos itens do PPPoA

Item	Descrição
<i>Description</i> (descrição)	Digite a descrição característica sobre este serviço.
VPI	Digite o valor VPI fornecido pelo seu ISP.
VCI	Digite o valor VCI fornecido pelo seu ISP.
<i>User name</i> (nome do utilizador)	Digite o nome do utilizador fornecido pelo seu ISP.
<i>Password</i> (senha)	Digite a senha fornecida pelo seu ISP.
<i>Auto Connect</i> (ligação automática)	Se esta caixa de verificação for seleccionada, o dispositivo realizará automaticamente a ligação de linha discada, de novo, em resposta a uma solicitação de acesso à LAN quando a rede estiver desligada.
<i>User Idle Timeout</i> (tempo esgotado por inactividade do utilizador)	Digite o tempo de inactividade para corte automático de ligação. A ligação da rede é desligada automaticamente caso nenhuma transmissão de dados se efectue dentro do tempo estabelecido. Isto é conveniente para contabilidade de rede baseada em tempo. Se o tempo for ajustado para 0, implica que a ligação nunca fica desligada.
<i>Enable NAT on this interface</i> (ligar NAT nesta interface)	Selecione esta caixa de verificação para ligar o NAT. Com isso, os utilizadores SOHO podem fazer múltiplos hosts acederem à rede através de um endereço IP público.

Clique em <Configure> (configurar) quando a configuração estiver completa.

4) PPPoE

Para criar uma ligação WAN do PPPoA, seleccione a opção **PPPoA** da lista de modo ATM (ver I) e clique em <Configure> (configurar) para entrar na seguinte página:

WAN connection: PPPoE

Description:

VPI:

VCI:

User name:

Password:

Auto Connect:

User Idle Timeout (in minutes):

Enable NAT on this interface

Figura 13 PPPoE

Tabela 1 Descrição dos itens do PPPoE

Item	Descrição
<i>Description</i> (descrição)	Digite a descrição característica sobre este serviço.
VPI	Digite o valor VPI fornecido pelo seu ISP.
VCI	Digite o valor VCI fornecido pelo seu ISP.
<i>User name</i> (nome do utilizador)	Digite o nome do utilizador fornecido pelo seu ISP.
<i>Password</i> (senha)	Digite a senha fornecida pelo seu ISP.
<i>Auto Connect</i> (ligação automática)	Se esta caixa de verificação for seleccionada, o dispositivo realizará automaticamente a ligação de linha discada, de novo, em resposta a uma solicitação de acesso à LAN quando a rede estiver desligada.
<i>User Idle Timeout</i> (tempo esgotado por inactividade do utilizador)	Digite o tempo de inactividade para corte automático de ligação. A ligação da rede é desligada automaticamente em caso de não ocorrer nenhuma transmissão de dados dentro do tempo estabelecido. Isto é conveniente para contabilidade de rede baseada em tempo. Se o tempo for ajustado para 0, implica que a ligação nunca fica desligada.
<i>Enable NAT on this interface</i> (ligar NAT nesta interface)	Selecione esta caixa de verificação para ligar o NAT. Com isso, os utilizadores SOHO podem fazer múltiplos hosts acederem à rede através de um endereço IP público.

Clique em <Configure> (configurar) quando a configuração estiver completa.



Aviso:

Não configure os mesmos valores VPI e VCI para todos os serviços.

Como ilustrado na I, o serviço configurado com êxito será adicionado à lista de serviços da WAN.

WAN connections

WAN services currently defined:

Service Name	IP/Bridge Interface Name	Description	Creator		
PppoeUp	Unattached	PPPoE WAN uplink	Factory Defaults	Edit...	
Rfc1483Up	ipwan	RFC1483 WAN uplink	Factory Defaults	Edit...	
rfc1483-0	rfc1483-0	dhcp/static	WebAdmin	Edit...	Delete...

[Create a new service...](#)

[Route setup...](#)

Figura 14 Lista de serviços da WAN

I. Editar um serviço da WAN

Para modificar um serviço ou optar por configuração avançada, clique no <Edit...> (editar...) correspondente para entrar na página. Se necessário, modifique os valores relacionados e clique em <Change> (alterar). Para obter detalhes da configuração de parâmetros do Canal ATM, consulte a secção II "Configuração QoS".

II. Excluir um serviço da WAN

Para excluir um serviço existente da WAN, clique no botão <Delete...> (excluir...) correspondente para entrar na página e clique em <Delete this connection> (excluir esta ligação).

Delete WAN connection

WAN connection: delete 'dhcp/static'

Please confirm deletion of this connection:

Description: dhcp/static
 Creator: WebAdmin
 VPI: 0
 VCI: 40
 Type: RFC1483 bridged

Delete this connection

Figura 15 Excluir uma ligação da WAN



Aviso:

Os dois primeiros itens da lista de serviços da WAN são serviços padrões e não podem ser excluídos.

4.2.2 Conversão de Protocolo DNS

O DR814Q tem a função de conversão de protocolo DNS. Geralmente, o endereço do servidor DNS obtido pelo seu PC através do DHCP é o endereço IP da porta LAN. Também poderá especificar o endereço do servidor DNS no seu PC como o endereço IP da porta LAN. O DR814Q transmite a consulta do DNS enviada pelo seu PC para o servidor DNS estabelecido no DR814Q.

As páginas de configuração abaixo são usadas para determinar a lista do servidor DNS. A consulta DNS enviada pelo seu PC é transmitida ao servidor DNS na lista existente. Quando o seu ISP alterar o servidor DNS, não haverá necessidade de modificar o endereço IP do servidor DNS no seu PC.

WAN **DNS Relay** DDNS

DNS Relay

This page allows you to enter a list of DNS server IP addresses that the DNS relay can forward to.

Edit DNS server list

Use this section to edit existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You can edit up to three addresses at a time.

There are currently no DNS servers in the list. Use the section below to add a new DNS server.

Add new DNS server

Use this section to add a new DNS server to the DNS relay's list.

New DNS server IP address: . . .

Figura 16 Conversão de Protocolo DNS (1)

Para criar um novo servidor DNS, digite o seu endereço IP, suponhamos 218.72.1.1, no campo [*New DNS server IP address*] (novo endereço IP do servidor DNS) e clique em <Apply> (aplicar). Este endereço será adicionado à lista de endereços IP do servidor DNS (ver 4.2.2).

DNS Relay

This page allows you to enter a list of DNS server IP addresses that the DNS relay can forward DNS queries to.

Edit DNS server list

Use this section to edit existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You cannot have more than three addresses at a time.

DNS server IP address	Hostname	Delete?
218 . 72 . 1 . 1		<input type="checkbox"/>

Add new DNS server

Use this section to add a new DNS server to the DNS relay's list.

New DNS server IP address: . . .

Figura 17 Conversão de Protocolo DNS (2)



Na lista de endereços IP do servidor DNS, o primeiro endereço deverá ser o servidor DNS primário, o segundo para o servidor DNS secundário e assim sucessivamente.

Para modificar o endereço IP do servidor DNS na lista, modifique-o directamente no campo e clique em <Apply> (aplicar).

Para excluir o servidor DNS existente, seleccione a caixa de verificação [*Delete?*] (excluir?) correspondente e clique em <Apply> (aplicar).

4.2.3 DDNS

Serviço de Nomes de Domínio Dinâmico (DDNS). Através do PPPoE ou IP estático, o endereço IP que a porta WAN obteve é não-fixa, tornando inconveniente para os utilizadores da Internet acederem ao servidor da LAN. O DDNS resolve este problema. Depois de o utilizador configurar esta função DDNS, o DR814Q actualiza o mapeamento entre o nome do domínio e o endereço IP automaticamente, garantindo aos utilizadores da Internet acesso à LAN através do nome do domínio.

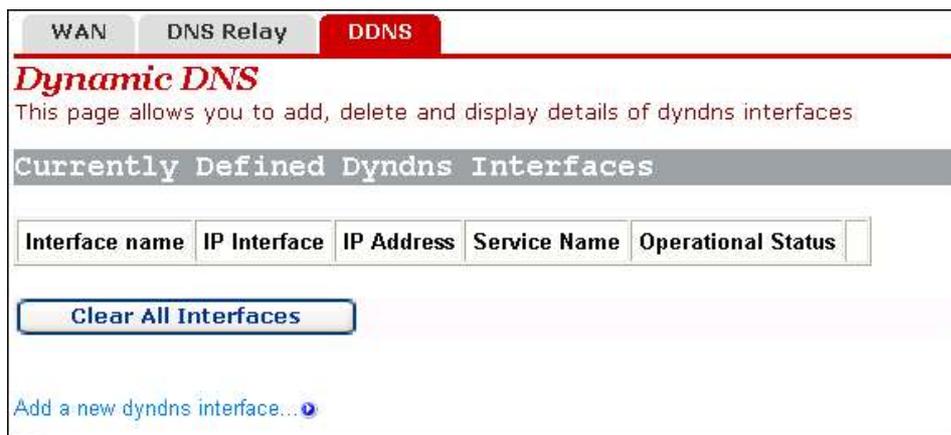


Figura 18 Configuração DNS Dinâmica (1)

Clique em <Add a new dyndns interface...> (adicionar um novo interface dyndns...) para entrar na página de configuração do DDNS (ver 4.2.3).



Figura 19 Configuração DNS Dinâmica (2)

Tabela 1 Descrições dos itens do DDNS

Item	Descrição
<i>IP interface</i> (interface IP)	Selecione o interface no qual deseja ligar a função DDNS.
<i>Service Name</i> (nome do serviço)	Selecione o website onde pretende obter o serviço DDNS.
<i>User Name</i> (nome do utilizador)	Digite o nome do utilizador que registrou com o servidor DDNS.
<i>Password</i> (senha)	Digite a senha que registrou com o servidor DDNS.

<i>Host Name</i> (nome do host)	Digite o nome do domínio que solicitou a partir do servidor DDNS.
---------------------------------	---

 **Nota:**

Como a ferramenta de cliente do serviço DDNS, a função DDNS deve cooperar com o servidor DDNS. Visite **www.3322.org**, www.dyndns.org ou **www.tzo.com** para solicitar um nome de domínio antes de ligar a função DDNS. Depois de o utilizador completar as configurações do DDNS no DR814Q, o mapeamento entre o nome do domínio e o endereço IP da porta WAN é estabelecido.

Exemplo: Se o utilizador tiver solicitado pelo nome de domínio lullaby a partir de **www.3322.org**, consulte a 4.2.3 para as configurações para fazer o mapeamento entre o nome do domínio e o endereço IP da porta WAN no DR814Q. Clique em <Create> (criar) e poderá visualizar as configurações DDNS, como ilustrado abaixo.



Figura 20 Configuração DDNS com êxito

Para excluir a configuração DDNS, clique em <Delete> (excluir). Para apagar toda a configuração DDNS, clique em <Clear All Interfaces> (apagar todos os interfaces). Para visualizar a configuração detalhada do interface DDNS actual, clique em <Show Details...> (mostrar detalhes...).

4.3 Configuração LAN

Clique em [*LAN Setup*] (configuração LAN) na barra de navegação para entrar na página correspondente onde estão disponíveis três separadores: LAN, Servidor DHCP e Conversão de Protocolo DHCP. Clique no separador relativo para entrar na página de configuração pretendida.

4.3.1 LAN

Esta página permite-lhe estabelecer valores de atributos para a porta de Rede e para configurar os interfaces virtuais.

LAN	DHCP Server	DHCP Relay		
LAN connections				
This page allows you to change the IP address for the default LAN port. The name of the IP				
Default LAN Port				
Primary IP Address				
IP Address:	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Subnet Mask:	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
<input type="button" value="Apply"/>				
Note: there may be a short pause between clicking <i>Apply</i> and receiving a response.				
Advanced...				
Route setup...				
LAN port iplan virtual interfaces:				
IP Interface Name				
<input type="text" value="None"/>				
Create a new virtual interface...				
<small>Copyright 2003-2004 Huawei Technology</small>				

Figura 21 Ligações LAN

I. Configurar uma porta LAN

Para alterar o endereço IP da porta LAN, digite o endereço IP e/ou a máscara de sub-rede directamente no campo correspondente e clique em <Apply> (aplicar). Para a introdução relacionada com o endereço IP, consulte a secção 9“Apêndice – Endereço IP e Máscara de Sub-rede”.

Para realizar a configuração avançada no atributo da porta LAN, clique em <Advanced...> (avançada...) para entrar na página [Edit iplan] (editar iplan), como ilustrado na I. Se necessário, modifique os valores das opções e clique em <Change> (alterar).

Edit iplan	
Name	Value
IP Address:	<input type="text" value="192.168.1.1"/>
Mask	<input type="text" value="255.255.255.0"/>
MTU:	<input type="text" value="1500"/>
TCP MSS Clamp:	<input type="button" value="true"/> ▼
Rip Accept V1:	<input type="button" value="false"/> ▼
Rip Accept V2:	<input type="button" value="false"/> ▼
Rip Send V1:	<input type="button" value="false"/> ▼
Rip Send V2:	<input type="button" value="false"/> ▼
Rip Send Multicast:	<input type="button" value="false"/> ▼
Nat Enabled:	<input type="button" value="false"/> ▼

Figura 22 Modificar o interface iplan

I. Criar um novo interface virtual

Para criar um novo interface virtual, clique em <Create a new virtual interface...> (criar um novo interface virtual...) na página [LAN connections] (ligações LAN) (ver 4.3.1) para entrar na página ilustrada abaixo.

Create virtual interface	
Create virtual interface	
Configure new virtual interface:	
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="button" value="Apply"/>	

Figura 23 Criar um interface virtual

Digite o endereço IP e a máscara de sub-rede (não poderá configurar o endereço IP do interface virtual e aquele da porta LAN para a mesma sub-rede) e clique em <Apply> (aplicar). As informações neste interface virtual são exibidas na página ilustrada abaixo.

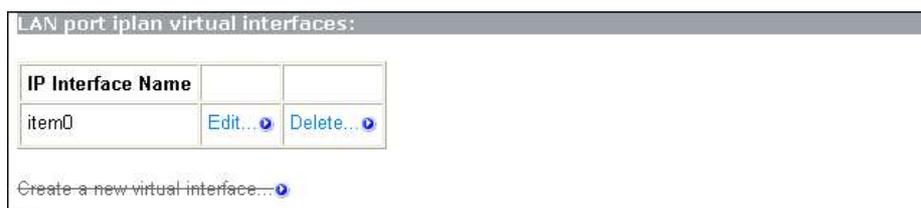


Figura 24 Interface virtual

O interface virtual criado pode ser usado para configuração DMZ. Para obter detalhes, consulte a secção 5.3 "Configuração de DMZ".

Para modificar as informações no interface virtual actual ou configurar de forma avançada, clique no botão <Edit...> (editar...) correspondente para entrar na página. Se necessário, modifique os valores das opções e clique em <Change> (alterar).

Para excluir o interface virtual actual, clique no botão <Delete...> (excluir...) correspondente para entrar na página e clique em <Delete this connection...> (excluir esta ligação...).

4.3.2 Servidor DHCP

O DR814Q pode agir como um servidor DHCP para atribuir automaticamente endereços IP dentro de uma certa faixa para qualquer PC que opere na LAN.

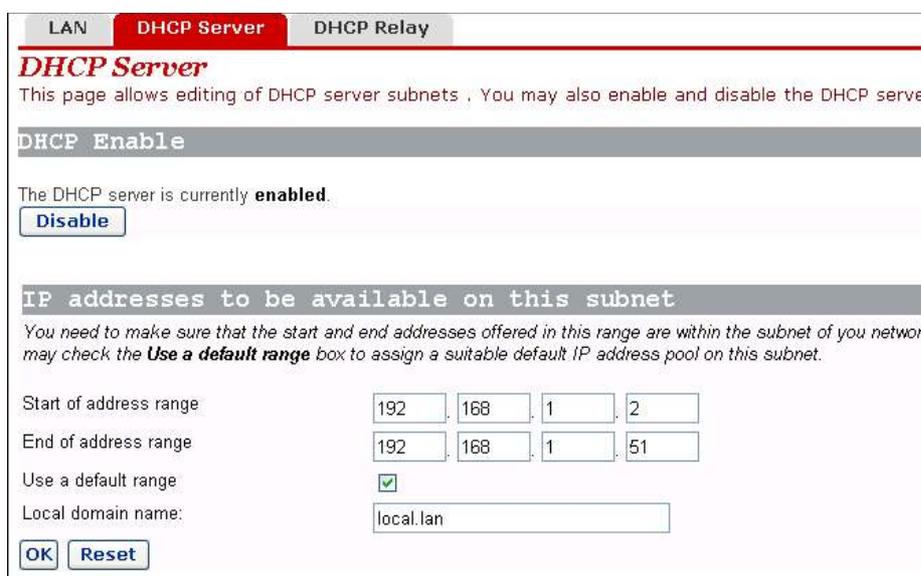


Figura 25 Servidor DHCP

I. Ligar/desligar o servidor DHCP

Se o servidor DHCP estiver actualmente desligado, poderá clicar em *<Enable>* (ligar) para o activar. Por outro lado, poderá também clicar em *<Disable>* (desligar) para desligar o servidor DHCP.

I. Configurar um servidor DHCP

O servidor DHCP ligado pode atribuir os endereços IP, de acordo com a faixa de endereços definida nesta página para um cliente DHCP que envie uma solicitação. Recomenda-se que seleccione a caixa de verificação [*Use a default range*] (usar uma faixa padrão) para atribuir um conjunto de endereços IP padrões convenientes para a sub-rede actual.

Se necessário, poderá também configurar a faixa de endereços DHCP manualmente. Neste caso, não seleccione a caixa de verificação [*Use a default range*] (retirando a selecção). Digite os endereços IP de início e de fim nos campos correspondentes e clique em *<OK>*.

Se necessário, poderá digitar os sufixos DNS comumente utilizados, tal como **google.com** na caixa de texto [*Local domain name*] (nome de domínio local). Então, poderá aceder à página principal do Google entrando com **http://www/** no browser da Web. Pequenas e médias empresas também podem configurar seus próprios sufixos DNS aqui, enquanto que os utilizadores domésticos não necessitam.

4.3.3 Conversão de Protocolo DHCP

O DR814Q tem a função de conversão de protocolo DHCP para transmitir pacotes entre o cliente DHCP e o servidor em diferentes segmentos de rede, com isso fazendo com que o cliente DHCP em múltiplas redes use o servidor DHCP através destes segmentos.

LAN	DHCP Server	DHCP Relay
DHCP Relay		
This page allows you to enter a list of DHCP server IP addresses that the relay will forward also enable and disable the DHCP relay from here, and choose which IP interfaces the relay		
The DHCP relay is currently <i>disabled</i> . You may not enable the DHCP relay because the DHCP server is already enabled.		
DHCP relay interfaces		
Use this section to edit the list of IP interfaces the DHCP relay should listen on.		
There are currently no IP interfaces configured, so the DHCP relay will listen on all available IP interfaces.		
Add new interface		
Use this section to tell DHCP relay to listen on another IP interface.		
New IP interface: <input type="text" value="ipwan"/> <input type="button" value="Add"/>		
Edit DHCP server list		
Use this section to edit existing DHCP server addresses present in the DHCP relay's list.		
There are currently no DHCP servers in the list. Use the section at the bottom of the page to add a new D		
Add new DHCP server		
Use this section to add a new DHCP server to the DHCP relay's list.		
New DHCP server IP address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>		
<input type="button" value="Apply"/>		
Copyright 2003-2004 Huawei Technolog		

Figura 26 Página de Conversão de Protocolo DHCP

I. Especificar um interface de conversão de protocolo DHCP

Na página [*DHCP Relay*] (conversão de protocolo DHCP) (ver 4.3.3), selecione um interface (suponhamos *iplan*) a partir da lista drop-down [*New IP interface*] (novo interface IP) para aplicar a função de conversão de protocolo DHCP e clique em <*Add*> (adicionar). Este interface aparecerá na página exibida abaixo.

DHCP relay interfaces

Use this section to edit the list of IP interfaces the DHCP relay should listen on.

Name	Delete?
iplan	<input type="checkbox"/>

Figura 27 Novo interface IP

Clique em <Apply> (aplicar) na I para aplicar esta configuração; aparecerá a informação “Changes successfully applied” (alterações aplicadas com êxito) na página ilustrada abaixo.

DHCP relay interfaces

Use this section to edit the list of IP interfaces the DHCP relay should listen on.

Changes successfully applied.

Name	Delete?
iplan	<input type="checkbox"/>

Figura 28 O novo interface IP aplicado

Siga as instruções acima para especificar outros interfaces.

Para excluir este interface, seleccione a caixa de verificação [Delete?] (excluir?) correspondente e clique em <Apply> (aplicar).



Aviso:

- Deverá configurar dois interfaces (pacotes de envio e de recebimento, respectivamente) da conversão de protocolo DHCP em par. Por exemplo, para configurar o host ligado à porta LAN para comunicar com o servidor DHCP no lado da WAN, precisará de configurar o iplan e o ipwan como sendo os interfaces de conversão de protocolo DHCP simultaneamente.
- Se nenhum interface for especificado, o DR814Q activa a função de conversão de protocolo DHCP em todos os interfaces por padrão.

I. Configurar um servidor DHCP

Para adicionar um servidor DHCP, digite o endereço IP (supomos 20.2.0.100) do servidor DHCP no campo [*New DHCP server IP address*] (novo endereço IP do servidor DHCP) (ver 4.3.3). Este endereço será adicionado à lista dos endereços IP do servidor DHCP, como ilustrado abaixo.

Edit DHCP server list

Use this section to edit existing DHCP server addresses present in the DHCP relay's list.

DHCP server IP address	Delete?
20 . 2 . 0 . 100	<input type="checkbox"/>

Apply **Reset**

Add new DHCP server

Use this section to add a new DHCP server to the DHCP relay's list.

New DHCP server IP address: . . .

Apply

Figura 29 Configurar um servidor DHCP

Para modificar o endereço IP do servidor DHCP na lista, modifique-o directamente no campo e clique em <Apply> (aplicar).

Para excluir o servidor DHCP existente, seleccione a caixa de verificação [*Delete?*] (excluir?) correspondente e clique em <Apply> (aplicar).

II. Ligar/desligar a conversão de protocolo DHCP

Precisará de ligar a função de conversão de protocolo DHCP depois de a configuração estar completa. As funções do servidor DHCP e da conversão de protocolo DHCP do DR814Q não poderão

ser ligadas simultaneamente. Por padrão, não poderá ligar a conversão de protocolo DHCP porque o servidor DHCP já está ligado. O prompt é exibido como ilustrado na 4.3.3.

Clique em <DHCP Server> (servidor DHCP) na página acima (ver I) para entrar na página do servidor DHCP, clique em <Disable> (desligar) e, então, aparecerá <Enable> (ligar) na página (ver II). Se a conversão de protocolo DHCP estiver desactivada, poderá clicar em <Enable> (ligar) para a activar. Por outro lado, clique em <Disable> (desligar) para a desactivar.

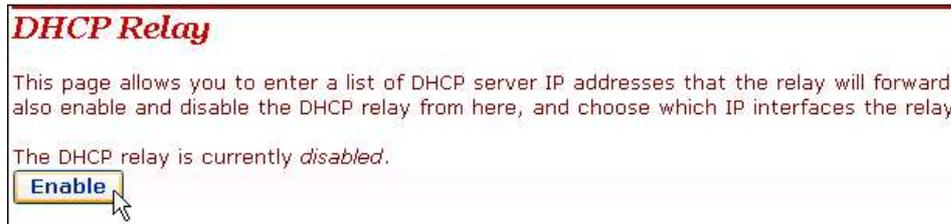


Figura 30 Ligar/desligar a conversão de protocolo DHCP

Aviso:

Para garantir que a conversão de protocolo DHCP é eficiente, é necessário que desligue o NAT entre o interface especificado e o interface correspondente à rede onde o servidor DHCP reside. Por exemplo, para especificar o host ligado à porta LAN para comunicar com o servidor DHCP no interface ipwan, deverá desligar o NAT entre o interface interno (iplan) e o interface externo (ipwan).

4.4 Dispositivo

Clique em [Device] (dispositivo) na barra de navegação para entrar na página correspondente onde cinco separadores estão disponíveis: *Password* (senha), *Remote* (remoto), *Restart* (reinício), *Backup* (cópia reserva) e *Upgrade* (actualização). Clique no separador relativo para entrar na página de configuração desejada.

4.4.1 Senha

Poderá aceder ao login na página de configuração da Web do DR814Q através de dois nomes de utilizador: admin e user. O administrador detém os máximos direitos, enquanto que o utilizador comum poderá apenas aceder a parte das páginas de configuração. Somente o administrador poderá entrar na página seguinte da [Password] (senha) para alterar as senhas de login para dois utilizadores. O utilizador comum poderá apenas alterar a sua própria senha.

Password Remote Restart Backup Upgrade

Change Password

Details for user 'admin'

Username: **admin**

Old Password:

New Password:

Confirm Password:

Details for user 'user'

Username: **user**

Old Password:

New Password:

Confirm Password:

Figura 31 Alterar a senha

Por padrão, “admin” e “user” são as senhas para administrador e utilizador comum, respectivamente.

Para alterar a senha, digite as informações relativas nas caixas de texto [*Old Password*] (senha antiga), [*New Password*] (nova senha) e [*Confirm Password*] (confirmar senha) e clique em <Apply> (aplicar).

4.4.2 Acesso Remoto

Se o acesso remoto estiver ligado, poderá visualizar a página de configuração actual e gerir o DR814Q remotamente.

Por padrão, o acesso remoto está ligado e o tempo esgotado por inactividade está ajustado em 0 (ver 4.4.2). Neste caso, o acesso remoto mantém-se activo.



Figura 32 Página de acesso remoto – acesso remoto ligado

A 4.4.2 indica que a porta para gestão remota é 8000, para que o utilizador possa gerir o DR814Q remotamente entrando em **http://xxx.xxx.xxx.xxx:8000** no browser da Web. O xxx.xxx.xxx.xxx é o endereço IP da porta WAN no DR814Q. Se múltiplos serviços WAN forem configurados e todos eles obtiverem os endereços IP, o endereço IP de qualquer serviço pode ser usado para acesso remoto.

Para desligar o acesso remoto, clique em <Disable> (desligar) na página [Remote Access] (acesso remoto) para abrir a página, como ilustrado abaixo.



Figura 33 Página de acesso remoto – acesso remoto desligado

Neste caso, poderá configurar o tempo esgotado por inactividade para um valor desejado diferente de 0, na caixa de texto na página. Então, quando clicar em <Enable> (ligar) para ligar o acesso remoto na vez seguinte, o DR814Q localizará o tempo de inactividade decorrido e finalizará a ligação remota para evitar ataques remotos, quando o tempo decorrido por inactividade exceder o tempo de inactividade configurado.

 **Aviso:**

Uma ligação remota é mantida somente quando o tempo esgotado por inactividade for ajustado em 0. Se ajustar o tempo esgotado num outro valor, o acesso remoto é desligado automaticamente sempre que o DR814Q reiniciar.

Como o acesso remoto está ligado por padrão, precisará de configurar a senha para evitar a invasão da rede pelos utilizadores da Internet.

4.4.3 Reiniciar/Restaurar as Configurações Padrões de Fábrica

Esta página permite-lhe reiniciar o DR814Q ou restabelecer todas as configurações para as configurações padrões de fábrica.



Figura 34 Páginas para Reiniciar o Router

Para reiniciar o DR814Q, clique em <Restart> (reiniciar).

Para restabelecer todas as configurações para as configurações padrões de fábrica, seleccione a caixa de verificação [*Reset to factory default settings*] (restabelecer para as configurações padrões de fábrica) e clique em <Restart> (reiniciar).

 **Aviso:**

Pode demorar vários segundos a reiniciar o DR814Q.

4.4.4 Fazer Cópia de Reserva/Restaurar Configuração

Esta página permite-lhe fazer uma cópia de reserva da configuração actual para o seu PC ou restaurar a configuração a partir de um arquivo salvo anteriormente.

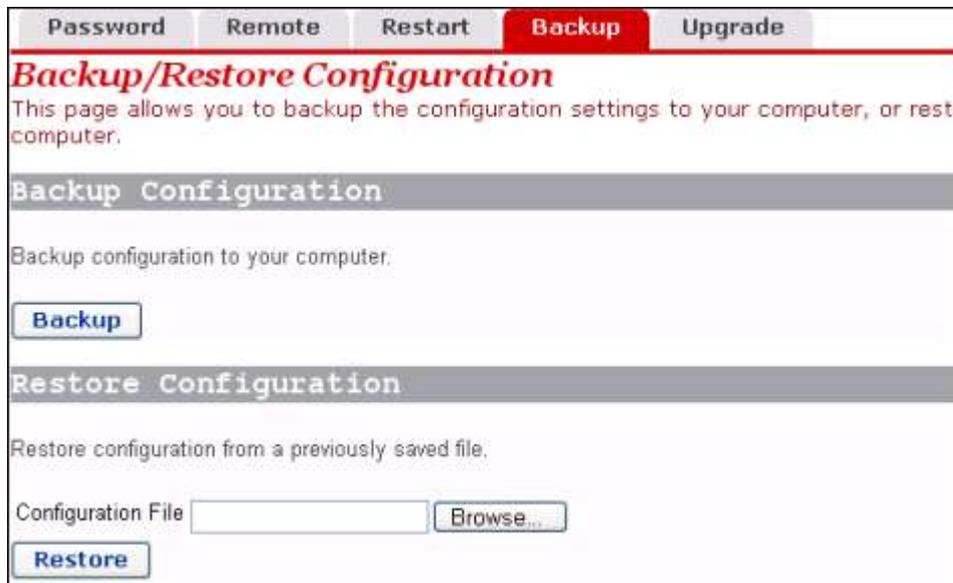


Figura 35 Página de Fazer Cópia de Reserva/Restaurar Configuração

1. Fazer cópia de reserva da configuração actual

Clique em <Backup> (cópia de reserva) para abrir a caixa de diálogo [File Download] (fazer download de arquivo), como ilustrado abaixo.



Figura 36 Caixa de diálogo de Download de Arquivo

Clique em <Save> (salvar) para abrir a janela [Save As] (salvar como), como ilustrado abaixo.

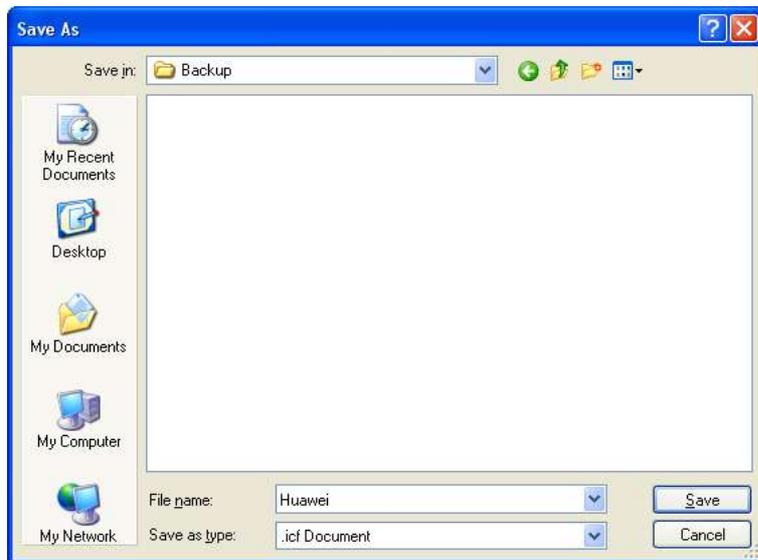


Figura 37 Salvar o arquivo de configuração

Selecione um directório para salvar o arquivo e digite um nome válido de arquivo (com o sufixo .icf) e, então, clique em <Save> (salvar) para fazer uma cópia de reserva da configuração actual no arquivo.

I. Usar o arquivo para restaurar a configuração

Para usar o arquivo salvo anteriormente para restaurar a configuração, clique em <Browse...> na 4.4.4 para abrir a janela [Choose file] (escolher arquivo), como ilustrado abaixo.

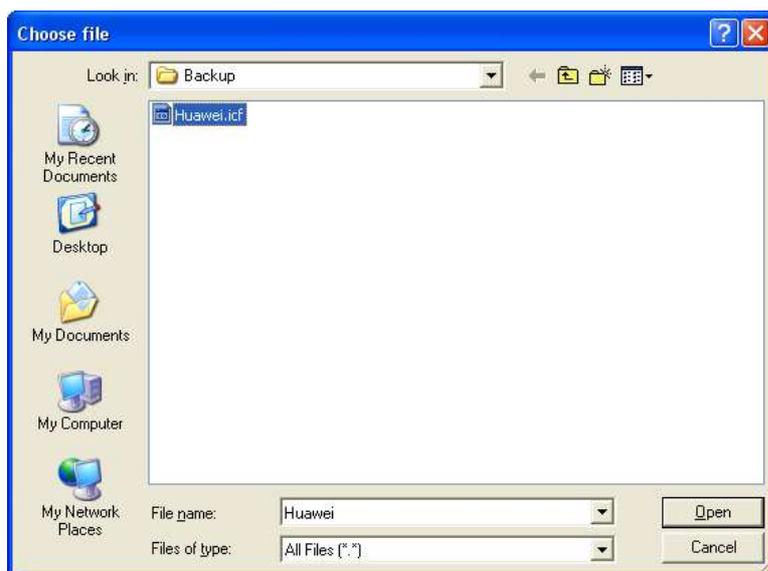
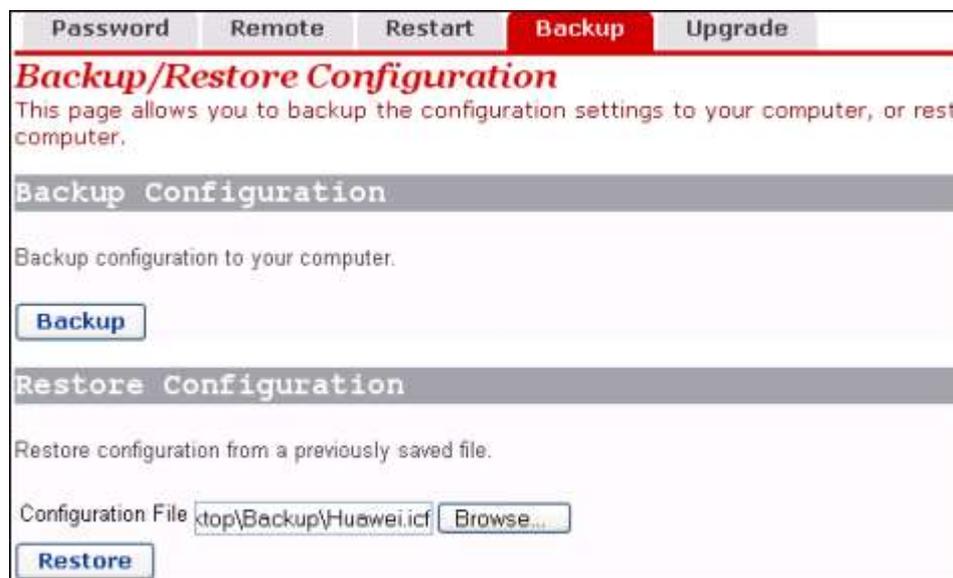


Figura 38 Escolher o arquivo de cópia de reserva

Localize o arquivo de configuração e clique em <Open> (abrir) para abrir a página, como ilustrado

abaixo. Clique em <Restore> (restaurar) para usar o arquivo para restaurar a configuração.



The screenshot shows a web interface with a navigation bar at the top containing tabs for 'Password', 'Remote', 'Restart', 'Backup', and 'Upgrade'. The 'Backup' tab is selected and highlighted in red. Below the navigation bar, the page title is 'Backup/Restore Configuration'. The main content area is divided into two sections: 'Backup Configuration' and 'Restore Configuration'. The 'Backup Configuration' section has a 'Backup' button. The 'Restore Configuration' section has a text input field for 'Configuration File' containing the path 'x:\top\Backup\Huawei.icf', a 'Browse...' button, and a 'Restore' button.

Figura 39 Restaurar a configuração

4.4.5 Actualização



The screenshot shows a web interface with a navigation bar at the top containing tabs for 'Password', 'Remote', 'Restart', 'Backup', and 'Upgrade'. The 'Upgrade' tab is selected and highlighted in red. Below the navigation bar, the page title is 'Firmware Update'. The main content area has a section titled 'Select Update File' with a link to 'Huawei'. Below this, there is a text input field for 'New Firmware Image', a 'Browse...' button, and an 'Update' button.

Figura 40 Actualização do software

Esta página permite-lhe actualizar o software do DR814Q. Digite o caminho local do arquivo de actualização do software transferido do website de suporte técnico da Huawei ou clique em <Browse...> para seleccionar este arquivo no seu PC e clique em <Update> (actualizar).

Durante a actualização, aparecerá uma barra de progresso na página, como ilustrado abaixo.

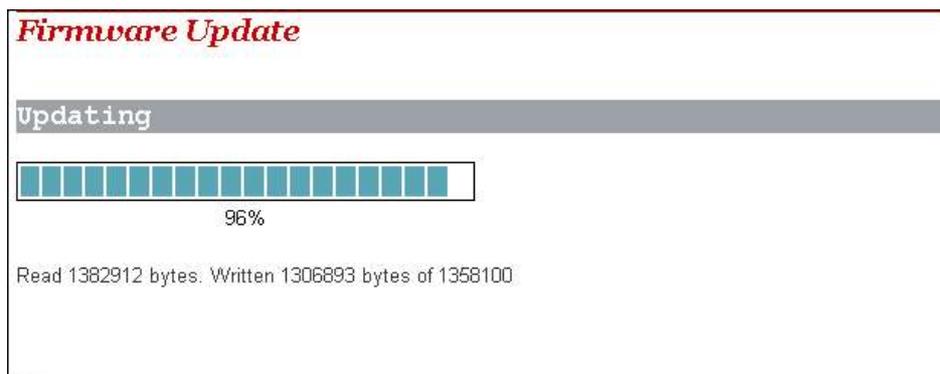


Figura 41 Progresso da actualização

A 4.4.5 mostra que a actualização está completa. Agora, precisará de reiniciar o DR814Q clicando em <Restart> (reiniciar).

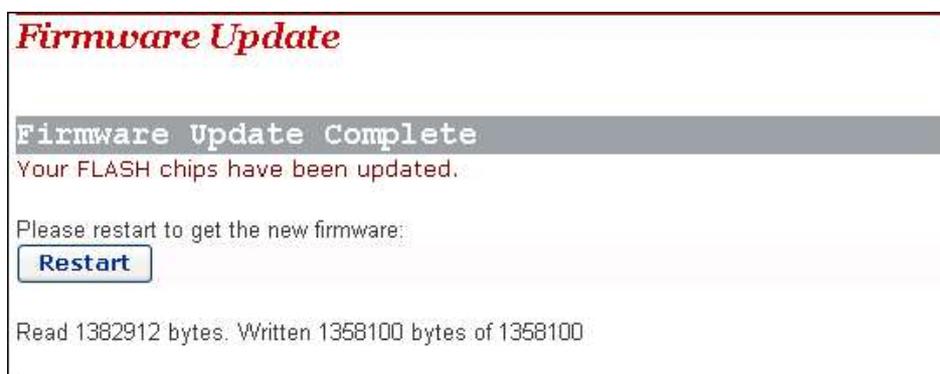


Figura 42 Completar a actualização



Aviso:

Após a actualização e o reinício, precisará de restaurar as configurações padrões de fábrica para garantir a configuração normal.

Clique em <Huawei> para aceder ao website de suporte técnico da Huawei para obter a última versão de software.

4.5 Estado

Clique em [Status] (estado) na barra de navegação para entrar na página correspondente onde estão disponíveis três separadores: *Status* (estado), *Log* (registro) e *Search Service* (serviço de busca). Clique no separador correspondente para entrar na página de configuração desejada.

4.5.1 Estado

Status | Log | Search Service

Status

This page shows the status of your connection

PPPoE Connection: Connection established [Disconnect](#)

Connected time so far: 00:08:33s

WAN IP Address: 18.0.0.100

Local IP Address: 192.168.1.1

Advanced Diagnostics

Connection Authentication: PPPoE Username/Password

PPPoE Dial-On-Demand: Disabled

IP address of PPP server: 18.0.0.1

Port Connection Status

Port	Type	Connected	Line State
DSL	atm	✓	N/A
Ethernet0	ethernet		N/A
Usb-ethernet	ethernet	✗	N/A

WAN Status

IP Address Type: Static or PPP

WAN Subnet Mask: 255.255.255.255

Default Gateway: 0.0.0.0

Primary DNS: 20.2.0.100

LAN Status

LAN Subnet Mask: 255.255.255.0

Act as Local DHCP Server: Yes

MAC Address: 00:0F:E2:00:00:01

Hardware Status

Up-Time: 03:50:41s

Current Time:

Version: DR814QV200DD001EX

CompileTime: Jul 16 2005 14:55:47

Vendor: [Huawei](#)

Defined Interfaces

PPPoE WAN uplink: [Show Statistics...](#) QoS:UBR Port:[dsl](#) VPI/VCI: 8/35 ✓

Figura 43 Página de configuração do estado

Esta página exhibe as informações úteis sobre a configuração do DR814Q, incluindo:

- Detalhes da ligação da rede
- Algumas informações importantes do sistema (informações de hardware e de versão)
- Tabela de redireccionamento IP
- Estado da ligação actual do DSL, Rede e porta USB

- Estado da porta WAN
- Estado da porta LAN
- Estatística em todos os interfaces

4.5.2 Registro

Esta página registra todos os tipos de eventos que ocorreram durante a operação do DR811/814.

The screenshot shows the 'Event log' page with the following content:

Status **Log** Search Service

Event log
This page shows recent events from your router

Showing all events

(most recent events last; times are since last reboot, or real time if available):

Time	
00:00:09	im:Changed iplan IP address to 192.168.1.1
00:36:07	webserver:Changed (null) IP address to 172.168.1.1
00:39:17	webserver:Object not found:Host hys5 not found/not using DHCP - unsuitable for Dynamic ZIPB
00:41:03	webserver:Changed (null) IP address to 172.16.1.1

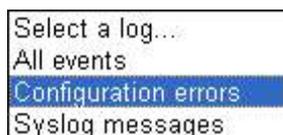
Clear these entries

Select events to view

Select a log... ▾

Figura 44 Registro

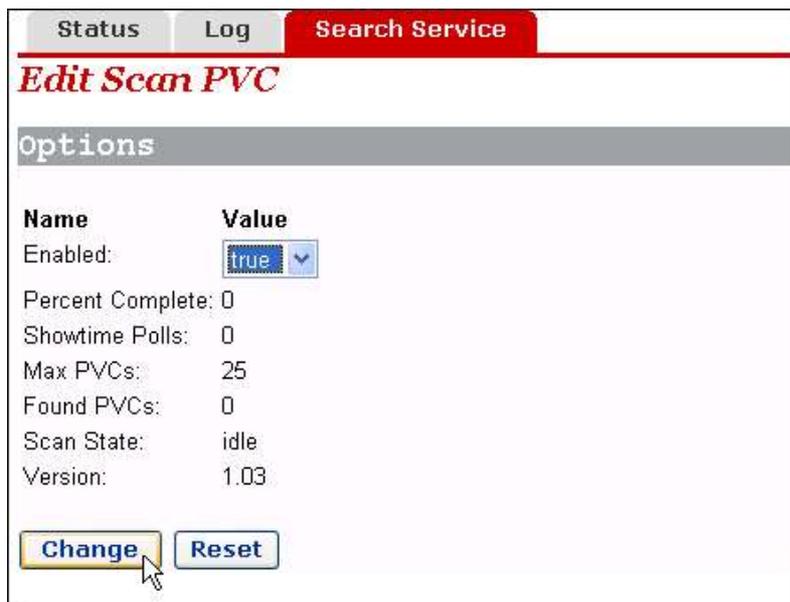
A lista drop-down na secção [Select events to view] (seleccionar eventos para visualizar) inclui as opções visíveis na figura abaixo. Seleccione um tipo de evento para visualizar as informações do evento correspondente.



Clique em <Clear these entries> (apagar estas entradas) para apagar os eventos exibidos actualmente.

4.5.3 Procura do PVC

A página [*Edit Scan PVC*] (editar Explorar PVC) permite-lhe procurar as configurações do PVC não usadas actualmente. Se o seu ISP tiver configurado serviço PVC dentro da faixa que pode ser procurada, após a procura estes serviços PVC serão automaticamente configurados na lista de serviços na página [*WAN Connections*] (ligações WAN) até o número de serviços alcançar oito nesta lista.



Name	Value
Enabled:	<input type="text" value="true"/>
Percent Complete:	0
Showtime Polls:	0
Max PVCs:	25
Found PVCs:	0
Scan State:	idle
Version:	1.03

Figura 45 Página para Explorar PVC

Selecione a opção **true** (verdade) da lista drop-down na 4.5.3 e clique em <Change> (alterar) para iniciar a procura. Este processo deve demorar cerca de cinco minutos.

Name	Value
Enabled:	false
Percent Complete:	0
Showtime Polls:	0
Max PVCs:	25
Found PVCs:	2
Scan State:	Success
Version:	1.03

Buttons: [Change](#) [Reset](#)

Figura 46 Procurar PVC

Como ilustrado na 4.5.3, foram encontrados dois PVCs. Clique em [*WAN Setup*] (configuração WAN) na barra de navegação; verá que os dois serviços encontrados pelo DR814Q serão automaticamente adicionados à lista de serviços da WAN, como ilustrado abaixo.

WAN services currently defined:

Service Name	IP/Bridge Interface Name	Description	Creator		
PppoeUp	ipwan	PPPoE WAN uplink	Factory Defaults	Edit...	
Rfc1483Up	Unattached	RFC1483 WAN uplink	Factory Defaults	Edit...	
ppp-0	ppp-0	Scanned ATM	scanpvc	Edit...	Delete...
rfc1483-0	rfc1483-0	Scanned ATM	scanpvc	Edit...	Delete...

Figura 47 Adicionar os serviços encontrados automaticamente

Se o serviço PPPoE ou PPPoA for encontrado, precisará de editar estes serviços adicionados automaticamente digitando um nome de utilizador e uma senha.

4.6 Salvar a Configuração

Entrar na página [*Save configuration*] (salvar configuração) depois de todas as configurações estarem completas. Clique em <Save> (salvar) para salvar as suas configurações de forma a que elas tenham efeito quando o DR814Q reiniciar.

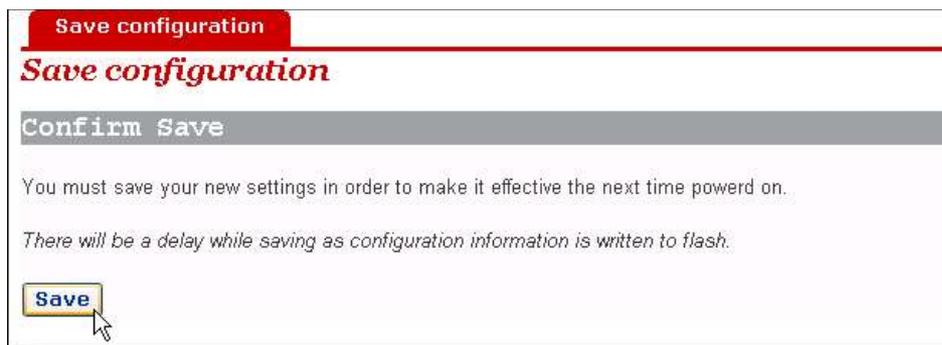


Figura 48 Salvar a configuração



Aviso:

Salve as suas configurações; caso contrário, elas perder-se-ão depois de o DR814Q reiniciar.

5 Configuração Avançada

Depois de completar o procedimento de configuração correctamente, o DR814Q pode aceder a todos os serviços da Internet. Este capítulo apresenta as configurações das funções avançadas do DR814Q para melhorar os desempenhos, satisfazendo assim vários requisitos na configuração da rede.

5.1 Ligar as Portas LAN aos PVCs

Clique em [LAN/PVC] para entrar na página [Attachment Setting] (configuração de anexação). Poderá ligar a porta de Rede a um PVC e configurar os parâmetros QoS correspondentes para o PVC.

I. Configurações da Ligação do PVC

Com a função de ligação do PVC, poderá ligar qualquer uma das quatro portas de Rede (portas LAN) a qualquer um dos quatro PVCs de fluxo ascendente. Cada PVC liga os dados a partir da porta de Rede ligada ao servidor de acesso de banda larga (BAS) para acomodar diferentes serviços de Internet através de diferentes portas de Rede. Os serviços, tais como o acesso a Internet, video-on-demand (vídeo-clubes) (VOD) e IPTV realizados por diferentes servidores de acesso, aumentam a segurança e a estabilidade do sistema e facilitam a carga dos BASs notoriamente.

Poderá também configurar uma porta de Rede como uma porta de gestão para administração dos dispositivos. Poderá aceder à página de gestão da configuração do seu DR814Q através de um host que esteja ligado à porta de gestão. Por padrão, as quatro portas LAN do DR814Q são todas portas de gestão.

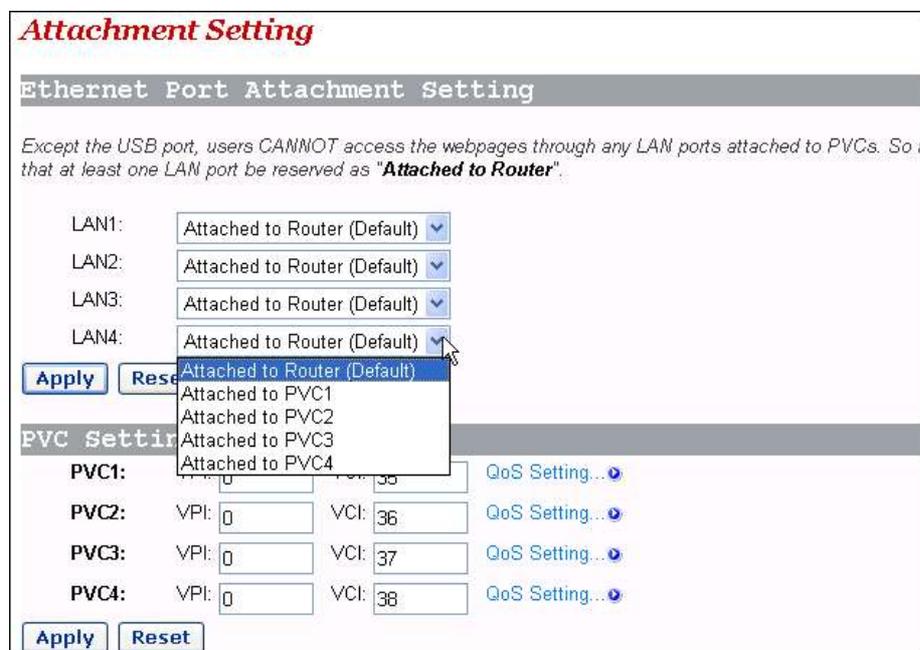


Figura 49 Configurações da Ligação do PVC

Como ilustra a I, há cinco opções para cada porta de Rede (LAN1 a LAN4) na lista drop-down:

Anexada ao PVC1/2/3/4 e anexada ao Router (Padrão).

Na configuração destas portas LAN, precisará de clicar em <Apply> (aplicar) para salvar a sua configuração e fazê-la surtir efeito. Então, na secção [*PVC Setting*] (configuração do PVC), configure os VPIs/VCI para os PVCs correspondentes. Os valores de VPI/VCI são fornecidos pelo seu ISP. Clique em <Apply> (aplicar), nesta secção, para salvar a sua configuração.



Aviso:

- Poderá gerir o seu DR814Q somente através do PC ligado à porta de gestão ou à porta USB.
 - Se todas as quatro portas de Rede estiverem configuradas para estarem ligadas aos PVCs, poderá ainda aceder à página de gestão das configurações através da porta USB. Consulte a secção 8“Apêndice - Configuração USB ” para obter mais informações sobre a porta USB.
 - Os valores VPI/VCI de PVCs diferentes não podem ser idênticos uns aos outros ou os mesmos àqueles das outras páginas de configuração.
-

O exemplo a seguir ilustra a configuração em suposição:

- Ligue uma porta LAN ao PVC 0/35 para aceder ao Website IPTV que o seu ISP estabeleceu. O Website usa o DHCP para atribuir endereços IP dinamicamente.
- Ligue as outras duas portas LAN ao PVC 0/100 e os PCs que se ligam a estas portas acederão à Internet através das ligações de linha discada PPPoE.
- Redireccione a última porta LAN para aceder à Internet e aplique o serviço PPPoE ligado por NAT a esta porta. Ligue-a ao PVC 8/35. O nome do utilizador e a senha que o seu ISP atribuiu são **username** e **myPassword**, respectivamente.

Siga estes passos para configurar o seu DR814Q.

- 1) Na página [*Rede Port Attachment Setting*] (configuração de anexação da porta de Rede) (ver I), seleccione a opção *Attached to PVC1* (anexa ao PVC1) da lista drop-down da LAN1 para ligar LAN1 ao PVC1 e LAN2 e LAN3 ao PVC2 da mesma forma. Deixe a configuração padrão

da LAN4 *Attached to Router* (anexa ao router) inalterada. Clique em *<Apply>* (aplicar) para salvar a sua configuração.

2) Na secção [*PVC Setting*] (configuração do PVC), configure **0/35** como o valor de VPI/VCI do PVC1, **0/100** como aquele do PVC2. Clique em *<Apply>* (aplicar) na secção [*PVC Setting*] (configuração do PVC), para salvar as suas configurações. Uma vez que não usa o PVC3 e o PVC4 aqui, não há necessidade de especificar os valores de VPI/VCI para eles.

The screenshot shows a web-based configuration interface for a router. It is divided into two main sections: "Attachment Setting" and "PVC Setting".

Attachment Setting: This section has a header "Ethernet Port Attachment Setting" and a warning: "Except the USB port, users CANNOT access the webpages through any LAN ports attached to PVCs. So it that at least one LAN port be reserved as 'Attached to Router'". Below this, there are four rows for LAN ports:

LAN1:	Attached to PVC1
LAN2:	Attached to PVC2
LAN3:	Attached to PVC2
LAN4:	Attached to Router (Default)

At the bottom of this section are "Apply" and "Reset" buttons.

PVC Setting: This section lists four PVCs with their respective VPI and VCI values:

PVC1:	VPI: 0	VCI: 35	QoS Setting...
PVC2:	VPI: 0	VCI: 100	QoS Setting...
PVC3:	VPI: 0	VCI: 37	QoS Setting...
PVC4:	VPI: 0	VCI: 38	QoS Setting...

At the bottom of this section are "Apply" and "Reset" buttons.

Figura 50 Configuração real na página de Configuração de Ligação

3) Clique em *<Quick Setup>* (instalação rápida) na barra de navegação e seleccione a opção de Login do PPPoE na página [*WAN Connections*] (ligações WAN). Configure os valores de VPI e VCI para **8** e **35**, respectivamente, digite **userName**, **myPassword** e **myPassword** nas caixas de texto PPPoE Username, PPPoE Password e PPPoE Password (confirmar), respectivamente e clique em *<Apply>* (aplicar) para salvar as suas configurações.

WAN connections
This page allows you to set up some authentication & log

Login Type

No Login / DHCP
 PPPoE Login

PPPoE Login Setup

VPI:
 VCI:
 PPPoE Username:
 PPPoE Password:
 PPPoE Password (confirm):
 PPPoE Access concentrator: (optional)

NOTE:
REMEMBER TO SAVE
CONFIG BEFORE
REBOOTING !!!

Figura 51 Definir a informação de autenticação do PPPoE

4) Demora cerca de dois minutos até que as suas configurações façam efeito. A I representa estas configurações. A configuração real está na página de ligações WAN. Clique em <Status> (estado) na barra de navegação para aparecer a página [Status] (estado), como ilustrado em 4.5.1. Poderá notar que o item de Endereço IP da WAN é um endereço IP público em vez do original 0.0.0.0. Então, poderá aceder à Internet através de um PC ligado à porta LAN4.

Status

PPPoE Connection: Connection established

Connected time so far: 00:14:56s

WAN IP Address: 42.42.42.42
Local IP Address: 192.168.1.1
MAC Address: 00:0F:E2:04:1B:85
Primary DNS: 20.2.0.100
Secondary DNS: 10.72.66.36

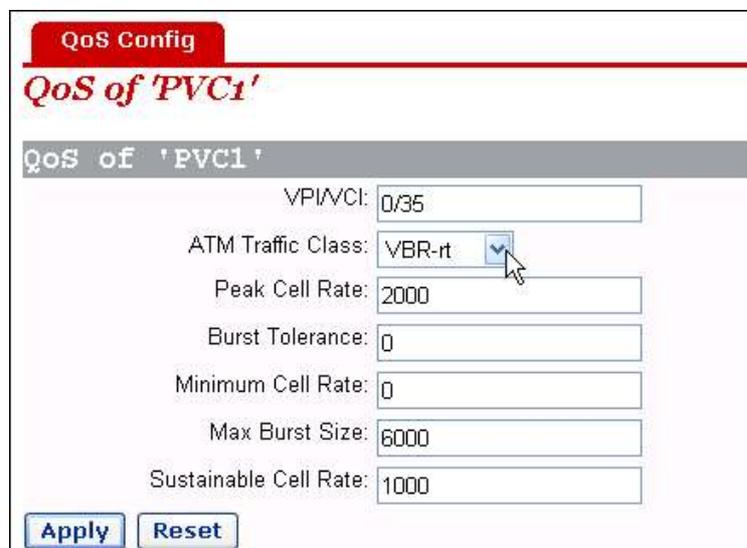
Figura 52 Configurações reais na página de Estado

5) Verifique a ligação das portas LAN aos PVCs. Ligue um PC, o qual está configurado para obter um endereço IP automaticamente, à porta LAN1. Poderá, então, aceder ao Website IPTV do seu ISP. Similarmente, ligue os PCs às portas LAN2 e LAN3 e aceda à Internet pela ligação PPPoE. Depois de ter entrado com o nome do utilizador e a senha, o PC poderá obter um endereço IP rapidamente e estabelecer uma ligação com o Website.

II. Configuração QoS

Para os pacotes de fluxo ascendente sobre a linha ADSL, o seu DR814Q suporta múltiplos serviços de modo de transferência assíncrona (ATM), tais como CBR, VBR-rt, VBR, UBR e ABR. O DR814Q oferece diferentes medidas, espaço em cache, prioridades de cronograma e modelagem de serviço para alocar largura de banda apropriada aos serviços ATM de diferentes tipos. Isto assegura um QoS de alto desempenho.

Clique em <QoS Setting...> (configuração QoS....) na secção [PVC Setting] (configuração PVC), como ilustrado em I, para entrar na página [QoS Config] (configuração QoS) de um PVC correspondente, como ilustrado abaixo.



The screenshot displays the 'QoS Config' interface for a specific PVC. The title bar reads 'QoS Config' and the main heading is 'QoS of 'PVC1''. Below this, the configuration parameters are listed in a table-like format:

VPI/VCI:	0/35
ATM Traffic Class:	VBR-rt
Peak Cell Rate:	2000
Burst Tolerance:	0
Minimum Cell Rate:	0
Max Burst Size:	6000
Sustainable Cell Rate:	1000

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

Figura 53 Página QoS Config

Poderá configurar diferentes tipos de serviço ATM para PVCs especificados a partir da lista drop-down *ATM Traffic Class* (classe de tráfego ATM) e configurar os parâmetros do QoS para o tipo de serviço seleccionado. Para obter mais informações, consulte a II.

Tabela 1 Descrições dos tipos de serviço ATM comumente usados

Tipo de serviço	Descrição
UBR (taxa de bits não especificada)	Adequado para serviços que não são críticos em tempo real e com grande tráfego em regime acelerado. A UBR requer serviços de melhor efeito no lado da rede. Quando solicitar serviços, não será solicitado para configurar parâmetros do QoS, excepto para PCR, que limita a taxa superior. O lado da rede não garante o QoS para serviços UBR. As células da UBR serão descartadas primeiro num congestionamento de rede. Uma ligação com erro é executada pelos protocolos de camadas superiores. As aplicações típicas são FTP e E-mail.
CBR (taxa de bits constante)	Adequado para serviços que requeiram largura de banda estática e que requeiram a prioridade mais alta. Este tipo de serviço pode proporcionar tráfego estável com o mínimo de regime acelerado. Somente o parâmetro PCR é necessário para a aplicação do serviço CBR. A fonte pode transmitir células numa PCR negociada ou numa taxa inferior a ela.
VBR-rt (taxa de bits variável em tempo real)	Sensível ao atraso e à instabilidade do fluxo de dados, mas em todos os restantes aspectos similar à CBR. Os serviços VBR-rt permitem regime acelerado limitado. A taxa de transmissão no lado da fonte pode ser diferente em tempo diferente. Os parâmetros requeridos para aplicação do serviço VBR-rt incluem PCR, SCR e MBS ou BT. As aplicações típicas da VBR-rt são serviços de voz e de vídeo interactivo e IPTV.
VBR (taxa de bits variável não em tempo real)	Adequado para serviços em regime acelerado não em tempo real. Comparada à VBR-rt, uma característica distinta dos serviços VBR é que os requisitos de tempo real não são tão cruciais e a prioridade para dados de serviço processados no lado da rede é também menor que aquela dos parâmetros VBR-tithe requerida pelos serviços VBR que incluem PCR, SCR e MBS (ou BT), os mesmos daqueles da VBR-rt.

Mantenha 0 inalterado para aquelas opções não relacionadas com a configuração. Como ilustrado na II, se **VBR-rt** for seleccionado da lista drop-down *ATM Traffic Class* (classe de tráfego ATM), precisará de configurar valores para *Peak Cell Rate* (taxa de células de pico), *Max Burst Size* (tamanho em regime acelerado máximo) e *Sustainable Cell Rate* (taxa de células sustentável) e deixar **0** nas caixas de texto *Burst Tolerance* (tolerância em regime acelerado) e *Minimum Cell Rate* (taxa de células mínima).

Este exemplo explica como deverá configurar os parâmetros QoS do ATM. Deverá configurar de

modo a satisfazer os seguintes requisitos para que os parâmetros QoS do ATM do seu DR814Q façam efeito:

- O *multiplexer* de acesso à linha de assinante digital (DSLAM) tem um controlo mínimo ou mesmo nenhum controlo sobre a porta LAN e taxas de fluxo ascendente do PVC, completamente dependente da linha ADSL. A taxa de fluxo ascendente real do ADSL pode ser 896 Kbps quando muito, se o DSLAM suportar somente o ADSL.

- Múltiplos PVCs são configurados sobre uma única linha ADSL.

- Suponhamos que:

- A taxa de fluxo descendente de cada PVC é estritamente especificada pelo escritório central (CO), enquanto que as taxas de fluxo ascendente dos PVCs são todas configuradas para 896 Kbps. O PVC1 e o PVC2 são configurados em cada linha ADSL, entre os quais o utilizador usa o PVC1 para aceder à Internet e o PVC2 para fornecer serviço de conversação de vídeo.

Análise:

Embora uma taxa de fluxo ascendente de 896 Kbps seja configurada para PVC1 e PVC2, respectivamente, no CO, os serviços de áudio e vídeo executados sobre eles podem ainda ser interferidos. Por exemplo, um serviço de carga ascendente, que consome uma largura de banda maior que 500 Kbps, irrompe no PVC1 quando uma conferência de vídeo, que necessita de uma largura de banda mínima de 384 Kbps para ambas as taxas, de fluxo ascendente e descendente, é realizada sobre o PVC2. Isto resulta numa largura de banda disponível para PVC2 menor que 384 Kbps, causando, assim, a interrupção do serviço de áudio e vídeo.

Para evitar isso, configure os parâmetros QoS como segue:

- 1) Clique em *<QoS Setting...>* (configuração do QoS...) na secção [*PVC Setting*] (configuração do PVC), como ilustrado em I, para entrar na página [*QoS Config*] (configuração do QoS) do PVC2.
- 2) Seleccione a opção **VBR-rt** a partir da lista drop-down *ATM Traffic Class* (classe de tráfego ATM).
- 3) Configure *Peak Cell Rate* (taxa de células de pico) para **2000** (aproximadamente 800 Kbps), *Max Burst Size* (tamanho em regime acelerado máximo) para **6000** e *Sustainable Cell Rate* (taxa de células sustentável) para **1000** (aproximadamente 400 Kbps).
- 4) Clique em *<Apply>* (aplicar) para salvar as suas configurações.

The screenshot displays the 'QoS Config' window for 'QoS of PVC2'. The configuration parameters are as follows:

Parameter	Value
VPI/VCI	0/36
ATM Traffic Class	VBR-rt
Peak Cell Rate	2000
Burst Tolerance	0
Minimum Cell Rate	0
Max Burst Size	6000
Sustainable Cell Rate	1000

Buttons: Apply, Reset

Figura 54 Configuração do QoS

Para PVC1, mantenha as configurações UBR padrões inalteradas. Desta forma o PVC1 poderá ocupar toda a largura de banda de fluxo ascendente, quando não houver tráfego no PVC2 e o PVC2 poderá sempre ser garantido com uma largura de banda média de 400 Kbps, para serviços de áudio e vídeo sobre si. Isto garante carga ascendente normal sobre o PVC1 e comunicação em tempo real não interrompida sobre o PVC2.

5.2 Segurança

Clique em [*Security*] (segurança) na barra de navegação para entrar na página correspondente, onde quatro separadores estão disponíveis: *Interface*, *Policy* (política), *Trigger* (excepção de segurança) e *IDS*. Clique no separador pretendido para entrar na respectiva página de configuração.

5.2.1 Interface

Toda as políticas de firewall foram planeadas para aceder entre os interfaces de segurança. Esta página permite-lhe ligar a função de segurança e configurar os interfaces de segurança.

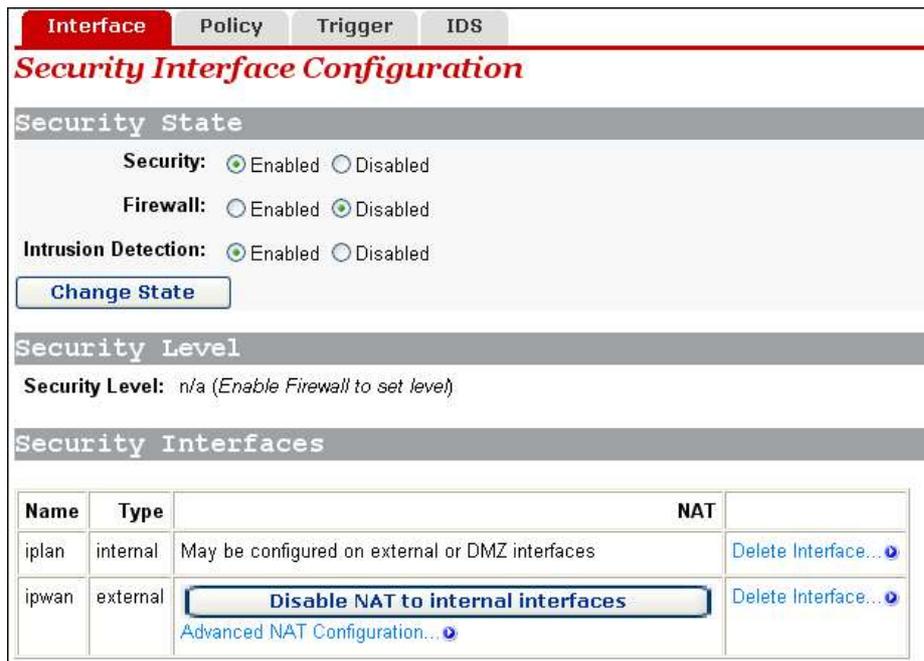


Figura 55 Adicionar um interface de segurança

I. Estado de segurança

Para ligar/desligar a função de segurança, seleccione a opção **Enabled/Disabled** (ligar/desligar) correspondente e clique em *<Change State>* (alterar estado).

Igualmente, tal operação poderá também ser usada para ligar/desligar a firewall e a detecção de intrusão.



Aviso:

- Poderá ligar a firewall, a detecção de intrusão e o NAT apenas quando a função de segurança estiver ligada.
- Se a função de segurança estiver desligada, a firewall, a detecção de intrusão e o NAT também estarão necessariamente desligados.

I. Nível de segurança

Depois de a firewall ter sido ligada, aparece a lista drop-down do [*Security Level*] (nível de segurança) na secção [*Security Level*], como ilustrado abaixo.

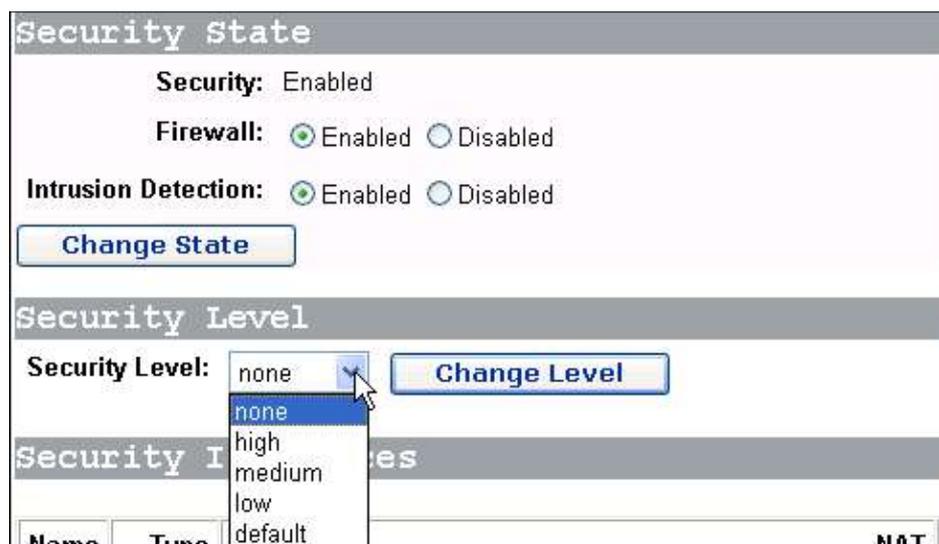


Figura 56 Lista drop-down do Nível de Segurança

Esta lista drop-down inclui as seguintes opções:

- nenhum: (configuração padrão) Indica que nem os utilizadores externos nem os internos têm direito de acesso.
 - alto: Indica que os utilizadores internos têm alguns direitos de acesso e os utilizadores externos não têm nenhum direito de acesso.
 - médio: Indica que os utilizadores externos e internos têm mais direitos de acesso.
 - baixo: Indica que os utilizadores externos e internos têm o máximo de direitos de acesso.
 - padrão: Indica que os utilizadores internos podem aceder a todos os serviços de Internet e os utilizadores externos são impedidos de aceder à rede interna.
- Para configurar o nível de segurança correspondente, seleccione uma opção da lista drop-down e clique em <Change Level> (alterar nível).

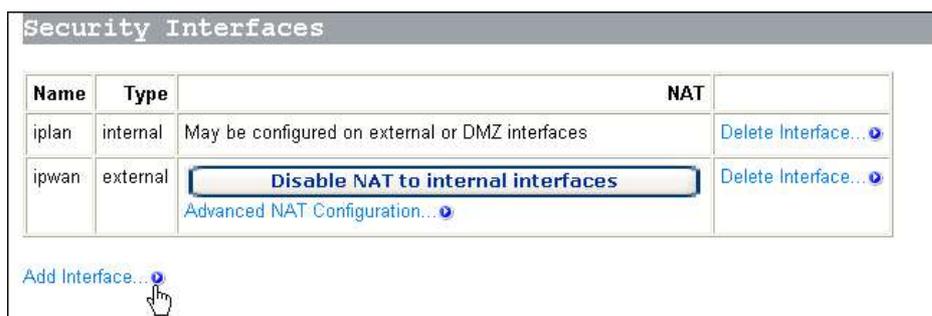
 **Aviso:**

•Por padrão, o nível de segurança **none** (nenhum) não é configurado com as políticas de filtragem de porta. Neste caso, os utilizadores internos não podem aceder a todos os serviços Internet e a rede interna não pode ser acedida de fora também. Para ligar o direito de acesso a um serviço, precisará de configurar a política da porta correspondente. Para obter detalhes, consulte a secção 5.2.2“Política”.

•As políticas de filtragem de porta padrões são configuradas para níveis de segurança diferentes de **none**. Depois de um nível de segurança ter sido configurado, aparece a política correspondente na página de filtragem de porta. Poderá também configurar uma política manualmente, conforme a necessidade. Para obter detalhes, consulte a secção 5.2.2“Política”.

II. Interface de segurança

Poderá estabelecer a política de firewall correspondente entre um grupo de interfaces de segurança. A tabela de interfaces de segurança lista as informações sobre os interfaces de segurança existentes. Por padrão, o DR814Q define todos os interfaces como sendo de segurança e não poderá depois criar um novo interface de segurança. Se criou um interface virtual (consultar a secção 4.3.1“LAN”), aparecerá <Add Interface...> (adicionar interface...) na página, como ilustrado abaixo.



Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface... 
ipwan	external	Disable NAT to internal interfaces Advanced NAT Configuration... 	Delete Interface... 

[Add Interface...](#) 

Figura 57 Interface de segurança

Neste caso, poderá adicionar um interface de segurança clicando em <Add Interface...> para entrar na página ilustrada abaixo.

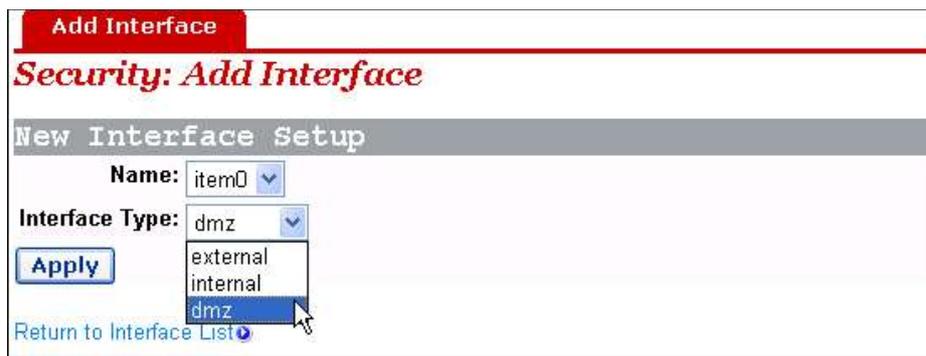


Figura 58 Segurança – adicionar um interface

Selecione um tipo de interface, **external** (externa), **internal** (interna) ou **DMZ** da lista drop-down do [Interface Type] (tipo de interface) e clique em <Apply> (aplicar). O interface configurado foi adicionado à tabela de interfaces de segurança na secção [Security Interfaces] (interfaces de segurança), como ilustrado abaixo.

Security Interfaces			
Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface...>
ipwan	external	Disable NAT to internal interfaces	Delete Interface...>
		Enable NAT to DMZ interfaces	
		Advanced NAT Configuration...>	
item0	dmz	Enable NAT to internal interfaces	Delete Interface...>
		Advanced NAT Configuration...> (Enable NAT for Advanced Configuration)	

Figura 59 Tabela de interfaces de segurança

Para excluir um interface de segurança, clique no botão <Delete Interface...> (excluir interface...) correspondente e clique em <Delete> (excluir) na página [Delete Interface] (excluir interface).

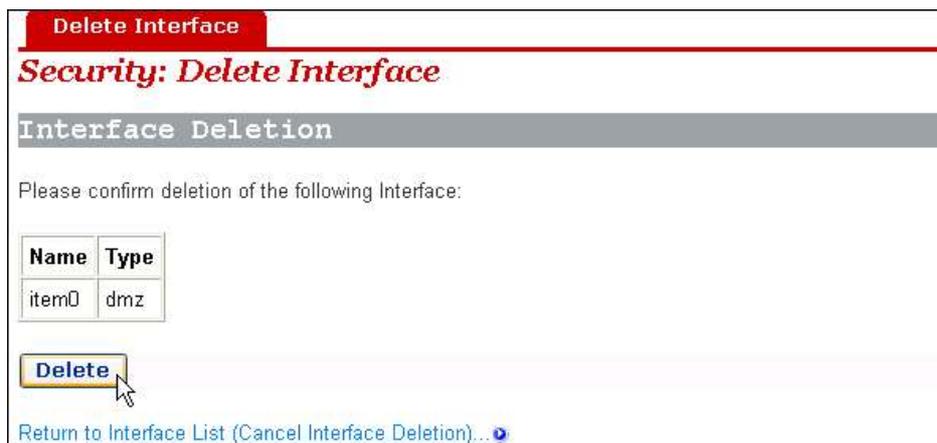


Figura 60 Excluir um interface de segurança

III. Configuração NAT

A tecnologia NAT pode traduzir um endereço privado interno num endereço IP público válido e, desta forma, os PCs na LAN podem compartilhar um endereço IP público para acesso de rede.

Poderá clicar nos três botões na página como ilustrado em II, para ligar/desligar o NAT entre os três tipos de interfaces. Após o NAT ter sido ligado, poderá configurar o NAT de forma avançada. Clique em *<Advanced NAT Configuration...>* (configuração NAT avançada...) para entrar na página de configuração, como ilustrado abaixo.

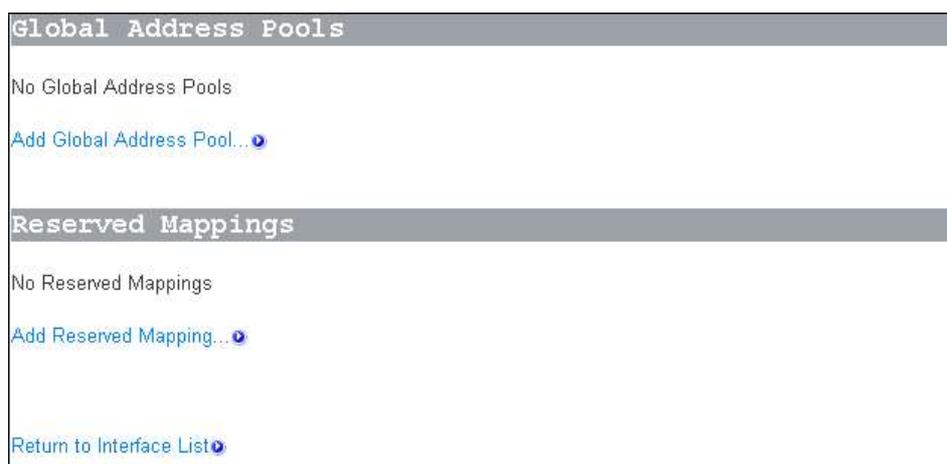


Figura 61 Configuração NAT Avançada

- 1) Conjunto de endereços globais

Esta página permite-lhe adicionar um endereço IP público obtido do seu ISP para o conjunto de endereços globais. Após o NAT ter sido ligado, os endereços internos são traduzidos aleatoriamente para um endereço não usado neste conjunto.

Para adicionar um endereço IP público ou um conjunto de endereços, clique em <Add Global Address Pool...> (adicionar conjunto de endereços globais...) para entrar na página de configuração, como ilustrado abaixo.

Figura 62 Adicionar um conjunto de endereços IP globais

Tabela 1 Descrições dos itens do conjunto de endereços IP globais

Item	Descrição
<i>Interface Type</i> (tipo de interface)	Seleccione o tipo de interface correspondente a um endereço IP público da lista drop-down.
<i>Use Subnet Configuration</i> (usar configuração de sub-rede)	Seleccione o método para especificar o endereço da lista drop-down. A opção <i>Use Subnet Mask</i> (usar máscara de sub-rede) indica que se especifique um segmento de rede. A opção <i>Use IP Address Range</i> (usar faixa do endereço IP) indica que se especifique uma faixa do endereço IP.
<i>IP Address</i> (endereço IP)	Digite o endereço IP de um segmento se a opção <i>Use Subnet Mask</i> (usar máscara de sub-rede) estiver seleccionada. Digite o endereço IP de início, se a opção <i>Use IP Address Range</i> (usar faixa do endereço IP) estiver seleccionada.
<i>Subnet Mask/IP Address 2</i> (máscara de sub-rede/endereço IP 2)	Digite a máscara de sub-rede do segmento, se a opção <i>Use Subnet Mask</i> (usar máscara de sub-rede) estiver seleccionada. Digite o endereço IP de fim, se a opção <i>Use IP Address Range</i> (usar faixa do endereço IP) estiver seleccionada.

Clique em <Add Global Address Pool> (adicionar conjunto de endereços globais) depois de a configuração estar completa. Este endereço IP será adicionado ao conjunto de endereços.

2) Servidor virtual

Depois de o NAT ter sido ligado, os dispositivos da rede interna não podem ser acedidos a partir da Internet. Para fornecer serviços públicos, tais como servidor de Web, Email e FTP para o exterior, um servidor virtual precisa de ser configurado para fazer o computador de rede com endereço IP estático privado fornecer estes serviços. Embora o endereço de serviço interno não possa ser acedido por utilizadores externos directamente, o DR814Q pode identificar solicitações de serviço através do número da porta e encaminhá-las para o servidor virtual.

Para configurar um servidor virtual, clique em <Add Reserved Mapping...> (adicionar mapeamento reservado...) na secção [Reserved Mappings] (mapeamentos reservados) (ver III) para entrar na página ilustrada abaixo.

Figura 63 Página de configuração do servidor virtual

Tabela 1 Descrições dos itens do servidor virtual

Item		Descrição
IP Address (endereço IP)	Global (global)	O endereço padrão, 0.0.0.0, pode ser reservado, o que significa que o endereço obtido a partir da porta WAN é usado. Ou poderá digitar o endereço a partir do conjunto de endereços globais.
	Internal (interno)	Digite o endereço IP do PC interno que fornece serviços de aplicação.
Transport (transporte)	Type (tipo)	Seleccione o tipo de protocolo para o serviço de aplicação a partir da lista drop-down.

<p><i>External Port Range</i> (faixa da porta externa)</p>	<p>A maioria dos serviços de aplicação encaminha os pacotes que chegam e que saem através da mesma porta. Neste caso, poderá apenas configurar <i>Start</i> (início) e <i>End</i> (fim) como este número de porta. Mas alguns serviços de aplicação encaminham pacotes que chegam e que saem, respectivamente, através de portas diferentes. Neste caso, precisará de digitar a faixa da porta usada pelos pacotes que chegam.</p>
<p><i>Internal Port Range</i> (faixa da porta interna)</p>	<p>A maioria dos serviços de aplicação encaminha os pacotes que chegam e que saem através da mesma porta. Neste caso, poderá apenas configurar <i>Start</i> (início) e <i>End</i> (fim) como este número de porta. Mas alguns serviços de aplicação encaminham pacotes que chegam e que saem, respectivamente, através de portas diferentes. Neste caso, precisará de digitar a faixa da porta usada pelos pacotes que saem.</p>

Clique em *<Add Reserved Mapping>* (adicionar mapeamento reservado) depois de a configuração estar completa.

Exemplo: Para configurar o PC com o endereço 192.168.1.100 como um servidor virtual para fornecer um serviço FTP para o exterior (com o número de porta 21), consulte a configuração na III. Desta forma, todas as solicitações do FTP dos utilizadores da Internet serão encaminhadas para o PC (servidor) com o endereço de IP fixado 192.168.1.100.

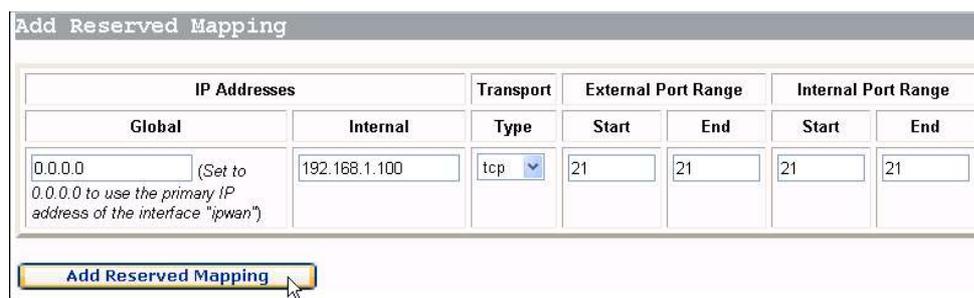


Figura 64 Exemplo de configuração de servidor virtual

Nota:

O NAT pode operar entre:

- O interface externo e o interface interno
- O interface externo e a DMZ
- A DMZ e o interface interno.

5.2.2 Política

A política de segurança é uma regra estabelecida para limitar dados que chegam e que saem entre diferentes tipos de interfaces. O DR814Q oferece um módulo de segurança poderoso para suportar as políticas de firewall configuradas entre os interfaces externo e interno, entre o interface externo e a DMZ e entre a DMZ e o interface interno, respectivamente, com isso, satisfazendo os vários requisitos sobre segurança de rede. A firewall deve ser ligada antes da criação de uma política.

The screenshot shows a web interface for 'Security Policy Configuration'. At the top, there are tabs for 'Interface', 'Policy' (which is selected), 'Trigger', and 'IDS'. Below the tabs is the title 'Security Policy Configuration' and a sub-header 'Current Security Policies'. A table lists three policies with columns for 'Interface Type 1', 'Interface Type 2', 'Validators', and 'Policy Configuration'. The 'Policy Configuration' column contains two links: 'Port Filters...' and 'Host Validators...'. At the bottom left, there is a link 'Return to Interface List'.

Interface Type 1	Interface Type 2	Validators	Policy Configuration	
external	internal	Only listed hosts blocked	Port Filters...	Host Validators...
external	dmz	Only listed hosts blocked	Port Filters...	Host Validators...
dmz	internal	Only listed hosts blocked	Port Filters...	Host Validators...

[Return to Interface List](#)

Figura 65 Configuração da política de segurança

I. Filtro de porta

Poderá configurar a política de filtragem de porta para limitar a transmissão de dados de um tipo de protocolo.

Para configurar um grupo de interfaces (supomos interface externo e interface interno) com a política de filtragem de porta, clique no botão <Port Filters...> (filtros de porta) correspondente para entrar na página ilustrada abaixo.

Firewall Port Filters: external-internal

Source Address	Destination Address	IP Protocol	Source Port		Destination Port		Direction		
			Min	Max	Min	Max	Inbound	Outbound	
Any	Any	TCP	0	65535	80	80	false	true	Delete
Any	Any	UDP	0	65535	53	53	false	true	Delete
Any	Any	TCP	0	65535	21	21	false	false	Delete
Any	Any	ICMP	N/A	N/A	N/A	N/A	false	true	Delete

[Add TCP or UDP Filter](#)
[Add Raw IP Filter](#)
[Return to Policy List](#)

Figura 66 Filtro de porta de firewall

Esta página lista as políticas configuradas actualmente. Seleccione nível de segurança de firewall diferente para exibir as políticas de filtragem de porta correspondentes. Outros tipos de solicitações de pacote não configurados com as políticas serão bloqueados pela firewall.

Para excluir uma política, clique no botão *<Delete>* (excluir) correspondente e, depois, clique em *<Delete>* (excluir), para confirmar, na janela (pop-up).

Para adicionar uma política para o número da porta do protocolo, clique em *<Add TCP>* (adicionar TCP) ou *<UDP Filter>* (filtro UDP) para entrar na página ilustrada abaixo.

Firewall Add TCP/UDP Port Filter: external-internal

Source address	Destination address	Protocol	Source port	Destination port	Direction	
					Inbound	Outbound
IP Address: <input type="text" value="0.0.0.0"/> Mask: <input type="text" value="0.0.0.0"/>	IP Address: <input type="text" value="0.0.0.0"/> Mask: <input type="text" value="0.0.0.0"/>	TCP	Range Start - End <input type="text" value="0"/> - <input type="text" value="65535"/>	Range Start - End <input type="text" value="0"/> - <input type="text" value="65535"/>	Allow	Allow

[Apply](#)

Figura 67 Política de filtragem de porta TCP/UDP

Tabela 1 Descrições dos itens do filtro de porta TCP/UDP

Item		Descrição
Source address (endereço da fonte)	IP Address (endereço IP)	Digite o endereço IP da fonte. O endereço padrão 0.0.0.0 indica qualquer nó na rede.
	Mask (máscara)	Digite a máscara de sub-rede da fonte. A máscara padrão 0.0.0.0 indica qualquer nó na rede.
Destination address (endereço do destino)	IP Address (endereço IP)	Digite o endereço IP do destino. O endereço padrão 0.0.0.0 indica qualquer nó na rede e está normalmente reservado.
	Mask (máscara)	Digite a máscara de sub-rede do destino. A máscara padrão 0.0.0.0 indica qualquer nó na rede e está normalmente reservado.
Protocol (protocolo)		Selecione um tipo de protocolo (TCP ou UDP) da lista drop-down e aplique a política de filtragem aos pacotes deste tipo.
Source port (porta da fonte)	Range Start-End (faixa início-fim)	Digite a faixa da porta da fonte. A faixa padrão de 0 a 65535 indica qualquer nó e está normalmente reservado.
Destination port (porta do destino)	Range Start-End (faixa início-fim)	Digite a faixa da porta do destino. Geralmente, este parâmetro precisa de ser configurado. Por exemplo, para controlar serviços de Web, digite o número de porta correspondente 80 . Para controlar serviços FTP, digite o número de porta 21 .
Direction (direcção)	Inbound (de entrada)	A direcção dos dados que chegam. Selecione <i>Allow</i> (permitir) para permitir que os hosts externos acedam aos hosts internos. Selecionar <i>Block</i> (bloquear) para proibir que os hosts externos acedam aos hosts internos.
	Outbound (de saída)	A direcção dos dados que saem. Selecione <i>Allow</i> (permitir) para permitir que os hosts internos acedam aos hosts externos. Selecionar <i>Block</i> (bloquear) para proibir hosts internos de aceder a hosts externos.

Clique em <Apply> (aplicar) depois de a configuração estar completa. Esta política será adicionada à lista de políticas de filtragem de porta.

Exemplo: Se pretender que utilizadores internos acedam ao servidor HTTP externo (com o número de porta 80), mas não quiser que utilizadores externos acedam ao servidor HTTP interno, poderá

efectuar a respectiva configuração, como ilustrada abaixo.

Firewall Add TCP/UDP Port Filter: external-internal

Source address	Destination address	Protocol	Source port	Destination port	Direction	
					Inbound	Outbound
IP Address: 0.0.0.0	IP Address: 0.0.0.0	TCP	Range Start - End 0 - 65535	Range Start - End 80 - 80	Block	Allow
Mask: 0.0.0.0	Mask: 0.0.0.0					

Figura 68 Exemplo de configuração de filtragem de porta

Para adicionar uma política para um protocolo, clique em <Add Raw IP Filter> (adicionar filtro IP bruto) na I, para entrar na página ilustrada abaixo.

Firewall Add Raw IP Filter: external-internal

Source address	Destination address	IP Protocol	Direction	
			Inbound	Outbound
IP Address: 0.0.0.0	IP Address: 0.0.0.0	Number or name: TCP	Allow	Block
Mask: 0.0.0.0	Mask: 0.0.0.0			

Apply

Figura 69 Política de filtragem baseada no tipo de protocolo

Tabela 1 Descrições dos itens da política de filtragem

Item	Descrição	
Source address (endereço da fonte)	IP Address (endereço IP)	Digite o endereço IP da fonte. O endereço padrão 0.0.0.0 indica qualquer nó na rede.
	Mask (máscara)	Digite a máscara da sub-rede da fonte. A máscara padrão 0.0.0.0 indica qualquer nó na rede.

Item		Descrição
<i>Destination address</i> (endereço do destino)	<i>IP Address</i> (endereço IP)	Digite o endereço IP do destino. O endereço padrão 0.0.0.0 indica qualquer nó na rede e está normalmente reservado.
	<i>Mask</i> (máscara)	Digite a máscara da sub-rede do destino. A máscara padrão 0.0.0.0 indica qualquer nó na rede e está normalmente reservado.
<i>IP Protocol</i> (protocolo IP)	<i>Number or name</i> (número ou nome)	Digite um nome ou número de protocolo e aplique esta política de filtragem aos pacotes deste tipo. O nome do protocolo pode ser TCP, UDP ou ICMP. Para outros protocolos, precisará de digitar os seus números de protocolo. Por exemplo, digite 2 para IGMP e 46 para RSVP.
<i>Direction</i> (direcção)	<i>Inbound</i> (de entrada)	A direcção dos dados que chegam. Seleccione <i>Allow</i> (permitir) para permitir que os hosts externos acedam aos hosts internos. Seleccione <i>Block</i> (bloquear) para proibir que os hosts externos acedam aos hosts internos.
	<i>Outbound</i> (de saída)	A direcção dos dados que saem. Seleccione <i>Allow</i> (permitir) para permitir que os hosts internos acedam aos hosts externos. Seleccione <i>Block</i> (bloquear) para proibir que os hosts internos acedam aos hosts externos.

Clique em <Apply> (aplicar) depois de a configuração estar completa. Esta política será adicionada à lista das políticas de filtragem de porta.

Exemplo: Por padrão, não é permitido aos hosts externos executarem o “ping” na porta WAN, mesmo se o nível de segurança estiver configurado para *low* (baixo). Para permitir que os hosts internos e os hosts externos executem o “ping” um com o outro, poderá efectuar a respectiva configuração, como ilustrada abaixo.

Firewall Add Raw IP Filter: external-internal

Source address	Destination address	IP Protocol	Direction	
			Inbound	Outbound
IP Address: 0.0.0.0	IP Address: 0.0.0.0	Number or name: ICMP	Allow	Allow
Mask: 0.0.0.0	Mask: 0.0.0.0			

Figura 70 Exemplo de política de filtragem para um protocolo (2)

I. Validadores de host

Com a especificação do endereço IP e a configuração da política correspondente, poderá restringir o direito de acesso de um host ou hosts num segmento de rede.

Para configurar validadores de host para um grupo de interfaces, clique no botão <Host Validators...> (validadores de host) correspondente na secção [Current Security Policies] (políticas de segurança corrente) (ver 5.2.2) para entrar na página ilustrada abaixo.

Configure Validators: external-internal

Host Validators

No Host Validators Defined

[Add Host Validator...](#)

[Return to Policy List...](#)

[Return to Interface List...](#)

Figura 71 Página de validadores de host

Para adicionar uma política de um validador de host, clique em <Add Host Validator...> (adicionar validador de host...) para entrar na página ilustrada abaixo.

Firewall Add Host Validator: external-internal

Add Host Validator

Host IP Address:

Host Subnet Mask:

Direction: ▼

Figura 72 Configurar um validador de host

Tabela 1 Descrições dos itens do validador de host

Item	Descrição
<i>Host IP Address</i> (endereço IP do host)	Digite o endereço IP do host ou do segmento de rede a ser limitado.
<i>Host Subnet Mask</i> (máscara de sub-rede do host)	Digite a máscara da sub-rede do host ou do segmento de rede a ser limitado.
<i>Direction</i> (direcção)	Selecione a direcção da transmissão de dados. Selecione <i>inbound</i> (de entrada) para bloquear somente os dados que chegam. Seleccionar <i>outbound</i> (de saída) para bloquear somente os dados que saem. Seleccionar <i>both</i> (ambos) para bloquear os dados que chegam e os que saem.

Exemplo: Para bloquear um host com o endereço IP 192.168.1.10 na LAN, para aceder a uma rede externa e permitir que utilizadores externos acedam a este host, poderá realizar a configuração, como ilustrada abaixo e clicar em <Apply> (aplicar).

Firewall Add Host Validator: external-internal

Add Host Validator

Host IP Address:

Host Subnet Mask:

Direction:

Figura 73 Exemplo de configuração de validador de host (1)

Exemplo: Se o utilizador encontrar um host suspeito (com o endereço IP 10.1.1.2) numa rede externa, poderá configurar a política do validador de host, como ilustrado abaixo, para bloquear o seu ataque no endereço interno.

Firewall Add Host Validator: external-internal

Add Host Validator

Host IP Address:

Host Subnet Mask:

Direction:

Figura 74 Exemplo de configuração de validador de host (2)

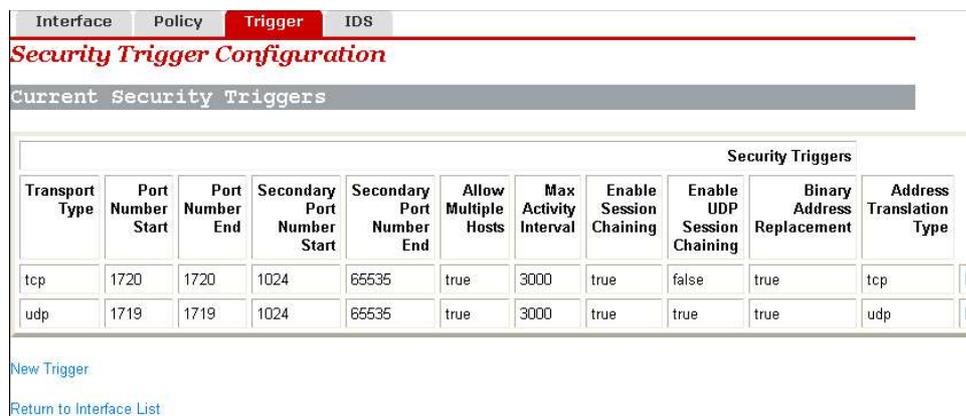
Como ilustrado na I, *inbound* (de entrada) foi seleccionado da lista drop-down [*Direction*] (direcção) e, assim, o dispositivo bloqueia somente os dados a partir do endereço 10.1.1.2 para o host interno, enquanto que o host interno ainda pode enviar dados ao endereço 10.1.1.2.

 **Aviso:**

- O validador de host pode ser utilizado para limitar o fluxo de dados entre as portas WAN e LAN.
 - A política de segurança começa a fazer efeito somente quando a firewall for ligada.
-

5.2.3 Trigger (excepção de segurança)

Uma excepção de segurança é usada para gerir protocolos de aplicações que estabelecem sessões separadas. Alguns protocolos de aplicações, tais como o NetMeeting, abrem as sessões primárias e ligações secundárias ao mesmo tempo, durante operações correntes. A excepção de segurança comunica ao mecanismo de segurança a necessidade de lidar com estas sessões secundárias e o router fornece indicações acerca de como controlá-las. A excepção de segurança controla as ligações dinamicamente, permitindo as sessões secundárias somente quando for necessário. Estas excepções de segurança não são limitadas pela firewall.



Security Triggers											
Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Address Translation Type	
tcp	1720	1720	1024	65535	true	3000	true	false	true	tcp	
udp	1719	1719	1024	65535	true	3000	true	true	true	udp	

[New Trigger](#)
[Return to Interface List](#)

Figura 75 Excepção de segurança

Esta página permite-lhe:

- Visualizar as informações na lista de excepções de segurança corrente.
- Criar uma nova excepção de segurança e adicioná-la à lista de excepções de segurança correntes.
- Excluir uma excepção de segurança existente.

Para criar uma nova excepção de segurança, clique em *<New Trigger>* (nova excepção de segurança) para entrar na página ilustrada abaixo.

Security: Add Trigger

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement
tcp			1024	65535	Allow		Allow	Allow	Allow

[Return to Trigger List](#)

[Return to Interface List](#)

Figura 76 Adicionar uma excepção de segurança

Tabela 1 Descrições dos itens de excepção de segurança

Item	Descrição
<i>Transport Type</i> (tipo de transporte)	Da lista drop-down, seleccione um tipo de transporte (TCP ou UDP) para o qual a excepção de segurança adicionada recentemente é especificada.
<i>Port Number Start</i> (início do número da porta)	Digite o início da faixa da porta de excepção de segurança que a sessão primária utiliza.
<i>Port Number End</i> (fim do número da porta)	Digite o fim da faixa da porta de excepção de segurança que a sessão primária utiliza.
<i>Secondary Port Number Start</i> (início do número da porta secundária)	Digite o início da faixa da porta de excepção de segurança que a sessão secundária utiliza.
<i>Secondary Port Number End</i> (fim do número da porta secundária)	Digite o fim da faixa da porta de excepção de segurança que a sessão secundária utiliza.
<i>Allow Multiple Hosts</i> (permitir múltiplos hosts)	Seleccione <i>Allow</i> (permitir) se pretender que uma sessão secundária seja iniciada por diferentes hosts remotos. Seleccione <i>Block</i> (bloquear) se pretender que uma sessão secundária seja iniciada somente por um host remoto.
<i>Max Activity Interval</i> (intervalo máx. entre actividades)	Digite o intervalo máximo entre actividades (em milissegundos) para sessões de porta secundárias depois de a sessão primária iniciar.

Item	Descrição
<i>Enable Session Chaining</i> (ligar encadeamento de sessões)	Selecione <i>Allow</i> (permitir) ou <i>Block</i> (bloquear) para determinar se o encadeamento multinível de sessões TCP é aceite ou não.
<i>Enable UDP Session Chaining</i> (ligar encadeamento de sessões UDP)	Selecione <i>Allow</i> (permitir) ou <i>Block</i> (bloquear) para determinar se o encadeamento multinível de sessões UDP é aceite ou não. Antes disso, deverá ligar o encadeamento de sessões.
<i>Binary Address Replacement</i> (substituição de endereço binário)	Selecione <i>Allow</i> (permitir) ou <i>Block</i> (bloquear) para determinar se será utilizada a substituição de endereço binário na excepção de segurança corrente ou não.
<i>Address Translation Type</i> (tipo de tradução de endereço)	Especifique o tipo de substituição de endereço numa excepção de segurança. Antes disso, deverá configurar a substituição de endereço binário para <i>Allow</i> (permitir).

Clique em <Apply> (aplicar) depois de a configuração estar completa. A página [*Security Trigger Configuration*] (configuração de excepção de segurança) é exibida, contendo detalhes da excepção de segurança recém configurada.

Para excluir um excepção de segurança existente, clique no botão <Delete> (excluir) correspondente na 5.2.3 e clique em <Delete> (excluir).

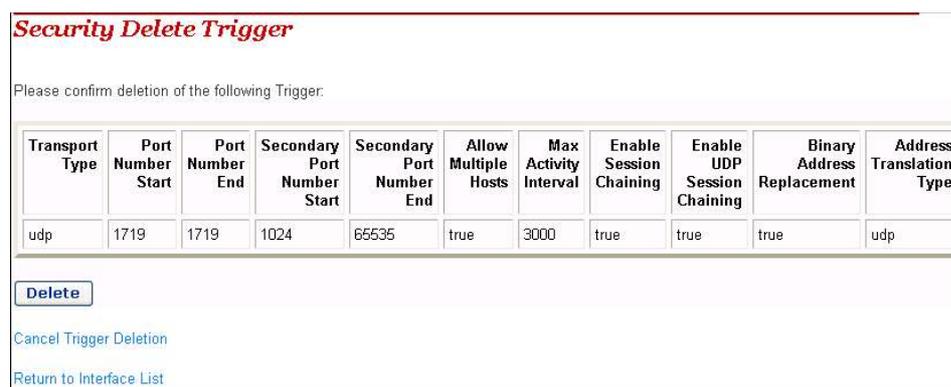


Figura 77 Excluir uma excepção de segurança

De fato, o DR814Q forneceu uma Porta de Acesso em Nível de Aplicação (ALG) para o *NetMeeting*. As aplicações de *NetMeeting* podem também ser normais, mesmo se a excepção de segurança da

porta não estiver configurada. O seguinte exemplo mostra como configurar uma excepção de segurança de porta, se o DR814Q não fornecer a ALG para o *NetMeeting*.

Suponhamos que o seu PC está ligado ao interface LAN do DR814Q e que deseja usar o *NetMeeting* para ter uma conversação de áudio/vídeo com utilizadores da Internet e para aplicar um quadro branco e partilha de programa.

Análise:

Uma chamada de *NetMeeting* é estabelecida na porta TCP 1720. Após a ligação ter sido estabelecida, o *NetMeeting* precisa de reactivar a porta TCP 1503 para usar o quadro branco e partilha de programa. O *NetMeeting* também precisa de ligar a porta do TCP e os protocolos UDP dentro da faixa de 1024 a 65535 para transmitir sinais de áudio e vídeo. Depois de a firewall ter sido ligada, poderá configurar as políticas de filtragem de porta e os servidores virtuais do TCP e protocolos UDP para todas as portas dentro da faixa. Deste modo, os utilizadores da Internet podem chamar activamente um utilizador LAN durante a utilização do *NetMeeting*. No entanto, uma possível omissão na configuração da política de filtragem e do servidor virtual pode causar uma falha no estabelecimento da conversação de áudio/vídeo. Além disso, a configuração do servidor virtual expõe quase todas as portas de host da LAN à Internet, resultando na insegurança do host.

Para resolver estes problemas, poderá efectuar a configuração respectiva, como ilustrado abaixo, para fazer a porta TCP 1720 efectuar uma excepção de segurança sobre a porta TCP/UDP dentro da faixa de 1024 a 65535.

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Tr
tcp	1720	1720	1024	65535	Allow	30000	Allow	Block	Allow	tc

Figura 78 Exemplo de configuração de excepção de segurança

Desta forma, todas as aplicações fornecidas pelo *NetMeeting* podem ser usadas normalmente depois de um utilizador da LAN chamar o utilizador da Internet e poderá apenas adicionar a política de acesso adequada para pacotes na porta TCP 1720 na página correspondente (ver I). Para fazer com que os utilizadores da Internet chamem os utilizadores da LAN e utilizem o *NetMeeting* normalmente, poderá apenas configurar o servidor virtual na porta TCP 1720, na página correspondente (ver III), e combiná-lo com a excepção de segurança da porta mencionada anteriormente.

5.2.4 IDS

O IDS protege a rede corrente contra os seguintes ataques:

- Rejeição de serviço (DoS).
- Monitorização de portas.
- Manipulação de dados da Web.

O IDS também implementa a função de lista negra. Ele não permite a entrada a hosts externos que tentem invadir a rede acedendo ao DR814Q, dentro de um limite de tempo específico.

Interface	Policy	Trigger	IDS
Firewall Configure Intrusion Detection			
Use Blacklist	true		
Use Victim Protection	true		
Victim Protection Block Duration	600		seconds
DOS Attack Block Duration	1800		seconds
Scan Attack Block Duration	86400		seconds
Scan Detection Threshold	5		per second
Scan Detection Period	60		seconds
Port Flood Detection Threshold	10		per second
Host Flood Detection Threshold	20		per second
Flood Detection Period	10		seconds
Maximum TCP Open Handshaking Count	100		per second
Maximum Ping Count	15		per second
Maximum ICMP Count	100		per second
<input type="button" value="Apply"/>			
<input type="button" value="Clear Blacklist"/>			
Return to Interface List			
Copyright 2003-2004 Huawei Tech			

Figura 79 Configuração do IDS

Tabela 1 Descrições dos itens de configuração do IDS

Item	Descrição
<i>Use Blacklist</i> (usar lista negra)	Selecione verdadeiro ou falso para ligar ou desligar a função de lista negra. Quando os ataques de hosts externos (Ascend Kill, Echo Scan, WinNuke, Xmas Tree Scan, IMAP SYN/FIN Scan, SMURF, TCP SYN Flood, Net Bus Scan e Back Orifice Scan) são encontrados, estes hosts são colocados na lista negra e seus pacotes são filtrados dentro do limite de tempo configurado.
<i>Use Victim Protection</i> (usar proteção de vítima)	Selecione <i>true</i> (verdadeiro) ou <i>false</i> (falso) para ligar ou desligar a proteção <i>Smurf</i> que protege o DR814Q contra ataques causados por “pings” com um endereço de <i>broadcast</i> (difusão). O atacante pode difundir “pings” com o endereço MAC da vítima servindo-se do endereço MAC da fonte. Sem esta protecção, os hosts na LAN enviarão pacotes de resposta à vítima, que ao receber estes pacotes, verá o seu sistema bloqueado. Com esta protecção, o DR814Q irá detectar e libertar os pacotes ICMP enviados pelo atacante e continuar a fazê-lo dentro de um limite de tempo específico.
<i>Victim Protection Block Duration</i> (duração do bloqueio de proteção de vítima)	Duração de bloqueio dos ataques da manipulação de dados da Web (Smurf) no host. Se o dispositivo detectar estes ataques, irá filtrar todos os pacotes ICMP que atacam o host e continuará a fazê-lo dentro de um limite de tempo específico. O valor padrão é 10 minutos.
<i>DOS Attack Block Duration</i> (duração do bloqueio de ataque de DoS)	Duração de bloqueio dos ataques DoS no host. Se o DR814Q detectar estes ataques, irá filtrar todos os pacotes que atacam o host e continuará a fazê-lo dentro de um limite de tempo específico. O valor padrão é 30 minutos. Os ataques DoS irão impedir que utilizadores legítimos acessem aos serviços normais da Internet. Os ataques DoS que o dispositivo pode detectar incluem Smurf Attack, SYN/FIN/RST Flood, ICMP Flood, Ping Flood, Ascend Kill, WinNuke Attack e Echo Chargen.
<i>Scan Attack Block Duration</i> (duração do bloqueio de ataques de monitorização)	Duração de bloqueio dos ataques de monitorização de portas no host. Se o DR814Q detectar estes ataques, irá filtrar todos os pacotes que atacam o host e continuará a fazê-lo dentro de um limite de tempo específico. O valor padrão é 24 horas.

Item	Descrição
<p><i>Scan Detection Threshold</i> (limiar de detecção de monitorização)</p>	<p>Limiar dos pacotes de monitorização de portas. Quando o DR814Q detectar pacotes de monitorização de portas (tais como SYN/ACK, FIN ou RST) enviados por um host por segundo e o número de pacotes alcançar o limiar, o dispositivo considera-os como ataques de monitorização de portas.</p> <p>Os ataques de monitorização de portas que o dispositivo pode detectar incluem Echo scan, Xmas Tree scan, IMAP scan, TCP SYN ACK scan, TCP FIN RST scan, NetBus scan, Back Orifice scan e SubSeven. A maioria dos ataques de monitorização de portas é o ataque do Trojan Horse (cavalo de Tróia).</p>
<p><i>Scan Detection Period</i> (período de detecção da monitorização)</p>	<p>Duração estatística de monitorização de porta. Quando o dispositivo detectar que a monitorização de porta inicia a contagem decrescente para o tempo configurado, o dispositivo bloqueará todos os pacotes que atacam o host e continuará a fazê-lo dentro do limite de tempo configurado na caixa de texto [<i>Scan Attack Block Duration</i>] (duração do bloqueio de ataque de monitorização de portas).</p> <p>O valor padrão é 60 segundos.</p>
<p><i>Port Flood Detection Threshold</i> (limiar de detecção do Flood da porta)</p>	<p>Quando o dispositivo detectar que os pacotes TCP SYNC enviados por um host por segundo a uma porta fixa excede este limiar, o dispositivo irá cronometrar o ataque Flood. Se a temporização alcançar o limite configurado na caixa de texto [<i>Flood Detection Period</i>] (período de detecção do flood), o DR814Q conclui que o host está a executar um ataque Flood à porta e inicia o bloqueio dos pacotes enviados pelo host.</p> <p>O valor padrão é 10.</p>
<p><i>Host Flood Detection Threshold</i> (limiar de detecção do Flood do host)</p>	<p>Quando o dispositivo detectar que os pacotes TCP SYNC enviados por segundo excedem este limiar, o dispositivo irá cronometrar o ataque Flood. Se a temporização alcançar o limite configurado na caixa de texto [<i>Flood Detection Period</i>] (período de detecção do flood), o DR814Q conclui que o host está a executar um ataque Flood à porta e começa a bloquear os pacotes enviados pelo host.</p> <p>O valor padrão é 20.</p>
<p><i>Flood Detection Period</i> (período de detecção do Flood)</p>	<p>Quando o DR814Q detectar que a duração do ataque Flood por um host alcança o período de detecção configurado, o dispositivo começa a bloquear os pacotes enviados pelo host.</p> <p>O valor padrão é 10 segundos.</p>

Item	Descrição
<i>Maximum TCP Open Handshaking Count</i> (contagem de <i>handshake</i> aberto do TCP máxima)	Quando a contagem de <i>handshaking</i> aberto que o DR814Q recebe por segundo a partir de um host excede o valor configurado, o dispositivo conclui que o ataque SYN/ACK foi detectado. O valor padrão é 100.
<i>Maximum Ping Count</i> (contagem de "ping" máxima)	O atacante deve enviar um número de pacotes de "ping" para uma rede. Estes pacotes consomem largura de banda em demasia e tornam os serviços normais de rede indisponíveis. Quando o dispositivo detecta que a contagem de pacotes de "ping" enviados por um host por segundo excede o valor configurado, o dispositivo conclui que o ataque Ping Flood foi detectado. O valor padrão é 15.
<i>Maximum ICMP Count</i> (contagem ICMP máxima)	O atacante deve enviar um número de pacotes ICMP (solicitação sem eco) a uma rede. Estes pacotes consomem largura de banda em demasia e tornam os serviços normais de rede indisponíveis. Quando o dispositivo detectar que a contagem de pacotes ICMP enviados por um host por segundo excedem o valor configurado, o dispositivo concluirá que o ataque ICMP Flood foi detectado. O valor padrão é 100.

Para modificar a configuração IDS corrente, digite os valores relevantes das opções IDS e clique em <Apply> (aplicar).

Para apagar a lista negra, clique em <Clear Blacklist> (apagar lista negra).



Aviso:

Por padrão, o modo de segurança encontra-se ligado.

5.3 Configuração de DMZ

A característica de Zona Desmilitarizada (DMZ) do DR814Q permite-lhe configurar uma DMZ numa LAN. Os hosts, que são configurados no mesmo segmento desta DMZ, podem efectuar comunicação bidirecional com outros utilizadores da Internet ou servidores. Ao mesmo tempo, poderá ligar o NAT e configurar uma política entre o interface DMZ e o interface interno, e entre o interface DMZ e o interface externo. Isto proporciona não só uma protecção da segurança para os hosts na DMZ, mas

também satisfaz as necessidades de instalação do servidor em LANs, por empresas de pequeno e médio porte, para fornecer serviços, tais como FTP e Web, para comunicação bidirecional com os utilizadores.

A seguinte figura representa os passos necessários para configurar a DMZ:

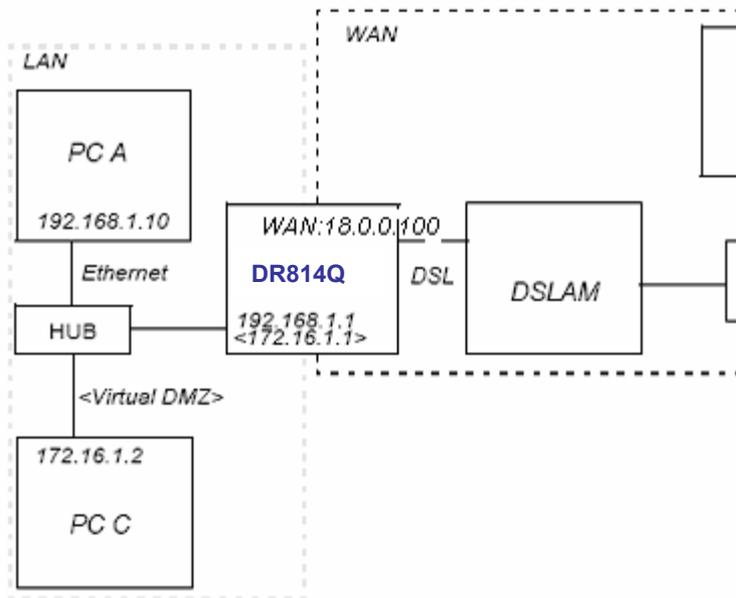


Figura 80 Configuração da DMZ

1. Criar um interface virtual

Para criar um interface virtual, consulte a secção 4.3.1“LAN”.

Digite os seguintes parâmetros na página [Create virtual interface] (criar interface virtual), como ilustrado abaixo, e clique em <Apply> (aplicar).

A captura de tela mostra a interface web 'Create virtual interface'. O título da página é 'Create virtual interface' em uma barra vermelha. Abaixo do título, há o texto 'Configure new virtual interface:'. O formulário contém dois campos de entrada: 'IP Address' e 'Netmask'. O campo 'IP Address' contém os valores 172, 16, 1 e 1. O campo 'Netmask' contém os valores 255, 255, 0 e 0. Abaixo do formulário, há um botão 'Apply'.

Figura 81 Criar um interface virtual

O resultado aparece na página [LAN connections] (ligações LAN) (ver 4.3.1), demonstrando que um

interface virtual chamado item0 foi adicionado à lista.

I. Adicionar um interface de segurança

Consulte a secção II "Interface de segurança " para adicionar um interface de segurança.

Realize a configuração na página [Add Interface] (adicionar interface), como ilustrado abaixo, e clique em <Apply> (aplicar).



The screenshot shows a web interface for adding a security interface. At the top, there is a red header with the text "Add Interface". Below this, the main title is "Security: Add Interface" in a stylized font. Underneath, there is a grey bar with the text "New Interface Setup". The form contains two dropdown menus: "Name:" with the value "item0" and "Interface Type:" with the value "dmz". Below the dropdowns is a blue "Apply" button. At the bottom left, there is a blue link that says "Return to Interface List" with a small arrow icon.

Figura 82 Adicionar um interface de segurança

Aqui, o item0 é um interface virtual adicionado anteriormente.

II. Configurar a política de filtragem de porta para interfaces externo-dmz e externo-interno, respectivamente

Para configurar a política de filtragem de porta para interfaces externo-dmz e externo-interno, respectivamente, consulte a secção I "Filtro de porta ".

Entre na página [Firewall Port Filters: external-dmz] (filtros de porta da firewall: externo-dmz) para configurar uma política, garantindo que os utilizadores possam aceder aos serviços da Internet (tais como HTTP, FTP e Telnet) especificados pela zona DMZ através do interface externo. Enquanto isso, entre na página [Firewall Port Filters: external-internal] (filtros de porta do firewall: externo-interno) para configurar a política de filtragem de porta, garantindo desligar os utilizadores sob o interface externo para aceder aos serviços de host sob o interface interno.

III. Configurar um host DMZ no mesmo segmento de uma zona DMZ

Certifique-se de que o endereço IP do host DMZ está no mesmo segmento daquele do interface virtual configurado acima. Por exemplo, configure o endereço IP para 172.16.1.100, a máscara para

255.255.0.0 e ligue o serviço de Internet correspondente e ligue este host DMZ à porta LAN do DR814Q.

IV. Configurar o servidor virtual correspondente

Para configurar o servidor virtual correspondente, consulte a secção III "2) Servidor virtual".

Configure o host DMZ como um servidor virtual para fornecer serviços de Internet, tais como http, ftp e telnet.

Desta forma, a DMZ inteira é configurada completamente e de modo seguro.

5.4 Configuração de rota

A configuração de rota estática faz com que o DR814Q comunique com PCs em diferentes segmentos de rede. Esta opção permite-lhe criar rotas IP estáticas para os endereços de destino, por um nome de interface IP ou um endereço de porta de acesso.

Para aceder à página de configuração do DR814Q, siga um dos seguintes passos:

- Clique em [WAN Setup] (configuração da WAN) na barra de navegação para entrar na página [WAN Connections] (ligações WAN) e clique em <Route setup...> (configurar rota...).
- Clique em [LAN Setup] (configuração da LAN) na barra de navegação para entrar na página [LAN Connections] (ligações LAN) e clique em <Route setup...> (configurar rota...).
- Clique em [Status] (estado) na barra de navegação para entrar na página [Status] (estado) e clique em <Route setup...> (configurar rota...).

Valid	Destination	Netmask	Gateway	Advertise	Delete?
✓	0.0.0.0	0.0.0.0	192.200.200.1	false	<input type="checkbox"/>

[Advanced Options...](#)

[Create new Ip V4Route...](#)

Figura 83 Configuração de rota

Esta página permite-lhe:

- Visualizar as informações sobre as rotas existentes
- Modificar as informações das rotas na lista de rotas
- Adicionar uma nova rota
- Excluir uma rota existente

Esta página permite-lhe também visualizar as seguintes informações sobre as rotas existentes:

- Se a rota é válida  ou inválida 
- Endereço IP do destino (*Destination*)
- Endereço da porta de acesso (*Gateway*)
- Máscara de rede (*Netmask*)
- Se a rota é informada através do RIP (verdadeiro ou falso)

Para alterar o endereço do destino, o endereço da porta de acesso, a máscara de rede e o estado de informação de uma rota, altere as configurações nas caixas de texto relevantes e clique em *<Apply>* (aplicar).

Para modificar as configurações de custo ou de interface para a rota, clique em *<Advanced Options...>* (opções avançadas...) para entrar na página [*Advanced Settings*] (configurações avançadas). Altere o valor relativo e clique em *<OK>*.

Advanced Settings	
Edit - Advanced Settings	
Name	Value
Destination	<input type="text" value="0.0.0.0"/>
Netmask	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text" value="192.200.200.1"/>
Cost	<input type="text" value="1"/>
Interface	<input type="text" value="none"/>
Advertise	<input type="text" value="false"/>
<input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	

Figura 84 Página de Configurações Avançadas

Para excluir uma rota existente, selecione a caixa de verificação *[Delete?]* (excluir?) correspondente na 5.4 e clique em *<Apply>* (aplicar).

Para adicionar uma nova rota, clique em *<Create new Ip V4Route...>* (criar nova rota Ip V4...) na 5.4, para entrar na página *[IP V4Route]* (rota IP V4). Digite os valores relativos das opções de rota e clique em *<OK>*. Clique em *<Cancel>* (cancelar) para cancelar as configurações e voltar à página de configuração de rotas.

Ip V4Route	
Create Ip V4Route	
Name	Value
Destination	<input type="text" value="0.0.0.0"/>
Netmask	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text"/>
Cost	<input type="text" value="1"/>
Interface	<input type="text" value="none"/>
Advertise	<input type="text" value="false"/>
<input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	

Figura 85 Criar uma rota

 **Aviso:**

Para serviços DHCP ou IP Estático, deverá digitar o endereço seguinte no [Gateway] (porta de acesso) arquivado (não o poderá deixar em branco), enquanto puder configurar a lista drop-down [Interface] para o valor padrão (Nenhum) ou para outro.

Para outros serviços (IPoA, PPPoA e PPPoE), poderá especificar um valor do interface ou da porta de acesso. Se ambos estiverem especificados, somente o valor do interface surtirá efeito.

Exemplo: A 5.4 ilustra uma ligação física que requer rotas estáticas.

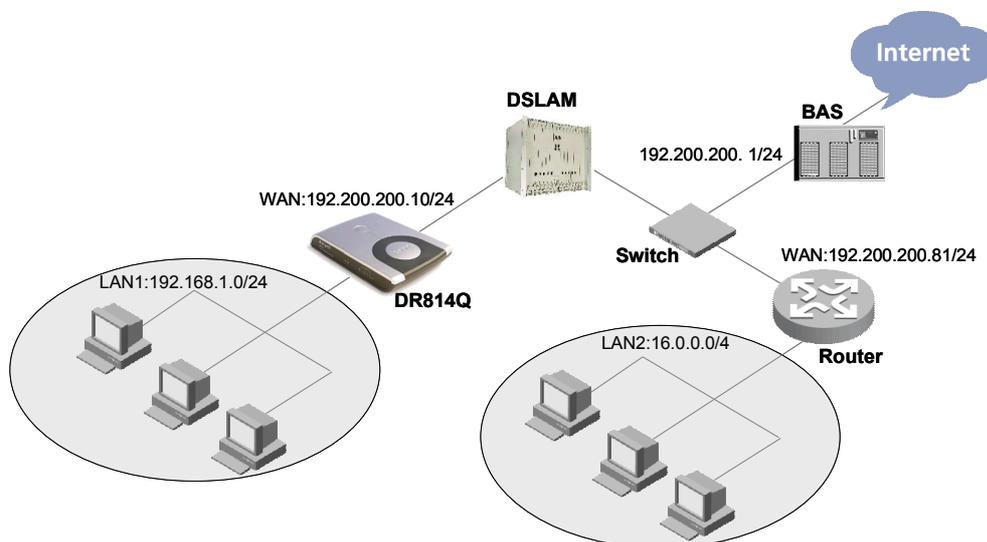


Figura 86 Diagrama da rede para configuração de rota estática

Na 5.4, supomos que um serviço DHCP está configurado para o DR814Q, o endereço da porta de acesso é 192.200.200.1 e há uma rota padrão servidor de acesso de banda larga (BAS). Um router está ligado a um outro segmento de rede, LAN2 (16.0.0.0/4), no lado da WAN e o endereço IP da porta WAN é 192.200.200.81. Para fazer os hosts na LAN1 acederem aos hosts na LAN2, normalmente precisará de criar uma rota, como ilustrado abaixo, de forma a que o DR814Q possa escolher rotas para pacotes correctamente.

Create Ip V4Route

Name	Value
Destination	<input type="text" value="16.0.0.0"/>
Netmask	<input type="text" value="240.0.0.0"/>
Gateway	<input type="text" value="192.200.200.81"/>
Cost	<input type="text" value="1"/>
Interface	<input type="text" value="none"/> ▼
Advertise	<input type="text" value="false"/> ▼

Figura 87 Exemplo de configuração de rota estática

5.5 Serviço

Dois separadores, SNTP e ZIPB, estão disponíveis na página [Service] (serviço). Clique no separador correspondente para entrar na página de configuração.

5.5.1 SNTP

Configure o DR814Q como um cliente SNTP e, assim, poderá obter informações precisas de hora/data a partir do servidor SNTP correspondente. Se o seu *router* não estiver ligado ao servidor SNTP, poderá ajustar a hora/data no DR814Q.

SNTP ZIPB SNMP

Current System Time: **May 08 2005 11:32:09**

Current Time Zone: **CCT**

Current Synchronized NTP Server: **time.nist.gov**

Synchronize Client with NTP Server now!

Select a Local Timezone (+UTC/GMT time):

SNTP - NTP Server Configuration Parameters

NTP servers:

IP Address	DNS Hostname
time.nist.gov	<input type="button" value="Delete"/>

Add NTP Server IP Address:

Add NTP Server Hostname:

Copyright 2003-2004 Huawei Tec

Figura 88 Configuração SNTP

Esta página permite-lhe:

- Visualizar a configuração de hora do sistema corrente
- Ajustar o fuso horário
- Configurar o servidor NTP na Internet para fazer o relógio do DR814Q sincronizar o seu relógio interno.

Para sincronizar a hora local do *router* com o servidor SNTP, clique em <Synchronize> (sincronizar).

Para ajustar o fuso horário, seleccione uma opção desejada da lista drop-down correspondente e clique em <Set Timezone> (ajustar fuso horário).

Para adicionar um servidor NTP, digite o endereço IP ou o nome do domínio do servidor SNTP no campo [NTP servers:] (servidores NTP:) e clique em <Add> (adicionar).

Para excluir um servidor NTP existente, clique no botão <Delete> (excluir) correspondente.

5.5.2 ZIPB

A ZIPB (ponte PPP de instalação zero) pode garantir que um utilizador SOHO possa obter um endereço IP público através do *router* e resolver o problema de todos os *routers* SOHO com NAT ligadas levarem a que parte da aplicação seja incapaz de funcionar normalmente.

SNTP ZIPB SNMP

ZIPB is currently *disabled*.

Enable

Choose which computer will use the public IP address:

None ▾

Apply

ZIPB advanced configuration

*Configure the specifics of how you wish ZIPB to operate here. At a minimum, ZIPB requires one LAN interface and one WAN interface. If no interfaces are chosen, ZIPB will automatically use the first available LAN and WAN interfaces. ZIPB will also do this if you choose an IP interface incorrectly. **Note:** Some settings may be disabled and re-enable ZIPB.*

LAN interface: none ▾

WAN interface: none ▾

OK **Reset**

Figura 89 Configuração da ZIPB

Esta página permite-lhe:

- Ligar/desligar o modo ZIPB
- Especificar o host ZIPB
- Configurar o ZIPB de forma avançada.

Se a ZIPB estiver actualmente desligada, clique em <Enable> (ligar) para ligá-la. Se estiver ligada, clique em <Disable> (desligar) para desligá-la.

Seleccione o PC que usará o endereço IP público na LAN da lista drop-down e clique em <Apply> (aplicar).

Para efectuar a configuração ZIPB avançada, siga estes passos:

- Selecione o interface LAN no qual a ZIPB será executada a partir da lista drop-down [*LAN interface*] (interface LAN).
- Selecione o interface WAN no qual a ZIPB será executada a partir da lista drop-down [*WAN interface*] (interface WAN).
- Clique em <OK> depois de a configuração da ZIPB estar completa.



Aviso:

- Certifique-se de que a ZIPB está desligada antes de alterar a configuração da ZIPB. Altere a configuração e clique em <OK>. A nova configuração surtirá efeito depois de ter ligado a alteração da ZIPB. Qualquer alteração na configuração não terá efeito se a ZIPB estiver ligada.
 - As alterações de configuração na ZIPB não serão salvas e, assim, precisará de reconfigurá-la sempre que reiniciar o *router*. Isto é, faça o host ZIPB anterior obter o endereço IP novamente através do DHCP e, então, especifique um novo host da ZIPB da lista drop-down.
 - Poderá ligar a ZIPB somente para dois serviços WAN: PPPoE e PPPoA.
-

5.5.3 SNMP

O DR814Q suporta a função proxy de protocolo de gestão de rede simples (SNMP), trocando informações SNMP com os sites de gestão de rede através do SNMP.

community Name	Write Enable	ServerIP	
public	false	0.0.0.0	Delete
password	true	0.0.0.0	Delete
ADSL	true	127.0.0.2	Delete

Add a community:

community

WriteEnable

ServIP

Figura 90 Página de Configuração de Cliente SNMP

Poderá criar uma comunidade SNMP na página correspondente à 5.5.3 e esta comunidade será exibida na lista de comunidades. O DR814Q autentica os pacotes SNMP de acordo com as informações definidas na lista.

Para adicionar uma comunidade, consulte as seguintes informações para efectuar as configurações e clique em <Add> (adicionar).

- community*: Digite o nome da comunidade, identificando unicamente uma comunidade SNMP. Os pacotes em desacordo com o nome da comunidade serão descartados.
- WriteEnable*: Especifique o acesso certo para a comunidade. Se *Read-Only* (somente de leitura) estiver seleccionado, esta comunidade poderá somente visualizar as informações do DR814Q; se *Read-Write* (leitura-escrita) estiver seleccionado, esta comunidade pode visualizar ou modificar as informações do DR814Q.
- ServIP*: Especifique o endereço IP do site de gestão que envia pacotes de SNMP. É recomendado que mantenha a configuração padrão 0.0.0.0, a qual indica que o endereço IP da fonte, que envia os pacotes SNMP, não é restrito.
- Para excluir a comunidade actual, clique no <Delete> (excluir) correspondente.

6 Localização de Defeitos

Este capítulo fornece as soluções para os problemas que possa encontrar, quando instalar ou utilizar o DR814Q, e fornece instruções para usar vários utilitários do IP para diagnosticar problemas. Contacte o Suporte ao Cliente se estas sugestões não resolverem os problemas.

6.1 Localização de Defeitos do DR814Q

Sintoma 1: O LED de energia não acende.

Solução: Verificar se:

- O transformador de energia que vem com o DR814Q está a ser utilizado.
- O transformador de energia está firmemente ligado ao DR814Q e à tomada de energia.

Sintoma 2: O LED ADSL2+ Link não se acende após o cabo do telefone ter sido ligado.

Solução: Verifique se o cabo do telefone está firmemente ligado à porta ADSL e à porta do telefone.

Sintoma 3: O LED LAN não acende depois de o cabo Rede ter sido ligado.

Solução: Verificar se:

- A ligação da energia está boa.
- O cabo de Rede está firmemente ligado à porta.
- Está a utilizar o cabo correcto. Para verificar isto, ligue as duas extremidades do cabo às portas LAN do DR814Q e verifique se o LED correspondente acende. Se não, troque o cabo e siga os passos descritos na secção 2.3“Ligação do Dispositivo ” para estabelecer a ligação.
- O PC tem um NIC de Rede instalado correctamente.

Sintoma 4: Não se recorda da sua senha.

Solução: Se não alterou a senha, use o nome do utilizador (**admin**) e a senha (**admin**) padrões. Mantenha pressionado o botão Reset por pelo menos cinco segundos para restaurar as configurações padrões no DR814Q. Então, poderá usar o nome do utilizador e a senha padrões.



Aviso:

O reset no DR814Q remove todas as configurações optimizadas e restaura os padrões.

Sintoma 5: Falha ao aceder à página de configuração da Web.

Solução: Siga os procedimentos para verificar se:

- 1) A versão do Internet Explorer é Microsoft Internet Explorer 5.5 ou Netscape 6.0 ou mais recente.
- 2) O PC e o DR814Q estão no mesmo segmento de rede.
- 3) Use o comando *ping* numa janela MS-DOS para verificar a ligação da rede:
 - Efectue o “ping” em 127.0.0.1 para ver se o protocolo TCP/IP está instalado.
 - Efectue o “ping” em 192.168.1.1 (o endereço IP padrão da porta de acesso) para verificar se há ligação entre o PC e o DR814Q na LAN.
- 4) Se as ligações físicas estão normais, mas ainda não pode aceder às páginas de configuração da Web do DR814Q; certifique-se de que o servidor proxy e a ligação de linha discada estão desligados.

Sintoma 6: Falha ao aceder à Internet com o seu PC.

Solução: Siga o procedimento:

- 1) Verifique se o LED ADSL2+ Link fica continuamente aceso. Se não, verifique a ligação da linha ADSL.
- 2) Verifique se o endereço IP foi obtido e poderá executar o “ping” no endereço IP da porta LAN do DR814Q, se configurar o PC para obter os endereços IP do host e do servidor DNS automaticamente (recomendado). Consulte a secção 6.2.1 “Ping” para rever as instruções de como usar o utilitário “ping”. Se não puder executar o “ping” na porta, verifique se o cabo Rede está correcto.
- 3) Quando o PC em utilização for especificado com um endereço IP privado, certifique-se de que: O PC reside no mesmo segmento daquele da porta LAN do DR814Q. O endereço IP da porta de acesso é especificado como aquele da porta LAN do DR814Q. O endereço IP do DNS é especificado como aquele da porta LAN do DR814Q ou do Servidor DNS que o ISP aloca. O host está apto a executar o “ping” no endereço IP da porta LAN do DR814Q.

4) Se o host pode comunicar com o DR814Q normalmente, mas não pode efectuar a ligação à Internet, faça login na página [*Status*] (estado) do DR814Q (consulte a secção 4.5“Estado”) primeiro e verifique se a porta WAN do DR814Q obteve o endereço IP da Internet e se a rota padrão existe.

Sintoma 7: Não pode aceder às páginas Web através do PC na LAN.

Solução: Siga o procedimento para verificar:

1) O endereço IP do servidor DNS especificado no PC está correto. Se especificar o PC para obter o endereço do servidor DNS dinamicamente, verifique com o seu ISP se o endereço configurado no DR814Q está correcto e, então, poderá usar o utilitário “ping” para testar a ligação com o servidor DNS do seu ISP.

2) Geralmente, se um host pode executar o “ping” no endereço IP da Internet, mas não pode abrir as páginas da Web, o servidor DNS do ISP está com uma falha temporária. Neste caso, poderá escolher um dos seguintes modos para resolver o problema: Alterar manualmente o endereço IP do DNS do seu PC para o endereço de um servidor DNS que esteja a funcionar normalmente. Efectuar login na página da Web do DR814Q e modificar manualmente a configuração para Conversão de Protocolo DNS (consulte a secção 4.2.2“Conversão de Protocolo DNS ") e, então, verificar pelo comando **nslookup**, como descrito na secção 6.2.2“Nslookup”.

Sintoma 8: Falha ao salvar as alterações feitas nas páginas de configuração da Web.

Solução: Certifique-se de que clicou em <Apply> (aplicar) para confirmar todas as alterações que efectuou. Depois de completar todas as configurações, entre na página [*Save Configuration*] (salvar configuração) para salvá-las, fazendo, desta forma, com que elas surtam efeito quando o DR814Q for ligado na próxima vez.

Sintoma 9: Poderá aceder à maioria dos websites, mas, às vezes, é esgotado o tempo de ligação a alguns websites. Quando configura o DR814Q para operar no modo ponte e o seu PC para estabelecer uma ligação de linha discada, poderá aceder aos websites normalmente. Como ocorre este problema?

Solução: Este problema é devido ao facto do valor de MTU do cliente para o DR814Q ter sido configurado por excesso. Para resolver o problema, entre na página de edição específica (consulte a secção 4.2.1“WAN”) para alterar o valor MTU para outro menor, tal como 1440, e seleccione *true*

(verdadeiro) da lista drop-down [*TCP MSS Clamp*].

Para além disso, se falhar ao enviar um E-mail na LAN, mas tiver êxito quando alterar um servidor SMTP, ou se falhar ao transferir arquivos pelo software de comunicação ponto-a-ponto, mas tiver êxito a transferir fotos para outros utilizadores, isto pode ser causado pelas configurações do MTU para o interface LAN, se tiver certeza que o servidor funciona bem. Entre na página do separador [*LAN Connections*] (ligações LAN) (consulte a secção 4.3.1“LAN”) para alterar o valor MTU para outro menor, tal como 1440, e seleccione *true* (verdadeiro) da lista drop-down [*TCP MSS Clamp*].

Sintoma 10: Alguns serviços estão indisponíveis uma vez que a firewall está ligada.

Solução: Como as regras da firewall do DR814Q são muito rigorosas, recomenda-se que alguém familiarizado com os serviços WAN e com a configuração de *router* ligue a firewall e configure as regras da firewall. Antes da criação das regras da firewall, deverá estar esclarecido sobre o desenvolvimento dos serviços de Internet. Recomenda-se que desligue a firewall.

6.2 Ferramentas de Diagnóstico

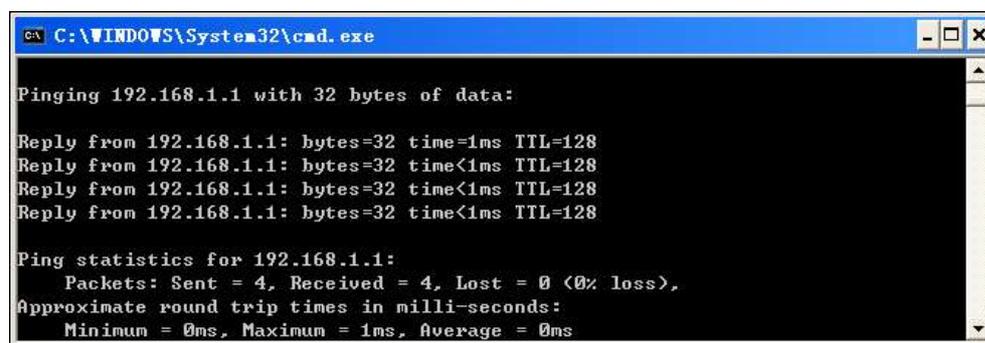
6.2.1 Ping

Use o comando **Ping** para verificar se o seu PC pode reconhecer outros computadores na rede. Um comando **ping** envia mensagens para o computador especificado. Se o computador receber as mensagens, irá responder com a mensagem de resposta. Antes de usar o comando, deverá conhecer o endereço IP do host de destino com o qual o seu PC está a tentar comunicar.

No prompt do DOS, introduza o seguinte comando:

```
ping 192.168.1.1
```

Se o host de destino receber o pacote, a janela de prompt do comando exibe o conteúdo, como ilustrado na 6.2.1.



```
C:\WINDOWS\System32\cmd.exe

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 91 Usar o comando **ping** – o ping ocorre com êxito

Se o PC de destino não for acessível, a mensagem de tempo de solicitação esgotado será exibida,

como segue:

A screenshot of a Windows Command Prompt window. The title bar reads "C:\WINDOWS\System32\cmd.exe". The command prompt shows the user at "C:\Documents and Settings\Administrator>" typing "ping 192.168.2.1". The output shows four "Request timed out." messages, followed by "Ping statistics for 192.168.2.1:" and "Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),".

```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 92 Usar o comando **ping** – o ping falha

Para verificar a ligação com o DR814Q, use o comando **Ping** com o endereço IP padrão da porta LAN (192.168.1.1) ou com o endereço que atribuiu.

Para verificar a ligação com a Internet, introduza um nome de domínio da Internet, tal como **www.yahoo.com** (216.115.108.243). Se desejar procurar o endereço IP de um website, use o comando **nslookup**, como instruído na secção 6.2.2 “Nslookup” para detalhes.

Para outros sistemas de operação que funcionam com o protocolo IP, poderá entrar com o mesmo comando “ping” num prompt do comando ou através de um utilitário da administração do sistema.

6.2.2 Nslookup

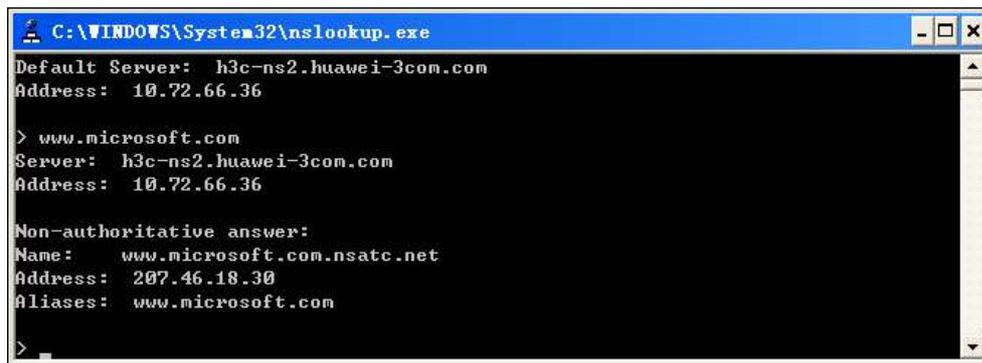
O comando **nslookup** é utilizado para consultar o endereço IP associado a um nome de domínio. Poderá especificar o nome de domínio comum e usar o comando **nslookup** para procurar no servidor DNS (normalmente localizado através do seu ISP). Se esse nome não estiver na tabela DNS do seu ISP, a solicitação é, então, enviada para um servidor de nível maior, até o nome ser localizado. O servidor devolve, então, o endereço IP associado.

Num computador baseado em Windows, poderá executar o comando **nslookup** do menu [*Start*] (Iniciar). Escolha [*Start/Run*] (iniciar/executar) e na caixa de texto aberta, digite o seguinte:

Nslookup

Clique em <OK> e aparecerá uma janela de prompt de comando. A janela [*Command Prompt – nslookup*] é exibida com o seguinte símbolo: (>). No prompt, digite o nome do domínio do Website desejado, por exemplo **www.microsoft.com**.

A janela exibe o endereço IP associado, como ilustrado abaixo.



```
C:\WINDOWS\System32\nslookup.exe
Default Server:  h3c-ns2.huawei-3com.com
Address:  10.72.66.36

> www.microsoft.com
Server:  h3c-ns2.huawei-3com.com
Address:  10.72.66.36

Non-authoritative answer:
Name:    www.microsoft.com.nsatc.net
Address:  207.46.18.30
Aliases:  www.microsoft.com

>
```

Figura 93 Usar o comando `nslookup`

Alguns websites com tráfego pesado usam múltiplos servidores para transportar as mesmas informações. Assim, é comum ter vários endereços IP associados a um nome de domínio da Internet.

Para sair do utilitário `nslookup`, introduza `exit` (sair).

7 Apêndice - Protocolo TCP/IP

7.1 Instalar o TCP/IP

O PC através do qual configura o seu DR814Q, deve ter o TCP/IP instalado. Se não tiver certeza se o TCP/IP está instalado, siga estes passos.



Aviso:

Por padrão, o TCP/IP está instalado no Windows 2000/XP. Os seguintes passos são descritos para o Windows 98/ME/NT.

- 1) Escolha [*Start/Settings/Control Panel*] (iniciar/configurações/painel de controle).
- 2) Faça duplo-clique no ícone *Network Connection* (ligação à rede) para abrir a caixa de diálogo [*Network*] (rede) e seleccione o separador [*Configuration*] (configuração) (ver 7.1).
- 3) Verifique a lista na página do separador [*Configuration*] (configuração) para ver se o item, que contém o TCP/IP e o nome do NIC que está a utilizar actualmente, existe. Se não, clique em <Add> (adicionar) para abrir a caixa de diálogo [*Select Network Component Type*] (seleccionar tipo de componente de rede) (ver 7.1).

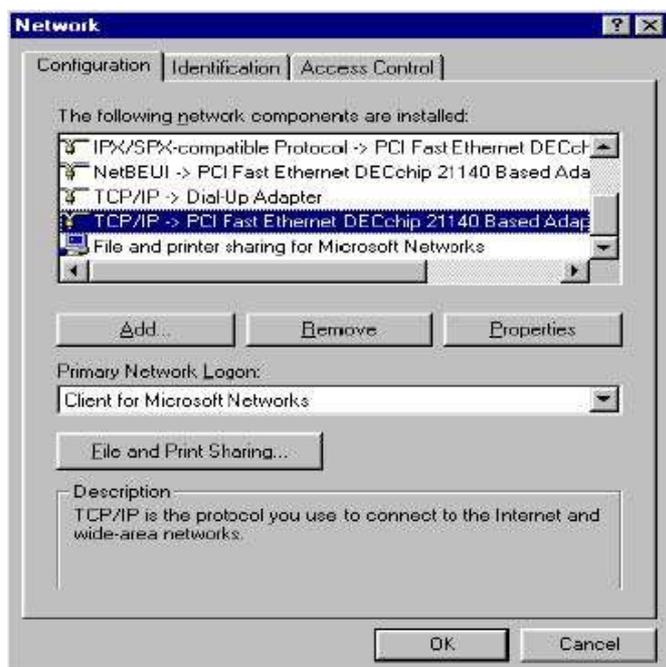


Figura 94 Caixa de diálogo da Rede

4) Faça duplo-clique em *Protocol* (protocolo) da lista da caixa de diálogo [*Select Network Component Type*] (seleccionar tipo de componente de rede) (ou clique em *Protocol* e clique <Add...> (adicionar)) para abrir a caixa de diálogo [*Select Network Protocol*] (seleccionar protocolo de rede) (ver 7.1).

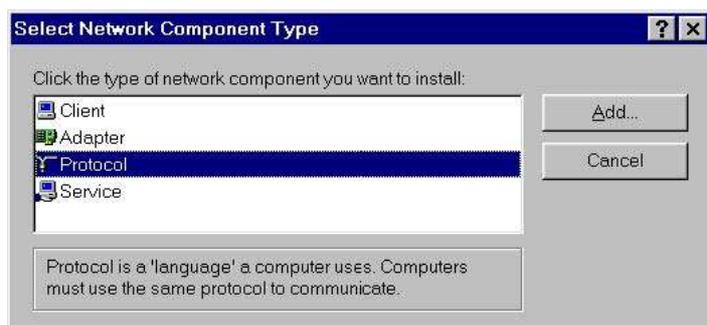


Figura 95 Seleccionar a caixa de diálogo do Tipo de Componente de Rede

5) Seccione **Microsoft** da lista de *Manufacturers* (fabricantes) na caixa de diálogo [*Select Network Protocol*] (seleccionar protocolo de rede), faça duplo-clique em **TCP/IP** na lista de *Network Protocols* (protocolos de rede) (ou clique em **TCP/IP** e clique em <OK>) para voltar ao

menu [Network] (rede). Então, poderá ver o item TCP/IP na secção que lista os componentes de rede instalados.

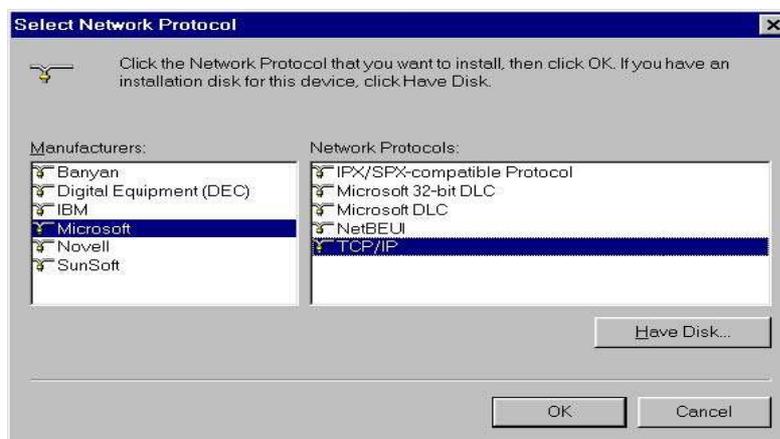


Figura 96 Seleccionar a caixa de diálogo de Protocolo de Rede

6) Clique em <Properties> (propriedades) na caixa de diálogo [Network] (rede) para abrir a caixa de diálogo [TCP/IP Properties] (propriedades do TCP/IP) (ver 7.1). Seleccione o separador [IP address] (endereço IP) e seleccione a opção *Obtain an IP address automatically* (obter um endereço IP automaticamente). Clique em <OK> e reinicie o seu PC para completar a instalação do TCP/IP.

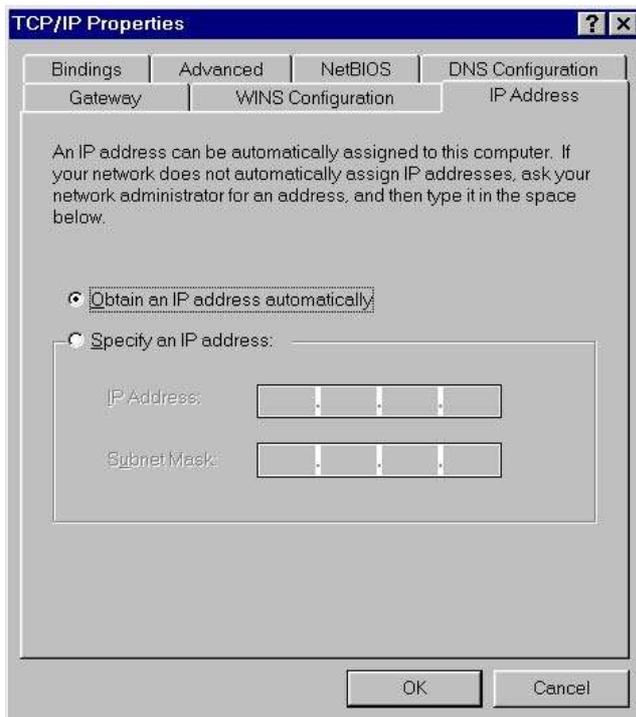


Figura 97 Caixa de diálogo das Propriedades do TCP/IP

7.2 Configurar o TCP/IP

7.2.1 Especificar para Obter um Endereço IP Automaticamente

Se estiver a executar o Windows 98/ME/NT, consulte a informação descrita na secção da 7.1 para especificar para obter um endereço IP automaticamente. Se estiver a executar o Windows 2000/XP, realize a seguinte operação.

- 1) Escolha [*Start/Settings/Control Panel*] (iniciar/configurações/painel de controle) para abrir a caixa de diálogo [*Control Panel*] (painel de controle). Faça duplo-clique no ícone *Network Connection* (ligação à rede) para abrir a caixa de diálogo [*Network Connection*] (ligação à rede) e, então, faça duplo-clique no ícone *Local Connection* (ligação local) para abrir a caixa de diálogo [*Local Area Connection Status*] (estado da ligação da área local) (ver 7.2.1).



Figura 98 Caixa de diálogo do Estado da Ligação da Área Local

2) Clique em <Properties> (propriedades) para abrir a caixa de diálogo [Local Area Connection Properties] (propriedades da ligação da área local) (ver 7.2.1). Selecciono o separador [General] (geral) e selecciono *Internet Protocol (TCP/IP)* (protocolo de internet (TCP/IP)) na secção [This connection uses the following items:] (esta ligação utiliza os seguintes itens:) e, então, clique em <Properties> (propriedades) para abrir a caixa de diálogo [Internet Protocol (TCP/IP) Properties] (propriedades do protocolo de internet (TCP/IP)), como ilustrado na 7.2.1.

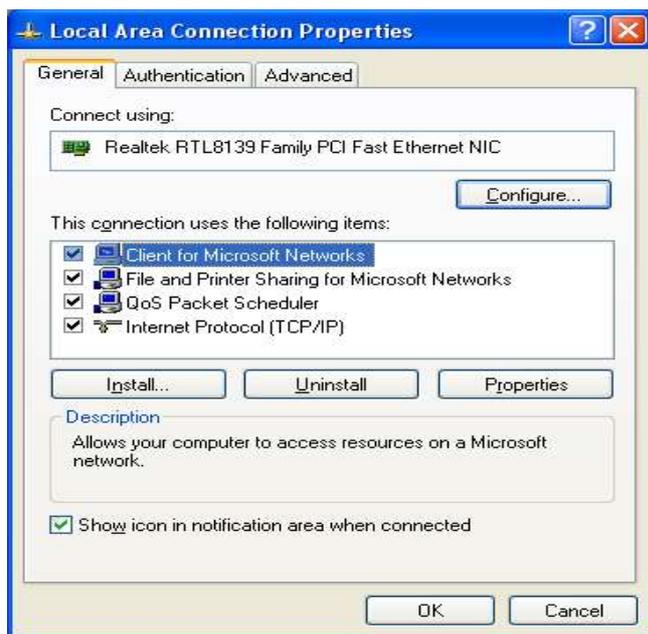


Figura 99 Propriedades de Ligação da Área Local

3) Na página do separador [General] (geral) da caixa de diálogo [Internet Protocol (TCP/IP) Properties] (propriedades do protocolo de internet (TCP/IP)) seleccione a opção *Obtain an IP address automatically* (obter um endereço IP automaticamente) e clique em <OK>.

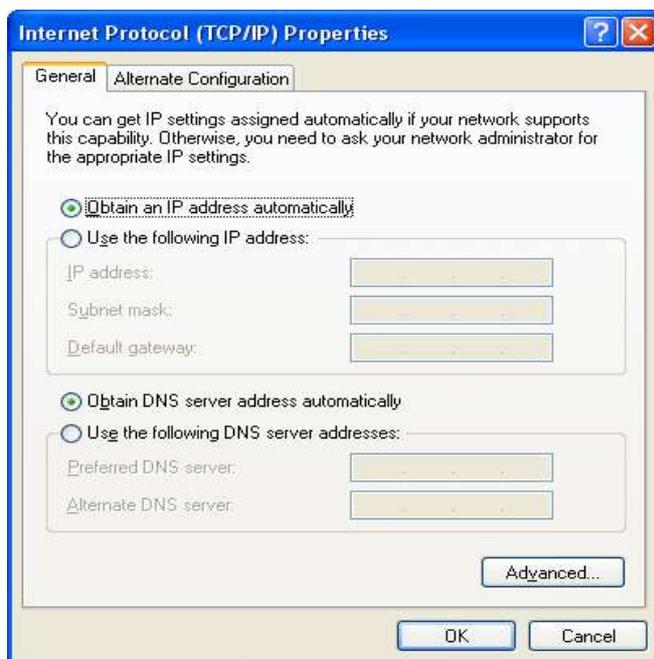


Figura 100 Caixa de diálogo das Propriedades de Protocolo de Internet (TCP/IP)

7.2.2 Especificar um Endereço IP Fixado

Uma vez que o DR814Q activa o DHCP por padrão, os PCs na LAN podem obter as relativas informações dinamicamente; assim, não há necessidade de atribuir endereços IP estáticos para PCs na LAN. Mas, em alguns casos, precisará ainda de estabelecer as configurações da rede para alguns ou até mesmo para todos os PCs numa rede.

Por padrão, o endereço IP da porta de Rede do DR814Q é 192.168.1.1. Escolha qualquer um de 192.168.1.2 a 192.168.1.254 para colocar o seu PC no mesmo segmento de 192.168.1.1/24. Siga o procedimento adequado para o seu sistema operativo para especificar endereços IP.

1) Especificar o endereço IP do seu PC.

•Windows 98/ME/NT: Na caixa de diálogo [*TCP/IP Properties*] (propriedades TCP/IP) (ver 7.1), seleccione o separador [*IP Address*] (endereço IP) e seleccione a opção *Specify an IP address* (especificar um endereço IP).

•Windows 2000/XP: Na caixa de diálogo [*Internet Protocol (TCP/IP) Properties*] (propriedades do protocolo de internet (TCP/IP)) (ver 7.2.1) seleccione o separador [*General*] (geral) e, então, a opção *Use the following IP address* (usar o seguinte endereço IP). Digite o endereço IP e a máscara de sub-rede nos campos correspondentes e clique em <OK>.

2) Especificar o endereço IP da porta de acesso.

•Windows 98/ME/NT: Na caixa de diálogo [*TCP/IP Properties*] (propriedades TCP/IP) (ver 7.1) seleccione o separador [*Gateway*] (porta de acesso). Digite o endereço IP padrão do seu DR814Q (**192.168.1.1**) na caixa de diálogo [*New gateway*] (nova porta de acesso) e clique em <Add> (adicionar).

•Windows 2000/XP: Na caixa de diálogo [*Internet Protocol (TCP/IP) Properties*] (propriedades do protocolo de internet (TCP/IP)) (ver 7.2.1), seleccione o separador [*General*] (geral). Digite o endereço IP padrão do seu DR814Q (**192.168.1.1**) na caixa de diálogo [*Default gateway*] (porta de acesso padrão) e clique em <OK>.

3) Especificar o endereço IP do servidor DNS.

•Windows 98/ME/NT: Na caixa de diálogo [*TCP/IP Properties*] (propriedades TCP/IP) (ver 7.1), seleccione o separador [*DNS configuration*] (configuração DNS) e digite o endereço IP padrão do seu DR814Q (**192.168.1.1**), assim como o endereço IP do servidor DNS no campo correspondente.

•Windows 2000/XP: Na caixa de diálogo [*Internet Protocol (TCP/IP) Properties*] (propriedades do protocolo de internet (TCP/IP)) (ver 7.2.1), clique em <Advanced...> (avançada...) para abrir a caixa de diálogo [*Advanced TCP/IP Configuration*] (configuração TCP/IP avançada). Seleccione o separador [*DNS*] e clique em <Add...> (adicionar...). Digite o endereço IP padrão do DR814Q (**192.168.1.1**) no campo [*DNS server*] (servidor DNS) e clique em <Add> (adicionar).

4) Fazer com que as configurações surtam efeito.

•Windows 98/ME/NT: Clique em <OK> e reinicie o seu PC para que as configurações acima façam efeito.

•Windows 2000/XP: Clique em <OK> para que as configurações acima façam efeito.

8 Apêndice - Configuração USB

8.1 Instalar o Driver USB

Certifique-se de que a função USB do seu PC opera adequadamente.

O Microsoft Windows 98/98 SE/ME/2000/XP suporta o driver USB. O seguinte procedimento de instalação é baseado no Windows XP. Utilize-o como referência quando estiver a executar qualquer outro sistema operativo.

I. Inserir o CD do driver no CD-ROM do seu PC.

O CD que vem com o DR814Q contém o driver USB.

II. Ligar uma extremidade do cabo USB na porta USB do DR814Q e a outra na porta USB do seu PC.

O cabo USB tem uma ligação Tipo A rectangular numa extremidade e uma ligação Tipo B quadrangular na outra extremidade. Ligue o Tipo A ao seu PC e o Tipo B ao DR814Q.

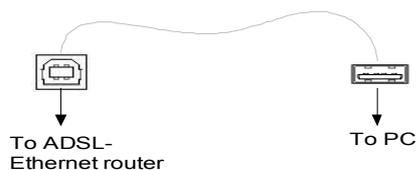


Figura 101 Ligação do cabo USB

III. Aparece a caixa de diálogo [Found New Hardware Wizard] (encontrado novo assistente de hardware) (ver III). Seleccione a opção *Install the software automatically* (instalar o software automaticamente) (recomendado) e clique em <Next> (próximo) para prosseguir.



Figura 102 Localizar novo hardware

IV. O PC procura o CD do arquivo de configuração do driver. Quando este arquivo for localizado, o PC começará a instalar o driver.



Figura 103 Instalar o software

A caixa de diálogo (ver IV) aparece durante a instalação, advertindo que o dispositivo não é compatível com Windows XP. Apenas clique em <Continue Anyway> (continuar mesmo assim) para prosseguir. Teste de logo da Microsoft.



Figura 104 Teste de logo da Microsoft

V. A caixa de diálogo (ver V) indica que a instalação está completa. Clique em <Finish> (finalizar) para sair da instalação.



Figura 105 Completar a instalação

8.2 Configurar as Propriedades IP

Após a instalação do driver USB estar completa, deverá configurar o PC para posicioná-lo na mesma sub-rede da porta USB do DR814Q. Estão disponíveis duas opções para configurar as propriedades IP:

- O seu DR814Q pode ser um servidor DHCP para atribuir endereços de IP aos PCs na LAN, de forma a que possa especificar o seu PC para obter o endereço IP automaticamente. Consulte a secção 7.2.1“Especificar para Obter um Endereço IP Automaticamente” para obter informações detalhadas.

- Se deseja especificar um endereço IP fixo ao PC, siga as instruções na secção 7.2.2“Especificar um Endereço IP Fixado” e use as seguintes informações.

A porta USB no DR814Q é pré-configurada com estas propriedades:

Endereço IP: 192.168.1.1

Máscara de sub-rede: 255.255.255.0

Portanto, o seu PC deverá ser configurado como se segue:

Endereço IP: 192.168.1.n (n é um número inteiro de 2 a 254)

Máscara de sub-rede: 255.255.255.0

9 Apêndice – Endereço IP e Máscara de Sub-rede

9.1 Endereço IP

Nota:

- Esta secção refere-se somente ao endereço IP do IPv4 (versão 4 do Protocolo de Internet) e o endereço IP do IPv6 não está coberto.
 - Esta secção descreve o conhecimento básico de números binários, bits e bytes.
-

Um endereço IP, como o número de telefone na Internet, é usado para identificar o nó individual (um PC ou dispositivo de rede) na Internet. Cada endereço IP contém quatro conjuntos de números, cada um de 0 a 255 e separados por pontos, por exemplo 20.56.0.211. Estes números, da esquerda para a direita, denominam-se **campo 1**, **campo 2**, **campo 3** e **campo 4**.

A representação de quatro conjuntos de dígitos separados por pontos, para endereço IP, denomina-se **notação decimal pontuada**.

9.1.1 Estrutura do Endereço IP

Como um número de telefone, o endereço IP contém dois componentes. Por exemplo, os três primeiros dígitos de um número de telefone de sete dígitos identificam um grupo com milhares de linhas de telefone, enquanto que os últimos quatro dígitos identificam uma linha específica neste grupo.

Similarmente, um endereço IP contém dois componentes:

- ID da rede

Identifica um segmento de rede específico na Internet ou na intranet.

- ID do host

Identifica um PC específico ou um dispositivo no segmento.

A parte inicial de cada endereço IP é o ID da rede e o restante refere-se ao grau de variância do host do ID da rede que depende da classe de rede (consulte a secção 9.1.2“Classes dos Endereços IP”). A 9.1.1 descreve a estrutura do endereço IP.

Tabela 1 Estrutura do endereço IP

Classe	Campo 1	Campo 2	Campo 3	Campo 4
Classe A	ID da rede	ID do host		

Classe B	ID da rede	ID do host
Classe C	ID da rede	ID do host

A seguir, alguns exemplos de endereços IP válidos:

Classe A: 10.30.6.125 (ID da rede = 10, ID do host = 30.6.125)

Classe B: 129.88.16.49 (ID da rede = 129.88, ID do host = 16.49)

Classe C: 192.60.201.11 (ID da rede = 192.60.201, ID do host = 11)

9.1.2 Classes dos Endereços IP

Os três endereços IP comuns são Classe A, B e C. (A Classe D é para uso especial e está para além do âmbito desta discussão.) Estas classes têm diferentes usos e características.

A rede classe A é a maior na Internet. Esta permite pelo menos 16 milhões de hosts por rede. 126 de tais redes classe A podem reunir pelo menos dois biliões de PCs. Estas redes de grande escala são completamente adequadas para as organizações fundamentais de LAN ou Internet, tal como o Fornecedor de Serviços de Internet (ISP).

A rede classe B é relativamente menor que a rede classe A, mas ainda permite 16.384 redes classe B e 65.000 hosts em cada rede classe B. Este tipo de rede é adequado para as grandes organizações, tais como empresas e governos.

A rede classe C é a menor. Permite mais de dois milhões (2.097.152 exactamente) de redes classe C e 254 hosts em cada rede classe C. As LANs que se ligam à Internet são normalmente desta classe de redes.

A seguir, os pontos-chave sobre o endereço IP:

- A forma mais fácil de determinar a classe de um endereço IP é olhando para o seu número no campo 1:

Classe A: O número é de 1 a 126.

Classe B: O número é de 128 a 191.

Classe C: O número é de 192 a 223.

(Os números para uso especial não são dados aqui.)

- Nem todos os campos de um ID de host podem ser 0s ou 255s, pois estes números estão reservados para uso especial.

9.2 Máscara de Sub-rede

Nota:

Uma máscara de sub-rede é parecida com um endereço IP regular e uma máscara de sub-rede pode significar a divisão do ID de rede e do ID de host: Um bit configurado em 1 significa que este bit é parte do ID de rede e um bit configurado em 0 significa que este bit é parte do ID de host.

As máscaras de sub-rede são usadas para definir sub-redes. Um número de sub-rede é um número de bits emprestados da porção do host do endereço IP.

Por exemplo, para dividir um endereço de Classe C 192.168.1.1 em duas sub-redes, precisará de configurar a máscara de sub-rede como se segue:

255.255.255.128

É muito mais directo definir o endereço em notação binária.

11111111. 11111111. 11111111.10000000

Para qualquer endereço da Classe C, todos os bits do campo 1 ao campo 3 são parte do ID de rede, mas verifique que na máscara especifica o primeiro bit no campo 4 também está incluído. Uma vez que este bit extra tem apenas dois valores (0 e 1), isto significa que há duas sub-redes. Cada sub-rede usa os 7 bits restantes no campo 4 para os seus IDs de host, que vão de 1 a 126 hosts (em vez do usual 0 a 255 para um endereço da Classe C).

Similarmente, para dividir uma rede da classe C em quatro sub-redes, configura a máscara, como se segue:

255.255.255.192 ou 11111111. 11111111. 11111111.11000000

Os dois bits extras no campo 4 podem ter quatro valores (00, 01, 10 e 11); assim, há quatro sub-redes. Cada sub-rede usa os seis bits restantes no campo 4 para seus IDs de host, que vão de 1 a 62.

 **Nota:**

Às vezes, uma máscara de sub-rede não especifica nenhum bit de ID de rede adicional e, assim, não existe nenhuma sub-rede. Tal máscara é chamada de máscara de sub-rede padrão. Estas máscaras são:

- Classe A: 255.0.0.0
- Classe B: 255.255.0.0
- Classe C: 255.255.255.0

São chamadas assim porque são usadas para uma rede configurada inicialmente sem sub-redes.

10 Apêndice – Especificações Técnicas

Tabela 2 Especificações técnicas

Item	Descrição
Portas e botões	Quatro portas de Rede 10/100Base-TX Uma porta ADSL Uma porta USB Um botão de Reset para restaurar as configurações padrões de fábrica
Consumo de energia	< 12W
Fonte de alimentação (externa)	12 V _{CC} , 1 A
Dimensões físicas (A x L x P)	31,5 × 193 × 123 mm (1,2 × 7,6 × 4,8 pol.)
Peso	Aproximadamente 310g (11 oz)
Temperatura de operação	0°C a 40°C (32°F a 104°F)
Temperatura de armazenamento	-10°C a +70°C (14°F a 158°F)
Humidade de operação (sem condensação)	20% a 85%
Humidade de armazenamento (sem condensação)	10% a 90%
Certificação	FCC Classe B CE

11 Apêndice - Glossário

100Base-TX

Cabo da categoria 5 com distância de transmissão máxima de 100 metros (328 pés) e taxa de transmissão máxima de 100 Mbps.

10Base-T

Cabo da categoria 3/4/5 com distância de transmissão máxima de 150 metros (492 pés) e taxa de transmissão máxima de 10 Mbps.

ADSL

Linha de assinante digital assimétrica. O tipo mais popular de DSL para utilizadores domésticos. O termo assimétrico refere-se às suas taxas de dados desiguais para download e upload (a taxa de download é maior que a taxa de upload). A taxa assimétrica beneficia utilizadores domésticos porque são os que tipicamente fazem muito mais download do que upload de dados da Internet.

ATM

Modo de transferência assíncrona. Uma tecnologia que usa pacotes de comprimento fixo, chamados células, para a rede de comutação por pacote. A célula, que consiste num cabeçalho da célula e o texto, são comutados sobre uma rede ATM pública ou privada. Os segmentos ATM individuais no circuito ATM ligam-se uns com os outros, formando as ligações ponta-a-ponta.

Binário

O sistema de números binários usa apenas dois dígitos, 0 e 1, para representar todos os números. Neste sistema, o dígito decimal 1 é representado por 1, 2 por 10, 3 por 11, 4 por 100, etc.. Embora este sistema seja conveniente para expressar números em décimas, os endereços IP, na verdade, usam números binários. Por exemplo, o endereço IP 209.191.4.240 é convertido para 11010001.10111111.00000100.11110000 em binário.

Ligação em Ponte

Os dados são enviados da sua rede para o seu ISP e em retorno o seu ISP envia os dados aos dispositivos na rede pelos endereços físicos. Comparado ao redireccionamento, a ligação em ponte faz com que seja mais eficaz a transferência de dados através de endereços da rede. O DR814Q pode realizar tanto o redireccionamento como a ligação em ponte. Quando ambas as funções estão ligadas, o DR814Q determina a rota dos dados IP e liga com ponte todos os outros tipos de dados.

Broadcast (difusão)

Uma tecnologia usada para enviar dados a todos os computadores numa rede.

DHCP

Protocolo de configuração de host dinâmico. O DHCP automatiza a atribuição e a gestão dos endereços IP. Quando um PC se liga à LAN, o DHCP associa-o a um endereço IP a partir de um conjunto de endereços compartilhados e, após um período especificado, o DHCP retorna o endereço ao conjunto.

Servidor DHCP

Servidor de protocolo de configuração de host dinâmico. Um servidor DHCP é um computador responsável por atribuir endereços IP aos computadores numa LAN.

DNS

Sistema de nome de domínio. O DNS traduz nomes de domínios em endereços IP. As informações DNS são distribuídas hierarquicamente em toda a Internet entre os computadores chamados servidores DNS. Por exemplo, **www.yahoo.com** é o nome do domínio associado ao endereço IP 216.115.108.243. Quando começa a aceder a um website, um servidor DNS procura o nome do domínio solicitado e procura o seu endereço IP correspondente. Se o servidor DNS não for capaz de encontrar o endereço IP, vai comunicar com os servidores DNS de alto nível para determinar o endereço IP.

Nome de domínio

Um nome de domínio é a tradução do seu endereço IP associado. Um nome de domínio deve ser único e é controlado pela Corporation for Assigned Names and Numbers (Corporação para Nomes e Números Atribuídos) (ICANN). Um nome de domínio é um elemento-chave de um URL que identifica um arquivo específico num website.

DSL

Linha de assinante digital. Uma tecnologia que permite que tanto dados digitais como sinais de voz analógica se movimentem sobre as linhas telefónicas de cobre existentes.

Rede

Tecnologia de rede de computador mais commumente instalada, utilizando normalmente cabos. As velocidades de dados de Rede são 10 Mbps e 100 Mbps.

Firewall

Uma firewall pode proteger o seu computador ou uma LAN contra ataques e outros acessos inesperados. Utilizadores não autorizados podem tentar atacar a sua rede a fim de o impedir ou a outros na LAN de acederem aos serviços.

Usando a firewall, poderá bloquear certos tipos de tráfego IP commumente usados pelos hackers para proteger sua rede. Poderá também restringir os tipos de tráfego IP enviados da sua rede para fora. Alguma protecção de firewall pode ser fornecida pelos serviços de filtragem de pacotes e de tradução de endereço de rede.

FTP

Protocolo de transferência de arquivos. Um programa usado para transferir arquivos entre computadores ligados à Internet. Os usos comuns incluem o upload de arquivos novos e atualizados para um servidor da Web e o download de arquivos de um servidor da Web.

HTTP

Protocolo para transferência de hipertexto. É o protocolo principal usado para transferir dados entre websites, de forma a que possa ser exibido pelo browser da Web.

Hub

Um hub recebe dados dos dispositivos e encaminha-os. Normalmente realiza a função de comutação ligando um dispositivo, tal como uma ponte de Rede ou um router, a um grupo de computadores numa LAN e permitindo a comunicação entre esses dispositivos.

ICMP

Protocolo de mensagem de controlo de Internet. Um protocolo de Internet usado para relatar erros e outras informações relacionadas com a rede. O comando **ping** faz uso do ICMP.

IEEE

Instituto de Engenheiros Eléctricos e Electrónicos. É uma sociedade de profissionais técnicos que promove o desenvolvimento de normas que frequentemente se tornam normas nacionais e internacionais.

Endereço IP

Endereço de protocolo de Internet. O endereço é um host (computador) na Internet, que consiste em quatro números decimais, cada um de 0 a 255, separados por pontos, tal como 209.191.4.240. Um endereço IP consiste num ID de rede que identifica a rede particular à qual o host pertence e num ID de host que identifica unicamente o próprio host naquela rede. Uma máscara de rede é usada para definir o ID de rede e o ID de host. Como os endereços IP são difíceis de memorizar, em vez disso, eles normalmente têm um nome de domínio associado que pode ser especificado.

ISP

Fornecedor de serviço de Internet. Uma empresa que fornece acesso à Internet.

LAN

Rede de área local. Uma rede limitada a uma área geográfica pequena, tal como uma casa, um escritório ou um prédio pequeno.

MAC

Endereço de controle de acesso ao equipamento. É o endereço de hardware permanente de um dispositivo, atribuído pelo seu fabricante. Os endereços MAC são expressos como seis pares de dois

dígitos hexadecimais, separados por hífens, tal como 00-0F-1F-80-65-25.

MTU

Unidade de transmissão máxima. É o maior tamanho de pacote que é transmitido sobre a rede física.

NAT

Tradução de endereço de rede. Possibilita aos computadores numa LAN o acesso à Internet pela partilha do mesmo endereço IP. Quando um computador acede à Internet, o seu endereço IP privado é traduzido para um endereço público da porta WAN.

Máscara de rede

Uma máscara de rede é uma sequência de bits aplicada a um endereço IP para seleccionar o ID de rede. Selecciona o bit configurado para 1 e ignora o bit ajustado para 0. Por exemplo, se a máscara de rede 255.255.255.0 for aplicada ao endereço IP 100.10.50.1, o ID de rede é 100.10.50 e o ID de host é 1.

NIC

Cartão de interface de rede. Um adaptador fornece o interface físico para a sua rede. O NIC de Rede normalmente tem uma ligação RJ-45.

Pacote

Dados que consistem de unidades transmitidas numa rede denominam-se pacotes. Cada pacote consiste num cabeçalho, o qual contém as informações sobre os endereços da fonte e do destino do pacote e um campo de dados.

Ping

Um programa usado para verificar se o host associado a um endereço IP pode ligar-se à rede. Também pode ser usado para revelar o endereço IP para um dado nome de domínio.

Porta

Um ponto de acesso físico num dispositivo, tal como um computador ou router, através do qual os dados fluem para/do dispositivo.

PPP

Protocolo ponto-a-ponto. É um protocolo de comunicação para transmissão de dados entre dispositivos sobre a linha telefónica padrão. A porta WAN no DR814Q usa dois tipos de PPP, isto é, PPPoA e PPPoE.

PPPoA

Protocolo ponto-a-ponto sobre ATM. Um dos dois tipos de interface PPP. O outro tipo é o PPPoE. Poderá especificar somente um interface PPPoA para cada VC.

PPPoE

Protocolo ponto-a-ponto sobre Rede. Um dos dois tipos de interface PPP. O outro tipo é o PPPoA. Poderá especificar múltiplas interfaces PPPoE para cada VC.

Protocolo

Um conjunto de regras para gerir a transmissão de dados. As duas extremidades ligadas devem obedecer a estas regras para transmitir dados.

Remoto

Uma localização separada geograficamente. Por exemplo, um funcionário em viagem que executa login na intranet da empresa é um utilizador remoto.

RJ-11

O conector padrão usado para ligar telefones, máquinas de fax e Modems a uma porta do telefone. É um conector de 6 pinos que utiliza quatro fios.

RJ-45

A ficha de 8 pinos usada para transmitir dados sobre as linhas telefônicas. Cabos de passagem direta usam normalmente o conector deste tipo.

SNMP

Protocolo de gestão de rede simples (SNMP), uma gestão de rede padrão, é amplamente usado na rede TCP/IP. O SNMP oferece um modo de gerir os nós das redes a partir do host localizado no centro da rede, tais como o servidor, estação de trabalho, router, ponte e hub. Realiza normalmente a gestão através da administração de estrutura distribuída e do proxy.

Sub-rede

Uma sub-rede é uma porta separada de uma rede. A máscara de sub-rede é usada para sub-dividir uma rede somando-se bits adicionais à porção do host do endereço IP. Um host em uma sub-rede está fisicamente ligado na rede, no entanto, cada uma delas é uma divisão individual da rede.

TCP/IP

Protocolo de controlo de transmissão/protocolo de internet.

Ele define um conjunto de protocolos básicos, não apenas o protocolo TCP/IP, para a comunicação de rede.

Telnet

Um programa interativo, baseado em caracteres, usado para aceder a um computador remoto. O HTTP e o FTP permitem-lhe apenas fazer download de arquivos a partir de um computador remoto, enquanto que o Telnet permite-lhe executar login e usar um computador a partir de uma localização

remota.

Fluxo ascendente (upstream)

O fluxo ascendente flui dos utilizadores para a Internet.

USB

Barramento de série universal. Um interface de série que liga os dispositivos, tais como impressoras e scanners, ao computador. O DR814Q fornece uma porta USB para ligar a um computador.

VC

Circuito virtual. Uma ligação do router DSL ao ISP.

VCI

Identificador de canal virtual. Em conjunto com o identificador de caminho virtual (VPI), o VCI identifica unicamente um circuito virtual (VC). O ISP fornece o valor do VCI para cada VC.

VPI

Identificador de canal virtual. Em conjunto com o identificador de caminho virtual (VPI), o VCI identifica unicamente um circuito virtual (VC). O ISP fornece o valor do VPI para cada VC.

WAN

Uma rede que abrange uma área vasta, tal como um país ou um continente, é chamada de WAN. Em relação ao router ADSL, a WAN refere-se à Internet.

Browser de Web

Um programa de software que usa o protocolo para transferência de hipertexto (HTTP) para fazer download de informações a partir de (e upload para) websites e exibe as informações que consistem em texto, imagens gráficas, áudio e vídeo. Os browsers de Web mais populares são o Netscape Navigator e o Microsoft Internet Explorer.

Página da Web

Um arquivo de website que contém tipicamente texto, imagens gráficas e hyperlinks para outras páginas. Quando aceder a um website, a primeira página exibida é denominada *home page* (página inicial).