

**DSLlink**<sup>®</sup>  
**260E**  
Conexão Banda Larga

# Manual do Usuário



[www.dslink.com.br](http://www.dslink.com.br)



Fabricado e comercializado sob licença exclusiva de Opticom Communications, LLC, 1050 Connecticut Avenue, NW, Suite 1000, Washington DC 20036, USA, Â+1 202 772-4291, [www.opticom.co.il](http://www.opticom.co.il). A Opticom Communications reserva-se o direito de melhorar, aprimorar e modificar os recursos e especificações de seus produtos sem prévia notificação. © Copyright 2001-2006. Todos os direitos autorais reservados. A duplicação, uso ou distribuição não autorizada constitui uma violação das leis aplicáveis. Todas as marcas são registradas e pertencem aos seus respectivos proprietários. Fotos meramente ilustrativas. 060621

Nenhuma parte desta publicação poderá ser reproduzida seja de que forma for sem a permissão escrita anterior. Outras marcas comerciais ou marcas registradas mencionadas neste documento são marcas comerciais ou marcas registradas de suas respectivas empresas.

Revisão 3.3

Junho 2006

# Índice

<b>1</b>	<b>Introdução .....</b>	<b>1</b>
	Características.....	1
	Conteúdo da caixa do produto .....	1
	Requisitos do Sistema.....	2
<b>2</b>	<b>Hardware e Conexão.....</b>	<b>3</b>
	Painel Frontal.....	3
	Painel Traseiro .....	3
	Conectando o Hardware .....	4
	Passo 1. Conecte-se à tomada telefônica.....	4
	Passo 2. Conecte-se a um PC ou hub/switch.....	5
	Passo 3. Ligue o conector PWR.....	5
	Passo 4. Ligue o DSLink 260E e energize seus sistemas.....	5
<b>3</b>	<b>Configuração do PC Local.....</b>	<b>6</b>
	Configurando seus PCs como clientes DHCP .....	6
	PCs com sistema operacional Windows <sup>®</sup> 95, 98 e Me: .....	6
	Estações de trabalho Windows NT 4.0: .....	7
	PCs com sistema operacional Windows 2000 e XP: .....	7
	Para atribuir informações IP estáticas a seus PCs .....	7
<b>4</b>	<b>Iniciando com o Configuration Manager .....</b>	<b>9</b>
	Acessando o Configuration Manager .....	9
	Botões e Ícones Comumente Usados.....	10
	Visualizando informações básicas do sistema.....	10
	Efetivando Alterações para Armazenamento Permanente.....	11
	Reiniciando o DSLink 260E com o uso do Configuration Manager.....	11
	System Mode.....	12
	Quick Configuration.....	12
	Exemplos de Quick Configuration .....	14
	RFC 1483 Bridge .....	14
	RFC 1577 Router .....	15

	RFC 2364 PPPoA.....	15
<b>5</b>	<b>Configuração Básica.....</b>	<b>16</b>
	Modo Bridge .....	16
	Parte 1: Configurando o DSLink 260E .....	16
	Parte 2: Verifique o status de sua conexão.....	20
	Parte 3: Configurando o PC. ....	20
	Modo PPP Connection.....	21
	Parte 1: Configurando o DSLink 260E .....	21
	Parte 2: Verifique o status de sua conexão.....	23
	Parte 3: Configurando o PC. ....	24
	Modo Router Connection .....	24
	Parte 1: Configurando o DSLink 260E .....	24
	Parte 2: Verifique o status de sua conexão.....	26
	Parte 3: Configurando o PC. ....	27
<b>6</b>	<b>Configurando Rotas IP .....</b>	<b>28</b>
	Visualizando a Tabela de Roteamento IP .....	28
	Adicionando Rotas IP .....	28
<b>7</b>	<b>Configuração DHCP .....</b>	<b>30</b>
	Modos DSLink 260E DHCP .....	30
	Configurando o Servidor DHCP .....	30
	Parte 1. Criando pools de endereços IP.....	30
	Parte 2. Ativando o Modo DHCP Server .....	32
	Parte 3. Configurando seus PCs como clientes DHCP .....	32
	Modificando Pools de Endereços.....	32
	Visualizando Atribuições de Endereço DHCP Atuais .....	33
	Configurando a Retransmissão DHCP .....	33
	Parte 1. Definindo a(s) interface(s) de retransmissão DHCP.....	33
	Parte 2. Ativando modo de retransmissão DHCP .....	34
	Parte 3. Configurando seus PCs como clientes DHCP .....	34
<b>8</b>	<b>Configuração NAT .....</b>	<b>35</b>
	Sua Instalação NAT Padrão.....	35
	Visualizando Sua Configuração NAT .....	35
	Visualizando Regras NAT e Estatísticas de Regras .....	38

Visualizando Conversões NAT Atuais .....	38
Adicionando Regras NAT .....	39
A regra napt: Efetuando conversões entre endereços IP públicos e privados .....	39
A regra rdr: Permitindo acesso externo a um computador da LAN41	
A regra basic: Executando conversões 1:1 .....	42
A regra filter: Configurando uma regra basic com critérios adicionais .....	43
A regra bitmap: Executando conversões bidirecionais .....	45
A regra PASS : Permitindo que endereços específicos passem sem conversão.....	46

## 9 Configurando Endereços do Servidor DNS e DDNS ..... 47

Visão Geral da Retransmissão DNS .....	47
Configurando a Retransmissão DNS .....	47
Configurando DDNS.....	49

## 10 Configuração RIP..... 50

Configurando o RIP .....	50
Visualizando Estatísticas do RIP .....	51

## 11 Firewall, Filtros de IP, Filtro de Bridge e Bloqueio de

Protocolos .....	53
Configurando o Firewall.....	53
Configurando Definições Globais de Firewall.....	53
Configuração de IP Filter .....	55
Visualizando sua configuração de IP Filter .....	55
Configurando Definições Globais de IP Filter.....	56
Criando Regras de Filtros de IP .....	57
Exemplos de regra filter de IP .....	63
Visualizando Estatísticas de Filtros de IP .....	63
Gerenciando Sessões Atuais de Filtros IP .....	64
Configuração de Bridge Filter.....	65
Visualizando sua configuração de Bridge Filter .....	65
Configurando Definições Globais de Bridge Filter.....	65
Criando Regras de Filtros Bridge .....	66
Visualizando Estatísticas de Filtros Bridge.....	67
Para bloquear protocolos específicos .....	67

<b>12</b>	Tarefas de Administração.....	69
	Alterando a data e hora do sistema .....	69
	Adicionando um usuário/Alterando sua senha de logon.....	69
	Atualização da imagem .....	70
	Diagnósticos .....	71
	Configurações de portas .....	72
	Visualização dos alarmes do sistema .....	72
	Sistema de Log.....	73
	Backup / Restore da Configuração .....	73
	Autodetect .....	74
	Configuração SNMP.....	74
<b>13</b>	Visualização dos parâmetros DSL .....	75
<b>14</b>	Solução de problemas .....	77

# 1 Introdução

Parabéns por ter adquirido o roteador/ bridge DLink 260E. Sua LAN (rede local) agora será capaz de acessar a Internet usando sua conexão ADSL de alta velocidade.

Este manual lhe mostrará como instalar e configurar seu DLink 260E e como personalizar sua configuração para obter o máximo de seu novo produto.

## Características

---

- Modem ADSL externo para acesso à Internet em alta velocidade
- Roteador Ethernet 10/100Base-T para proporcionar conectividade com a Internet a todos os computadores de sua LAN
- Funções de conversão de endereços de rede (NAT) e de filtragem de IP para proporcionar proteção por firewall para seus computadores
- Configuração da rede através de DHCP
- Programa de configuração que pode ser acessado por meio de um navegador HTML

## Conteúdo da caixa do produto

---

Seu DLink 260E deve chegar com o seguinte:

- Um roteador ADSL/ADSL2/ADSL2+
- Uma fonte universal
- Um cabo de rede
- Um cabo telefônico
- Um CD com software e manual do usuário (este manual)
- Um manual de instalação rápida com termo de garantia
- Microfiltros (somente quando indicado na parte externa da embalagem)

## Requisitos do Sistema

---

Para utilizar seu DSLink 260E, será preciso o seguinte:

- Serviço ADSL funcionando corretamente em sua linha telefônica, com pelo menos um endereço de Internet público para sua LAN.
- Um ou mais computadores contendo uma placa de interface de rede (NIC) Ethernet 10Base-T/100Base-T.
- Um hub/switch Ethernet, caso esteja conectando o dispositivo a mais de um computador.
- Para a configuração do sistema usando o programa estilo Web fornecido: um navegador da Web como, por exemplo, Internet Explorer v5.0 ou posterior, ou Netscape v5.0 ou posterior.

## 2 Hardware e Conexão

### Painel Frontal

---

O painel frontal contém indicadores denominados LEDs, que indicam o status da unidade.



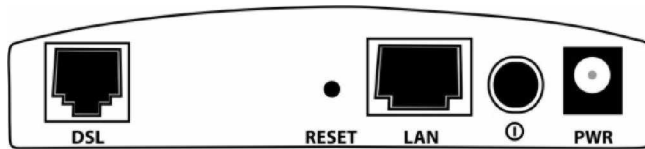
DSLlink 260E

Identificação	Cor	Função
PWR	verde	Aceso: A unidade está ligada Apagado: A unidade está desligada
DSL	verde	Aceso: Enlace ADSL estabelecido e ativo Piscando: Sem enlace ADSL
PPP	verde	Pisca quando ocorre atividade de dados ADSL. Pode ficar continuamente aceso quando o tráfego de dados é intenso.
LAN	verde	Aceso: Enlace LAN estabelecido e ativo Apagado: Sem enlace LAN
ALM	vermelho	Pisca acendendo-se e apagando-se para indicar que o software do dispositivo está operacional. Apaga-se após 10-15 segundos.

### Painel Traseiro

---

O painel traseiro contém as portas para as conexões de dados e de alimentação da unidade. As funções estão descritas conforme abaixo (da esquerda para a direita):



DSLInk 260E

Identificação	Função
<i>DSL</i>	Conecta o dispositivo a uma tomada de telefone ADSL usando o cabo fornecido
<i>Reset Button</i>	Redefinição para os padrões de fábrica. Para redefinir o dispositivo para os padrões de fábrica, não é necessário desligar o dispositivo. Basta introduzir um clipe de papéis no orifício. Pressione o botão 3 vezes e, em seguida, solte. Depois, aguarde o dispositivo terminar a inicialização.
<i>LAN</i>	Conecta o dispositivo à porta Ethernet de seus PCs, ou à porta uplink do hub de sua LAN, usando o cabo fornecido
	Liga e desliga a unidade
<i>PWR</i>	Conecta-se à saída da fonte DC fornecida

## Conectando o Hardware

Siga os procedimentos abaixo para conectar dispositivos relacionados. Antes de começar, desligue a alimentação de todos os dispositivos. Estes incluem seu(s) computadores e o DLink 260E.

### Passo 1. Conecte-se à tomada telefônica

Conecte uma extremidade do cabo telefônico RJ11 à porta identificada como **DSL** no painel traseiro do dispositivo. Conecte a outra extremidade à sua tomada telefônica com serviço ADSL.



**Nota**

Dependendo do tipo de serviço oferecido por seu ISP, poderá ser necessário um divisor adicional. Se este for o caso, consulte seu ISP para informações sobre a conexão efetiva.

Passo 2. Conecte-se a um PC ou hub/switch.

- A um único PC – Conecte uma extremidade de um cabo Ethernet “direto” à porta identificada como **LAN** e a outra extremidade à porta Ethernet de seu PC.
- A um hub/switch - Conecte uma extremidade de um cabo Ethernet “cruzado” (**não fornecido**) a um hub/switch e a outra extremidade à porta LAN do DSLink 260E.
- A uma porta uplink do hub/switch: - Use um cabo “direto” para conectá-lo à porta uplink e o outro para a porta **LAN** do DSLink 260E.

Passo 3. Ligue o conector PWR.

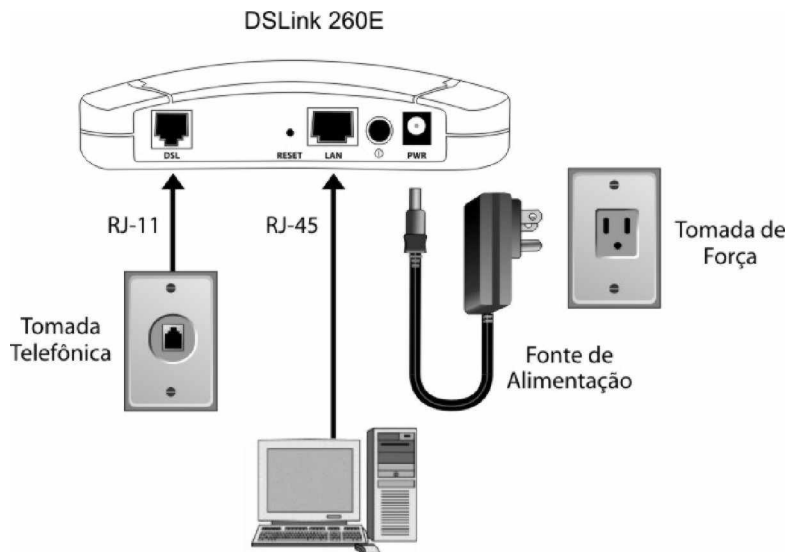
Conecte a saída da fonte ao conector **PWR** na parte traseira do dispositivo e a entrada da fonte, a uma tomada de parede ou régua de alimentação.

Passo 4. Ligue o DSLink 260E e energize seus sistemas.

Pressione a chave liga/desliga no painel traseiro do dispositivo para ligá-lo.

Ligue e inicialize seu(s) computador(es) e quaisquer dispositivos LAN.

O diagrama abaixo ilustra um exemplo de conexão:



## 3 Configuração do PC Local

Por padrão, o DSWLink 260E age como servidor DHCP e atribui automaticamente todas as configurações Internet necessárias a seus PCs, ou seja, os clientes DHCP. O endereço IP e o pool DHCP predefinidos são os seguintes:

Porta LAN	
Endereço IP	192.168.1.1
Máscara de sub-rede	255.255.255.0
Pool DHCP	192.168.1.3~252

Estas instruções partem do princípio de que seu PC satisfaz os seguintes pré-requisitos:

1. Já está conectado à porta LAN do dispositivo através de sua placa de interface de rede (NIC).
2. Possui o software de adaptador Ethernet apropriado.
3. O protocolo TCP/IP está instalado. Em caso negativo, consulte a documentação da Microsoft para instalar o TCP/IP.

É preciso apenas configurar os PCs para aceitarem as informações quando elas forem transferidas. Siga as instruções que correspondam ao sistema operacional instalado em cada PC.

### Configurando seus PCs como clientes DHCP

PCs com sistema operacional Windows<sup>®</sup> 95, 98 e Me:

1. Na barra de tarefas do Windows, clique no botão **Iniciar**, aponte para **Configurações** e, em seguida, clique em **Painel de controle**.
2. Clique duas vezes no ícone **Rede**.
3. Na guia **Configuração**, selecione a rede TCP/IP associada à sua placa de rede e, em seguida, clique em **Properties**.
4. Na caixa de diálogo Properties de TCP/IP, clique na guia **Endereço IP**.
5. Clique no botão de opção identificado como **Obtain an IP Address Automatically**.
6. Clique em **OK** duas vezes para confirmar e salvar suas alterações.
7. Será solicitado salvar o Windows. Clique em **Sim**.

Estações de trabalho Windows NT 4.0:

1. Na barra de tarefas do Windows NT, clique no botão **Iniciar**, aponte para **Configurações** e, em seguida, clique em **Painel de controle**.
2. Na janela Painel de controle, clique duas vezes no ícone **Rede**.
3. Na caixa de diálogo Rede, clique na guia **Protocols**.
4. Na guia **Protocols**, selecione **TCP/IP** e, em seguida, clique em **Properties**.
5. Na caixa de diálogo **Properties** de TCP/IP Microsoft, clique no botão de opção identificado como **Obter um endereço IP de um servidor DHCP**.
6. Clique **OK** duas vezes para confirmar e salvar suas alterações e, em seguida, feche o Painel de controle.

PCs com sistema operacional Windows 2000 e XP:

1. Na barra de tarefas do Windows, clique no botão **Iniciar**, aponte para **Configurações** e, em seguida, clique em **Painel de controle**.
2. Clique duas vezes no ícone **Conexões de rede e dial-up** (ou **Conexões de rede** para o Windows XP).
3. Clique com o botão direito do mouse no ícone **Conexão local** e, em seguida, selecione **Properties**.
4. Realce **Internet Protocol (TCP/IP)** e, em seguida, clique em **Properties**.
5. Na caixa de diálogo **Internet Protocol Properties (TCP/IP)**, clique no botão de opção identificado como **Obtain an IP Address Automatically**. Clique também no botão de opção identificado como **Obtain DNS server address**.
6. Clique em **OK** duas vezes para confirmar e salvar suas alterações e, em seguida, feche o Painel de controle.

### Para atribuir informações IP estáticas a seus PCs

Em alguns casos, você pode querer atribuir IP estático a seu PC diretamente se:

- No modo **bridge**, está concluída a configuração inicial e será preciso usar o endereço IP e o gateway fornecidos por seu ISP.
- Foi obtido um ou mais endereços IP públicos que quer associar sempre a computadores específicos (por

exemplo, se estiver usando um computador como servidor de rede público).

- São mantidas diferentes sub-redes em sua LAN.

Antes de começar, entre em contato com seu ISP caso não tenha as seguintes informações:

- Endereço IP e máscara de sub-rede.
- Gateway padrão.
- Servidor DNS.

Em cada PC ao qual queira atribuir informações estáticas, siga as instruções para a exibição de cada uma das propriedades TCP/IP. Em vez de ativar a atribuição dinâmica dos endereços IP relativos ao computador, clique nos botões de opção que permitem inserir manualmente o endereço IP, o DNS e o gateway padrão.

## 4 Iniciando com o Configuration Manager

Seu DSLink 260E inclui um *Configuration Manager* com interface Web, que possibilita configurar as definições do dispositivo para que satisfaçam as necessidades de sua rede.

### Acessando o Configuration Manager

---

O programa pode ser acessado de qualquer computador conectado ao DSLink 260E por meio de portas LAN.

1. Em um computador da LAN, abra seu navegador da Web, digite o seguinte URL na caixa de endereço (ou localização) e pressione <Enter>:

`http://192.168.1.1`

2. Quando a tela de logon for exibida, digite seu nome do usuário e senha e, em seguida, clique em **OK**.

Na primeira vez que iniciar o programa, use estes valores padrão:








*Default User Name:* root

*Default Password:* root



Após um logon bem-sucedido, é exibida a página **System View**.

## Botões e Ícones Comumente Usados


















Botão	Função
	Armazena na memória temporária do sistema quaisquer alterações feitas na página atual.
	Reexibe a página atual com estatísticas atualizadas.
	Quando estiverem sendo exibidas estatísticas acumuladas, este botão redefine as estatísticas para seus valores iniciais.
	Inicia a ajuda on-line relativa ao tópico atual em uma janela do navegador separada. A ajuda está disponível na página de qualquer tópico principal.
	Excluir uma entrada.
	Modificar uma entrada.
	Visualizar detalhes de uma entrada.

## Visualizando informações básicas do sistema

A página System View é exibida ao acessar pela primeira vez o programa ou ao clicar na aba **Home**:

**System View**

Use this page to get the summary on the existing configuration of your device.

Device		DSL					
<b>Model:</b>	DSLInk 260E	<b>Operational Status:</b>	 Startup Handshake				
<b>H/W Version:</b>	810100	<b>Last State:</b>	0x0				
<b>S/W Version:</b>	2.5.051005e5	<b>DSL Version:</b>	E.37.4.9				
<b>Serial Number:</b>	260E36H058000005	<b>Annex Type:</b>	ADSL2				
<b>Mode:</b>	Routing And Bridging	<b>Standard:</b>	ADSL2+ Auto				
<b>Up Time:</b>	0:0:44	<b>Connected Standard:</b>	ADSL2+ Auto				
<b>Time:</b>	Thu Jan 01 00:14:44 1970	<b>Data Boost:</b>	-				
<b>Time Zone:</b>	GMT	<b>Profile:</b>	Brazil				
<b>Daylight Saving Time:</b>	OFF						
<b>Name:</b>		<b>Speed</b>	<b>Latency</b>	<b>Speed</b>	<b>Latency</b>		
<b>Domain Name:</b>		0 Kbps	-	0 Kbps	-		
<b>WAN Interfaces</b>							
Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
eca-0	Bridged	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	8/35	
<b>LAN Interface</b>							
Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:01:38:1f:58:a8	192.168.1.1	255.255.255.0	-	10BT	Half	
<b>Services Summary</b>							
Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	 inside						
eca-0	 outside						

Modify Refresh Help

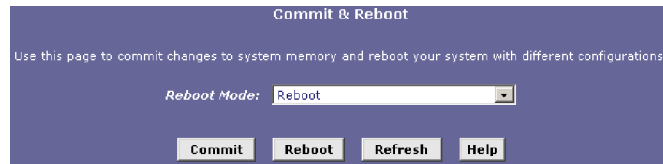
A tabela System View fornece um instantâneo da configuração de seu sistema. Pode-se clicar nos links fornecidos que permitem configurar cada definição (se disponível). Consulte os capítulos apropriados neste documento para obter mais informações.

## Efetivando Alterações para Armazenamento Permanente

Sempre que forem alteradas as definições do sistema, as alterações são colocadas inicialmente em armazenamento temporário (denominado memória de acesso aleatório ou RAM). Suas alterações tornam-se efetivas quando são enviadas, mas serão perdidas se o dispositivo for redefinido ou desligado.

Siga estes passos para efetivar alterações para armazenamento permanente.

1. Selecione **Admin > Commit & Reboot**. É apresentada a página Commit & Reboot:



2. Clique em **Commit**. (Desconsidere a seleção na lista suspensa Reboot Mode; ela não afeta o processo de efetivação).

As alterações são salvas no armazenamento permanente.

Quando efetivar suas alterações, observe que:

- Se for alterar as informações de endereço IP da LAN, **deverá** efetivar as alterações e, em seguida, reinicializar o sistema para ativá-las.
- Todas as outras alterações são ativadas quando forem efetivadas (nenhuma reinicialização é necessária).

### Reinicializando o DSLink 260E com o uso do Configuration Manager

Se, após reinicializar o DSLink 260E, for descoberto que ele não funciona corretamente com a nova configuração, poderá reinicializá-lo usando as opções que ativarem novamente uma configuração anterior ou a configuração padrão do fabricante.

É possível selecionar entre as três opções a seguir quando da reinicialização:

Definição	Descrição
<i>Reboot</i>	Reinicializa o dispositivo para ativar suas novas definições (se houver).
<i>Reboot from Last Configuration</i>	Reinicializa o dispositivo usando as definições atuais na memória permanente, incluindo quaisquer alterações que foram recém efetivadas.
<i>Reboot from Backup Configuration</i>	Reinicializa o dispositivo usando as definições armazenadas na memória de backup. Estas são as definições que estavam em vigor antes de terem sido

Definição	Descrição
	efetivadas as novas definições na sessão atual.
<i>Reboot from Default Configuration</i>	Reinicializa o dispositivo para definições padrão fornecidas por seu ISP ou pelo fabricante. A escolha desta opção apaga qualquer definição personalizada.

## System Mode

A página **System Mode** é usada para configurar o modo de operação de cada uma das interfaces criadas. Esta página deve ser usada em conjunto com a tela de **Bridge Configuration**, conforme descrito no item 3 do capítulo 5 deste manual.

Feature	Enabled	Disabled
<i>Bridging:</i>	<input type="radio"/>	<input checked="" type="radio"/>
<i>WAN to WAN Bridging:</i>	<input type="radio"/>	<input checked="" type="radio"/>
<i>BRAS:</i>	<input type="radio"/>	<input checked="" type="radio"/>
<i>ZIPB:</i>	<input type="radio"/>	<input checked="" type="radio"/>

Submit Cancel Help

## Quick Configuration

A página **Quick Configuration** permite que seu DLink 260E seja configurado com rapidez para conexão à Internet. Seu ISP deve lhe fornecer as informações necessárias para a conclusão da configuração rápida.

Home | System Mode | **Quick Configuration**

Quick Configuration

Use this page to quickly configure the system.

ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	1483 Bridged IP LLC
VPI:	0
VCI:	35
Bridge:	Enabled
IGMP:	Disabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Use DHCP:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Default Route:	Disabled
Gateway IP Address:	0 0 0 0

Para configurar rapidamente o sistema, vá para **Home > Quick Configuration**. É exibida a página Quick Configuration.

Quick Configuration

Use this page to quickly configure the system.

<b>ATM Interface:</b>	0
<b>Operation Mode:</b>	Enabled
<b>Encapsulation:</b>	1483 Bridged IP LLC
<b>VPI:</b>	8
<b>VCI:</b>	35
<b>Bridge:</b>	Enabled
<b>IGMP:</b>	Disabled
<b>IP Address:</b>	0 0 0 0
<b>Subnet Mask:</b>	0 0 0 0
<b>Use DHCP:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Default Route:</b>	Disabled
<b>Gateway IP Address:</b>	0 0 0 0
<b>PPP</b>	
<b>Username:</b>	GSPN
<b>Password:</b>	
<b>Use DNS:</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>DNS</b>	
<b>Primary DNS Server:</b>	0 0 0 0
<b>Secondary DNS Server:</b>	0 0 0 0

Insira os campos fornecidos conforme abaixo.

Campo	Descrição
<i>ATM Interface</i>	Selecione a interface ATM que deseja usar (geralmente <b>atm-0</b> ) para esta conexão.
<i>Operation Mode</i>	Selecione <b>Yes</b> . Se definido como <b>No</b> , o dispositivo não poderá fornecer conectividade com a Internet para sua rede.
<i>Encapsulation</i>	Selecione o tipo de conexão que seu ISP utiliza para comunicar-se com seu DLink 260E.
<i>VCI e VPI</i>	Digite os valores VPI/VCI fornecidos por seu ISP.
<i>Bridge</i>	Esta definição ativa ou desativa a ponte entre o DLink 260E e seu ISP. Seu ISP pode também referir-se a isto usando "RFC 1483" ou "Ethernet no ATM".
<i>IGMP</i>	Esta definição ativa ou desativa o Internet Group Management Protocol. Entre em contato com seu ISP sobre ativar ou não esta definição.
<i>IP Address e Subnet mask</i>	Se seu ISP tiver atribuído um endereço IP público à sua LAN, digite o endereço IP e a máscara de sub-rede associada nas caixas fornecidas.

	Do contrário, mantenha o padrão 0.0.0.0/0.0.0.0.
<i>Default Route</i>	Quando desativada, o endereço IP especificado acima será usado como rota padrão para sua LAN
<i>Gateway IP Address</i>	Especifica o endereço IP que identifica o servidor do ISP através do qual sua conexão com a Internet será roteada.
<i>User Name e Password</i>	Caso selecionado o PPP como o tipo de Encapsulamento, digite o nome do usuário e a senha que usará para o logon em seu ISP.
<i>Use DNS</i>	Clique em Enable para ativar o serviço de encaminhamento de DNS, que encaminha para seus PCs da LAN o endereço do servidor DNS que sua conexão PPP obteve do seu ISP. Esta opção só pode ser usada quando o Roteador/Bridge atua como um servidor DHCP para a sua LAN.
<i>Primary/Secondary DNS Server</i>	É possível apenas manter o padrão 0.0.0.0. Caso sejam digitados os endereços DNS Primário e Secundário fornecidos por seu ISP, estes servidores DNS serão utilizados além de quaisquer servidores DNS descobertos automaticamente.

Após concluir as definições necessárias, clique em **Submit**.

Em seguida, vá para **Admin > Commit & Reboot** e clique em **Commit** para armazenar suas alterações na memória permanente.

## Exemplos de Quick Configuration

### RFC 1483 Bridge

<b>ATM Interface:</b>	0
<b>Operation Mode:</b>	Enabled
<b>Encapsulation:</b>	1483 Bridged IP LLC
<b>VPI:</b>	8
<b>VCI:</b>	35
<b>Bridge:</b>	Enabled
<b>IGMP:</b>	Disabled
<b>IP Address:</b>	0 0 0 0
<b>Subnet Mask:</b>	0 0 0 0
<b>Use DHCP:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Default Route:</b>	Disabled
<b>Gateway IP Address:</b>	0 0 0 0
<b>PPP</b>	
<b>Username:</b>	GSPN
<b>Password:</b>	
<b>Use DNS:</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>DNS</b>	
<b>Primary DNS Server:</b>	0 0 0 0
<b>Secondary DNS Server:</b>	0 0 0 0

RFC 1577 Router

<b>ATM Interface:</b>	0
<b>Operation Mode:</b>	Enabled
<b>Encapsulation:</b>	1483 Routed IP LLC(1577)
<b>VPI:</b>	8
<b>VCI:</b>	35
<b>Bridge:</b>	Disabled
<b>IGMP:</b>	Enabled
<b>IP Address:</b>	10 100 17 99
<b>Subnet Mask:</b>	255 255 255 240
<b>Use DHCP:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Default Route:</b>	Enabled
<b>Gateway IP Address:</b>	10 100 17 94
<b>PPP</b>	
<b>Username:</b>	
<b>Password:</b>	
<b>Use DNS:</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>DNS</b>	
<b>Primary DNS Server:</b>	0 0 0 0
<b>Secondary DNS Server:</b>	0 0 0 0

RFC 2364 PPPoA

<b>ATM Interface:</b>	0
<b>Operation Mode:</b>	Enabled
<b>Encapsulation:</b>	PPPoA LLC
<b>VPI:</b>	8
<b>VCI:</b>	35
<b>Bridge:</b>	Disabled
<b>IGMP:</b>	Enabled
<b>IP Address:</b>	0 0 0 0
<b>Subnet Mask:</b>	0 0 0 0
<b>Use DHCP:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Default Route:</b>	Enabled
<b>Gateway IP Address:</b>	0 0 0 0
<b>PPP</b>	
<b>Username:</b>	cisco
<b>Password:</b>	*****
<b>Use DNS:</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>DNS</b>	
<b>Primary DNS Server:</b>	0 0 0 0
<b>Secondary DNS Server:</b>	0 0 0 0

# 5 Configuração Básica

Este capítulo fornece as configurações básicas para fazer com que seu dispositivo funcione e que sua rede seja conectada à Internet. As instruções partem do princípio de que o dispositivo não está predefinido com nenhuma configuração ATM VCC, PPP e IPoA. Para cada método de conexão, são fornecidos parâmetros de exemplo para uma melhor compreensão. Deve ser consultado seu ISP para determinar seu modo de conexão e digitar os valores reais fornecidos por seu ISP.

Seu dispositivo pode já estar pré-configurado com as definições necessárias para fazer com que sua rede seja conectada à Internet. Entre em contato com seu ISP para determinar se é necessário alterar algum valor existente.

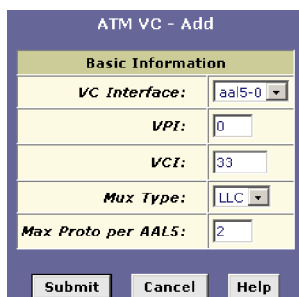
## Modo Bridge

---

Parte 1: Configurando o DSLink 260E

### 1. Criando uma interface ATM VC.

- a. Selecione **WAN > ATM VC > Add**. É exibida a página ATM VC-Add.





- b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
<i>VCC Interface</i>	Selecione uma interface VCC entre as interfaces disponíveis, p.ex., <b>aal5-0</b> .
<i>VPI/VCI</i>	Digite os valores VPI/VCI fornecidos por seu ISP, p.ex., <b>0/33</b> .
<i>Mux Type</i>	Selecione <b>LLC</b> ou <b>VC</b> conforme o exigido por seu ISP.
<i>Max Proto per AAL5</i>	Mantenha o padrão.


Após digitar os campos acima, clique em **Submit**.

- c. Quando aparecer a página de confirmação, clique em **Close**.
- d. Então retornará à tabela **ATM VC Configuration** e verá a entrada ATM VC recém-adicionada.

ATM VC Configuration					
This page is used to view and configure ATM VCCs					
Interface	Vpi	Vci	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	33	LLC	2	 

## 2. Criando uma interface EoA.

- a. Selecione **WAN > EoA > Add** para adicionar uma nova interface EoA.



EOA Interface - Add

EOA Information	
EOA Interface:	<input type="text" value="eoa-1"/>
Interface Sec Type:	<input type="text" value="Public"/>
Lower Interface:	<input type="text" value="aal5-0"/>
Conf. IP Address:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Netmask:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
MTU:	<input type="text" value="65535"/>
Use DHCP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Default Route:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Gateway IP Address:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

- b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
EOA Interface	Selecione uma interface EoA entre as interfaces disponíveis, p.ex., <b>eoa-0</b> .
IPF Type	<b>Public.</b>
Lower Interface	Selecione a interface ATM VCC que foi criada no Passo 1, p.ex., <b>aal5-0</b> .
Config. IP Address/Net Mask	<b>0.0.0.0/0.0.0.0.</b> Para usar o dispositivo como bridge, não é necessário definir o endereço IP e a máscara de sub-rede. Basta manter o padrão.
MTU	Maximum Transmission Unit (MTU) é o maior tamanho de um pacote ou quadro, especificado em octetos

Campo	Descrição
	(bytes de oito bits), que podem ser enviados em um pacote. O Internet's Transmission Control Protocol usa o MTU para determinar o tamanho máximo de cada pacote em qualquer transmissão.
Use DHCP	Disable
Default Route	Disable
Gateway IP Address	Deixe vazio. Não é preciso definir o gateway.

Após digitar os campos acima, clique em **Submit**.

- c. Quando aparecer a página de confirmação, clique em **Close**.
- d. Então retornará à tabela **EOA** e verá a entrada EOA recém-adicionada.

RFC1483/Ethernet over ATM(EoA) Config  
This Page is used to View, Add, Modify and Delete EoA Interfaces.

Interface	Interface Sec Type	Lower Interface	Config IP Address	Netmask	Use DHCP	Default Route	Gateway Address	Status	Action
eoa-0	Public	aal5-0	0.0.0.0	0.0.0.0	Disable	Disable	0.0.0.0		

Add Refresh Help

### 3. Ativação da função Bridging.

- a. Selecione a aba **Bridging** para visualizar a página Bridge Configuration.

Bridge Configuration  
Use this page to Add and Modify Bridging information

Bridging: **Enable/Disable**  
WAN to WAN Bridging: **Enable/Disable**  
ZIPB: **Enable/Disable**

Interface Name	Action
eth-0	
eth-0	Add

Cancel Refresh Help

A página **Bridge Configuration** possui links (em vermelho) para a página **System Mode**, onde você pode ativar/desativar os serviços de bridging correspondentes. A página de **Bridge Configuration** também mostra uma tabela para especificar as interfaces que suportam bridging. A tabela pode estar vazia se não há ainda nenhuma interface configurada para bridging.

- b. A interface **eth-0** á deve estar adicionada à tabela de bridge. Se não estiver, selecione-a da lista e clique em **Add**.
- c. Depois que você criou as interfaces você deve ativar os serviços de bridging no sistema como um todo. Clique na aba Home e depois em System Mode. A tela abaixo será mostrada

Feature	Enabled	Disabled
<i>Bridging:</i>	<input type="radio"/>	<input checked="" type="radio"/>
<i>WAN to WAN Bridging:</i>	<input type="radio"/>	<input checked="" type="radio"/>
<i>BRAS:</i>	<input type="radio"/>	<input checked="" type="radio"/>
<i>ZIPB:</i>	<input type="radio"/>	<input checked="" type="radio"/>

Submit Cancel Help

- d. Certifique-se de que **Enable** esteja selecionado para o item **Bridging** e clique em **Submit**. A página de confirmação é exibida para confirmar suas alterações.

#### 4. Configuração da LAN.

- a. Selecione **Bridging > LAN Config**.
- b. Não modifique as definições; basta manter o padrão mostrado conforme a figura abaixo:

LAN Configuration	
System Mode:	Routing And Bridging
Get LAN Address:	<input checked="" type="radio"/> Manual <input type="radio"/> External DHCP Server <input type="radio"/> Internal DHCP Server
LAN IP Address:	192 168 1 1
LAN Network Mask:	255 255 255 0
Speed:	100BT
Duplex:	Full
JGMP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MTU:	1500

#### 5. Efetive suas alterações.



Selecione **Admin > Commit & Reboot** e clique em **Commit** para armazenar suas alterações na memória permanente.

Parte 2: Verifique o status de sua conexão.

O item Interface WAN deve exibir a interface que foi criada para comunicar-se com seu ISP. Uma bola verde no campo Status indica uma conexão bem-sucedida.

System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL					
<b>Model:</b>	DLink 260E	<b>Operational Status:</b>	Startup Handshake				
<b>H/W Version:</b>	B10100	<b>Last State:</b>	0x18				
<b>S/W Version:</b>	2.5.051005e5	<b>DSL Version:</b>	E.37.4.9				
<b>Serial Number:</b>	260E36H05B000014	<b>Annex Type:</b>	ADSL2				
<b>Mode:</b>	Routing And Bridging	<b>Standard:</b>	ADSL2+ Auto				
<b>Up Time:</b>	0:0:16	<b>Connected Standard:</b>	ADSL2+ Auto				
<b>Time:</b>	Thu Jan 01 00:00:16 1970	<b>Data Boost:</b>	-				
<b>Time Zone:</b>	GMT	<b>Profile:</b>	Brazil				
<b>Daylight Saving Time:</b>	OFF						
<b>Name:</b>		<b>Up</b>	<b>Down</b>				
<b>Domain Name:</b>		<b>Speed</b>	<b>Latency</b>				
		0 Kbps	-				
		0 Kbps	-				
WAN Interfaces							
Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
g0a-0	Bridged	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	8/35	
LAN Interface							
Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:01:38:41:5A:69	192.168.1.1	255.255.255.0	-	10BT	Half	
Services Summary							
Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✓	✗	✗	✗	✓	✗
g0a-0	✓ outside	✓	✗	✗	✗	✗	✗

Modify Refresh Help

Parte 3: Configurando o PC.

#### Opção 1: Seu PC utiliza o IP fornecido por seu ISP.

Se este for o caso, configure seu PC para utilizar o IP estático fornecido por seu ISP, por exemplo:

**IP address:** 10.100.16.2

**Subnet mask:** 255.255.255.0

**Default gateway:** 10.100.16.254



**Nota**

Com a configuração acima, seu PC deve ser capaz de acessar a Internet agora, mas perderá a conexão local com a porta LAN do dispositivo. Se quiser configurar o DLink 260E por meio do Navegador da Web novamente, deverá ser reconfigurado o PC para **192.168.1.x** para estar na mesma sub-rede da porta LAN do dispositivo.

#### Opção 2: Seu cliente utiliza o software PPPoE para conectar-se a seu ISP.

Basta manter a definição de seu PC como cliente DHCP e executar o software PPPoE para fazer a conexão.

## Modo PPP Connection

Parte 1: Configurando o DStLink 260E

### 1. Criando uma interface ATM VCC.



- a. Selecione **Routing > ATM VC > Add** para visualizar a página ATM VC-Add.

- b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
<i>VCC Interface</i>	Selecione a interface VCC entre as interfaces disponíveis, p.ex., <b>aal5-0</b> .
<i>VPI/VCI</i>	Insira os valores VPI/VCI fornecidos por seu ISP, p.ex., <b>0/35</b> .
<i>Mux Type</i>	Selecione <b>LLC</b> ou <b>VC</b> , conforme solicitado pelo seu ISP.
<i>Max Proto per AAL5</i>	Mantenha o padrão.

Após digitar os campos acima, clique **Submit**.

- c. Quando aparecer a página de confirmação, clique em **Close**.
- d. Então retornará à tabela **ATM VC Configuration** e verá a entrada ATM VCC recém-adicionada.

Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	35	LLC	2	 

## 2. Criando a interface PPP.

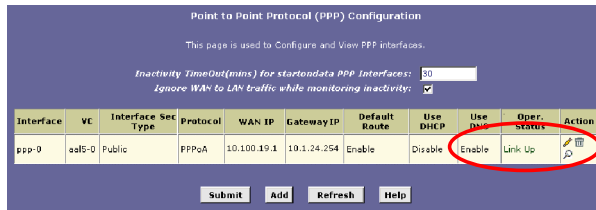
- a. Selecione **Routing > PPP > Add** para adicionar uma nova interface PPP.

- b. Digite os campos fornecidos conforme abaixo.

Campo	Descrição
PPP Interface	Selecione a interface PPP entre as interfaces disponíveis, p.ex., <b>ppp-0</b> .
ATM VCC	Selecione o ATM VCC que foi criada no passo 1, p.ex., <b>aal5-0</b> .
Interface Sec Type	<b>Public</b>
Status	Selecione <b>Start</b> ou <b>StartOnData</b> . <b>Start</b> – Para estabelecer conexão sempre que for ligado o DLink 260E. <b>StartOnData</b> – Para estabelecer conexão sempre que o dispositivo obtiver requisição para conectar-se à Internet, como quando é aberto um navegador requisitando páginas da Web.
Protocol	<b>PPPoA</b> ou <b>PPPoE</b> conforme exigido por seu ISP.
Service Name	Para <b>PPPoA</b> , não há necessidade de configuração. Para <b>PPPoE</b> , digite o Nome do Serviço se este for requisitado por seu ISP. Do contrário, deixe em

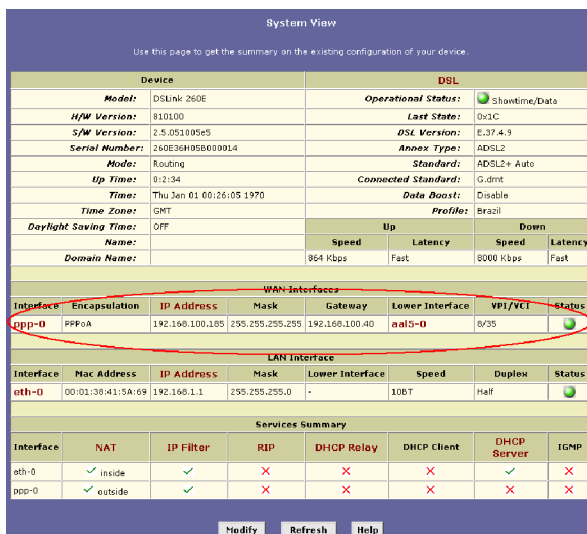
Campo	Descrição
	branco.
Use Dhcp	Selecione <b>Disable</b> a menos que seu ISP o instrua a ativar este serviço.
Use DNS	<b>Enable</b>
Default Route	<b>Enable</b>
Security Protocol	Selecione <b>PAP</b> ou <b>CHAP</b> conforme exigido por seu ISP.
Login Name	O nome de login fornecido por seu ISP.
Password	A senha fornecida por seu ISP.

- c. Então retornará à página PPP Configuration e verá a nova interface PPP. **Oper. Status Link Up** indica que o link está atualmente ativo.



Parte 2: Verifique o status de sua conexão.

O item WAN Interface deve exibir a interface que foi criada para comunicar-se com seu ISP. Uma bola verde no campo Status indica uma conexão bem-sucedida.



Parte 3: Configurando o PC.

Mantenha a configuração de seu PC como cliente DHCP.  
Nenhuma configuração adicional é necessária.

## Modo Router Connection

Esta seção descreve os métodos de conexão por Router  
**RFC1577 e RFC1483**

Parte 1: Configurando o DLink 260E

### 1. Criando uma interface ATM VCC.

- a. Selecione **WAN > ATM VC > Add** para adicionar uma nova interface ATM VCC.

- b. Digite os campos fornecidos conforme abaixo.



Campo	Descrição
<i>VCC Interface</i>	Selecione uma interface VCC entre as interfaces disponíveis, p.ex., <b>aal5-0</b> .
<i>VPI/VCI</i>	Digite os valores VPI/VCI fornecidos por seu ISP, p.ex., <b>0/35</b> .
<i>Mux Type</i>	Selecione <b>LLC</b> ou <b>VC</b> conforme exigido por seu ISP.
<i>Max Proto per AAL5</i>	Mantenha o padrão.

Após digitar os campos acima, clique em **Submit**.

- c. Quando aparecer a página de confirmação, clique em **Close**.
- d. Então retornará à tabela **ATM VC Configuration** e verá a entrada ATM VC recém-adicionada.

**ATM VC Configuration**

This page is used to view and configure ATM VCs

Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	35	LLC	2	 

## 2. Criando uma interface IPoA.

- a. Selecione **WAN > IPoA > Add** para adicionar uma nova interface IPoA.

**IPoA Interface - Add**

**IPoA Information**

<i>IPoA Interface:</i>	<input type="text" value="ipoa-0"/>
<i>Conf. IP Address:</i>	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<i>Interface Sec Type:</i>	<input type="text" value="Public"/>
<i>Netmask:</i>	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<i>MTU:</i>	<input type="text" value="65535"/>
<i>RFC 1577:</i>	<input type="radio"/> Yes <input checked="" type="radio"/> No
<i>Use DHCP:</i>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<i>Default Route:</i>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<i>Gateway IP Address:</i>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

- b. Então entre os campos abaixo.

Campo	Descrição
<i>IPoA Interface</i>	Selecione uma interface IPoA entre as interfaces disponíveis, p.ex., <b>ipoa-0</b> .
<i>Conf. IP Address</i>	Digite o endereço IP fornecido por seu ISP, p.ex., <b>10.100.17.89</b> .
<i>Interface Sec Type</i>	<b>Public</b>
<i>Net Mask</i>	Digite o endereço IP fornecido por seu ISP, p.ex., <b>255.255.255.248</b> .
<i>IPoA Type</i>	Para RFC 1577-IP Clássico e ARP sobre ATM, selecione <b>Yes</b> . Para RFC 1483 Router, selecione <b>No</b> .
<i>Default Route</i>	<b>Enable</b>
<i>Gateway IP Address</i>	Digite o endereço IP fornecido por seu ISP, p.ex., <b>10.100.17.94</b> .

Após digitar os campos acima, clique em **Submit**.

- c. Quando aparecer a página de confirmação, clique em **Close**.
- d. Então retornará à tabela **IPoA Configuration** e verá a entrada IPoA recém-adicionada.

IP over ATM (IPoA) Configuration  
This Page is used to View, Add and Delete IPoA Interfaces.

Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Config IP Address	Netmask	Gateway Address	Status	Action
ipoa-0	Public	Yes	-	-	10.100.17.89	255.255.255.248	10.100.17.94		

### 3. Mapeando a interface IPoA em uma interface baixa.

Na tabela **IPoA Configuration**, localize a nova entrada IPoA e clique em **Map** na coluna **Action**.

Na página **IPoA Interface-Map**, da lista drop-down, selecione o ATM VC que você criou no passo 1 para ser mapeada nesta interface IPoA e então clique em **Add**. Então clique em **Close** para sair da página de confirmação.

IPoA Interface - Map

IPoA Map Information	
<b>IPoA Interface:</b>	ipoa-0
	Lower I/F    Action
<b>Lower Interface:</b>	No Low I/F !
	<input type="text" value="aal5-0"/> <input type="button" value="Add"/>

Você retornará para a página **IPoA Configuration** e verá que a interface baixa foi mapeada nesta interface IPoA.

IP over ATM (IPoA) Configuration  
This Page is used to View, Add and Delete IPoA Interfaces.

Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Config IP Address	Netmask	Gateway Address	Status	Action
ipoa-0	Public	Yes	aal5-0	0.0.0.0	10.100.17.89	255.255.255.248	10.100.17.94		

Parte 2: Verifique o status de sua conexão.

O item WAN Interface deve exibir a interface que foi criada para comunicar-se com seu ISP. Uma bola verde no campo Status indica uma conexão bem-sucedida.

**System View**

Use this page to get the summary on the existing configuration of your device.

Device		DSL			
<b>Model:</b>	DLink 260E	<b>Operational Status:</b>	Showtime/Data		
<b>H/W Version:</b>	810100	<b>Last State:</b>	0x1C		
<b>S/W Version:</b>	2.5.051005a5	<b>DSL Version:</b>	E.37.4.9		
<b>Serial Number:</b>	260E36H05B000014	<b>Annex Type:</b>	ADSL2		
<b>Mode:</b>	Routing	<b>Standard:</b>	ADSL2+ Auto		
<b>Up Time:</b>	0:30:9	<b>Connected Standard:</b>	G.dmt		
<b>Time:</b>	Thu Jan 01 00:53:40 1970	<b>Data Boost:</b>	Disable		
<b>Time Zone:</b>	GMT	<b>Profile:</b>	Brazil		
<b>Daylight Saving Time:</b>	OFF	<b>Up</b>		<b>Down</b>	
<b>Name:</b>		<b>Speed</b>	<b>Latency</b>	<b>Speed</b>	<b>Latency</b>
<b>Domain Name:</b>		864 Kbps	Fast	8000 Kbps	Fast

WAN Interfaces							
Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ipoa-0	Routed	192.168.100.87	255.255.255.0	192.168.100.1	aal5-0	8/35	

LAN Interface							
Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:01:38:41:5A:69	192.168.1.1	255.255.255.0	-	10BT	Half	

Services Summary							
Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	inside						
ipca-0	outside						

Parte 3: Configurando o PC.

Mantenha a configuração de seu PC como cliente DHCP.  
Nenhuma configuração adicional é necessária.

# 6 Configurando Rotas IP

Você pode usar o Configuration Manager para definir rotas específicas para seus dados de Internet e de rede. Este capítulo fornece instruções para a criação de rotas.

A maioria dos usuários não precisa definir rotas IP. Poderá ser preciso definir rotas se:

- A instalação de sua rede incluir duas ou mais redes ou sub-redes.
- For conectar-se a dois ou mais serviços de ISP.
- For conectar-se a uma LAN corporativa remota.

## Visualizando a Tabela de Roteamento IP

Para visualizar a tabela de roteamento do DSLink 260E, selecione **Routing > IP Route**. É exibida a página a seguir:

Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	Dynamic	
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	
192.168.1.2	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	

A página IP Route Table inclui rotas que foram predefinidas no dispositivo, rotas podem ter sido adicionadas e rotas que o dispositivo tenha identificado automaticamente através de comunicação com outros dispositivos.

A tabela de roteamento deve refletir um gateway padrão, que direcione o tráfego Internet de saída para seu ISP. Este gateway padrão está mostrado na linha que contém o endereço de destino 0.0.0.0.

## Adicionando Rotas IP

1. Selecione **Routing > IP Route > Add**. É exibida a página IP Rota – Add:

IP Route Information			
Destination:	0	0	0
Netmask:	255	255	0
Gateway/NextHop:	0	0	0

2. Especifique o destino, a máscara da rede e o gateway ou o próximo salto desta rota.

Para criar uma rota que defina o gateway padrão de sua LAN, digite **0.0.0.0** nos campos **Destination** e **Net Mask**. Digite o endereço IP de seu ISP no campo **Gateway/NextHop**.

Não é possível especificar um nome de interface, tipo de rota ou origem da rota. Estes parâmetros são utilizados apenas para rotas que são identificadas automaticamente à medida que o dispositivo se comunica com outros dispositivos de roteamento. Para as rotas que forem criadas, a tabela de roteamento exibe os valores padrão do sistema nestes campos.

3. Clique em **Submit**.  
A Tabela de Roteamento IP agora exibirá a nova rota.
4. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

# 7 Configuração DHCP

É possível configurar sua rede e o DSLink 260E para usar o Dynamic Host Configuration Protocol (DHCP). Este capítulo fornece instruções para a implementação do DHCP em sua rede.

## Modos DSLink 260E DHCP

---

O dispositivo pode ser configurado como um servidor DHCP, agente de retransmissão DHCP ou, em alguns casos, um cliente DHCP.

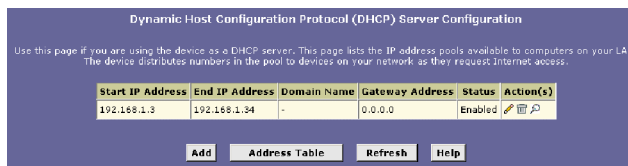
- **DHCP Server** - Ele manterá o pool de endereços e os distribuirá para seus computadores da LAN. Se o pool de endereços incluir endereços IP privados, então deverá também configurar o serviço Conversão de Endereços de Rede, para que os endereços privados possam ser convertidos para seu endereço IP público na Internet. Tanto o servidor DHCP quanto o NAT estão ativados na configuração padrão.
- **DHCP relay agent** - Se seu ISP executa a função de servidor DHCP para sua rede, então poderá configurar o dispositivo como agente de retransmissão DHCP. Quando o DSLink 260E recebe uma requisição para acesso à Internet a partir de um computador de sua rede, ele contata seu ISP para as informações de IP necessárias e, em seguida, retransmite as informações partilhadas de volta ao computador.
- **DHCP Client** - Caso tenha outro PC ou dispositivo em sua rede que já esteja executando a função de servidor DHCP, poderá configurar a porta LAN do DSLink 260E para ser um cliente DHCP daquele servidor.

## Configurando o Servidor DHCP

---



### Parte 1. Criando pools de endereços IP

1. Selecione **LAN > DHCP Server**. É exibida a página DHCP Server Configuration:



Dynamic Host Configuration Protocol (DHCP) Server Configuration

Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
192.168.1.2	192.168.1.34	-	0.0.0.0	Enabled	 

Cada pool que for criado exibe uma linha na tabela sobre esta página. É possível criar até oito pools. Neste exemplo, foi criado um pool para a interface LAN. Pools adicionais podem ser necessários quando o dispositivo for configurado com várias interfaces LAN.

2. Para adicionar um pool de endereços IP, clique em **Add**.  
É exibida a página DHCP Server Pool – Add.

Os campos **Start IP Address**, **End IP Address**, **Net Mask**, e **Gateway Address** são obrigatórios; os outros são opcionais.

Campo	Descrição
<i>Start/End IP Addresses</i>	Especifique os endereços primário e secundário do pool.
<i>Mac Address</i>	Permite atribuir endereço IP específico a um computador específico, identificado por este endereço MAC. Se este for o caso, então deve ter especificado o mesmo endereço IP nos campos Start/End IP Address.
<i>Net Mask</i>	Especifica a máscara de sub-rede associada do endereço IP nesta faixa.
<i>Domain Name</i>	O nome de domínio a ser utilizado por clientes DHCP.
<i>Gateway Address</i>	O endereço do gateway padrão. Normalmente, ele é o endereço IP da porta LAN do dispositivo.
<i>DNS</i>	O endereço IP do servidor DNS. Normalmente ele é encontrado em seu ISP.
<i>SDSN...SWINS (opcional)</i>	Os endereços IP dos dispositivos que executam variados serviços para clientes DHCP.

3. Clique em **Submit**.

É exibida a página de confirmação para indicar que o pool foi adicionado com sucesso.

4. Clique em **Close** para retornar à página DHCP Configuration.

## Parte 2. Ativando o Modo DHCP Server

1. Selecione **LAN > DHCP Mode**, na lista suspensa DHCP Mode, selecione **DHCP Server** e, em seguida, clique em **Submit**.

É exibida uma página para confirmar a alteração.

2. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

## Parte 3. Configurando seus PCs como clientes DHCP

Para cada computador que queira configurar para receber informações de IP automaticamente, configure as propriedades de TCP/IP para "Obtain an IP address automatically" (o texto real poderá variar dependendo de seu sistema operacional).

## Modificando Pools de Endereços

Selecione **LAN > DHCP Server** e, em seguida, clique no ícone Modify no pool DHCP que quiser modificar. É exibida a página DHCP Server Pool – Modify:

Ao modificar um pool de endereços, terá permissão **apenas** para:

- Alterar o nome de domínio associado ao pool.
- Excluir da distribuição endereços IP dentro de sua faixa. Para excluir um endereço IP, digite-o nos campos fornecidos e clique em **Add**.

Se quiser alterar outros atributos, será preciso excluir o pool e criar um novo.

Após digitar suas alterações, clique em **Submit** e certifique-se de utilizar o recurso Commit para salvar suas alterações na memória permanente.

Visualizando Atribuições de Endereço DHCP Atuais

Para visualizar uma tabela de todas as atribuições de endereço IP atuais, selecione **LAN > DHCP Server > Address Table**. A página DHCP Server Address Table é a seguinte:

DHCP Server Address Table					
IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
192.168.1.3	255.255.255.0	00:10:60:90:1A:8D	192.168.1.3	Dynamic	2587715 Second(s)
192.168.1.101	255.255.255.0	00:05:5D:A6:3E:E9	192.168.1.3	Dynamic	2587696 Second(s)

## Configurando a Retransmissão DHCP

Parte 1. Definindo a(s) interface(s) de retransmissão DHCP

1. Selecione **LAN > DHCP Relay**. É exibida a página DHCP Relay Configuration:

Dynamic Host Configuration Protocol (DHCP) Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.

DHCP Server Address:

Interfaces Running DHCP Relay	Action
ppp-0	<input type="button" value="Remove"/>
eth-0	<input type="button" value="Add"/>

Esta página oferece uma caixa de texto para a digitação do endereço IP do servidor DHCP de seu ISP e uma tabela que apresenta uma lista das interfaces existentes em seu DLink 260E que possam retransmitir Informações sobre DHCP.

2. Digite o endereço IP do servidor DHCP de seu ISP nos campos fornecidos.

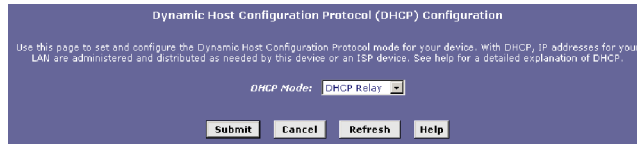
Se não possuir este número, não será necessário inseri-lo aqui. Requisições para informações de IP provenientes de sua LAN serão transferidas para o gateway padrão, que deve rotear a requisição da forma apropriada.

3. Se a interface identificada como eth-0 já não estiver sendo exibida, selecione-a na lista suspensa e clique em **Add**.
4. Clique em **Submit**.  
É exibida uma página para confirmar suas alterações.

#### Parte 2. Ativando modo de retransmissão DHCP

1. Selecione **LAN > DHCP Mode**, na lista suspensa DHCP Mode, selecione **DHCP Relay** e, em seguida, clique em **Submit**.

É exibida uma página para confirmar a alteração.



2. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

#### Parte 3. Configurando seus PCs como clientes DHCP

Para cada computador que queira configurar para receber informações de IP automaticamente, configure as propriedades de TCP/IP para "Obtain an IP address automatically" (o texto real poderá variar dependendo de seu sistema operacional).

# 8 Configuração NAT

Este capítulo fornece uma visão geral da Conversão de Endereços de Rede (NAT, network address translation) e instruções para modificar a configuração padrão em seu dispositivo.

## Sua Instalação NAT Padrão

Por padrão, a NAT é ativada, com uma regra *network address port translation* (napt) configurada que converte qualquer endereço privado no lado LAN no endereço IP público atribuído por seu ISP no lado WAN.

## Visualizando Sua Configuração NAT

Para visualizar suas configurações NAT, selecione **Services > NAT**. É exibida a página NAT Configuration:

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	6
GRE Timeout(sec):	300
ESP Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

A tabela NAT Global Information contém os seguintes campos:

Campo	Descrição
<i>TCP Idle Timeout (seg)</i>	Para a sessão de conversão NAT sobre dados que utilizem o protocolo TCP, a conversão não mais será executada se nenhum pacote de dados correspondente for recebido após decorrido o tempo especificado.
<i>TCP Close Wait (seg)</i>	Para a conversão NAT sobre dados usando o protocolo TCP, após a sessão de comunicação ter sido encerrada, a conversão não mais será executada se nenhum pacote de dados correspondente for recebido após decorrido o tempo especificado.

<b>Campo</b>	<b>Descrição</b>
<i>TCP Def Timeout (seg)</i>	Para a sessão de conversão NAT sobre dados que utilizem o protocolo TCP, a conversão não mais será executada se nenhum pacote de dados correspondente for recebido após decorrido o tempo especificado.
<i>UDP Timeout (seg)</i>	O mesmo que TCP Idle Timeout, mas para pacotes UDP.
<i>ICMP Timeout (seg)</i>	O mesmo que TCP Idle Timeout, mas para pacotes ICMP.
<i>GRE Timeout (seg)</i>	O mesmo que TCP Idle Timeout, mas para pacotes GRE.
<i>Default Nat Age (seg)</i>	Para todas as outras sessões de conversão NAT, o número de segundos após o qual uma sessão de conversão não mais será válida.
<i>NAPT Port Start/End</i>	Quando uma regra napt é definida, as portas de origem serão convertidas para números seqüenciais nesta faixa.

Se você alterar algum valor, clique em **Submit** e, em seguida, efetive suas alterações armazenando-as na memória permanente do sistema.

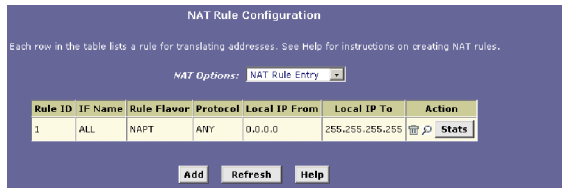
Então pode clicar em **Global Stats** para visualizar dados acumulados sobre quantas regras NAT foram chamadas e quantos dados foram convertidos. É exibida uma página similar à abaixo:

NAT Rule Global Statistics	
<b>Total NAT Sessions</b>	
Total Translation Sessions:	0 Sessions
Number of FTP ALG Sessions:	0 Sessions
Number of SNMP ALG Sessions:	0 Sessions
Number of Real Audio ALG Sessions:	0 Sessions
Number of Remote-Command Sessions:	0 Sessions
Number Of L2TP ALG Sessions:	0 Sessions
Number Of MIRC ALG Sessions:	0 Sessions
Number Of CUCME ALG Sessions:	0 Sessions
Number Of H323 Q931 ALG Sessions:	0 Sessions
Number Of H323 RAS ALG Sessions:	0 Sessions
Number Of H323 H245 ALG Sessions:	0 Sessions
Number Of H323 RTP ALG Sessions:	0 Sessions
Number Of CUSEEME UDP ALG Sessions:	0 Sessions
Number Of PPTP ALG Sessions:	0 Sessions
Number Of RTSP ALG Sessions:	0 Sessions
Number Of Timbuktu ALG Sessions:	0 Sessions
Number Of T120 ALG Sessions:	0 Sessions
Number Of LDAP ALG Sessions:	0 Sessions
Number Of SGI Compcore ALG Sessions:	0 Sessions
Number Of MSN Messenger ALG Sessions:	0 Sessions
Number Of IKE ALG Sessions:	0 Sessions
Number Of ESP ALG Sessions:	0 Sessions
Number Of SIP ALG Sessions:	0 Sessions
<b>Translation Statistic</b>	
Packets w/o Matching Translation Rules:	0 Packets
Number Of In-Packets Translated:	0 Packets
Number Of Out-Packets Translated:	0 Packets
Number Of Fragments Processed:	0 Packets
<b>Active NAT Sessions</b>	
Active Translation Sessions:	0 Sessions
Active Rules:	0 Sessions
Active Session Using FTP ALG:	0 Sessions
Active Session Using SNMP ALG:	0 Sessions
Active Session Using Real Audio ALG:	0 Sessions
Active Session Using Remote-Command-Session:	0 Sessions
Active Session Using L2TP ALG:	0 Sessions
Active Session Using MIRC ALG:	0 Sessions
Active Session Using CUCME ALG:	0 Sessions
Active Session Using H323 Q931 ALG:	0 Sessions
Active Session Using H323 RAS ALG:	0 Sessions
Active Session Using H323 H245 ALG:	0 Sessions
Active Session Using H323 RTP ALG:	0 Sessions
Active Session Using CUSEEME UDP ALG:	0 Sessions
Active Session Using PPTP ALG:	0 Sessions
Active Session Using RTSP ALG:	0 Sessions
Active Session Using Timbuktu ALG:	0 Sessions
Active Session Using T120 ALG:	0 Sessions
Active Session Using LDAP ALG:	0 Sessions
Active Session Using SGI Compcore ALG:	0 Sessions
Active Session Using MSN Messenger ALG:	0 Sessions
Active Session Using IKE ALG:	0 Sessions
Active Session Using ESP ALG:	0 Sessions
Active Session Using SIP ALG:	0 Sessions

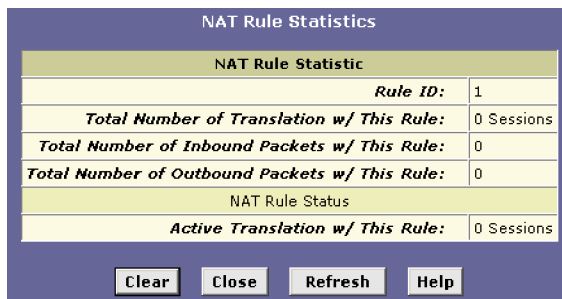
Clear Close Refresh Help

## Visualizando Regras NAT e Estatísticas de Regras

Para visualizar as Regras NAT atualmente definidas em seu sistema, selecione **Services > NAT > NAT Rule Entry**. É exibida a página NAT Rule Configuration:



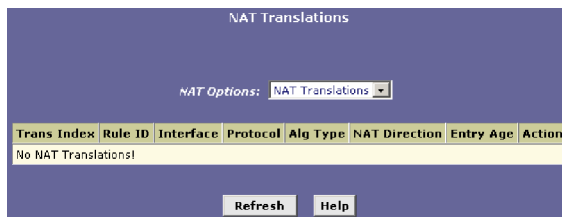
Para visualizar dados sobre a frequência com que uma regra NAT específica foi utilizada, clique em **Stats**. É exibida uma página similar à abaixo:



As estatísticas mostram quantas vezes esta regra foi chamada e quantas sessões atualmente ativas estão utilizando esta regra.

## Visualizando Conversões NAT Atuais

Para visualizar uma lista de conversões NAT que tenham recentemente sido executadas e que permaneçam em vigor (para qualquer uma das regras definidas), selecione **Services > NAT > NAT Translations**. É exibida a página NAT Translations:



Para cada sessão de conversão atual NAT, a tabela contém os seguintes campos:

Campo	Descrição
<i>Trans Index</i>	O número seqüencial atribuído à sessão IP utilizado por esta sessão de conversão NAT.
<i>Rule ID</i>	A identificação da regra NAT chamada.
<i>Interface</i>	A interface do dispositivo sobre o qual a regra NAT foi chamada (a partir da definição da regra).
<i>Protocol</i>	O protocolo IP utilizado pelos pacotes de dados que estiverem sofrendo conversões (a partir da definição da regra) Exemplo: TCP,

<b>Campo</b>	<b>Descrição</b>
	UDP, ICMP.
<i>Alg Type</i>	O <i>Application Level Gateway</i> (ALG), se houver, que foi utilizado para ativar esta conversão NAT (ALGs são configurações especiais que determinados aplicativos exigem para funcionar enquanto a NAT estiver ativada).
<i>NAT Direction</i>	A direção (de entrada ou de saída) da conversão (a partir da definição da porta).
<i>Entry Age</i>	O tempo decorrido, em segundos, da sessão de conversão NAT.

### Adicionando Regras NAT

Esta seção explica como criar regras para as diferentes versões NAT.

A regra napt: Efetuando conversões entre endereços IP públicos e privados

A versão NAT napt foi utilizada em sua configuração padrão. A versão napt converte todos os endereços IP de origem privados do lado LAN em um único endereço IP público. Ela também converte os números da porta de origem em números de porta que são definidos na página NAT Global Configuration.

1. Selecione **Services > NAT > NAT Rule Entry > Add**.

**NAT Rule - Add**

NAT Rule Information				
<i>Rule Flavor:</i>	<input type="text" value="NAPT"/>			
<i>Rule ID:</i>	<input type="text"/>			
<i>IF Name:</i>	<input type="text" value="ALL"/>			
<i>Local Address From:</i>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<i>Local Address To:</i>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>
<i>Global Address:</i>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

2. Clique na lista suspensa Rule ID para atribuir um número a uma regra.  

Rule ID determina a ordem na qual as regras são chamadas (a regra de número mais baixo é chamada primeiro, e assim por diante). Em alguns casos, duas ou mais regras podem ser definidas para agir sobre o mesmo conjunto de endereços IP. Assim que um pacote de dados corresponder a uma regra, os dados passarão a agir conforme essa regra e não ficarão sujeitos a regras de número mais alto.
3. Na Lista suspensa Rule Flavor, selecione **NAPT**, se necessário.
4. Na lista suspensa IFName, selecione a interface do DSLink 260E à qual esta regra se aplica.  

Normalmente, as regras NAT aplicam-se à comunicação entre sua LAN e a Internet. Como o dispositivo utiliza a interface WAN (identificada como *ppp-0* ou *eo-a-0*) para conectar sua LAN a seu ISP, esta será a seleção usual de IFName.
5. Selecione um protocolo ao qual esta regra se aplique, ou escolha **ALL** se a regra aplicar-se a todos os dados.
6. Nos campos **Local Address From/To**, digite os endereços IP inicial e final, respectivamente, da faixa de endereços privados que queira converter. Ou digite o mesmo endereço em ambos os campos para especificar um único valor.  

Se todos os endereços LAN precisarem ser convertidos, especifique 0.0.0.0 e 255.255.255.255, respectivamente.

Se for utilizar endereços privados não-sequenciais, é possível criar uma regra napt adicional para cada faixa de endereços em separado.
7. No campo Global Address, digite o endereço que deseja que sirva como o endereço publicamente conhecido para o computador da LAN.
8. Quando tiver acabado de inserir todas as informações, clique em **Submit**.  

É exibida uma página para confirmar a alteração.
9. Clique em **Close** para retornar à página NAT Configuration.  

A nova regra deve ser exibida na tabela NAT Rule.
10. Selecione **NAT Global Info** da lista **NAT Options** para ir para a página NAT Configuration. Certifique-se de que o botão **Enable** está ligado.
11. Na página NAT Configuration, clique em **Submit**.  

É exibida uma página para confirmar suas alterações.
12. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

A regra rdr: Permitindo acesso externo a um computador da LAN

É possível criar uma regra rdr para fazer com que um computador de sua LAN, como um servidor Web ou FTP, fique disponível para usuários da Internet sem ter que obter um endereço IP público para esse computador. O endereço IP privado do computador é convertido para seu endereço IP público em todos os pacotes de dados de entrada e de saída.



**Nota**

Sem uma regra rdr (ou regra bitmap), o DSLink 260E bloqueia tentativas por computadores externos de acesso a seus computadores da LAN.

NAT Rule - Add	
NAT Rule Information	
Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	
Local Address To:	
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535
Local Port:	Any other port 0
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

Siga estas instruções para adicionar uma regra rdr.

1. Exiba a página NAT Rule – Add, escolha um valor para Rule ID e selecione **RDR** como Rule Flavor.
2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.
3. Nos campos **Local Address From/To**, digite o mesmo endereço IP privado ou os endereços primário e secundário em uma faixa:
  - Caso venha a digitar o mesmo endereço IP em ambos os campos, o tráfego de entrada que corresponder aos critérios desta regra será redirecionado àquele endereço IP.
  - Caso venha a digitar uma faixa de endereços, o tráfego de entrada será redirecionado a qualquer computador disponível naquela faixa. Esta opção normalmente seria utilizada para balanceamento de carga, por meio do qual o tráfego é distribuído entre diversos servidores redundantes.

- Nos campos **Global Address From/To**, digite o endereço IP público que lhe foi atribuído por seu ISP.

Caso tenha várias interfaces WAN, em ambos os campos digite o endereço IP da interface à qual esta regra se aplica. Esta regra não será posta em execução para dados que chegam em interfaces WAN não especificadas aqui.

Caso tenha várias interfaces WAN e quiser que a regra seja posta em execução em uma faixa delas, digite os endereços IP inicial e final da faixa.

- Nos campos **Destination Port From/To**, entre ou selecione o ID da porta (ou uma faixa) que você espera encontrar nos pacotes que chegam, destinados aos computadores da LAN para os quais esta regra foi criada.

O tráfego de entrada que obedece este critério será redirecionado para o número da porta local que você especificou no próximo passo.

- Se o computador da LAN que você está disponibilizando publicamente está configurado para usar um número de porta não padrão para o tipo de tráfego que ele recebe, digite um número de porta não padrão no campo **Local Port**.
- Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra basic: Executando conversões 1:1

A versão basic converte o endereço IP privado (lado LAN) em um endereço público (lado WAN), como regras napt. No entanto, ao contrário das regras napt, as regras basic não convertem também os números de porta no cabeçalho de pacote; eles são passados sem conversão. Portanto, a regra basic não proporciona o mesmo nível de segurança que a regra napt.

A figura abaixo mostra os campos utilizados para a adição de uma regra basic.

NAT Rule - Add				
NAT Rule Information				
<b>Rule Flavor:</b>	BASIC			
<b>Rule ID:</b>	<input type="text"/>			
<b>IF Name:</b>	ALL			
<b>Protocol:</b>	ANY			
<b>Local Address From:</b>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<b>Local Address To:</b>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>
<b>Global Address From:</b>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<b>Global Address To:</b>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>				

- Exiba a página NAT Rule – Add, escolha uma Rule ID e selecione **BASIC** como Rule Flavor.

2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.
3. Nos campos **Local Address From/To**, digite os endereços IP inicial e final que identificam a faixa de endereços privados que queira converter. Ou digite o mesmo endereço em ambos os campos.  
  
Caso especifique uma faixa, cada endereço será convertido em seqüência para um endereço correspondente em uma faixa de endereços globais (especificada no passo 4).
4. Nos campos **Global Address From/To**, digite o endereço inicial e final que identificam o pool de endereços IP públicos para o qual seus endereços privados devem ser convertidos. Ou digite o mesmo endereço em ambos os campos (caso também tenha sido especificado um único endereço no passo 3).
5. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra filter: Configurando uma regra basic com critérios adicionais

Da mesma forma que na versão basic, a versão filter converte endereços IP públicos e privados um a um. A versão filter amplia a capacidade da regra basic.

Então pode usar a regra filter se quiser que ocorra a conversão de um endereço somente quando seus computadores da LAN iniciarem o acesso a destinos específicos. Os destinos podem ser identificados por seus endereços IP, tipo de servidor (como servidor FTP ou Web) ou ambos.

**NAT Rule - Add**

NAT Rule Information				
<i>Rule Flavor:</i>	FILTER			
<i>Rule ID:</i>				
<i>IF Name:</i>	ALL			
<i>Protocol:</i>	ANY			
<i>Local Address From:</i>	0	0	0	0
<i>Local Address To:</i>	255	255	255	255
<i>Global Address From:</i>	0	0	0	0
<i>Global Address To:</i>	0	0	0	0
<i>Destination Address From:</i>	0	0	0	0
<i>Destination Address To:</i>	255	255	255	255
<i>Destination Port From:</i>	Any other port		0	
<i>Destination Port To:</i>	Any other port		65535	

1. Exiba a página NAT Rule – Add, escolha a Rule ID, e selecione **FILTER** como Rule Flavor.
2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.
3. Nos campos **Local Address From/To**, digite os endereços IP inicial e final que identificam a faixa de endereços privados que queira converter. Ou digite o mesmo endereço em ambos os campos.  
 Caso especifique uma faixa, cada endereço será convertido em seqüência para um endereço correspondente em uma faixa de endereços globais (especificada no passo 4).
4. Nos campos **Global Address From/To**, digite o endereço inicial e final que identificam a faixa de endereços IP públicos para a qual seus endereços privados devem ser convertidos. Ou digite o mesmo endereço em ambos os campos (caso também tenha sido especificado um único endereço no passo 3).
5. Especifique **Destination Address** ou **Destination Addresses**, **Destination Port** (ou **Destination Ports**), ou ambos. É possível especificar um único valor inserindo esse valor em ambos os campos.
  - Especifique um endereço de destino (ou faixa) caso queira que esta regra aplique-se apenas ao tráfego de saída até o endereço (ou faixa).  
 Caso digite apenas a parte da identificação da rede do endereço de destino, a regra será aplicada ao tráfego de saída para todos os computadores na rede.

- Especifique uma porta de destino (ou faixa) caso queira que esta regra se aplique a qualquer tráfego de saída para os tipos de servidores identificados por esse número de porta.
  - Especifique tanto um endereço de destino (ou faixa) quanto uma porta de destino (ou faixa) caso queira que esta regra de conversão seja aplicada aos acessos do tipo de servidor especificado no local especificado.
6. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra bitmap: Executando conversões bidirecionais

Ao contrário das outras versões NAT, a versão bitmap executa conversões de endereço nas direções tanto de saída quanto de entrada.

Na direção de entrada, quando a interface especificada recebe um pacote destinado a seu endereço IP público, este endereço é convertido para o endereço IP privado de um computador em sua LAN.

Na direção de saída, o endereço IP de origem privado em um pacote de dados é convertido para o endereço IP público da LAN.

Regras bitmap podem ser utilizadas para proporcionar acesso externo a um dispositivo LAN. Elas não proporcionam o mesmo nível de segurança das regras rdr, pois as regras rdr também re-roteiam pacotes de entrada com base na identificação da porta. Regras bitmap não levam em conta o número de porta e, portanto, permitem acesso externo independentemente do tipo de porta de destino especificado no pacote de entrada.

NAT Rule Information	
Rule Flavor:	BIMAP
Rule ID:	
IF Name:	ALL
Local Address:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Global Address:	0 0 0 0

Submit Cancel Help

1. Exiba a página NAT Rule – Add, escolha a Rule ID, e selecione **BITMAP** como Rule Flavor.
2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.
3. No campo Local Address, digite o endereço IP privado do computador ao qual esteja concedendo acesso externo.
4. No campo Global Address, digite o endereço que deseja que sirva como o endereço publicamente conhecido para o computador da LAN.

5. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

A regra PASS : Permitindo que endereços específicos passem sem conversão

É possível criar uma regra PASS para permitir que uma faixa de endereços IP permaneça sem conversão quando outra regra a converteria.

NAT Rule - Add				
NAT Rule Information				
Rule Flavor:	PASS			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>				

Deve ser atribuída uma identificação de regra à regra PASS que seja um número inferior ao da identificação atribuída a uma regra que se pretenda transpor. Caso queira que um endereço IP específico ou faixa de endereços não fiquem sujeitos a uma regra existente, por exemplo, identificação de regra nº 5, será possível criar uma regra PASS com identificação nº 1 a 4.

1. Exiba a página NAT Rule – Add Page, escolha a Rule ID, e selecione **Pass** como Rule Flavor.
2. Selecione a interface e, se desejado, um protocolo ao qual esta regra se aplique.
3. Nos campos **Local Address From** e **Local Address To** campos, digite os endereços primário e secundário IP que definem uma faixa de endereços privados que queira que passem sem conversão. Caso queira que uma regra PASS aja em apenas um endereço, digite esse endereço em ambos os campos.
4. Siga os passos 8-12 sob a regra napt para efetivar suas mudanças.

# 9 Configurando Endereços do Servidor DNS e DDNS

Este capítulo descreve como configurar a função de retransmissão DNS e DDNS do DSLink 260E.

## Visão Geral da Retransmissão DNS

Ao executar a retransmissão DNS, o DSLink 260E propriamente dito não é um servidor DNS, ele transmite requisições DNS dos PCs da LAN para um servidor DNS no ISP. Em seguida, ele retransmite a resposta DNS aos PCs.

O DSLink 260E detecta o endereço DNS de uma ou ambas as maneiras a seguir:

- **Detectado através de PPP**
- **Configurado no DSLink 260E**

## Configurando a Retransmissão DNS



Siga estes passos para configurar a retransmissão DNS:

1. Configure os PCs da LAN.  
Basta definir os PCs da LAN como clientes DHCP do DSLink 260E.
2. No DSLink 260E, vá para **LAN > DHCP Server**, insira o endereço IP da LAN (p.ex., **192.168.1.1**) ou **0.0.0.0** como o endereço DNS no pool de servidores DHCP.  
Por padrão, 0.0.0.0 já é definido como o DNS do pool DHCP.
3. Determina de que forma o roteador detectará o endereço DNS do servidor:

### Opção 1: Usando a conexão PPP para detectar o DNS

**Use DNS** deve ser ativado nas propriedades da interface PPP.

Vá para **Routing > PPP** e verifique os detalhes da interface PPP. Se **Use DNS** estiver desativado, será preciso excluir a interface e criá-la novamente com a nova configuração.

Interface	VC	Interface Sec Type	Protocol	WAN IP	Gateway IP	Default Route	Use DHCP	Use DNS	Oper. Status	Action
ppp-0	eal5-0	Public	PPPoA	10.100.19.1	10.1.24.254	Enable	Disable	Enable	Link up	 

### Opção 2: Configurando DNS no roteador ADSL/Ethernet

É possível configurar o endereço DNS do servidor para ser retransmitido sobre o roteador se uma das seguintes circunstâncias aplicar-se:

- Sem utilizar a conexão PPP para o ISP (ou se for utilizado um protocolo que não seja PPP, como o EoA).
- Então utiliza a conexão PPP e **Use DNS** já está **ativado**. Em seguida, esses endereços configurados serão utilizados além daqueles endereços DNS detectados através de PPP.
- Então utiliza a conexão PPP e **Use DNS** está **desativado**. Em seguida, esses endereços configurados serão utilizados.

Siga estes passos para configurar a retransmissão DNS no roteador:

- (a) Vá para **Service > DNS** para exibir a página DNS Configuration.

Página DNS Configuration

- (b) Digite o endereço IP do servidor DNS em uma linha vazia e clique em **Add**. Clique no botão de opção **Enable** e, em seguida, clique em **Submit**.
- (c) Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

## Configurando DDNS

Para exibir a página DDNS, **Services > DDNS**:

- 1- Em **Host Name** coloque o nome do host , em **Interface** selecione a interface na qual a função será aplicada e clique em **Add Host**;
- 2- Clique em **Add Service** para exibir a página Dynamic DNS Service – Add:

**Interface:** configure a mesma interface do Item 1;

**Service Name:** DYNDNS / TZO;

**Username:** nome de usuário requerido para o sistema DDNS;

**Password:** senha requerida para o sistema DDNS;

**Type Of System:** Dynamic DNS / Static DNS / Custom DNS;

**Wildcard:** Enable / Disable;

**Mail Backup:** Enable / Disable;

**Offline Support:** Enable / Disable.

- 3- Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

# 10 Configuração RIP

Seu DSLink 260E pode ser configurado para comunicar-se com outros dispositivos de roteamento para determinar o melhor percurso para enviar os dados para seu destino pretendido. Este capítulo descreve como configurar seu DSLink 260E para usar um destes, denominado Routing Information Protocol (RIP).

A maioria das redes de pequeno porte em home offices ou escritórios não precisa usar o RIP. Então poderá querer configurar o RIP se qualquer uma das seguintes circunstâncias aplicar-se à sua rede:

- Sua rede inclui um roteador adicional ou PC ativado por RIP. O DSLink 260E e o roteador precisarão comunicar-se por meio do RIP para compartilhar suas tabelas de roteamento.
- Sua rede conecta-se por meio da linha ADSL a uma rede remota, como uma rede corporativa. Para que sua LAN possa detectar as rotas utilizadas dentro de sua rede corporativa, as duas devem ser configuradas com RIP.
- Seu ISP exige que seja executado o RIP para comunicação com dispositivos em sua rede.

## Configurando o RIP

1. Selecione **Services > RIP**. É exibida a página RIP Configuration:

RIP Configuration

Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used.

Enable  Disable

Age(seconds):

Update Time(seconds):

IF Name	Metric	Send Mode	Receive Mode	Action
ppp-0	1	RIP1	RIP1	<input type="button" value=""/>
eth-0	1	RIP1COMPAT	RIP1	<input type="button" value="Add"/>

2. Se necessário, altere **Age e Update Time**.

Estas são configurações globais para todas as interfaces que utilizarem o RIP.

- Age é a quantidade de tempo em segundos que a tabela RIP do dispositivo reterá cada rota que ela detectar nos computadores adjacentes.
- Update Time especifica com que freqüência o DSLink 260E enviará sua tabela de roteamento a seus vizinhos.

3. Na coluna **IFName**, selecione a interface sobre a qual deseja ativar o RIP.

Para comunicação com dispositivos ativados por RIP em sua LAN, selecione eth-0 ou o nome da interface Ethernet virtual apropriada.

Para comunicação com seu ISP ou uma LAN remota, selecione o ppp, eoa ou outra interface WAN correspondentes.

4. Selecione a valor métrico (contagem de saltos) para a interface . É possível selecionar qualquer número inteiro de 1 a 15.

5. Selecione um dos modos **Send** ou **Receive**.

A configuração de Send Mode indica a versão RIP que esta interface utilizará quando enviar informações sobre sua rota a outros dispositivos.

A configuração de Receive Mode indica a(s) versão(ões) RIP na(s) qual(is) as informações precisam ser passadas ao DSLink 260E para que possam ser aceitas em sua tabela de roteamento.

A versão 1 do RIP é o protocolo RIP original. Selecione RIP1 caso tenha dispositivos que se comuniquem com esta interface que só compreendam a versão 1 do RIP 1.

A versão 2 do RIP é a seleção preferida, pois ela oferece suporte para endereços IP “sem classe” (que são utilizados para a criação de sub-redes) e outros recursos. Selecione RIP2 se todos os outros dispositivos de roteamento existentes na rede autônoma oferecem suporte a esta versão do protocolo.

6. Clique em **Add**.

A nova entrada RIP será exibida na tabela.

7. Clique no botão de opção **Enable** para ativar o recurso RIP.

8. Quando acabar de definir as interfaces RIP, clique em **Submit**.

É exibida uma página para confirmar suas alterações.

9. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

---

## Visualizando Estatísticas do RIP

---

Para visualizar as estatísticas RIP, selecione **Services > RIP > Global Stats**:

RIP Global Statistics	
<b>RIP Active Sessions</b>	
<i>Request Sent:</i>	0 Packets
<i>Response Sent:</i>	0 Packets
<i>Request Received:</i>	0 Packets
RIP Packets w/ Error	
<i>Packets Received w/ Bad Version:</i>	0 Packets
<i>Packets Received w/ Bad Address Family:</i>	0 Packets
<i>Packets Received w/ Bad Request Format:</i>	0 Packets
<i>Packets Received w/ Bad Metrics:</i>	0 Packets
<i>Packets Received w/ Bad Response Format:</i>	0 Packets
<i>Packets Received w/ Invalid Port:</i>	0 Packets
<i>Packets Rejected:</i>	0 Packets
<i>Response Received:</i>	0 Packets
<i>Unknown Packets Received:</i>	0 Packets
<i>Packets Received from Non-Neighbor Router:</i>	0 Packets
<i>Packets Rejected for Authentication Failure:</i>	0 Packets
<i>Packets w/ Route Changed:</i>	0 Packets

Clear Close Refresh Help

# 11 Firewall, Filtros de IP, Filtro de Bridge e Bloqueio de Protocolos

## Configurando o Firewall

O Configuration Manager provê funções de firewall interno, permitindo que o sistema seja protegido contra ataques com negação de serviço (DoS, denial of service) e outros tipos de acessos maliciosos à sua LAN. É possível também especificar de que forma monitorar tentativas de ataques, e quem deve ser automaticamente notificado.

### Configurando Definições Globais de Firewall

1. Selecione **Services** > Firewall. É exibida a página Firewall Configuration.

Firewall Global Configuration	
<b>Blacklist Status:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Blacklist Period(min):</b>	<input type="text" value="10"/>
<b>Attack Protection:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>DOS Protection:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Max Half open TCP Conn.:</b>	<input type="text" value="25"/>
<b>Max ICMP Conn.:</b>	<input type="text" value="25"/>
<b>Max Single Host Conn.:</b>	<input type="text" value="75"/>
<b>Log Destination:</b>	<input type="checkbox"/> Email <input checked="" type="checkbox"/> Trace
<b>E-Mail ID of Admin 1:</b>	<input type="text"/>
<b>E-Mail ID of Admin 2:</b>	<input type="text"/>
<b>E-Mail ID of Admin 3:</b>	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Black List"/> <input type="button" value="Refresh"/> <input type="button" value="Help"/>	

2. Configure qualquer uma das seguintes definições:

Campo	Descrição
<i>Black List Status</i>	Caso queira que o dispositivo mantenha e utilize uma lista negra, clique em <i>Enable</i> . Clique em <i>Disable</i> se não quiser manter uma lista.
<i>Black List Period(min)</i>	Especifica o número de minutos que o endereço IP de um computador permanecerá na lista negra.

<b>Campo</b>	<b>Descrição</b>
<i>Attack Protection</i>	<p>Selecione <b>Enable</b> para utilizar as proteções do firewall interno que evitam os seguintes tipos comuns de ataques:</p> <ul style="list-style-type: none"> <li>○ IP Spoofing: Envio de pacotes pela interface WAN usando um endereço IP interno da LAN como o endereço de origem.</li> <li>○ Tear Drop: Envio de pacotes que contenham fragmentos sobrepostos.</li> <li>○ Smurf and Fraggle: Envio de pacotes que utilizam o endereço IP de difusão WAN ou LAN como o endereço de origem.</li> <li>○ Land Attack: Envio de pacotes que utilizam o mesmo endereço que o endereço de origem e de destino.</li> <li>○ Ping of Death: Comprimento ilegal de pacotes IP.</li> </ul>
<i>DoS Protection</i>	<p>Clique no botão de opção Enable para utilizar as seguintes proteções contra negação de serviço:</p> <ul style="list-style-type: none"> <li>○ SYN DoS</li> <li>○ ICMP DoS</li> <li>○ Proteção DoS por host</li> </ul>
<i>Max Half open TCP Connection</i>	<p>Define a porcentagem de sessões IP concorrentes que podem estar no estado de pendência (half-open state). Em comunicação TCP normal, os pacotes ficam no estado de pendência apenas um pequeno espaço de tempo enquanto uma conexão estiver sendo iniciada; o estado muda para active quando os pacotes estão sendo trocados, ou para closed quando o intercâmbio for concluído. Conexões TCP no estado de pendência podem esgotar as sessões IP disponíveis.</p> <p>Se a porcentagem for excedida, as sessões half-open serão fechadas e substituídas por novas sessões à medida que forem iniciadas.</p>
<i>Max ICMP Connection</i>	<p>Define a porcentagem de sessões IP concorrentes que podem ser utilizadas para mensagens ICMP.</p> <p>Se a porcentagem for excedida, as sessões IP ICMP mais antigas serão substituídas por novas sessões à medida que forem iniciadas.</p>
<i>Max Single Host Connection</i>	<p>Define a porcentagem da sessão IP concorrente que pode originar-se em um só computador. Esta porcentagem deve levar em conta o número de hosts da LAN.</p>

<b>Campo</b>	<b>Descrição</b>
<i>Log Destination</i>	Especifica de que forma as tentativas de violações das configurações de firewall serão rastreadas. Registros desses eventos podem ser enviados por meio de Ethernet a ser tratado por um utilitário Ethernet para ( <i>Trace</i> ) ou podem ser enviados por e-mail a administradores especificados.
<i>E-mail ID of Admin 1/2/3</i>	Especifica endereços de e-mail dos administradores que precisarem receber notificações de qualquer tentativa de violação do firewall. Digite os endereços no formato padrão Internet de e-mail, p.ex., <i>jxsmith@onecompany.com</i> .  A mensagem de e-mail conterá a hora da violação, o endereço de origem do computador responsável pela violação, o endereço IP de destino, o protocolo que estiver sendo utilizado, as portas de origem e de destino, e o número de violações que estiverem ocorrendo nos 30 minutos anteriores. Se estiver sendo utilizado o protocolo ICMP em vez das portas de origem e de destino, o e-mail informará o código e tipo de ICMP.

3. Clique em **Submit**.
4. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

## Configuração de IP Filter

O recurso IP Filter permite criar regras que controlem a transmissão de dados de entrada e de saída entre sua LAN e a Internet. Este capítulo explica como criar regras de filtros IP.

Visualizando sua configuração de IP Filter

Selecione **Services > IP Filter**. É exibida a página IP Filter:

**IP Filter Configuration**

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level:     Public Default Action:   
 Private Default Action:     DMZ Default Action:

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-		
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255		
30	Private	Enable	Incoming	Accept	N/A	Disable	-		
40	Private	Enable	Outgoing	Accept	ALL	Disable	-		
50	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq UDP 2.Dest Port equal to 53		

### Configurando Definições Globais de IP Filter

A página IP Filter Configuration permite configurar várias definições globais de IP Filter, e exibe uma tabela mostrando todas as regras de filtros IP existentes. As definições globais que podem ser configuradas são:

- **Security Level:** Quando High estiver selecionado, somente as regras às quais foi atribuído um valor de segurança de High estarão em vigor. O mesmo é verdade para as definições Medium e Low. Quando None estiver selecionado, IP Filtering fica desativado.
- **Private/Public/DMZ Default Action:** Esta definição especifica uma ação padrão a ser executada (Accept ou Deny) em interfaces do dispositivo privadas, públicas ou do tipo DMZ quando elas recebem pacotes que não correspondam a qualquer das regras de filtragem.
  - Public – A interface conecta-se à Internet. p.ex., interfaces PPP, EoA e IPoA. Normalmente, a definição global para interfaces públicas é *Deny*, para que todos os acessos à sua LAN iniciados em computadores externos sejam negados (descartados na interface pública), exceto para aqueles permitidos por uma regra IP Filter específica.
  - Private – Normalmente, a definição global para interfaces privadas é **Accept**, para que os computadores da LAN tenham acesso à conexão Internet dos roteadores ADSL/Ethernet.
  - DMZ – Refere-se a computadores que estão disponíveis para acessos tanto públicos quanto na rede (como um servidor Web público de uma empresa). Os pacotes recebidos em uma interface DMZ— seja de uma LAN ou origem externa—estão sujeitos a um conjunto de proteções que fica entre interfaces públicas e privadas. A definição global para Interfaces do tipo DMZ pode ser configurada como **Deny** para que todas as tentativas de acessar estes servidores sejam negadas por padrão; o administrador poderá, então, configurar regras de filtros IP para permitir acessos de determinados tipos.

## Criando Regras de Filtros de IP

1. Na página IP Filter principal, clique em **Add**. É exibida a página IP Filter Rule – Add:

**DSLink**

IP Filter Rule - Add

Enable    Disable

Basic Information			
<b>Rule ID:</b>	<input type="text"/>	<b>Action:</b>	<input type="radio"/> Accept <input checked="" type="radio"/> Deny
<b>Direction:</b>	<input type="radio"/> Incoming <input checked="" type="radio"/> Outgoing	<b>Interface:</b>	<input type="text" value="ALL"/>
<b>In Interface:</b>	<input type="text" value="ALL"/>	<b>Log Option:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Security Level:</b>	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low	<b>Blacklist Status:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Log Tag:</b>	<input type="text"/>		
<b>Start Time (HH MM SS):</b>	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>	<b>End Time (HH MM SS):</b>	<input type="text" value="23"/> <input type="text" value="59"/> <input type="text" value="59"/>
<b>Src IP Address:</b>	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
<b>Dest IP Address:</b>	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
<b>Protocol:</b>	<input type="text" value="any"/> <input type="text" value="TCP"/>		
<b>Apply Stateful Inspection:</b>	<input type="checkbox"/>		
<b>Source Port:</b>	<input type="text" value="any"/>	<input type="text" value="Any other port"/> <input type="text" value="0"/>	<input type="text" value="Any other port"/> <input type="text" value="0"/>
<b>Dest Port:</b>	<input type="text" value="any"/>	<input type="text" value="Any other port"/> <input type="text" value="0"/>	<input type="text" value="Any other port"/> <input type="text" value="0"/>
<b>TCP Flag:</b>	<input type="text" value="All"/>		
<b>ICMP Type:</b>	<input type="text" value="any"/> <input type="text" value="Echo Reply"/>		
<b>ICMP Code:</b>	<input type="text" value="any"/> <input type="text" value="0"/>		
<b>IP Frag Pkt:</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore	<b>IP Option Pkt:</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore
<b>Packet Size:</b>	<input type="text" value="any"/> <input type="text" value="0"/>		
<b>TOD Rule Status:</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		

2. Insira ou selecione os dados para cada campo que se aplicar à sua regra:

<b>Campo</b>	<b>Descrição</b>
<i>Rule ID</i>	As regras são processadas da mais baixa para a mais alta em cada pacote de dados, até ser encontrada uma correspondência. É recomendável atribuir identificações de regras em múltiplos de 5 ou 10 (p.ex., 10, 20, 30) para deixar espaço suficiente entre elas para inserir uma nova regra se necessário.
<i>Action</i>	A ação pode ser <i>Accept</i> (enviar para o destino) ou <i>Deny</i> (descartar o pacote).
<i>Direction</i>	<i>Incoming</i> refere-se a pacotes chegando da LAN, e <i>outgoing</i> refere-se a pacotes indo para a Internet.
<i>Interface</i>	A interface sobre a qual a regra vigorará.
<i>In Interface</i>	A interface da qual os pacotes devem ter sido enviados à interface especificada na seleção anterior. Esta opção só é válida para a direção de saída.
<i>Log Option</i>	Quando <b>Enabled</b> estiver selecionado, uma entrada de log será criada no sistema cada vez que esta regra for chamada.
<i>Security Level</i>	O nível de segurança que deve ser ativado globalmente para que esta regra passe a vigorar. A regra só ficará ativa se seu nível de segurança for o mesmo da definição globalmente configurada (mostrado na página principal de IP Filter). Por exemplo, se a regra for definida como Medium e o nível de firewall global for definido como Medium, a regra ficará ativa; mas se o nível de firewall global for definido como High ou Low, a regra ficará inativa.
<i>Black List Status</i>	Especifica se ou a violação desta regra resultará ou não na inclusão na Lista negra do endereço IP do computador transgressor, que impede que o roteador envie pacotes provenientes daquela origem por período de tempo especificado.
<i>Log Tag</i>	Uma descrição de até 16 caracteres a ser registrada no log caso um pacote viole esta regra. Certifique-se de definir Log Option como <i>Enable</i> caso seja configurado um Log Tag.

<b>Campo</b>	<b>Descrição</b>
<i>Start/End Time</i>	O intervalo de tempo durante o qual esta regra vigorará, especificado em unidades de uso militar.
<i>Src IP Address</i>	<p>Crítérios de endereço IP para o(s) computador(es) de origem do(s) qual(is) o pacote origina-se. Use a expressão abaixo para especificar o IP:</p> <p><b>any:</b> qualquer endereço IP de origem.</p> <p><b>lt:</b> <i>menor que</i></p> <p><b>lteq:</b> <i>menor ou igual a.</i></p> <p><b>gt:</b> <i>maior que</i></p> <p><b>eq:</b> <i>igual a</i></p> <p><b>neq:</b> <i>diferente de</i></p> <p><b>range:</b> dentro da faixa especificada, inclusive.</p> <p><b>out of range:</b> fora da faixa especificada.</p> <p><b>self:</b> o endereço IP da interface do roteador sobre a qual esta regra entra em vigor.</p>
<i>Dest IP Address</i>	<p>Os critérios da regra do endereço IP para o(s) computador(s) de destino (ou seja, o endereço IP do computador ao(s) qual(is) o pacote está sendo enviado).</p> <p>Além das opções descritas relativas ao campo Src IP Address, a seguinte opção está disponível:</p> <p><b>bcast:</b> Especifica que a regra será chamada para qualquer pacote enviado ao endereço de difusão da interface de recepção. (O endereço de difusão é utilizado para enviar pacotes a todos os existentes na LAN ou sub-rede conectada à interface especificada.) Quando seleciona esta opção, não é preciso especificar o endereço, e assim os campos de endereço ficam cinza (indisponíveis para entrada).</p>

<b>Campo</b>	<b>Descrição</b>
<i>Protocol</i>	Os critérios básicos do protocolo IP que devem ser satisfeitos para a regra a ser chamada. Usando as opções apresentadas na lista suspensa, é possível especificar se os pacotes devem conter o protocolo selecionado ( <i>eq</i> ), se eles não devem conter o protocolo especificado ( <i>neq</i> ), ou se a regra pode ser chamada independentemente do protocolo ( <i>any</i> ). TCP, UDP e ICMP são protocolos IP normalmente utilizados; outros podem ser identificados numericamente de 0 a 255, conforme definido pela IANA.
<i>Apply Stateful Inspection</i>	Se esta opção estiver ativada, <i>stateful filtering</i> é executado e a regra é aplicada também na outra direção na interface fornecida durante uma sessão IP.
<i>Source Port</i>	<p>Critérios do número de porta do(s) computador(es) a partir do(s) qual(is) o pacote é originado.</p> <p>Este campo ficará cinza (indisponível para entrada) caso não tenha especificado um critério do protocolo.</p> <p>Ver a descrição de Src IP Address para opções de seleção.</p>
<i>Dest Port</i>	<p>Critérios do número de porta para o(s) computador(s) de destino (ou seja, o número de porta do tipo de computador ao qual o pacote está sendo enviado).</p> <p>Este campo ficará cinza (indisponível para entrada) a menos que tenha sido selecionado TCP ou UDP como o protocolo.</p> <p>Ver a descrição de Src IP Address para opções de seleção.</p>
<i>TCP Flag</i>	Especifica se a regra deve aplicar-se apenas a pacotes TCP que contenham o sinalizador síncrono ( <i>SYN</i> ), apenas para aqueles que contenham o sinalizador não-síncrono ( <i>NOT-SYNC</i> ), ou a todos os pacotes TCP. Este campo ficará cinza (indisponível para entrada) a menos que tenha sido selecionado TCP como o protocolo.

---

<b>Campo</b>	<b>Descrição</b>
<i>ICMP Type</i>	Especifica se o valor no campo type dos cabeçalhos do pacote ICMP será utilizado como um critério. O valor do código pode ser qualquer valor decimal de 0 a 255. Então pode especificar se o valor deve ser igual ( <i>eq</i> ) ou diferente ( <i>neq</i> ) do valor especificado, ou pode selecionar <i>any</i> para ativar a regra a ser chamada sobre todos os pacotes ICMP. Este campo ficará cinza (indisponível para entrada), a menos que seja especificado ICMP como o protocolo.
<i>ICMP Code</i>	Especifica se o valor no campo code nos cabeçalhos do pacote ICMP será utilizado como um critério. O valor do código pode ser qualquer valor decimal de 0 a 255. É possível especificar se o valor deve ser igual ( <i>eq</i> ) ou diferente ( <i>neq</i> ) do valor especificado, ou pode ser selecionado <i>any</i> para ativar a regra a ser chamada sobre todos os pacotes ICMP. Este campo ficará cinza (indisponível para entrada) a menos que seja especificado ICMP como o protocolo.
<i>IP Frag Pkt</i>	Determina de que forma a regra se aplica a pacotes IP que contenham fragmentos. É possível escolher entre as seguintes opções: <ul style="list-style-type: none"><li>○ <b>Yes:</b> A regra será aplicada somente a pacotes que contenham fragmentos.</li><li>○ <b>No:</b> A regra será aplicada somente a pacotes que não contenham fragmentos.</li><li>○ <b>Ignore:</b> (Padrão) A regra será aplicada a pacotes que contenham ou não fragmentos, pressupondo-se que elas correspondam aos outros critérios.</li></ul>

---

<b>Campo</b>	<b>Descrição</b>
<i>IP Option Pkt</i>	<p>Determina se a regra deve aplicar-se a pacotes IP que tenham opções especificadas em seu cabeçalho de pacotes.</p> <ul style="list-style-type: none"> <li>○ <b>Yes:</b> A regra será aplicada somente a pacotes que contenham opções de cabeçalho.</li> <li>○ <b>No:</b> A regra será aplicada somente a pacotes que não contenham opções de cabeçalho.</li> <li>○ <b>Ignore:</b> (Padrão) A regra será aplicada a pacotes que contenham opções de cabeçalho, pressupondo-se que elas correspondam aos outros.</li> </ul>
<i>Packet Size</i>	<p>Especifica que a regra IP Filter só vigorará em pacotes cujo tamanho em bytes corresponda a estes critérios. (<i>lt</i> = menor que, <i>gt</i> = maior que, <i>lteq</i> = menor ou igual a, etc.)</p>
<i>TOD Rule Status</i>	<p>Time of Day Rule Status determina de que forma as definições de Start Time/End Time são utilizadas.</p> <ul style="list-style-type: none"> <li>○ <b>Enable:</b> (Padrão) A regra está em vigor para o período de tempo especificado.</li> <li>○ <b>Disable:</b> A regra não está em vigor para o período de tempo especificado, mas está em vigor para todos os outros períodos de tempo.</li> </ul>

3. Quando tiver acabado de selecionar os critérios, certifique-se de que **Enable** esteja selecionado e, em seguida, clique em **Submit**.

Se o nível de segurança da regra corresponder à definição globalmente configurada, será exibida uma esfera verde na coluna Status referente a essa regra, indicando que a regra agora está em vigor. Uma esfera vermelha será exibida quando a regra estiver desativada ou se seu nível de segurança for diferente do nível globalmente configurado.

4. Certifique-se de que as definições Security Level e Private/Public/DMZ Default Action na página IP Filter Configuration página estejam configuradas conforme o necessário e, em seguida, clique em **Submit**.

É exibida uma página para confirmar suas alterações.

5. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

## Exemplos de regra filter de IP

**Exemplo 1.** Impedindo que um computador específico em sua LAN utilize servidores web na Internet:

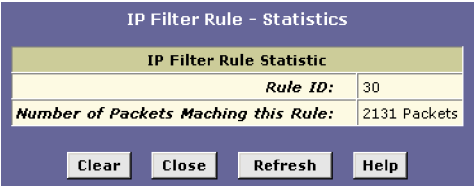
1. Adicione uma nova regra para pacotes de saída na interface ppp-0 a partir de qualquer interface de entrada.
2. Especifique um endereço IP de origem do computador que queira bloquear.
3. Especifique o protocolo = *TCP* e ative a definição de Store State.
4. Especifique a porta de destino = *80*, que é número de porta bem conhecido para servidores web.
5. Ative a regra clicando no botão de opção no topo da página.
6. Clique em **Submit** para criar a regra.
7. Na página IP Filter Configuration, defina Security Level como o mesmo nível que foi escolhido para a regra e defina tanto Private Default Action quanto Public Default Action como *Accept*.
8. Clique em **Submit** e efetive suas alterações.

**Exemplo 2.** Bloqueando acessos Telnet ao dispositivo:

1. Adicione uma nova regra para pacotes de entrada na interface ppp-0.
2. Especifique que o pacote deve conter o protocolo TCP e deve ser destinado à porta 23, o número de porta bem conhecido utilizado para o protocolo Telnet.
3. Ative a regra clicando no botão de opção no topo da página.
4. Clique em **Submit** para criar a regra e efetive suas alterações.

## Visualizando Estatísticas de Filtros de IP

Para visualizar estatísticas sobre a forma pela qual os pacotes foram aceitas ou negadas para a regra, selecione **Services > IP Filter > Stats** na linha correspondente a uma regra:



IP Filter Rule - Statistics	
IP Filter Rule Statistic	
<i>Rule ID:</i>	30
<i>Number of Packets Matching this Rule:</i>	2131 Packets

Clear Close Refresh Help

## Gerenciando Sessões Atuais de Filtros IP

Para visualizar todas as sessões IP atuais, selecione **Services > IP Filter > Session** para exibir a página IP Filters Session:

IP Filter Session										
Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
13	60	TCP	eth-0 Self	192.168.1.3 192.168.1.1	1164 80	30 0	Accept Unknown	30 0	Accept Unknown	
14	5	UDP	eth-0 Self	192.168.1.3 192.168.1.1	1163 53	30 0	Accept Unknown	30 0	Accept Unknown	
18	20	TCP	eth-0 Self	192.168.1.3 192.168.1.1	1160 80	30 0	Accept Unknown	30 0	Accept Unknown	
19	20	TCP	eth-0 Self	192.168.1.3 192.168.1.1	1161 80	30 0	Accept Unknown	30 0	Accept Unknown	

A tabela IP Filter Session exibe os seguintes campos:

Campo	Descrição
<i>Session Index</i>	A identificação atribuída pelo sistema à sessão IP (a todas as sessões, sejam elas afetadas ou não por uma regra filter de IP, é atribuído um índice de sessão).
<i>Time to expire</i>	O número de segundos no qual a conexão expirará automaticamente
<i>Protocol</i>	O protocolo IP subjacente utilizado na conexão, como TCP, UDP, IGMP, etc.
<i>I/F</i>	A interface sobre a qual a regra IP Filter está em vigor
<i>IP Address</i>	Os endereços IP envolvidos na comunicação. O primeiro mostrado é o iniciador da comunicação.
<i>Port</i>	Os endereços de hardware das portas envolvidas na comunicação
<i>In/Out Rule Index</i>	O número da regra IP Filter que é aplicada a esta sessão (atribuído quando a regra foi criada)
<i>In/Out Action</i>	A ação (aceitar, negar ou desconhecido), que estiver sendo executada sobre os dados que entram ou que saem da interface. Esta ação é especificada na definição da regra.

## Configuração de Bridge Filter

O recurso Bridge Filter permite criar regras que controlem a transmissão de dados de entrada e de saída entre sua LAN e a Internet. Este capítulo explica como criar regras de filtros Bridge.

Visualizando sua configuração de Bridge Filter

Selecione **Services > Bridge Filter**. É exibida a página Bridge Filter:

**Bridge Filter Configuration**

This page is used to view, add and modify raw packet filter rules, and subrules.

Enable     Disable  
 Default Action: Accept

Rule ID	Subrule ID	I/F	In I/F	Direction	Rule Action	Log Option	Oper. Status	Action(s)
15		Private	-	In	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864						
16		Private	ALL	Out	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864						
17		Private	-	In	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	4 bytes with mask 0xFFFFFFFF at offset 16 bytes from IP Header lies between 0xE0000000 and 0xEFFFFFFF						
18		Private	ALL	Out	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	4 bytes with mask 0xFFFFFFFF at offset 16 bytes from IP Header lies between 0xE0000000 and 0xEFFFFFFF						
19		Private	-	In	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 0 bytes from Link Header is equal to 0x3333						
32		Private	ALL	Out	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 0 bytes from Link Header is equal to 0x3333						
33		Private	-	In	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 12 bytes from Link Header is equal to 0x8100						
34		Private	ALL	Out	Deny	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 12 bytes from Link Header is equal to 0x8100						
35		Private	-	In	CallMgmt	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864						
36		DMZ	-	In	CallMgmt	Disable	<span style="color: red;">●</span>	<a href="#">Stats</a>
	1	2 bytes with mask 0xFFFF at offset 12 bytes from Link Header lies between 0x8863 and 0x8864						

### Configurando Definições Globais de Bridge Filter

A página Bridge Filter Configuration permite configurar definições globais de Bridge Filter, e exibe uma tabela mostrando todas as regras de filtros Bridge existentes. As definições globais que podem ser configuradas são:

- **Enable/Disable:** habilita ou não os filtros bridge já configurados.
- **Default Action:** Esta definição especifica uma ação padrão a ser executada (Accept, Deny ou CallMgmt)

## Criando Regras de Filtros Bridge

1. Na página Bridge Filter principal, clique em **Add**. É exibida a página Bridge Filter Rule – Add:

2. Insira ou selecione os dados para cada campo que se aplicar à sua regra:

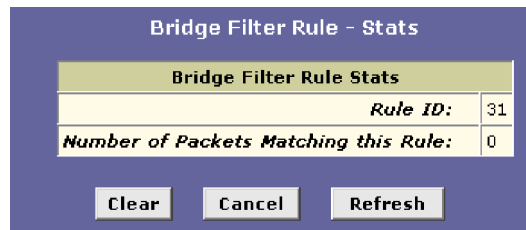
Campo	Descrição
<i>Rule ID</i>	As regras são processadas da mais baixa para a mais alta em cada pacote de dados, até ser encontrada uma correspondência. É recomendável atribuir identificações de regras em múltiplos de 5 ou 10 (p.ex., 10, 20, 30) para deixar espaço suficiente entre elas para inserir uma nova regra se necessário.
<i>Action</i>	A ação pode ser <i>Accept</i> (enviar para o destino) ou <i>Deny</i> (descartar o pacote).
<i>Direction</i>	<i>Incoming</i> refere-se a pacotes chegando da LAN, e <i>outgoing</i> refere-se a pacotes indo para a Internet.
<i>Interface</i>	A interface sobre a qual a regra vigorará.
<i>In Interface</i>	A interface da qual os pacotes devem ter sido enviados à interface especificada na seleção anterior. Esta opção só é válida para a direção de saída.
<i>Log Option</i>	Quando <b>Enabled</b> estiver selecionado, uma entrada de log será criada no sistema cada vez que esta regra for chamada.

3. Quando tiver acabado de selecionar os critérios, certifique-se de que **Enable** esteja selecionado e, em seguida, clique em **Submit**.

4. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Visualizando Estatísticas de Filtros Bridge

Para visualizar estatísticas sobre a forma pela qual os pacotes foram aceitas ou negadas para a regra, selecione **Services > Bridge Filter > Stats** na linha correspondente a uma regra:



Bridge Filter Rule Stats	
<b>Rule ID:</b>	31
<b>Number of Packets Matching this Rule:</b>	0

Clear Cancel Refresh

### Para bloquear protocolos específicos

---

O recurso Protocolos bloqueados evita que o roteador ADSL/Ethernet passe quaisquer dados que utilizem um protocolo específico. Ao contrário do recurso IP Filter recurso, é impossível especificar critérios adicionais para protocolos bloqueados, como usuários ou destinos específicos.

O bloqueio de determinados protocolos pode interromper ou desativar sua comunicação em rede ou acesso à Internet. Use este recurso a menos que tenha certeza de que um protocolo específico não é necessário nem desejado em sua rede.

Para bloquear protocolos específicos que estejam sendo executados sobre o sistema, selecione **Services > Blocked Protocols**. Marque o tipo de protocolo que deseja bloquear e clique em **Submit**. Certifique-se de utilizar o recurso de efetivação para salvar suas alterações na memória permanente.

Para desbloquear o protocolo específico, desmarque o protocolo e repita a tarefa de envio e efetivação.

**Blocked Protocols**

This page is used to Block/UnBlock the protocols running across the system.

Protocol	Blocked
PPPoE	<input type="checkbox"/>
IP Multicast	<input type="checkbox"/>
RARP	<input type="checkbox"/>
AppleTalk	<input type="checkbox"/>
NetBEUI	<input type="checkbox"/>
IPX	<input type="checkbox"/>
BPDU	<input type="checkbox"/>
ARP	<input type="checkbox"/>
IPV6 Multicast	<input type="checkbox"/>
802.1.Q	<input type="checkbox"/>

# 12 Tarefas de Administração

## Alterando a data e hora do sistema

---

O dispositivo mantém um registro da data e hora atuais, que são utilizadas para calcular e informar vários dados de desempenho. Pode ser selecionado **Home > Modify** para alterar a data e hora conforme o necessário. Você pode também especificar o nome do servidor e nome do domínio nos campos fornecidos.

System - Modify

**System Parameters**

**SNTP:**  Enable  Disable

**Date:**  Jan 1 2003

**Time:**  7 : 33 : 59

**Time Zone:** BRST -0300 Brazil Standard

**Daylight Saving Time:**  ON  OFF

**Name:**

**Domain Name:**

Submit Cancel Help

## Adicionando um usuário/Alterando sua senha de logon

---

A primeira vez que efetua logon no Configuration Manager, é usada a identificação do usuário e a senha padrão (*root* e *root*). O sistema permite dois níveis de privilégios: Root e User. O privilégio Root permite que você mude e efetive a configuração do DSLink 260E, enquanto o privilégio User permite apenas a leitura.

Para adicionar um usuário, ou mudar a senha de logon:

1. Selecione **Admin > User Config**. É exibida a página User Configuration:

User Configuration

This page displays user information. Use this page to add/delete users and change your password. Your new password can be up to 64 characters and is case-sensitive.

User ID	Privilege	Action(s)
root	Root	

Add Refresh Help

Para modificar a senha de logon, clique o ícone de alteração na coluna Actions(s) e então mude a senha atual

Para adicionar um novo usuário, clique em **Add** para mostrar a página **User Config-Add**. Então digite sua configuração nos campos fornecidos

Note que tanto a identificação do usuário como a senha levam em consideração se os caracteres são maiúsculos ou minúsculos.

2. Depois de fazer as mudanças, clique em **Submit**..
3. Selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

## Atualização da imagem

Esta opção permite atualizar o dispositivo para um novo firmware. Após a atualização, sua configuração personalizada ainda existirá e não será reinicializada aos padrões de fábrica. Para executar a tarefa de atualização, faça download do arquivo de firmware necessário para seu PC host e siga os passos abaixo:

1. Clique em **Admin > Local Image Upgrade > Browse** para localizar o arquivo de firmware.

O nome do arquivo de atualização deve ser um dos seguintes:

TEImage.bin  
 TEDsl.gsz  
 TEAppl.gsz  
 Filesys.bin  
 TEPatch.bin

2. Clique no botão **Upload** para iniciar a atualização. Depois de alguns segundos, uma mensagem como a seguinte deve aparecer (o nome do arquivo pode ser diferente):

File: TEDsl.gsz successfully saved to the flash. Please reboot for the new image to take effect.

3. Desligue a unidade, espere alguns segundos e ligue-a de novo para ativar o novo software



**Nota**

Não interrompa o processo de atualização, pois seu roteador poderá ser danificado.

**Image Upgrade**

This page is used to upload a new image to the system.

**Upgrade File:**

## Diagnósticos

Para executar diagnósticos em um ATM VC específico, selecione **Admin > Diagnostics**. Selecione o VC sobre o qual deseja executar diagnósticos e, em seguida, clique em **Submit**. O resultado do diagnóstico será exibido nesta página. Observe que apenas os VCs definidos no sistema aparecerão na lista suspensa.

**Diagnostics**

This page is used for performing diagnostics on the system.

**WAN Interface:**

Testing Connectivity to modem		
Testing Ethernet connection	UNKNOWN	<a href="#">Help</a>
Testing ADSL line for sync	UNKNOWN	<a href="#">Help</a>
Testing Ethernet connection to ATM	UNKNOWN	<a href="#">Help</a>
Testing Telco Connectivity		
Testing ATM OAM segment ping	UNKNOWN	<a href="#">Help</a>
Testing ATM OAM end to end ping	UNKNOWN	<a href="#">Help</a>
Testing ISP Connectivity		
Testing PPPoE server connectivity	UNKNOWN	<a href="#">Help</a>
Testing PPPoE server session	UNKNOWN	<a href="#">Help</a>
Testing authentication with server	UNKNOWN	<a href="#">Help</a>
Validating assigned IP address 0.0.0.0	UNKNOWN	<a href="#">Help</a>
Testing Internet Connectivity		
Ping default gateway 0.0.0.0	UNKNOWN	<a href="#">Help</a>
Ping Primary Domain Name Server	UNKNOWN	<a href="#">Help</a>
Query DNS for www.globespanvirata.com	UNKNOWN	<a href="#">Help</a>
Ping www.globespanvirata.com	UNKNOWN	<a href="#">Help</a>

## Configurações de portas

O serviço HTTP (Web Configuration Utility) e serviço Telnet do roteador são acessíveis com uso dos números de porta padrão 80 e 23, respectivamente. É possível que queira designar um servidor HTTP ou servidor Telnet publicamente acessível no lado de sua LAN e queira mudar do roteador HTTP/serviço Telnet para utilizar um número de porta não-padrão. Se este for o caso, selecione **Admin > Port Settings** para modificar as configurações de portas HTTP/Telnet e clique em **Submit**. Em seguida, selecione **Admin > Commit & Reboot** e clique em **Commit** para salvar suas alterações no armazenamento permanente.

Observe que se foi definido o servidor HTTP/Telnet incorporado do roteador para usar o número de porta não-padrão, quando acessar o servidor HTTP/Telnet a partir do mundo externo, o endereço IP deve ser seguido de ponto-e-vírgula e do número de porta não-padrão, conforme mostrado neste exemplo a seguir para um servidor HTTP (ou seja, o Gerenciador baseado na Web):

**http://10.0.1.16:61000**

onde **10.0.1.16** é o endereço IP da WAN do roteador e **61000** é o número de porta não-padrão que foi especificado na página Port Settings.

## Visualização dos alarmes do sistema

Para exibir a página Alarm, **Admin > Alarm**:

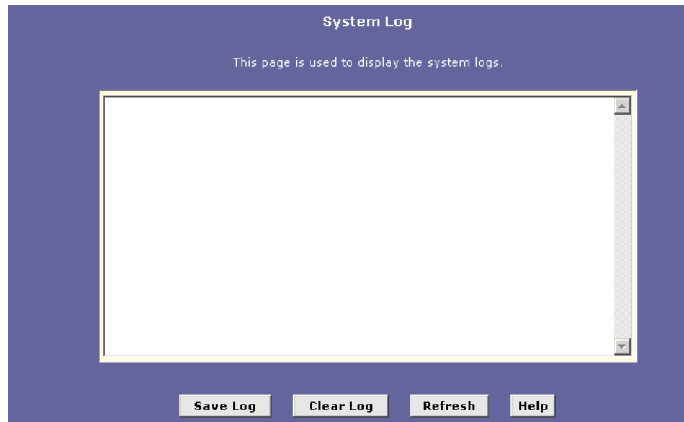
Cada linha da tabela exibe a hora e data em que ocorreu um alarme, o tipo de alarme e uma breve declaração indicando esta causa.

Então pode clicar na lista suspensa **Refresh Rate** para selecionar um intervalo de tempo recorrente após o qual a página será reexibida com novos dados.

## Sistema de Log

---

Para exibir a página System Log, **Admin > System Log**:

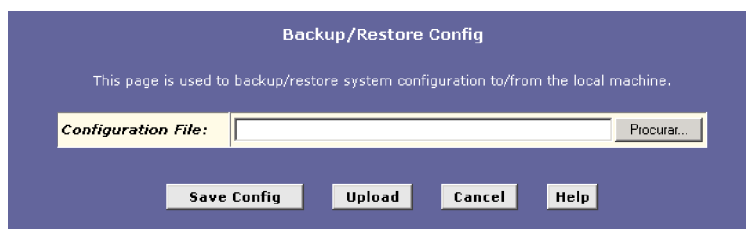


A tela exibe o log gerado, clique no botão **Save Log** para salvar ou **Clear Log** para apagar o log.

## Backup / Restore da Configuração

---

Para exibir a página Backup / Restore, **Admin > Backup / Restore**:



Para salvar a configuração do DSLink 260E, clique em **Save Config** e escolha o local que deseja salvar a configuração. Para restaurar a configuração do DSLink 260E, procure o arquivo committedcfg em **Configuration File** e clique em **Upload**.

## Autodetect

Para exibir a página Autodetect, **Admin > Autodetect**:

Escolha a interface em **Autodetect Mode** e clique em **Submit**. A tabela exibe o VPI, VCI e o Protocolo detectado.

## Configuração SNMP

- 1) Selecione **Admin > SNMP Config**;

- 2) **SNMP Trap** enable/disable
- 3) **Community Name** – nome da comunidade
- 4) **Access** – Read Only permissão para leitura ou Read Write permissão para leitura e escrita.
- 5) Clique em **Add Host**, adicione o endereço IP do servidor de gerencia em **Host Address** e clique em **Submit**.

- 6) Selecione **Admin > Commit & Reboot** e clique em **Commit** para armazenar suas alterações na memória permanente.

# 13 Visualização dos parâmetros DSL

Para visualizar os parâmetros de configuração e estatísticas de desempenho da linha DSL do DSLink 260E, selecione **WAN**. É exibida a página DSL Status:

DSL Status

This page displays DSL Status Information

Refresh Rate: 10 Seconds

Counters	Local		Remote	
	Intrvl	Fast	Intrvl	Fast
FEC:	0	0	0	0
CRC:	0	0	0	0
MCD:	0	0	0	0
OGD:	0	0	-	-
HEC:	0	0	0	0
SEF:	0	0	0	0
LOS:	0	0	0	0

DSL Status

Operational Status: Startup Handshake

Last Failed Status: Dx0

Startup Progress: DxA0

Failures	Local	Remote
MCD:	0	0
SEF:	0	0
LOS:	0	0
LCD:	0	0

Clear DSL Param Stats Refresh Help

A página DSL Status exibe as informações atuais sobre o desempenho da linha DSL. A página atualiza-se a cada 10 segundos.

Então pode clicar em **DSL Param** para exibir dados sobre a configuração da linha DSL, conforme mostrado abaixo.

DSL Parameter

DSL Parameters and Status

Vendor ID: 00B5GSPN

Revision Number: T93.3.19

Serial Number: 123456789abcdx

Local Tx Power: 0.0 dB

Remote Tx Power: 0.0 dB

Local Line Atten.: 0.5 dB

Remote Line Atten.: 0.5 dB

Local SNR Margin: 0.0 dB

Remote SNR Margin: 0.0 dB

Self Test: Passed

DSL Standard: T1.413

Trellis Coding: Disable

Framing Structure: Framing-0

Config Data	Up		Down	
	Intrvl	Fast	Intrvl	Fast
AS0(kbps):	-	-	0	0
AS1(kbps):	-	-	0	0
LS0(kbps):	0	0	-	-
LS1(kbps):	0	0	-	-
RValue:	0	0	0	0
SValue:	0	0	0	0
DValue:	0	0	0	0

Close Refresh Help

Na página DSL Status, então pode clicar em **Stats** para exibir as estatísticas de desempenho da linha DSL:

DSL Statistics					
<i>No. of 15 Min. Valid Data Intervals:</i>	1				
<i>No. of 15 Min. Invalid Data Intervals:</i>	0				
Current 15-Min Interval Statistics					
<i>Elapsed Time(MM:SS):</i>	0:9				
<i>Errored Seconds:</i>	0				
<i>Severely Errored Seconds:</i>	0				
<i>Unavailable Seconds:</i>	0				
Current Day Statistics					
<i>Elapsed Time(HH:MM:SS):</i>	0:15:9				
<i>Errored Seconds:</i>	1				
<i>Severely Errored Seconds:</i>	0				
<i>Unavailable Seconds:</i>	0				
Previous Day Statistics					
<i>Monitored Time(HH:MM:SS):</i>	0:0:0				
<i>Errored Seconds:</i>	0				
<i>Severely Errored Seconds:</i>	0				
<i>Unavailable Seconds:</i>	0				
Detailed Interval Statistic (Past 24 hrs)					
<a href="#">1-4</a>	<a href="#">5-8</a>	<a href="#">9-12</a>	<a href="#">13-16</a>	<a href="#">17-20</a>	<a href="#">21-24</a>
<div style="text-align: center;"> <input type="button" value="Close"/> <input type="button" value="Refresh"/> <input type="button" value="Help"/> </div>					

A página DSL Statistics informa os dados de erro relativos ao último intervalo de 15 minutos, ao dia atual e ao dia anterior.

Na parte inferior da página, a tabela **Detailed Interval Statistic** exibe links nos quais então pode clicar para exibir dados detalhados para cada intervalo de 15 minutos nas últimas 24 horas. Por exemplo, ao clicar em 1-4, são exibidos os dados relativos a tais intervalos de 15 minutos que formam as 4 horas anteriores (há 16 destes) mostra uma destas páginas.

# 14 Solução de problemas

Este apêndice sugere soluções para problemas com os quais é possível se deparar na instalação ou durante o uso de seu DSLink 260E e fornece instruções para o uso de vários utilitários IP para diagnosticar problemas.

Entre em contato com o Suporte ao Cliente se estas sugestões não solucionarem o problema.

<b>Problema</b>	<b>Sugestão de solução de problemas</b>
<b>LEDs</b>	
<i>O LED PWR não se acende após o produto ser ligado.</i>	Verifique se está sendo utilizada a fonte fornecida com o dispositivo e se ela está firmemente conectada ao DSLink 260E e a uma tomada/régua de alimentação.
<i>O LED DSL não se acende após o cabo telefônico ser conectado.</i>	Verifique se um cabo telefônico padrão está firmemente conectado à porta ADSL e à sua tomada telefônica. Aguarde 30 segundos para permitir que o dispositivo negocie uma conexão com seu ISP.
<i>O LED LAN não se acende após o cabo Ethernet ser conectado.</i>	Verifique se o cabo Ethernet está firmemente conectado ao hub ou PC de sua LAN e ao DSLink 260E. Certifique-se de que o PC e/ou o hub estejam ligados.  Verifique se está sendo utilizado o cabo correto. Veja "Conectando o Hardware" para obter mais informações.
<i>O LED ALM permanece aceso após o dispositivo ser ligado.</i>	O LED DIAG deve apagar-se após cerca de 10 a 15 segundos. Se ele não se apagar, desligue o DSLink 260E, aguarde 10 segundos e, em seguida, ligue-o novamente.
<b>Acesso à Internet</b>	
<i>O PC não consegue ter acesso à Internet</i>	Use o utilitário ping para verificar se seu PC pode comunicar-se com o Endereço IP da LAN do DSLink 260E (por padrão 192.168.1.1). Caso ele não consiga, verifique o cabeamento Ethernet.  Caso tenha atribuído estaticamente um endereço IP privado ao computador, (e não um endereço público registrado), verifique o seguinte:  Verifique se o endereço IP de gateway no computador é seu endereço IP público. Se não for, corrija o endereço ou configure o PC para receber informações de IP automaticamente.  Verifique com seu ISP se o servidor DNS especificado para o PC é válido. Corrija o endereço ou configure o PC para receber estas informações automaticamente.  Verifique se a regra NAT foi definida no DSLink 260E para converter o endereço privado em seu endereço IP público.
<i>Os PCs não conseguem exibir páginas da Web na Internet.</i>	Verifique se o servidor DNS especificado nos PCs é o correto para seu ISP. Pode ser usado o utilitário ping para testar a conectividade com o servidor DNS de seu ISP.

Problema	Sugestão de solução de problemas
<b>Programa Configuration Manager</b>	
<i>Se esqueceu/perdeu sua identificação do usuário ou senha do Configuration Manager .</i>	<p>Pode ser reiniciado o dispositivo para a configuração padrão pressionando o botão <b>Reset</b> 3 vezes no painel traseiro do dispositivo (usando um objeto com ponta como, por exemplo, um clipe para papéis).Em seguida, digite a identificação do usuário e senha padrão root/root.</p> <p><b>ADVERTÊNCIA:</b> A reinicialização do dispositivo remove qualquer configuração personalizada e devolve todas as configurações para seus valores padrão.</p>
<i>Impossível acessar o programa Configuration Manager de seu navegador.</i>	<p>Use o utilitário ping para verificar se seu PC pode comunicar-se com o Endereço IP da LAN do DSLink 260E (por padrão 192.168.1.1). Caso ele não consiga, verifique o cabeamento Ethernet.</p> <p>Verifique se está sendo utilizado Internet Explorer v5.0 ou posterior ou Netscape Navigator v4.7 ou posterior. O suporte para Javascript® deve ser ativado em seu navegador. O suporte para Java® pode também ser necessário.</p> <p>Verifique se o endereço IP de seu PC é definido como estando na mesma sub-rede como o endereço IP atribuído à porta LAN do DSLink 260E.</p>
<i>As alterações ao Configuration Manager não estão sendo retidas.</i>	Certifique-se de utilizar a função efetiva após quaisquer alterações.