



TECNOLOGIA E  
TRANSFORMAÇÃO

**MULTILASER**

# Manual do Usuário

RE160 Roteador 300 Mbps 2 antenas

# Sumário

<b>CAPÍTULO 1 VISÃO GERAL DO PRODUTO</b> .....	<b>4</b>
1 CONTEÚDOS DA EMBALAGEM.....	4
2 LEDs E PORTAS .....	4
<b>CAPÍTULO 2 GUIA RÁPIDO DE INSTALAÇÃO E CONFIGURAÇÃO</b> .....	<b>6</b>
1 INSTALAÇÃO FÍSICA .....	6
1.1 Preparação.....	6
1.2 Instalação física.....	7
2 CONFIGURAÇÃO DE CONEXÃO À INTERNET .....	9
2.1 Log in no Web Manager .....	9
2.2 Configuração de conexão à internet.....	10
3 VERIFIQUE AS CONFIGURAÇÕES DE CONEXÃO À INTERNET .....	12
4 Conectar-se ao dispositivo wireless.....	14
<b>CAPÍTULO 3 CONFIGURAÇÕES AVANÇADAS</b> .....	<b>21</b>
1 Avançada .....	21
1.1 Status .....	21
1.2 Configuração de conexão à internet.....	21
1.3 MAC Clone .....	27
1.4 WAN Speed .....	28
1.5 LAN Settings .....	28
1.6 DNS Settings.....	29
1.7 DHCP Server .....	30
1.8 DHCP Client List.....	30
2 Configurações sem fio.....	31
2.1 Configurações básicas do wireless .....	31
2.2 Segurança do wireless .....	32
2.3 Extensor Wireless .....	36
2.4 Configure o roteador 1:.....	48
2.5 Controle de acesso wireless.....	49
2.6 Cliente wireless .....	50

<b>3 Controle da banda larga</b> .....	<b>50</b>
3.1 Controle da banda larga .....	50
3.2 Estatísticas de tráfego.....	52
<b>4 Aplicativos especiais</b> .....	<b>53</b>
4.1 Redirecionamento de portas .....	53
4.2 DMZ Host.....	56
4.3 DDNS .....	56
4.4 UPNP.....	58
4.5 Roteamento estático.....	58
4.6 Tabela de roteamento .....	60
<b>5 Segurança</b> .....	<b>61</b>
5.1 Filtro URL.....	61
5.2 Filtro MAC.....	62
5.3 Filtro do cliente.....	65
<b>6 Ferramentas</b> .....	<b>67</b>
6.1 Reiniciar .....	67
6.2 Restaurar para configurações de fábrica .....	67
6.3 Backup/ Restaurar .....	68
6.5 Gerenciamento remoto baseado na web.....	70
6.6 Hora .....	71
6.7 Senha.....	72
6.8 Atualização do Firmware .....	72
<b>Anexo 1 Glossário</b> .....	<b>74</b>
Canal .....	74
SSID .....	74
1WPA/WPA 2 .....	74
Autenticação IEEE 802.1X .....	75
PPOE.....	75
DNS.....	76
WDS.....	76
<b>Anexo 2 Verifique a conexão WDS</b> .....	<b>77</b>
Configure PC2:.....	78
Configure PC3 e PC 4:.....	79
<b>Anexo 3 FAQs</b> .....	<b>81</b>

# CAPÍTULO 1 VISÃO GERAL DO PRODUTO

## 1 CONTEÚDOS DA EMBALAGEM

Desembale e verifique se os seguintes itens estão no pacote:

- (1) Roteador wireless banda larga
- (2) Fonte de alimentação
- (3) Guia rápido de instalação

Se qualquer um dos itens acima está incorreto, faltando ou danificado, por favor, entre em contato com o revendedor Multilaser para substituição imediata.

## 2 LEDs E PORTAS

Esta parte descreve as funções de hardware deste dispositivo. Os tópicos incluem:

1) Painéis frontal e traseiro do roteador wireless 2) Designações dos LEDs

- **Painel frontal**



**LEDs do painel frontal:**

LED	Status	Descrição
SYS	Piscando	Indica que o sistema está funcionando adequadamente
WLAN	Ligado	Wireless está ativado
	Piscando	Transmitindo dados
1/2/3	Ligado	Porta LAN está conectada corretamente
	Piscando	Porta LAN está transmitindo dados.
WAN	Ligado	Porta WAN está conectada corretamente
	Piscando	Porta WAN está transmitindo dados.

- Painel traseiro



**LEDs do painel traseiro:**

Porta	Descrição da função
WAN	Normalmente para conectar modem DSL, MODEM A CABO, ISP à internet.
1/2/3	Normalmente para conectar computadores, switches, etc.
WPS/ RST	Quando este botão é apertado por 7 segundos, os arquivos criados pelo roteador serão deletados e restaurados no padrão de fábrica; por 1 segundo, WPS será ativado e o LED do WPS ficará, então, piscando.
PWR	A fonte de alimentação está conectada e você pode utilizá-la para fornecer energia.

## **CAPÍTULO 2 GUIA RÁPIDO DE INSTALAÇÃO E CONFIGURAÇÃO**

### **1 INSTALAÇÃO FÍSICA**

#### **1.1 Prepação**

Antes de conectar as linhas de rede, por favor, verifique os seguintes itens:

Item	Description
Roteador Wireless	Utilizado com a fonte de alimentação fornecida.
Computador	Instalado com o IE8 ou outros superior.
Cabo Ethernet	Utilizado para ligar o computador ao roteador.
Serviço Banda Larga	Fornecido pelo ISP

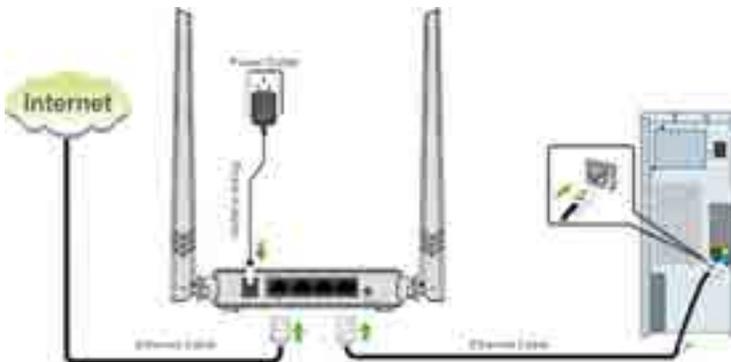
Configuração de conexão à internet	<ul style="list-style-type: none"><li>• Se você se conectar à Internet usando uma conexão de banda larga que exija um nome de usuário e uma senha fornecida pelo seu ISP, por favor selecione PPPoE;</li><li>• Se o seu ISP fornece todas as informações necessárias: endereço de IP, máscara de sub-rede, endereço de gateway e endereço(s) DNS, por favor, selecione IP Estático;</li><li>• Se você pode acessar a Internet assim que o seu computador se conecta diretamente a uma internet ADSL / modem a cabo, por favor, selecione DHCP;</li><li>• Se o seu ISP usa uma conexão PPTP, por favor, selecione PPTP;</li><li>• Se o seu ISP usa uma conexão L2TP, por favor, selecione L2TP;</li><li>• PPPoE Acesso Duplo (suportada somente em especial Área e.g. Rússia.).</li></ul>
------------------------------------	--

## 1.2 Instalação física

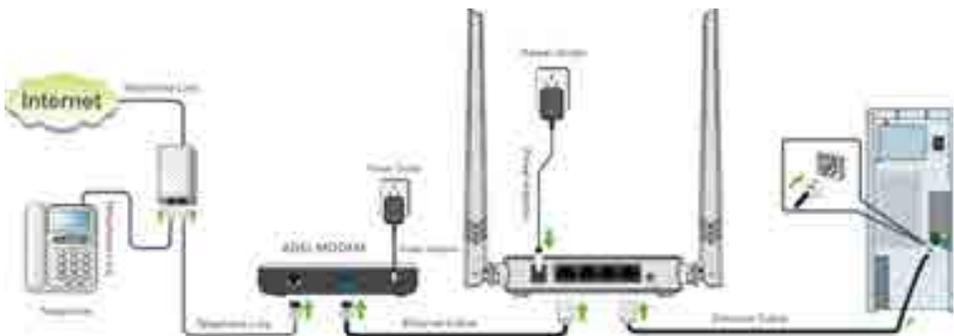
1. Conecte uma ponta da fonte de alimentação inclusa no dispositivo e conecte a outra ponta a uma tomada próxima. (Usar um adaptador de energia com tensão nominal diferente daquele fornecido com o dispositivo pode causar danos ao dispositivo).



2. Conecte uma das portas LAN do dispositivo à porta NIC em seu computador usando um cabo Ethernet.



3. Conecte o cabo Ethernet do lado da Internet à porta WAN do dispositivo. Se ele estiver conectado à linha telefônica, por favor, ligar a linha telefônica ao MODEM e conectar o MODEM à porta WAN do dispositivo.



4. Quando conectado, faça o login no Web manager para configurar a conexão à Internet.

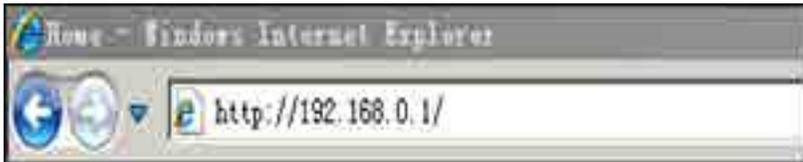
## 2 CONFIGURAÇÃO DE CONEXÃO À INTERNET

### 2.1 Log in no Web Manager

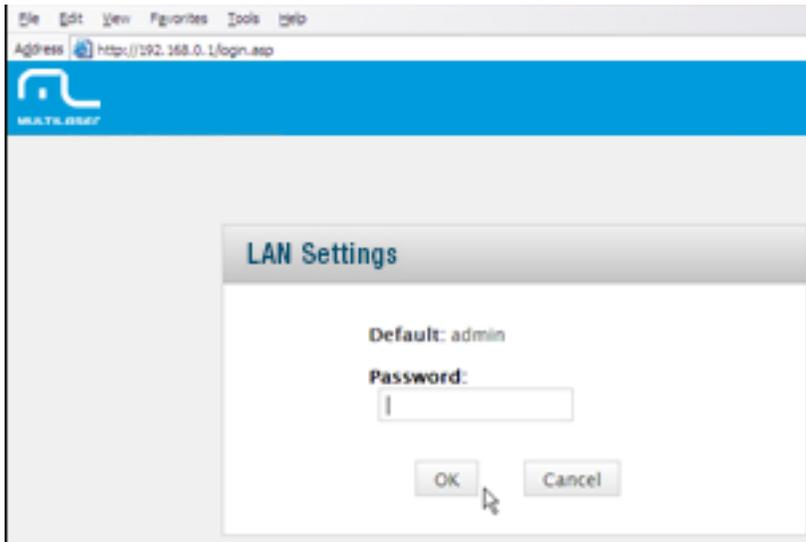
1. Abra um navegador, como o browser IE;



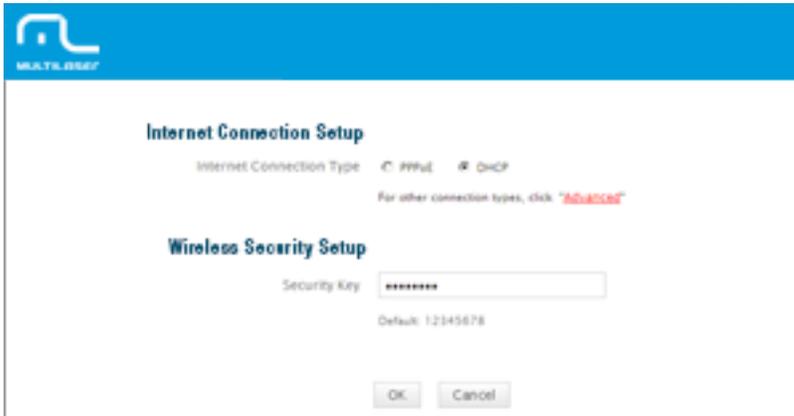
2. Na barra de endereços escreva 192.168.0.1 e pressione **Enter**;



3. Digite **admin** no campo da senha na caixa de diálogo e clique em **OK**.



4. Agora você pode acessar a página inicial do dispositivo para configurar rapidamente a conexão à internet e a segurança wireless.



The image shows two screenshots of a router's web interface. The top screenshot is titled "Internet Connection Setup" and features a blue header with a logo and the text "MULTI-BAND". Below the title, there are two radio buttons for "Internet Connection Type": "PPPoE" (unselected) and "DHCP" (selected). A red text prompt says "For other connection types, click 'Advanced'". The bottom screenshot is titled "Wireless Security Setup" and shows a "Security Key" field with a masked password "\*\*\*\*\*" and a "Default: 12345678" label. At the bottom of this screen are "OK" and "Cancel" buttons.

5. Se você não conseguir fazer o login, por favor, consulte Anexo 3 FAQs.

## 2.2 Configuração de conexão à internet

Tipos de conexão mais comuns da Internet estão disponíveis na página inicial: PPPoE e DHCP.

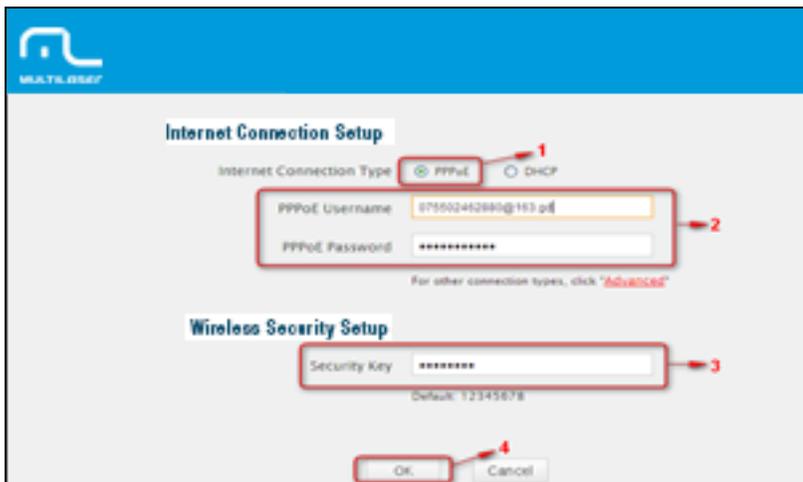
### DHCP

Selecione DHCP (IP Dinâmico) se você pode acessar a Internet assim que o seu computador se conecta diretamente a uma internet ADSL / modem a cabo; configure uma chave de segurança (8-63 caracteres) para proteger sua rede sem fio e, em seguida, clique em OK.



## PPPoE

Selecione PPPoE se você se conectar à Internet usando uma conexão de banda larga que exija um nome de usuário e uma senha fornecida pelo seu ISP; configure uma chave de segurança para proteger sua rede sem fio e, em seguida, clique em OK.



## Nota:

1. DHCP é o tipo de conexão de Internet padrão;
2. Se você não tem certeza sobre o seu nome de usuário e senha PPPoE, entre em contato com o seu provedor (ISP) para obter ajuda. Para outros tipos de conexão à Internet, por favor, vá para a seção 1.2: Configuração da conexão à Internet.

## 3 VERIFIQUE AS CONFIGURAÇÕES DE CONEXÃO À INTERNET

O sistema salta automaticamente para a página de status quando você terminar todas as configurações necessárias na página inicial. Aqui você pode ver o status do sistema e o status da conexão WAN do dispositivo.

1. Se você encontrar "Connected" e um endereço de IP WAN exibidos na página (como mostra abaixo), você tem um acesso à Internet com fio.



2. Se o status da conexão é "Disconnected", e não há nenhum endereço de IP WAN exibido (como mostra abaixo), a conexão entre o modem habilitado para Internet e seu dispositivo pode ter falhado. Por favor, verifique ou reconecte todos os dispositivos e cabos envolvidos de forma adequada e, em seguida, atualize a página. Se nada estiver errado, a palavra "Conexão" ou "Conectado" aparecerá.



 **Nota:**

Informações de diagnostico são apresentadas abaixo em ocasiões especiais para referência:

- 1). Você está conectado a Internet com sucesso.
- 2). Você pode ter colocado o nome de usuário e/ou senha errado. Por favor, entre em contato com o seu ISP para obter nome de usuário e senha corretos e tente novamente.
- 3). Cabo Ethernet não está conectado ou não está conectado corretamente à porta WAN do dispositivo. Por favor, reconecte-o corretamente.
- 4). Nenhuma resposta foi recebida do seu ISP. Por favor, verifique se você pode acessar a Internet quando seu computador está diretamente conectado a um modem habilitado. Caso não consiga, entre em contato com o seu ISP para obter assistência.

## 4 Conectar-se ao dispositivo wireless

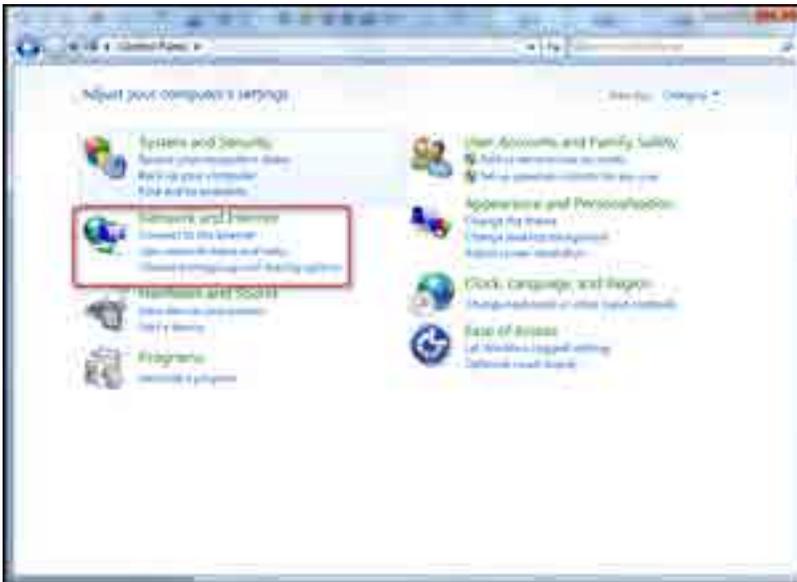
Após terminar as configurações acima, você pode procurar a rede sem fio do dispositivo (SSID) pelos seus aparelhos sem fio (notebook, iPad, iPhone, etc) e digitar uma chave de segurança para se conectar a ele sem fio.

### Operação WIN7

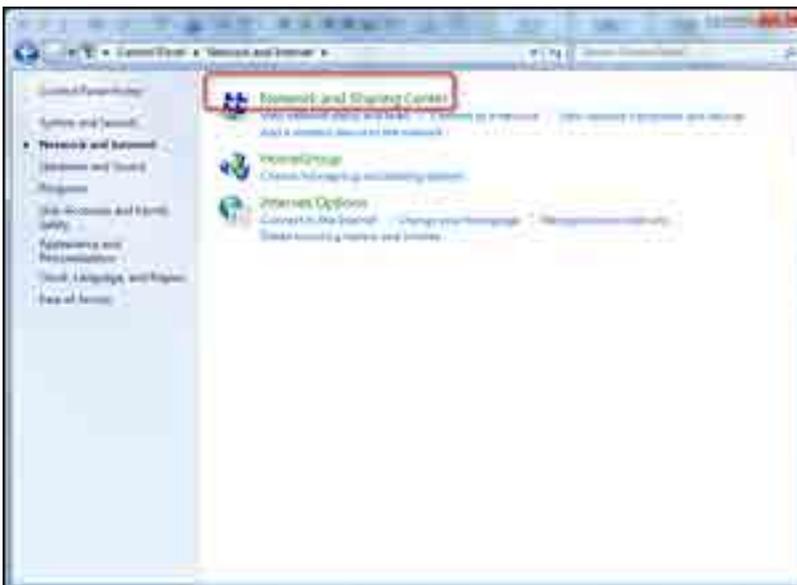
1. Se você estiver usando Windows 7 OS, siga as instruções:
  - 1) Aperte **Start** e selecione **Control Panel (Painel de Controle)**.



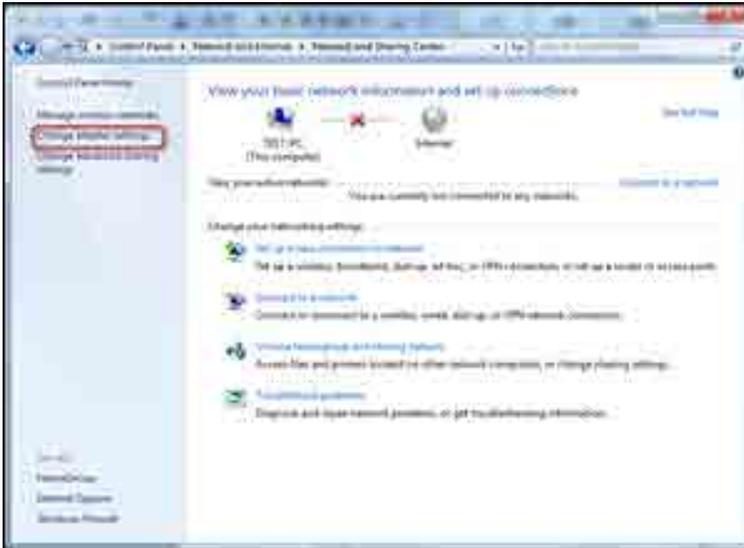
## 2) Aperte **Network and Internet (Rede e Internet)**.



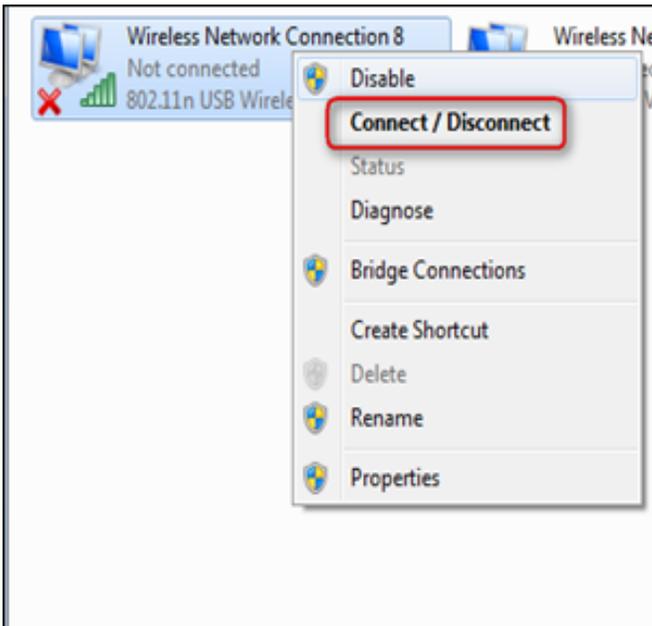
## 3) Clique em **Network and Sharing Center (Central de Rede e Compartilhamento)**.



4) Clique em **Change adapter settings (Alterar as configurações do adaptador)**.



5) Selecione a conexão sem fio desejada e clique em **Connect/Disconnect (Conecta/Desconecta)**.



6) Selecione a rede sem fio à qual você deseja se conectar e clique em **Connect (Conectar)**.



7) Digite a chave de segurança e clique em **OK**.



8) Você pode acessar a internet do dispositivo quando "Connected" aparecer ao lado do nome da rede sem fio que você selecionou.



## Operação Windows XP

2. Se você estiver usando Windows XP OS, siga as instruções:

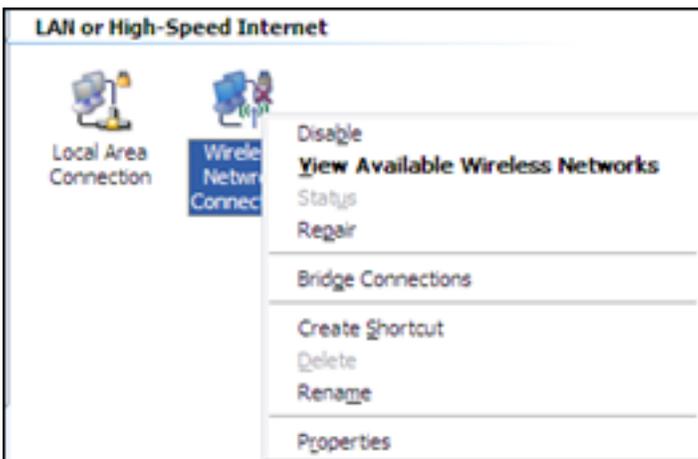
1) Clique em **Start** e selecione **Control Panel (Painel de Controle)**.



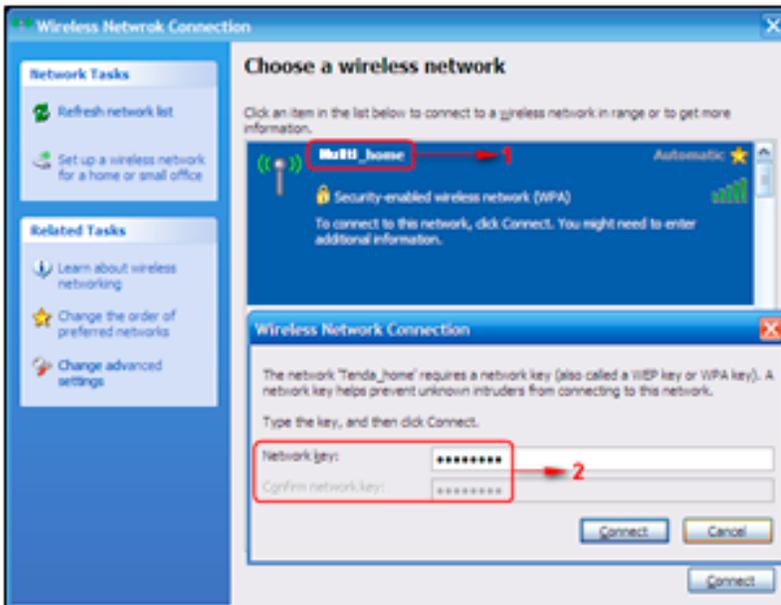
2) Clique em **Network Connections (Conexões de Rede)**.



3) Clique em **Wireless Network Connection(Conexões de Rede Wireless)** ( e depois seleccione **View Available Wireless Networks (Exibir Redes sem fio disponíveis)**).



4) Selecione a rede sem fio desejada, clique em **Connect (Conectar)**, digite a chave de segurança e clique em OK.



5) Você pode acessar a internet do dispositivo quando **"Connected"** (conectado) aparecer ao lado do nome da rede sem fio que você selecionou.



# CAPÍTULO 3 CONFIGURAÇÕES AVANÇADAS

## 1 Avançada

### 1.1 Status

Aqui você pode ver rapidamente o status de funcionamento do dispositivo. Se Porta WAN mostrar Desconectado, por favor, consulte **3 Verifique as configurações de Conexão a internet**.



### 1.2 Configuração de conexão à internet

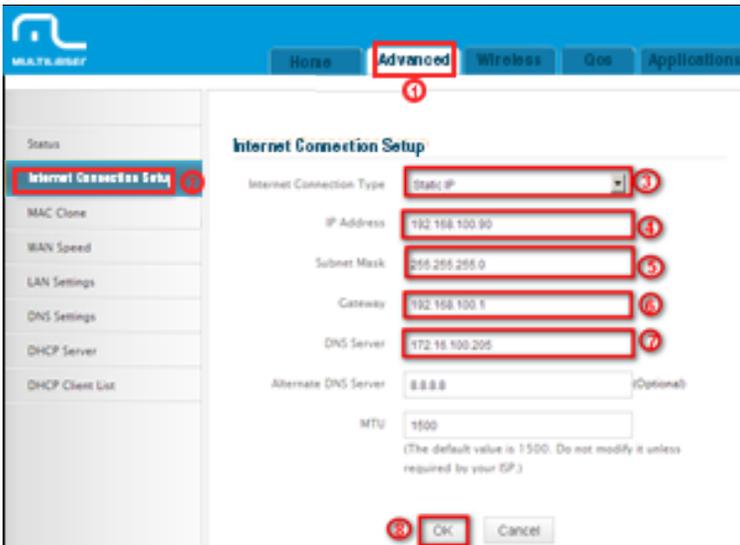
#### PPPoE

Selecione PPPoE se você se conectar à Internet usando uma conexão de banda larga que exija um nome de usuário e uma senha e digite o nome de usuário e a senha fornecidos pelo seu ISP.



## IP Estático

Selecione IP Estático se o seu ISP fornece todas as informações necessárias. Você terá que digitar o endereço de IP fornecido, máscara de sub-rede, endereço de gateway e endereço(s) DNS nos campos correspondentes.



1. Clique em **Advanced**.
2. Clique em **Internet Connection Setup**.
3. Internet connection selecione Static IP.
4. IP Address: Digite o endereço de IP fornecido pelo seu ISP. Consulte o seu ISP se você não souber o endereço de IP.
5. Subnet mask: Digite a máscara de sub-rede fornecida pelo seu ISP.
6. Gateway: Digite a WAN Gateway fornecida pelo seu ISP.
7. DNS Server: Digite o endereço DNS fornecido pelo seu ISP.
8. OK: Clique em OK e salve todas as suas configurações.

## DHCP

Selecione DHCP (IP Dinâmico) se você pode acessar a Internet assim que o seu computador se conecta diretamente a uma internet ADSL / modem a cabo.



1. **Internet connection Type:** Selecione DHCP.
2. **MTU:** Unidade máxima de transmissão. NÃO altere o padrão de fábrica de 1500, a menos que indicado pelo seu ISP. Pode ser necessário alterá-lo para melhor desempenho em alguns sites específicos ou utilização de software que não pode ser aberto ou habilitado, neste caso, tente 1450, 1400, etc.
3. OK: Clique em Ok para salvar suas configurações.

## PPTP

Selecione PPTP (Point-to-Point Tunneling Protocol-) se o seu ISP usa uma conexão PPTP. O PPTP permite conectar a um roteador para um servidor VPN.

**Por exemplo :**

Um ramo empresarial e sede podem usar esse tipo de conexão para implementar o acesso mútuo e seguro aos recursos de cada um.



1. **Internet connection Type:** Mostra o atual tipo de conexão com a Internet.
2. **PPTP Server Address:** Digite o endereço de IP de um servidor PPTP.
3. **User Name:** Digite o seu nome do usuário PPTP.
4. **Password:** Digite a senha.
4. **MTU:** Unidade máxima de transmissão. NÃO altere o padrão de fábrica de 1500, a menos que indicado pelo seu ISP. Pode ser necessário alterá-lo para melhor desempenho em alguns sites específicos ou utilização de software que não pode ser aberto ou habilitado, neste caso, tente 1450, 1400, etc.
5. **Address Mode:** Selecione "Dynamic" se você não tiver nenhuma informação de IP do seu ISP, caso contrário, selecione "Static". Consulte o seu ISP caso você precise de informação.
6. **IP Address:** Digite o endereço de IP fornecido pelo seu ISP. Consulte o seu ISP se você não souber o endereço de IP.
7. **Subnet mask:** Digite a máscara de sub-rede fornecida pelo seu ISP
8. **Gateway:** Digite a WAN Gateway fornecida pelo seu ISP. Consulte o seu ISP caso você precise de informação

## L2TP

Selecione L2TP (Layer 2 Tunneling Protocol) se o seu ISP utiliza uma conexão L2TP. O L2TP conecta o seu roteador a um servidor L2TP.

### Por Exemplo:

Um ramo empresarial e sede podem usar esse tipo de conexão para implementar o acesso mútuo e seguro aos recursos de cada um.



- Internet connection Type: Mostra o atual tipo de conexão com a Internet.
- L2TP Server Address: Digite o endereço de IP de um servidor L2TP.
- User Name: Digite o seu nome do usuário L2TP.
- Password: Digite a senha.
- MTU: Unidade máxima de transmissão. NÃO altere o padrão de fábrica de 1500, a menos que indicado pelo seu ISP. Pode ser necessário alterá-lo para melhor desempenho em alguns sites específicos ou utilização de software que não pode ser aberto ou habilitado, neste caso, tente 1450, 1400, etc.
- Address Mode: Selecione "Dynamic" se você não tiver nenhuma informação de IP do seu ISP, caso contrário, selecione "Static". Consulte o seu ISP caso você precise de informação.

g) IP Address: Digite o endereço de IP fornecido pelo seu ISP. Consulte o seu ISP se você não souber o endereço de IP.

h) Subnet mask: Digite a máscara de sub-rede fornecida pelo seu ISP

i) Gateway: Gateway: Digite a WAN Gateway fornecida pelo seu ISP. Consulte o seu ISP caso você precise de informação

**Nota:**

1. PPPOE, PPTP e L2TP não podem ser utilizados simultaneamente!

2. Apenas IP estático ou IP Dinâmico está disponível para conexões a internet PPTP e L2TP.

Note que PPTP e L2TP podem não estar disponíveis em alguns produtos

**PPPoE Acesso Duplo**

PPPoE Acesso Duplo suporta somente em especial Área e.g. Rússia.



1. **Internet connection Type:** Mostra o atual tipo de conexão com a Internet.
2. **PPPoE User Name:** Digite o seu nome do usuário fornecido pelo seu ISP.
3. **PPPoE Password:** Digite a senha fornecida pelo seu ISP.
4. **MTU:** Unidade máxima de transmissão. NÃO altere o padrão de fábrica de 1500, a menos que seja necessário.
5. **Service Name:** Descrição da conexão PPPoE. Deixe em branco a menos que o contrário seja exigido.
6. **Server Name:** Descrição do servidor. Deixe em branco a menos que o contrário seja exigido.
7. **Address Mode:** Selecione "Dynamic" se você não tiver nenhuma informação de IP do seu ISP, caso contrário, selecione "Static". Consulte o seu ISP caso você precise de informação.
8. **IP Address:** Digite o endereço de IP fornecido pelo seu ISP. Consulte o seu ISP se você não souber o endereço de IP.
9. **Subnet mask:** Digite a máscara de sub-rede fornecida pelo seu ISP.

### 1.3 MAC Clone

Alguns provedores de serviços de Internet (ISPs) exigem o endereço MAC do usuário final para acessar a rede. Este recurso copia o endereço MAC do seu dispositivo de rede para o roteador.



1. **MAC Address:** Configure o endereço WAN MAC do dispositivo.
2. **Clone MAC Address:** Clique para copiar o endereço MAC do seu computador para o dispositivo como um novo endereço MAC WAN.
3. **Restore Default MAC:** Redefina WAN MAC do dispositivo ao padrão de fábrica.

## 1.4 WAN Speed

Aqui você pode ajustar a velocidade e o modo duplex para a porta WAN. É aconselhável manter o padrão **Automático** para obter a melhor velocidade



## 1.5 LAN Settings

Clique em **Advanced > LAN Settings** para chegar à página abaixo:



1. **LAN MAC Address:** Mostra o endereço LAN MAC do dispositivo, que é imutável.
2. **IP Address:** Endereço de IP LAN do dispositivo. O padrão é 192.168.0.1. Você pode alterá-lo de acordo com sua necessidade.
3. **Subnet Mask:** Dispositivo de máscara de sub-rede LAN, 255.255.255.0 por padrão.

4. OK: clique em OK para salvar suas configurações.

**Nota:** Se o endereço de IP padrão for alterado, você deve digitar o novo endereço de IP para conectar.

## 1.6 DNS Settings

DNS é a abreviatura de Sistema de Nomes de Domínio.



- 1. Enable Manual DNS Assignment:** Clique para ativar as configurações de DNS.
- 2. Primary DNS Server:** Digite o endereço DNS primário fornecido pelo seu IPS.
- 3. Alternate DNS Server:** Digite o outro endereço DNS se seu ISP fornece esses endereços (opcional).
- 4. OK:** clique em OK para salvar suas configurações.

### Nota:

1. Não se podem abrir páginas da web se os endereços de servidor DNS são digitados incorretamente.
2. Não se esqueça de reiniciar o dispositivo para ativar as novas configurações quando você terminar todas as configurações.

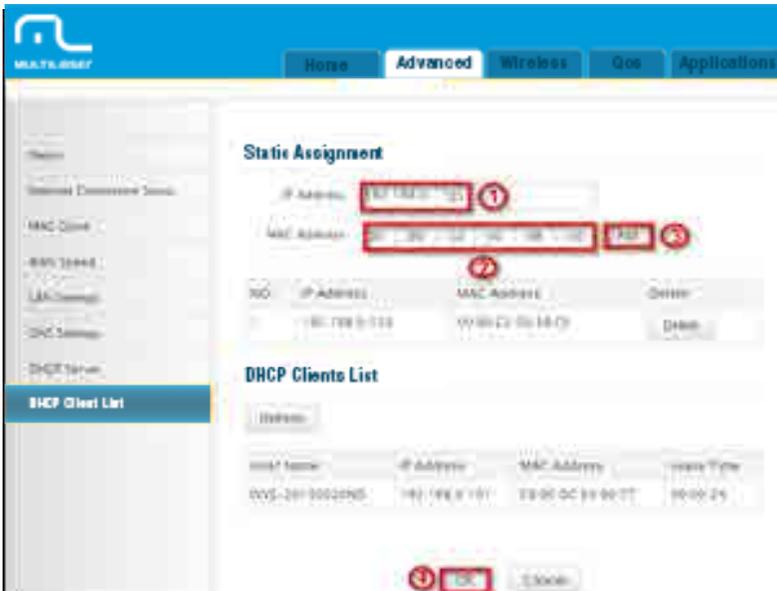
## 1.7 DHCP Server

O Dynamic Host Configuration Protocol (DHCP) é um protocolo de configuração automática utilizado em redes IP. Se você ativar o servidor DHCP embutido no dispositivo, ele irá configurar automaticamente as configurações de TCP / IP para todos os computadores da LAN (incluindo o endereço de IP, máscara de sub-rede, o gateway e DNS, etc), eliminando a necessidade de intervenção manual. Lembre-se apenas de configurar todos os computadores em sua LAN para ser clientes DHCP, selecionando "Obtain an IP Address Automatically", respectivamente, em cada um desses computadores. Quando ligados, esses computadores carregarão automaticamente as informações de IP a partir do servidor DHCP. (Esse recurso é ativado pelo padrão. NÃO o desative, a menos que necessário).



## 1.8 DHCP Client List

O DHCP Client List mostra informações de dispositivos que tenham obtido os endereços de IP a partir do dispositivo DHCP Server. Se você quiser alguns dispositivos da rede para obter sempre os mesmos endereços de IP, você pode adicionar manualmente uma entrada reserva DHCP estático para cada dispositivo.



1. **IP Address:** Digite o endereço de IP para reserva de DHCP estático.
2. **MAC Address:** Digite o endereço MAC de um computador para receber sempre o mesmo endereço de IP (o IP que você acabou de especificar).
3. **Add:** Clique em add para adicionar a entrada à lista de reserva de endereço MAC.
4. **OK:** clique em OK para salvar suas configurações.

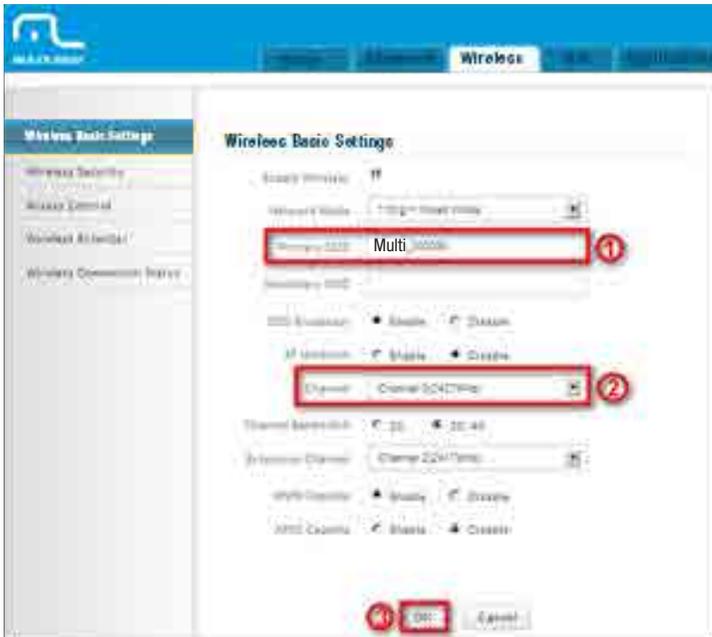
### Nota:

Se o endereço de IP que você reservou para o seu computador é usado atualmente por outro cliente, você não será capaz de obter um novo endereço de IP do servidor DHCP do dispositivo, então, você deve especificar manualmente um endereço de IP diferente para o seu computador para acessar a Internet.

## 2 Configurações sem fio

### 2.1 Configurações básicas do wireless

Se você deseja criar uma WLAN para compartilhar conexão à Internet, basta clicar em Wireless-> Wireless Basic settings. Altere o SSID, você pode nomeá-lo como quiser. Por exemplo, selecione 2437MHz (canal 6) e deixe as outras opções inalteradas e, em seguida clique em OK.



- 1. SSID:** Este é o nome público de sua rede sem fio. O padrão é Multi\_XXXXXX. XXXXXX são os últimos seis caracteres do endereço MAC do dispositivo. É recomendado que você o altere para uma melhor segurança e identificação.
- 2. Channel:** Selecione o canal menos utilizado por redes vizinhas a partir da lista suspensa ou automático. Os canais 1, 6 e 11 são recomendados.
- 3. OK:** Clique em OK para salvar suas configurações.

## 2.2 Segurança do wireless

### Configuração de segurança do wireless

Esta seção permite que você proteja a sua rede sem fio e bloqueie acessos não autorizados e sniffing de pacotes maliciosos. Para criptografar sua rede sem fio, siga as instruções:

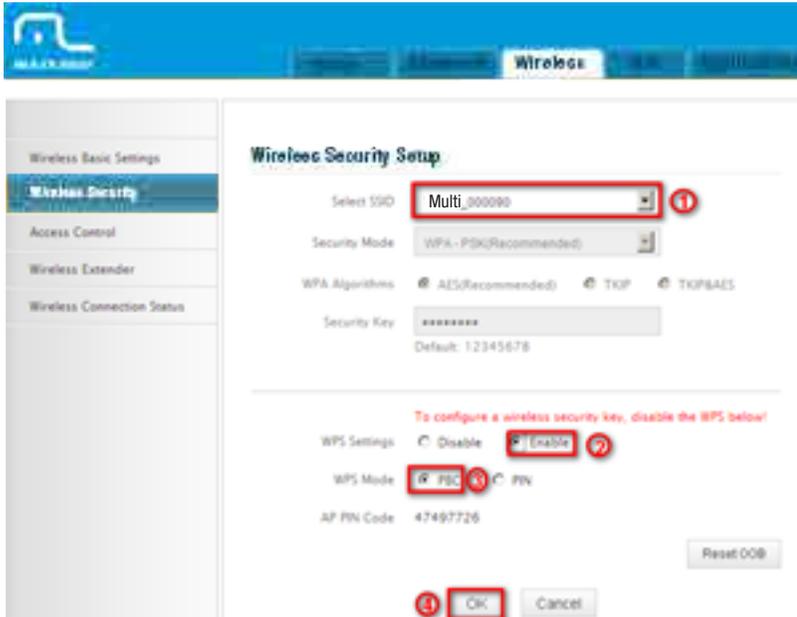
1. Selecione a rede sem fio (SSID) que você deseja criptografar.
2. Desative o WPS (WPS é habilitado no roteador pelo padrão. Se você quiser usar outros modos de segurança, você deve primeiro desativar o WPS).



**Instruções de operação:****PBC:** Para usar o WPS-PBC, tente as seguintes instruções:

Pressione o botão WPS hardware no roteador por cerca de 1 segundo e depois habilite WPS / PBC no aparelho do cliente depois de 2 minutos;

Pressione o botão WPS hardware no roteador por cerca de 1 segundo e depois habilite WPS / PBC no aparelho do cliente depois de 2 minutos;

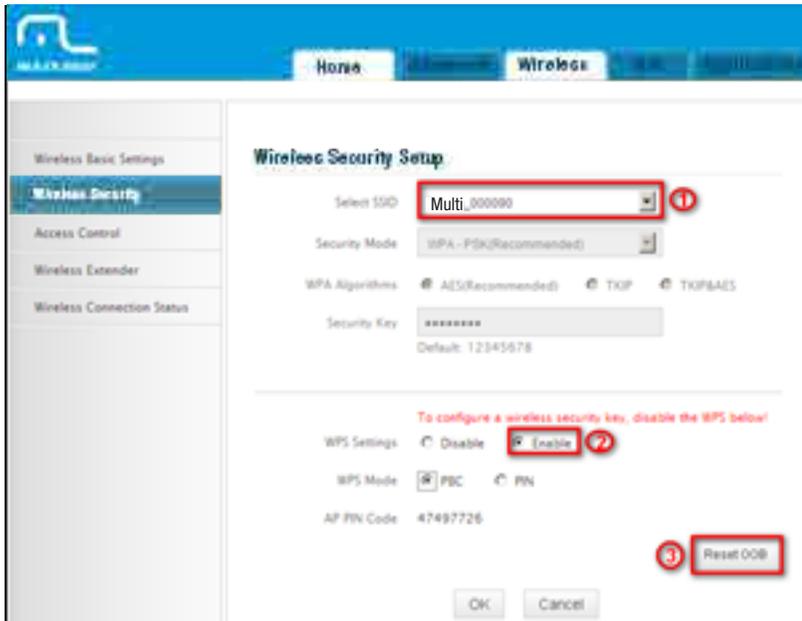


**PIN:** Na página de segurança wireless, ative WPS, selecione PIN e digite o código PIN de 8 dígitos do adaptador de rede, depois de 2 minutos permita WPS / PIN no aparelho do cliente;



### Nota:

1. Com o WPS ativado com sucesso, o LED WPS no roteador ficará piscando por aproximadamente 2 minutos e, durante este tempo, você pode ativar WPS em um adaptador sem fio, se o adaptador se conectar com sucesso a rede sem fio, o LED WPS irá mostrar uma luz fixa. Repita os passos acima, se você quiser adicionar mais adaptadores sem fio ao roteador.
2. **Reset OOB:** Clicar nesse botão irá resetar SSID ao padrão de fábrica e desativar o modo de segurança.
3. Configurações de wireless existentes ainda serão mantidas pelo padrão depois de uma conexão WPS bem sucedida. Especialmente as configurações de segurança e SSID no roteador ainda serão as mesmas. Se você quiser gerar uma chave de wireless aleatória por WPS, clique em Reset OOB e siga as instruções de configuração WPS acima.



### Nota:

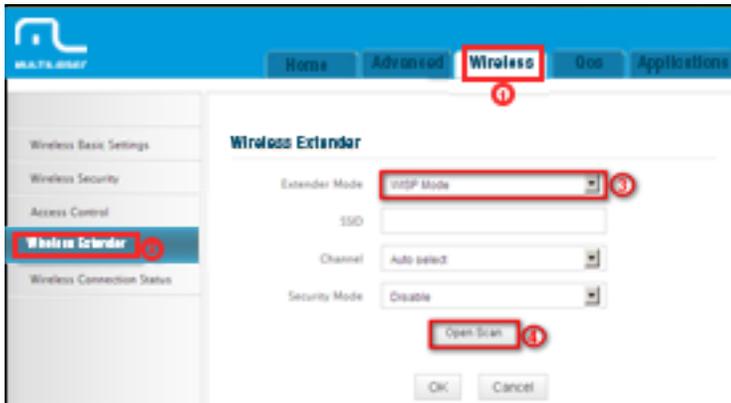
1. Para usar a segurança WPS, o cliente wireless também deve conseguir utilizar WPS.
2. Antes de pressionar o botão WPS hardware do dispositivo para conexão WPS / PBC, certifique-se de que o recurso WPS foi ativado no dispositivo.

## 2.3 Extensor Wireless

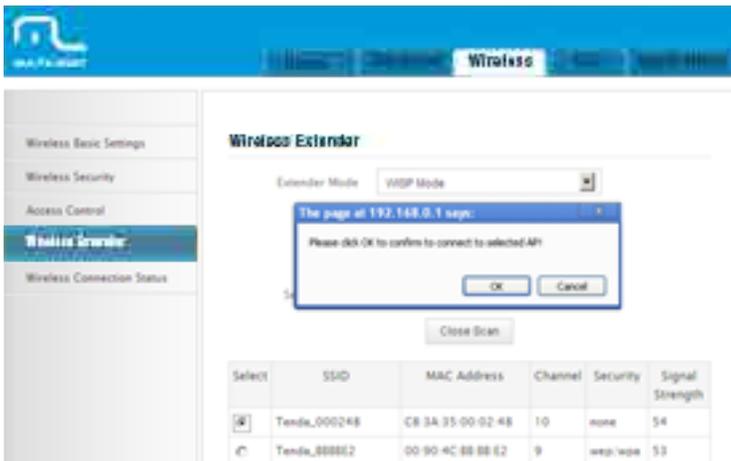
### WISP Mode

Se o seu roteador tem acesso à Internet a partir de um ponto de acesso wireless, por favor selecione o modo WISP. Siga a seguintes instruções:

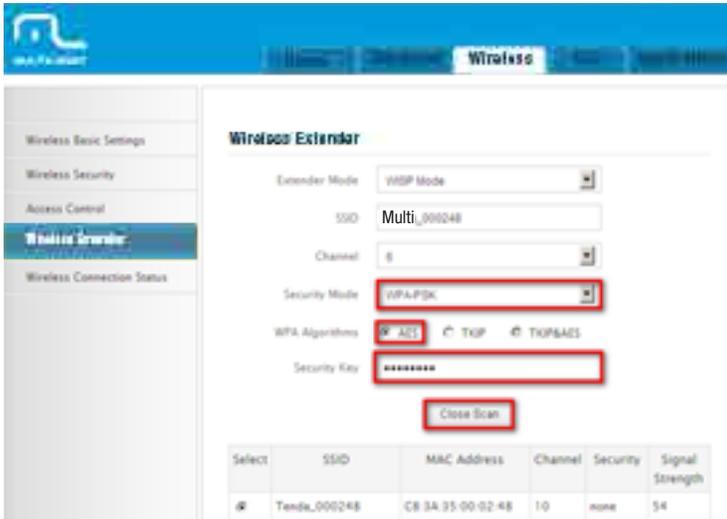
1. Clique em **Wireless>Wireless Extender**, selecione **WISP mode** e clique em **Open Scan**.



2. Clique em Open Scan, selecione o AP que você deseja se conectar, como Multi-000248, e clique em OK.



3. Veja e anote as configurações de segurança sem fio: modo de segurança, tipo cifra, chave de segurança.



Wireless Extender

Extender Mode: WISP Mode

SSID: Multi\_000248

Channel: 8

Security Mode: WPA-PSK

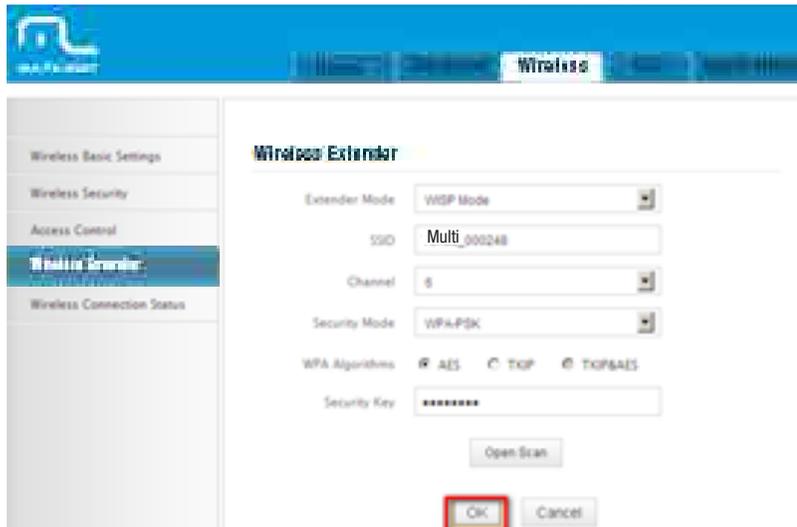
WPA Algorithms:  AES  TKIP  TKIP&AES

Security Key: \*\*\*\*\*

Close Scan

Select	SSID	MAC Address	Channel	Security	Signal Strength
<input checked="" type="checkbox"/>	Tenda_000248	C8 3A 35 00 02 48	10	none	54

4. Clique em Close Scan e OK.



Wireless Extender

Extender Mode: WISP Mode

SSID: Multi\_000248

Channel: 8

Security Mode: WPA-PSK

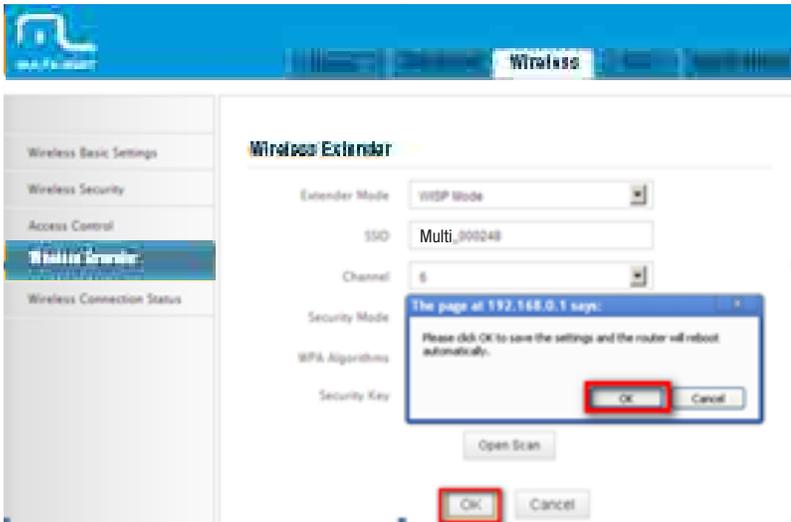
WPA Algorithms:  AES  TKIP  TKIP&AES

Security Key: \*\*\*\*\*

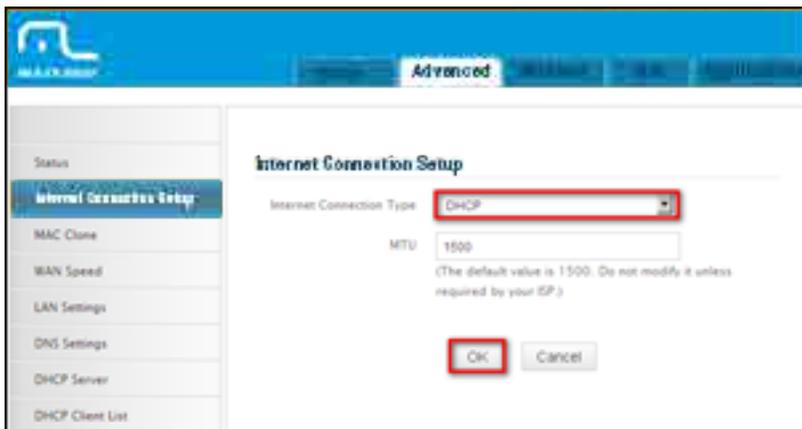
Open Scan

OK Cancel

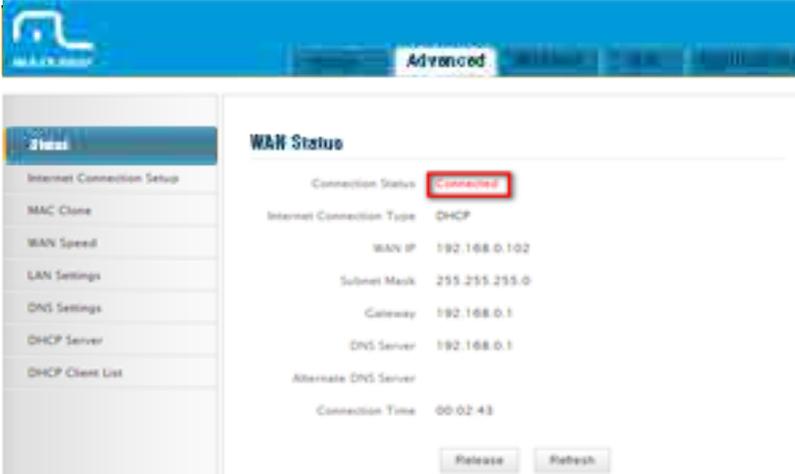
5. Salve as configurações e o roteador irá reiniciar automaticamente.



6. Internet Connection Setup: Clique em **Advanced**>**Internet Connection Setup**, selecione Internet Connection Setup, como DHCP, e clique **OK**.



7. Clique em **Advanced>Status** e o connection status mostrará **Connected**.



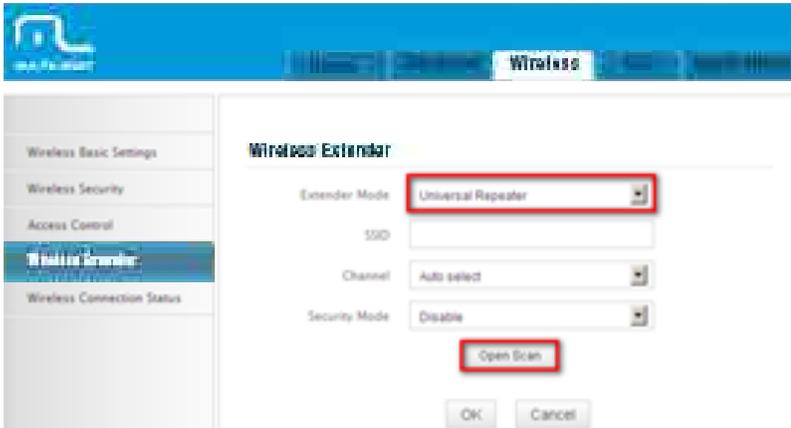
### Nota:

1. Quando as configurações acabarem, lembre-se de entrar na Internet Connection Setup para configurar a conexão de Internet.
2. Verifique se o SSID, canal e modo de segurança na página correspondem aos da rede sem fio adicionada. Se não correspondem, corrija-os manualmente.
3. Para a conexão wireless normal entre dois roteadores, não altere as configurações de SSID deste roteador, incluindo SSID, canal, modo de segurança e chave de segurança.

### Universal Repeater Mode

Neste modo, o roteador irá transmitir dados para um root AP associado, enquanto isso, a função AP será habilitada. O wireless repeater transmite sinal entre as estações e o root AP para maior alcance do wireless. Como mostram os passos a seguir:

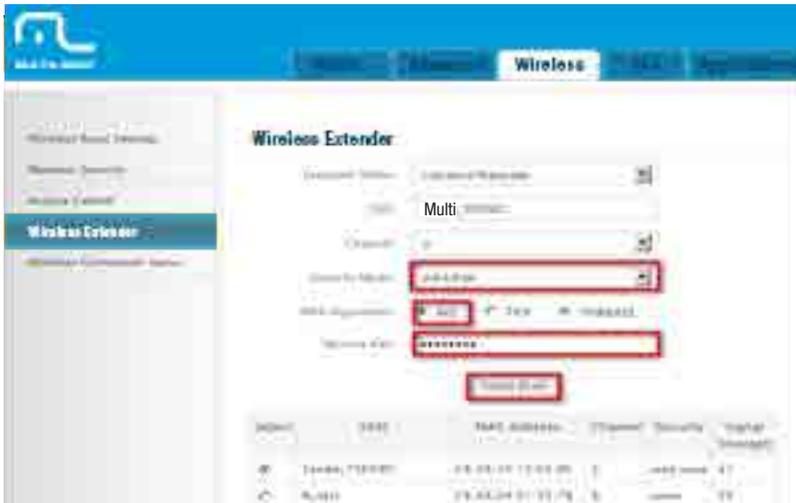
1. Clique em **Wireless>Wireless Extender**, selecione **Universal Repeater** no modo extender e clique em **Open Scan**.



2. Clique em **Open Scan**, selecione o AP que você deseja conectar, como Multi-15058C, e clique em **OK**.



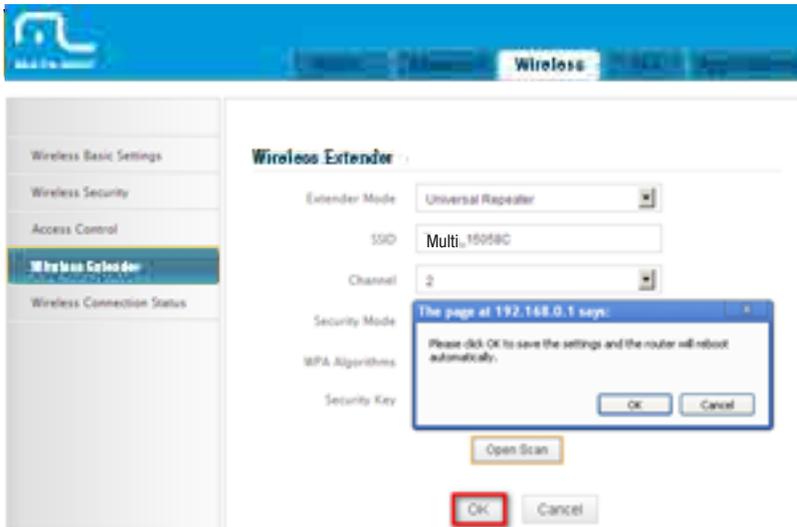
3. Veja e anote as configurações de segurança wireless: modo de segurança, tipo cifra, chave de segurança, etc, que devem estar de acordo com o dispositivo superior



4. Clique em **Close Scan** e **OK**.



5. Salve as configurações e o roteador irá reiniciar automaticamente.

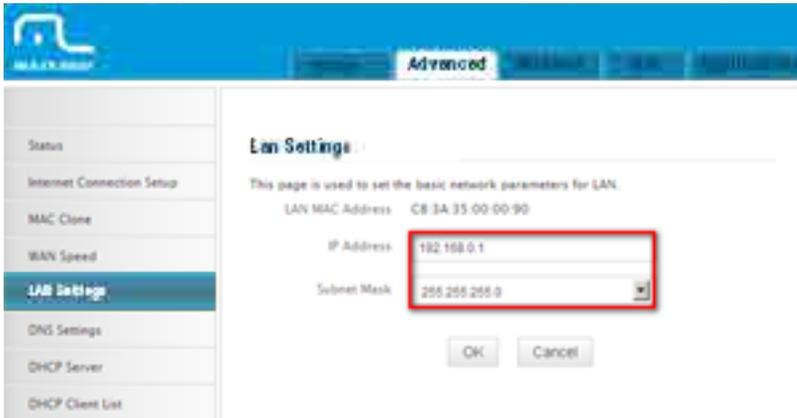


### Por exemplo:

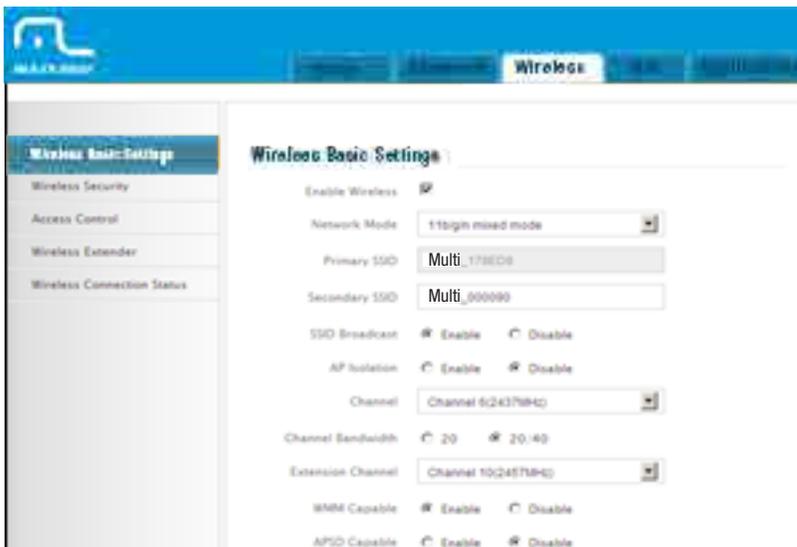
Como pode ser visto na figura acima, PC1 e PC2 tem acesso à Internet através de uma conexão sem fio ao roteador 1. Enquanto PC3 e PC4 estão muito distantes para se conectarem diretamente ao Roteador 1 e obter acesso à Internet. Agora você pode usar o recurso de bridge WDS para fazer com que PC3 e PC4 tenham acesso à Internet.

## Antes de começar:

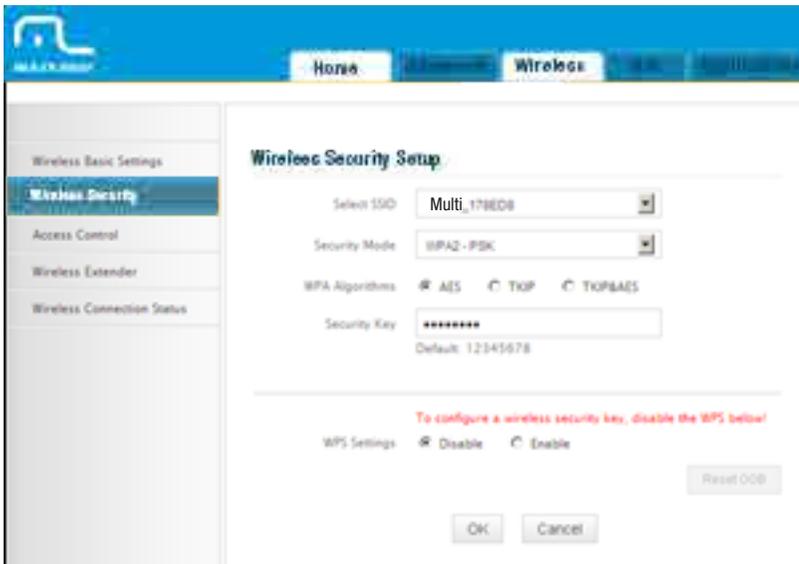
1. Veja e anote as configurações de segurança wireless: modo de segurança, tipo cifra, chave de segurança, etc no Router 1; Clique em Status>LAN Settings e olhe o endereço de IP.



2. Clique em **Wireless>Wireless Basic Settings** para verificar as configurações básicas de wireless do roteador um.



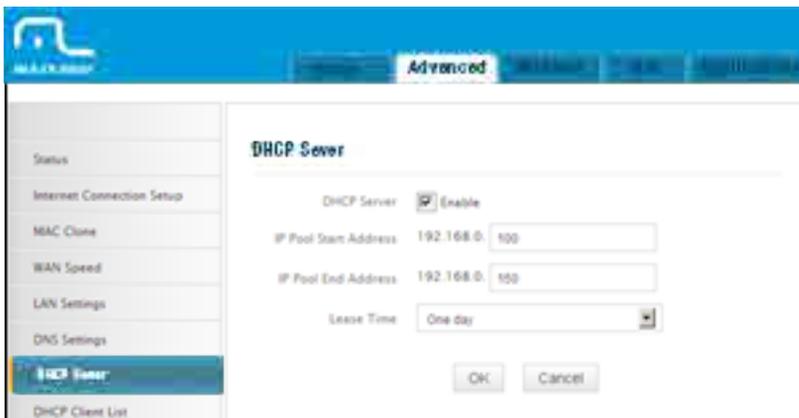
3. Clique em **Wireless>Wireless Security** para verificar as configurações de segurança de wireless do roteador um.



The screenshot shows the 'Wireless Security Setup' page. The left sidebar has 'Wireless Security' selected. The main content area includes the following fields and options:

- Select SSID: Multi\_178ED8
- Security Mode: WPA2-PSK
- WPA Algorithms:  AES  TKIP  TKIP/AES
- Security Key: [Redacted] (Default: 12345678)
- WPS Settings:  Disable  Enable
- Buttons: OK, Cancel, Reset OOB
- Warning: To configure a wireless security key, disable the WPS below!

5. Verifique se o servidor DHCP está habilitado no roteador 1: Clique em **Advanced>DHCP Server**.



The screenshot shows the 'DHCP Server' configuration page. The left sidebar has 'DHCP Server' selected. The main content area includes the following fields and options:

- DHCP Server:  Enable
- IP Pool Start Address: 192.168.0.100
- IP Pool End Address: 192.168.0.150
- Lease Time: One day
- Buttons: OK, Cancel

6. Ajuste o endereço de IP LAN do Roteador 2 para um endereço diferente, mas ainda no mesmo segmento de rede como o roteador 1.

**Como mostra abaixo:**

Roteador 1:

LAN IP: 192.168.0.1;

Subnet Mask: 255.255.255.0;

Roteador 2:

LAN IP: 192.168.0.10;

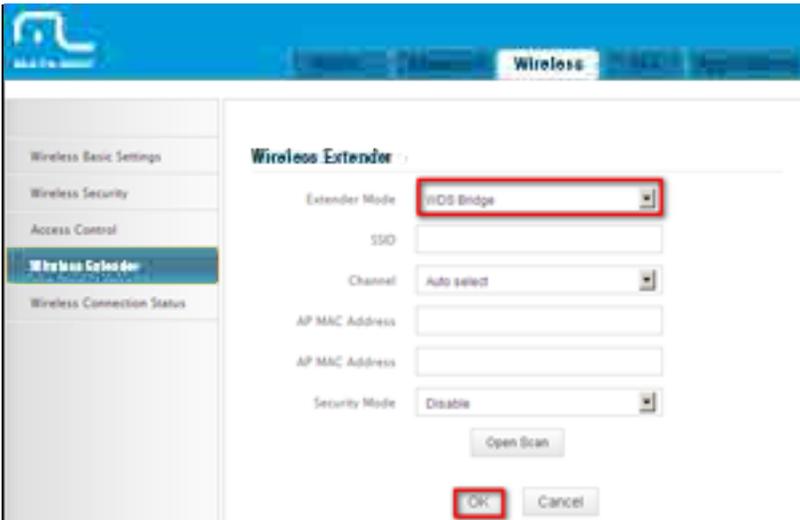
Subnet Mask: 255.255.255.0;

**Em seguida siga as instruções:**

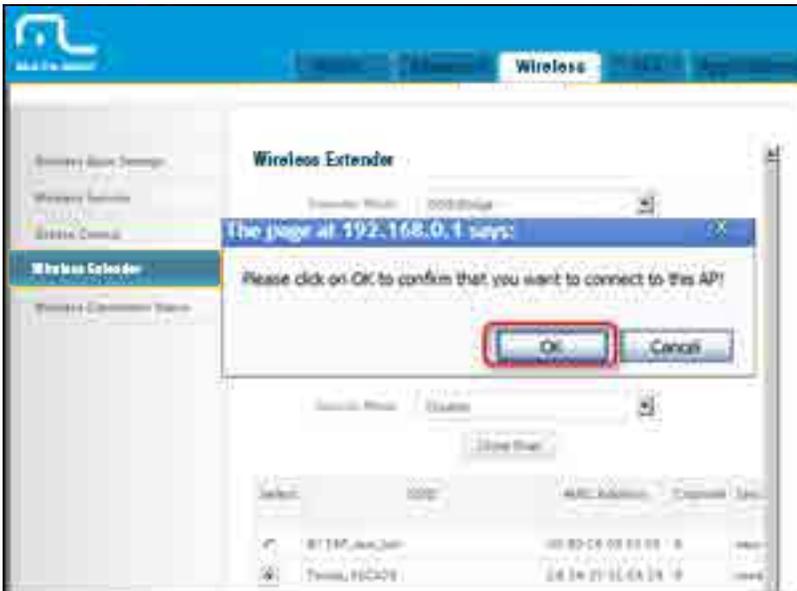
1. Configure o roteador 2:

1) Wireless Working Mode: Selecione WDS Bridge Mode.

2) Clique em **Open Scan** para procurar o Roteador 1.



3) Selecione a rede sem fio para conectar e clique em **OK**.



4) Verifique se o SSID, canal e endereço MAC do AP na página correspondem aos da rede sem fio adicionada. Se não, corrija-os manualmente.

5) Feche **Scan** e clique em **OK** para salvar suas configurações.

6) Vá para a página de segurança do wireless e defina as configurações de segurança wireless exatamente como elas estão no link partner (Roteador 1).

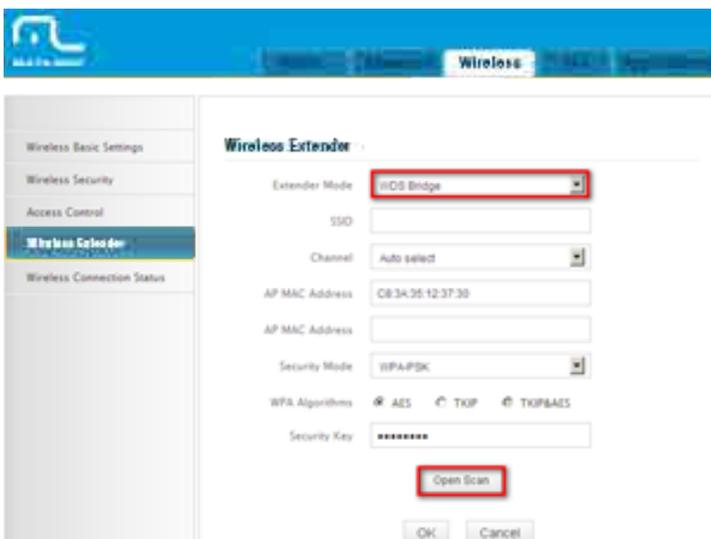


7) Vá para o servidor DHCP para desabilitar o DHCP no Roteador 2. Agora você terminou todas as configurações no roteador 2 necessárias para WDS.



## 2.4 Configure o roteador 1:

1. Vá para a seção wireless no Roteador 1 e especifique WDS (ou WDS Bridge) como o seu modo de funcionamento wireless.
2. Insira manualmente o endereço MAC do roteador 2 (Além disso, você pode usar a opção Scan, como mencionado acima) e clique em OK para finalizar as configurações.



## 2.5 Controle de acesso wireless

O recurso de controle de acesso permite que você especifique uma lista de aparelhos para Permitir ou Proibir uma conexão com sua rede sem fio através dos endereços MAC dos aparelhos. Todos os outros aparelhos não listados como Permitido serão Proibidos e vice-versa.

1. Selecione a rede sem fio (SSID) que você deseja habilitar o controle de acesso.
2. MAC Address Filter: Selecione Permit ou Forbid a partir da lista suspensa.



3. Para permitir que um aparelho sem fio se conecte à sua rede sem fio, selecione Permit, digite o seu endereço MAC, clique em Add e, em seguida, OK. Então, somente este aparelho listado como "Permitted" será capaz de se conectar à sua rede sem fio, todos os outros aparelhos sem fio serão proibidos.

**Exemplo:** Para proibir o computador com endereço MAC de C8: 3A: 35:65:82: E6 de se conectar à sua rede sem fio, faça o seguinte:



Passo1. Selecione um SSID, por exemplo, **Multilaser\_178ED8**.

Passo2. Selecione **Forbid** a partir do menu suspenso correspondente

Passo3. Digite C8:3A:35:65:82:E6 na caixa MAC address e clique em **Add**.

Passo4. Clique **OK** para salvar suas configurações. Você pode adicionar mais endereços MAC wireless se você desejar proibir.

## 2.6 Cliente wireless

Aqui você pode ver uma lista de aparelhos sem fio conectados ao roteador, incluindo seus endereços MAC e a banda larga.



**Nota:** A banda larga aqui se refere ao canal de banda larga ao invés da conexão wireless.

## 3 Controle da banda larga

### 3.1 Controle da banda larga

Use esta seção para gerenciar a alocação da banda larga para os aparelhos em sua LAN. Se houver vários computadores ligados ao seu roteador competindo por recursos limitados de banda larga, então você pode usar esse recurso para especificar uma quantidade razoável de banda larga para cada um desses computadores, de modo que todos consigam utilizar a internet.

**Bandwidth Control**

Enable Bandwidth Control  Enable ①

IP Address 192.168.0.100 - 100 ②

Upload/Download Upload ③

Bandwidth Range 128 - 128 ④

Enable  ⑤

Add To List ⑥

No.	IP Range	Destination	Bandwidth Range	Enable	Edit	Delete
1	192.168.0.100-100	Upload	128-128	✓	Edit	Delete

OK ⑦ Cancel

- 1. Enable Bandwidth Control:** Marque ou desmarque a caixa para ativar ou desativar o recurso de controle da banda larga.
- 2. IP Address:** Especifique o mesmo endereço de IP (por exemplo, 100, 100) ou dois endereços de IP diferentes (por exemplo, 100, 110) em ambas as caixas para especificar um único endereço de IP ou um intervalo no endereço de IP para o qual será aplicada a regra de controle de banda larga atual.
- 3. Upload/Download:** Selecione para controlar a banda larga em upload de dados ou download.
- 4. Bandwidth Range:** Especifique limite de upload / download da banda larga no computador especificado (s). A unidade é KByte / s. 1M = 128KByte / s. Note que o limite máximo de upload / download da banda larga não deve exceder o limite de banda larga WAN do seu roteador. (Consulte o seu ISP caso precise de informações).
- 5. Enable:** Marque para ativar regra atual. (Quando desabilitada, a entrada correspondente não entrará em vigor embora exista.)
- 6. Add to List:** Clique para adicionar a regra atual na lista de regras.
- 7. OK:** Clique para salvar suas configurações.

**Por exemplo:**

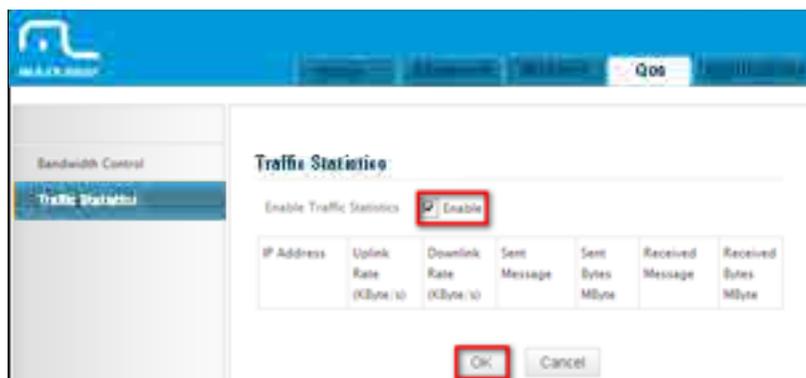
Se você estiver compartilhando uma conexão de banda larga 4M com um vizinho que sempre esgota os recursos de download de dados da banda larga, esse recurso vai ajudar.

Basta especificar a metade da banda larga 4M para o computador do seu vizinho (por exemplo 192.168.0.100) e você não terá mais necessidade de lutar por uma banda larga e seu vizinho terá uma banda larga de até 2M. Para fazer isso, siga as instruções abaixo:

1. Selecione Enable.
2. Digite "192.168.0.100" em ambas as caixas de endereço de IP.
3. Selecione Download.
4. Digite "256" em ambos os campos de variação da banda larga.
5. Selecione Enable.
6. Clique em Add To List
7. Clique em OK.

**3.2 Estatísticas de tráfego**

Estatísticas de Tráfego permite ver rapidamente a quantidade de tráfego que cada aparelho em sua rede está usando.



**1. Enable Traffic Statistics:** Marque / desmarque a caixa para ativar / desativar o recurso de estatísticas de tráfego. Para ver rapidamente a quantidade de tráfego que cada aparelho em sua rede está usando, habilite esta opção. No entanto, geralmente desativá-lo pode aumentar o desempenho da rede. Essa opção é desativada pelo padrão. No entanto, uma vez que é ativada, a página é atualizada a cada cinco minutos.

**2. OK:** Clique para ativar as configurações correspondentes.

**IP Address:** Mostra os endereços do IP dos computadores conectados ao dispositivo.

**Uplink Rate:** Mostra a velocidade de upload (KByte/s) do computador correspondente.

**Downlink Rate:** mostra a velocidade de download (KByte/s) do computador correspondente.

**Sent Message:** Mostra o número de pacotes enviados pelo computador correspondente através do dispositivo desde que Estatísticas foi habilitado.

**Sent Bytes:** Mostra o número de bytes enviados pelo computador correspondente através do dispositivo desde que Estatísticas foi habilitado. A unidade é MByte.

**Received Message:** Mostra o número de pacotes recebidos pelo computador correspondente através do dispositivo desde que Estatísticas foi habilitado.

**Received Bytes:** Mostra o número de bytes recebidos pelo computador correspondente através do dispositivo desde que Estatísticas foi habilitado. A unidade é MByte.

## 4 Aplicativos especiais

### 4.1 Redirecionamento de portas



O redirecionamento de portas é útil para servidores web, servidores FTP, servidores de e-mail, jogos e outros aplicativos de Internet especializados. Quando você habilita o redirecionamento de portas, os pedidos de comunicação da Internet para a porta WAN do seu roteador serão encaminhados para o endereço de IP LAN especificado. Como pode ser visto na figura acima, para deixar o PC3 acessar o serviço de portas no PC1, você deve primeiro definir as configurações de redirecionamento de porta no roteador em que o PC1 está conectado



1. **Start/End Port:** Especifique um intervalo de portas entre 1 ~ 65535 (para uma única porta, digite o número da porta em ambos os campos Start e End, por exemplo, 21 para FTP). Contate o fornecedor do serviço correspondente, se você não souber o número da porta do serviço para usar.
2. **LAN IP:** Especifique o endereço de IP do host interno. Certifique-se de designar estaticamente o endereço de IP do host para fazer esta função constante.
3. **Protocol:** Especifique o protocolo necessário para o serviço utilizando a(s) porta(s).
4. **Enable:** Marque para ativar as configurações atuais.
5. **OK:** clique para salvar as suas configurações.

Agora, seus amigos só precisam digitar ftp://xxx.xxx.xxx.xxx:21 em seus navegadores para acessar o seu servidor FTP xxx.xxx.xxx.xxx, é o endereço de IP WAN do roteador. Assumindo que é 172.16.102.89, então, seus amigos precisam digitar ftp://172.16.102.89:21 em seus navegadores.

**Por exemplo:** Você quer compartilhar alguns arquivos grandes com seus amigos que não estão em sua LAN, no entanto, não é conveniente transferir arquivos tão grandes como esses em toda a rede. Então, você pode configurar seu próprio computador como um servidor FTP e usar o recurso de redirecionamento de (intervalo de) porta para deixar que seus amigos acessem esses arquivos. Supondo-se que o endereço de IP estático do servidor de FTP (ou seja, o seu computador) seja 192.168.0.10, e que você queira que os seus amigos acessem esse servidor FTP através da porta padrão de 21 usando o protocolo TCP, faça o seguinte:

1. **Start/End Port:** Digite 21 em ambos os campos, Start Port e End Port.
2. **LAN IP:** Digite 192.168.0.10
3. **Protocol:** Selecione TCP.
4. **Enable:** marque para habilitar as configurações atuais.
5. **OK:** clique para ativar as suas configurações.



**Nota:** Se você incluir a porta 80 nesta seção, você deve definir a porta de gerenciamento remoto (interface web) para um número diferente de 80, como o 8080, caso contrário, o recurso de servidor virtual pode não terá efeito.

## 4.2 DMZ Host

A função DMZ (Zona desmilitarizada) desativa o firewall no roteador para um dispositivo para um serviço com finalidade especial, como jogos pela Internet ou videoconferência. Ativando o DMZ host você pode expor a sua rede local a possíveis ataques. Por isso, é aconselhável usá-lo com cautela.



**DMZ Host IP Address:** O endereço de IP do aparelho o qual o firewall do roteador será desativado. Certifique-se de configurar estaticamente o endereço de IP desse aparelho para que esta função seja consistente.

**Enable:** Marque/desmarque para habilitar/desabilitar o recurso de host DMZ.

**OK:** Clique para ativar as configurações.

**Nota:**

Uma vez ativado, o DMZ host perde a proteção do firewall do dispositivo e se torna vulnerável a ataques.

## 4.3 DDNS

DNS Dinâmico ou DDNS é um termo usado para a atualização em tempo real d Internet Domain Name System (DNS), nome de servidores. Nós usamos um endereço de IP numérico atribuído pelo provedor de serviços de Internet (ISP) para se conectar à Internet, o endereço pode ser tanto estável ("estático"), ou

pode mudar de uma sessão na Internet para a próxima ("dinâmico"). No entanto, um endereço numérico é difícil de lembrar, um endereço que muda de forma imprevisível faz com que a conexão seja impossível. O provedor de DDNS atribui um nome de host estático para o usuário; sempre que o usuário é atribuído um novo endereço de IP, esse fato é comunicado ao provedor DDNS pelo software executado em um computador ou dispositivo de rede naquele endereço, o provedor distribui a associação entre o nome do host e o endereço de servidores DNS da Internet para que eles possam resolver consultas DNS. Assim, o acesso ininterrupto aos serviços e dispositivos cujo endereço de IP numérico pode mudar é mantido. (Você precisa ter uma conta com um dos prestadores de serviços listados no primeiro menu suspenso).

The image shows a screenshot of a router's web interface for configuring DDNS. The interface has a blue header with the 'Applications' menu. On the left, there is a sidebar with navigation options: Port Range Forwarding, DMZ Host, DDNS (highlighted), UPnP Settings, Static Routing, and Routing Table. The main content area is titled 'DDNS' and contains the following fields:

- DDNS Service:** A radio button selection with 'Enable' selected and 'Disable' as an alternative.
- Service Provider:** A dropdown menu currently showing 'dyndns.org'.
- Username:** A text input field containing 'benda'.
- Password:** A text input field containing '123456'.
- Domain Name:** A text input field containing 'benda.dyndns.org'.

At the bottom of the form, there are two buttons: 'OK' and 'Cancel'.

**DDNS Service:** Selecione para ativar / desativar o recurso de DDNS.

**Service Provider:** Selecione seu provedor de serviço DDNS a partir do menu suspenso. (Aqui você pode ver uma lista de prestadores de serviços disponíveis. Note que os prestadores de serviços não listados aqui não estão disponíveis para uso.)

**User Name:** Digite o nome de usuário registrado.

**Password:** Digite a senha registrada.

**Domain Name:** Digite o nome de domínio que você deseja registrar, por exemplo, Multilaser.com.br

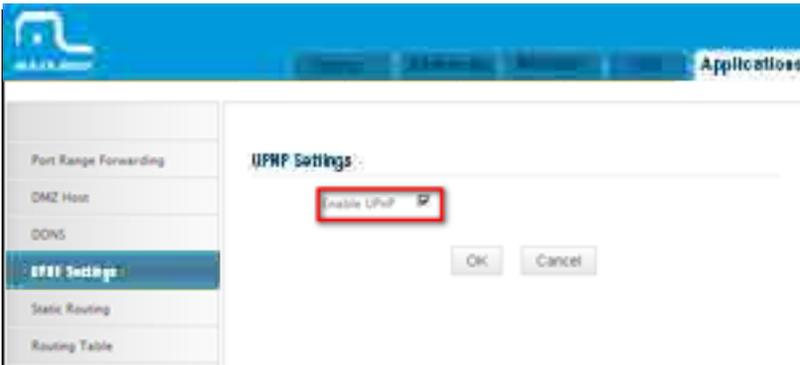
**OK:** Clique para ativar suas configurações.

**Nota:**

Este recurso geralmente é usado em conjunto com servidor virtual e está desativado pelo padrão. Configure as definições necessárias na interface de redirecionamento de porta e insira as informações fornecidas pelo seu provedor de serviço DDNS na tela DDNS. Outros podem acessar o seu servidor, basta digitar <http://Multilaser.com.br> em sua barra de endereços do navegador.

**4.4 UPnP**

O recurso Universal Plug and Play (UPnP) permite dispositivos de rede, tais como computadores de Internet, acessarem recursos no host local ou dispositivos, conforme necessário. Dispositivos habilitados para UPnP podem ser descobertos automaticamente pelo aplicativo de serviço UPnP na LAN. Esse recurso é ativado pelo padrão. Nenhuma configuração é necessária.



**Enable UPnP:** Marque/desmarque para habilitar/desabilitar o recurso UPnP.

**OK:** Clique para completar suas configurações.

**4.5 Roteamento estático**

Quando existem vários roteadores na rede, você pode querer configurar o roteamento estático. O roteamento estático determina o caminho dos dados na sua rede. Você pode usar este recurso para permitir que usuários em diferentes domínios de IP acessem a Internet através deste dispositivo. Não é recomendado usar essa configuração, a menos que você esteja familiarizado com o roteamento estático. Na maioria dos casos, é recomendado o roteamento dinâmico, pois este recurso permite que o roteador detecte as mudanças físicas da estrutura da rede automaticamente. Se você quiser usar o roteamento estático, certifique-se da função de DHCP do roteador está desativada.

The screenshot shows the 'Static Routing' configuration page. On the left is a sidebar with navigation options: Port Range Forwarding, DMZ Host, DDNS, UPNP Settings, Static Routing (selected), and Routing Table. The main area is titled 'Static Routing' and contains a table for adding routes. The table has three columns: 'Destination Network IP Address', 'Subnet Mask', and 'Gateway'. The first row shows the values '192.168.88.0', '255.255.255.0', and '192.168.10.2' respectively, with an 'Add' button to the right. Below this is a summary row with the same values and a 'Delete' button. At the bottom, there are 'OK' and 'Cancel' buttons.

Destination Network IP Address	Subnet Mask	Gateway	
192.168.88.0	255.255.255.0	192.168.10.2	Add
192.168.88.0	255.255.255.0	192.168.10.2	Delete

OK Cancel

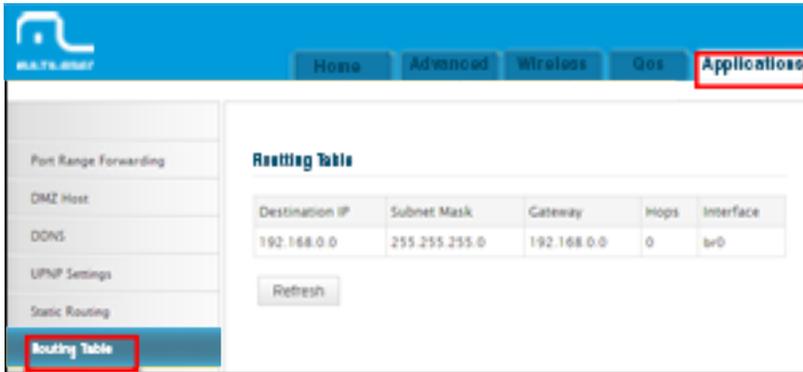
- 1. Destination Network IP Address:** Especifique um único endereço de IP, por exemplo, 172.17.0.100, ou um segmento IP net., por exemplo, 192.168.88.0.
- 2. Subnet Mask:** Especificar uma máscara de sub-rede que corresponde ao IP de destino especificado.
- 3. Gateway:** Especifique o endereço de IP para o próximo hop.
- 4. OK:** Clique para ativar suas configurações.

#### Nota:

1. O gateway deve estar no mesmo segmento do IP net, como o endereço de IP LAN / WAN do dispositivo.
2. A máscara de sub-rede deve ser inserida 255.255.255.255 se o endereço de IP de destino é um host.
3. Máscara de sub-rede deve ser inserida de acordo, se o endereço de IP de destino representa um segmento de rede IP. Ele deve corresponder ao endereço de IP especificado. Por exemplo, para o endereço de IP de 10.0.0.0, você pode inserir uma máscara de sub-rede de 255.0.0.0.

## 4.6 Tabela de roteamento

Esta página exibe a tabela de roteamento central do dispositivo que lista IP de destino, máscara de sub-rede, gateway, hop count e interface.



The screenshot shows the router's web interface. At the top, there is a navigation menu with buttons for 'Home', 'Advanced', 'Wireless', 'QoS', and 'Applications'. The 'Applications' button is highlighted with a red box. On the left side, there is a sidebar menu with options: 'Port Range Forwarding', 'DMZ Host', 'DDNS', 'UPnP Settings', 'Static Routing', and 'Routing Table'. The 'Routing Table' option is also highlighted with a red box. The main content area displays the 'Routing Table' with the following data:

Destination IP	Subnet Mask	Gateway	Hops	Interface
192.168.0.0	255.255.255.0	192.168.0.0	0	br0

Below the table is a 'Refresh' button.

A principal tarefa para um roteador é procurar um caminho de transferência ideal para cada pacote de dados passando por ele, e transferi-lo para o destino especificado. Para completar este trabalho, as lojas do roteador mantêm dados relacionados de vários caminhos de transferência, estabelecendo uma tabela de roteamento, para futura seleção de rota.

## 5 Segurança

### 5.1 Filtro URL

Para melhor controlar a LAN do computadores, você pode usar a funcionalidade do filtro URL para permitir ou não tais computadores a acessarem determinados sites dentro de um intervalo de tempo especificado.

The screenshot displays the 'URL Filter Settings' page. The left sidebar contains navigation options: 'URL Filter Settings' (selected), 'MAC Address Filter Settings', and 'Client Filter Settings'. The main content area is titled 'URL Filter Settings' and contains the following fields:

- Filter Mode:** A dropdown menu set to 'Forbidden Only' (1).
- Access Policy:** A dropdown menu set to '(1)' (2).
- Policy Name (Optional):** A text input field containing 'baidu' (3).
- Start IP:** A text input field containing '192.168.0.192' (4).
- End IP:** A text input field containing '192.168.0.192' (4).
- URL Character String:** A text input field containing 'baidu' (5).
- Time:** A time selection interface set to '0:00:00:00' (6).
- Device:** A dropdown menu set to 'Sun - Sat'.
- Enable:** A checked checkbox.
- Buttons:** 'Clear this item', 'Clear', 'OK', and 'Cancel'.

- 1. Filter Mode:** Selecione um modo de filtro adequado, por exemplo, Proibir Only.
- 2. Access Policy:** Selecione um número de políticas de acesso, por exemplo, 1, a partir da lista suspensa.
- 3. Policy Name:** Descreva sucintamente a regra atual, por exemplo, o Baidu, (Ele consiste apenas em números, letras ou sublinhado).
- 4. Start IP/End IP:** Digite o mesmo endereço de IP ou dois endereços de IP diferentes em ambas as caixas para especificar um único computador ou um intervalo de computadores para que a regra atual seja aplicada.
- 5. URL Character String:** digite o nome do domínio que você deseja filtrar, por exemplo, o Baidu.
- 6. Time:** Especifique um período de tempo para uma regra atual entrar em vigor. Se o campo é definido como 0:00-00:00, a regra será aplicada 24 horas por dia.

7. **Day(s):** Escolha um dia ou vários dias para uma regra atual entrar em vigor. Se a Sun-Sat é selecionada, a regra será aplicada 7 dias por semana.
8. **Enable:** Marque/desmarque para habilitar/desabilitar o recurso.
9. **OK:** Clique para ativar as configurações.

**Exemplo:**

Se você quiser impedir que todos os computadores em sua LAN acessem o youtube.com das 8:00-18:00 durante os dias úteis: de segunda a sexta-feira, então siga as instruções:

1. **Filter Mode:** Selecione Forbid Only.
2. **Access Policy:** Selecione um número de políticas de acesso, por exemplo, 1, a partir da lista suspensa.
3. **Policy Name:** Descreva sucintamente a regra atual, por exemplo, o Baidu, (Ele consiste apenas em números, letras ou sublinhado).
4. **Start IP/End IP:** Digite 2-254.
5. **URL Character String:** Digite baidu.
6. **Time: Selecione 8:00-18:00.Dia(s):** Selecione Monday to Friday.
7. **Enable:** Marque a caixa Enable.
8. **OK:** clique para salvar suas configurações.

**Nota:** Cada regra só pode incluir um nome de domínio. Basta adicionar mais regras conforme o seu desejo de filtrar vários nomes de domínio.

## 5.2 Filtro MAC

Esta seção permite que você defina os tempos específicos, clientes podem ou não acessar a Internet através de endereços MAC dos dispositivos.

**Forbid Only:** Especifique uma lista de aparelhos proibidos de acessar a Internet. Todos os outros aparelhos não listados como Forbidden serão permitidos.

**Permit Only:** Especifique uma lista de aparelhos permitidos a acessar a Internet. Todos os outros aparelhos não listados como Permit serão proibidos.

The screenshot shows the 'MAC Address Filter Settings' page. The fields are as follows:

- Filter Mode: Forbidden Only
- Access Policy: 1
- Policy Name(Optional): 1
- MAC Address: 04 57 65 4F 57 0E
- Time: 0 0 0 0
- Day(s): Sun - Sat
- Enable:
- Clear this item: Clear
- OK: [Highlighted]
- Cancel

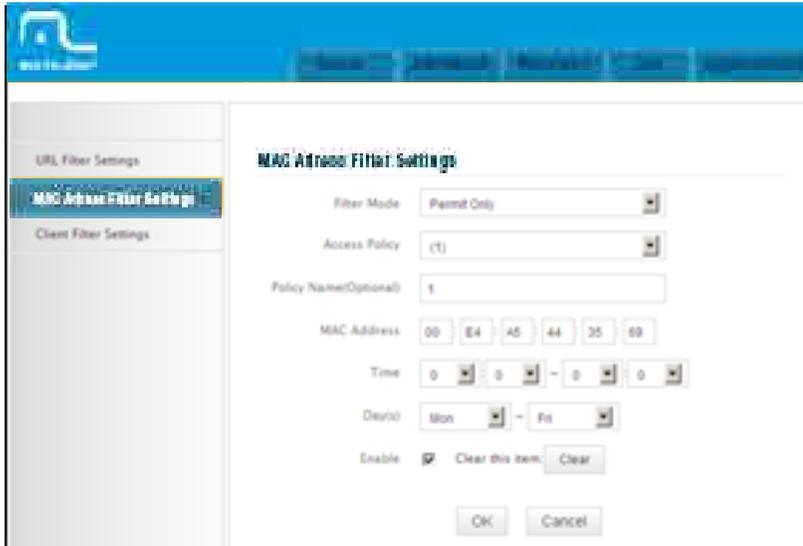
1. **Filter Mode:** Selecione um modo de filtro adequado, por exemplo, Proibir Only.
2. **Access Policy:** Selecione um número de políticas de acesso, por exemplo, 1, a partir da lista suspensa.
3. **Policy Name:** Descreva sucintamente a regra atual (consiste apenas em números, letras ou sublinhado).
4. **MAC Address:** Especifique um endereço MAC para uma regra de filtro correspondente MAC a ser aplicada.
5. **Time:** Especifique um período de tempo para uma regra atual entrar em vigor. Se o campo é definido como 0:00-00:00, a regra será aplicada 24 horas por dia.
6. **Day(s):** Escolha um dia ou vários dias para uma regra atual entrar em vigor. Se a Sun-Sat é selecionada, a regra será aplicada 7 dias por semana.
7. **Enable:** Marque/desmarque para habilitar/desabilitar o recurso.
8. **OK:** Clique para ativar as configurações.

### Por Exemplo:

Para permitir que um computador no endereço MAC 00: E4: A5: 44:35:69 acesse à internet de segunda-feira a sexta-feira.

- a) **Filter Mode:** Selecione **Permit Only**.
- b) **Access Policy:** Selecione um número de políticas de acesso, por exemplo, 1, a partir da lista suspensa.
- c) **Policy Name:** Descreva sucintamente a regra atual, por exemplo, Policy Name (consiste apenas em números, letras ou sublinhado).

- d) **MAC Address:** Digite 00:E4:A5:44:35:69.
- e) **Time:** Selecione 0 em todos os campos para aplicar a regra 24 horas por dia.
- f) **Day(s):** Selecione Monday to Friday.
- g) **Enable:** Marque a caixa Enable.
- h) **OK:** Clique para salvar as suas configurações.



The screenshot shows the 'MAC Address Filter Settings' page. The left sidebar contains navigation options: 'URL Filter Settings', 'MAC Address Filter Settings' (highlighted), and 'Client Filter Settings'. The main content area is titled 'MAC Address Filter Settings' and contains the following fields:

- Filter Mode:** A dropdown menu set to 'Permit Only'.
- Access Policy:** A dropdown menu set to '(1)'.
- Policy Name(Optional):** A text input field containing '1'.
- MAC Address:** A series of six input boxes containing '00', 'E4', 'A5', '44', '35', and '69' respectively.
- Time:** A series of six dropdown menus, all set to '0', representing hours and minutes.
- Day(s):** Two dropdown menus set to 'Mon' and 'Fri'.
- Enable:** A checked checkbox with a 'Clear this item' button next to it.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

## 5.3 Filtro do cliente

Esta seção permite que você defina os tempos específicos, clientes podem ou não podem acessar a Internet através de endereços de IP atribuídos dos dispositivos e porta de serviço.

**Forbid Only:** Somente computadores listados como Forbidden serão proibidos de acessar serviços especificados, outros não serão limitados;

**Permit Only:** Somente computadores listados como Permitted serão permitidos a acessar serviços especificados, outros serão proibidos;

1- **Filter Mode:** Selecione Permit Only.

2- **Access Policy:** Selecione um número de políticas de acesso, por exemplo, 1, a partir da lista suspensa

3- **Policy Name:** Descreva sucintamente a regra atual, por exemplo, 80.

4- **Start IP/End IP:** Digite o mesmo endereço de IP, por exemplo, 110, ou 2 endereços de IP diferentes, por exemplo, 110 e 120 em ambas as caixas para especificar um único computador ou um intervalo de computadores para a regra atual ser aplicada.

5- **Port:** Especifique o protocolo TCP / UDP do número da porta, por exemplo, 80.

6- **Type:** Selecione Both.

7- **Time:** Especifique um período de tempo para uma regra atual entrar em vigor. Se o campo é definido como 0:00-00:00, a regra será aplicada 24 horas por dia.

**8- Day(s):** Especifique um dia ou vários dias para uma regra atual para entrar em vigor.

**9- Enable:** Marque/desmarque para habilitar/desabilitar o recurso.

**10- OK:** clique para ativar as suas configurações

### Por exemplo:

Se você quer proibir computadores dentro do intervalo de endereços de IP 192.168.0.100 - 192.168.0.120 de acessar Internet, siga as instruções:



1. **Filter Mode:** Selecione Forbid Only.

2. **Access Policy:** Selecione um número de políticas de acesso, por exemplo, 1, a partir da lista suspensa.

3. **Policy Name:** Descreva sucintamente a regra atual, por exemplo, 123.

4. **Start IP:** Digite 100.

5. **End IP:** Digite 120.

6. **Port:** Digite 1-65535 para proibir todos os serviços e aplicativos da Internet.

7. **Type (or Protocol):** Selecione Both.

8. **Time:** Selecione 0 para todos os campos para aplicar a regra 24 horas por dia.

9. **Day(s):** Selecione Sun-Sat para aplicar a regra 7 dias por semana

10. **Enable:** Marque a caixa Enable

11. **OK:** Clique para ativar as suas configurações.

## 6 Ferramentas

### 6.1 Reiniciar

Reinicie o dispositivo para ativar suas configurações A conexão WAN será desligada durante a esse processo.



### 6.2 Restaurar para configurações de fábrica

Clique no botão Restaurar para padrão de fábrica para redefinir as configurações do padrão de fábrica no dispositivo. Você precisa reconfigurar o dispositivo para acessar a Internet, bem como muitas outras configurações, incluindo as configurações do wireless.



As configurações padrão de fábrica são listados abaixo:

IP Address: 192.168.0.1

Subnet mask: 255.255.255.0.

**Nota:**

Para ativar as suas configurações, você precisa reiniciar o dispositivo após ser redefinido.

**6.3 Backup/ Restaurar**

**Backup:** Uma vez configurado o dispositivo da maneira que você desejar, você pode salvar essas configurações em um arquivo de configuração em seu disco rígido local que, mais tarde, podem ser importados para o dispositivo no caso do dispositivo ser restaurado para as configurações padrão de fábrica. Para isso, siga as instruções:

1. Clique no botão **Backup** e especifique um diretório para salvar as configurações no seu disco rígido local.

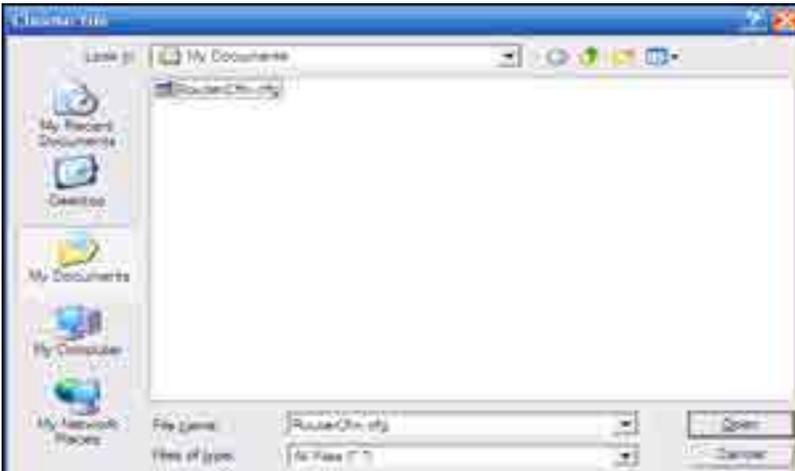


2. Clique em OK para salvar as configurações na pasta.



## Para restaurar as configurações anteriores, siga as instruções:

3. Clique no botão **Browse** para localizar e selecionar um arquivo de configuração que foi salvo anteriormente no disco rígido local.

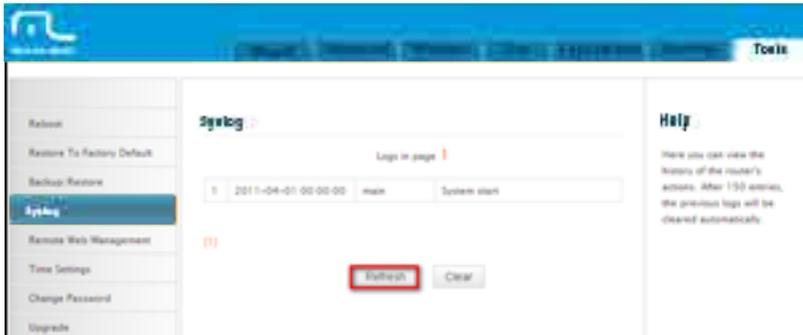


Clique no botão **Restore** para redefinir o dispositivo às configurações anteriores.



## 6.4 Syslog

Aqui você pode ver o histórico das ações do dispositivo. Depois de 150 entradas, os primeiros registros serão automaticamente apagados.



## 6.5 Gerenciamento remoto baseado na web

O gerenciamento remoto permite que o dispositivo seja configurado e gerenciado remotamente pela Internet através de um navegador.



1. **Enable:** Marque/desmarque para habilitar/desabilitar o recurso de host DMZ.
1. **Port:** Esta é a porta de gerenciamento a ser aberta para acesso externo. A configuração padrão é 8080. NÃO a altere, a menos que indicado pelo seu ISP.
2. **IP Address:** Aqui você pode especificar o intervalo de endereços de IP para gerenciamento remoto (quando configurado para 0.0.0.0, o dispositivo torna-se acessível remotamente para todos os computadores na Internet ou a outras redes externas).

### 3. OK: Clique para ativar suas configurações.

#### Nota:

1. Para acessar o dispositivo através da porta 8080, digite "http://xxx:8080" onde "xxx" representa o endereço de IP de Internet do dispositivo e 8080 é a porta de admin. remota. Assumindo que o endereço de IP de Internet do dispositivo é 220.135.211.56, então basta substituir o "xxx" com "220.135.211.56" (ou seja, http://220.135.211.56:8080).

2. Deixar o campo do endereço de IP em "0.0.0.0" faz com que o dispositivo seja remotamente acessível a todos os computadores na Internet ou a outras redes externas; preenchê-lo com um endereço de IP específico, por exemplo, 218.88.93.33, faz com que o dispositivo seja acessível remotamente apenas ao computador no endereço de IP especificado).

## 6.6 Hora

Esta página é utilizada para definir o horário do sistema do roteador. Você pode optar por definir a hora manualmente ou obter o horário GMT da Internet, o sistema será automaticamente conectado ao servidor NTP para sincronizar o horário.



#### Nota:

As informações de configuração do horário e data serão perdidas quando o dispositivo for desconectado da fonte de alimentação. No entanto, ele será atualizado automaticamente quando o dispositivo se reconectar à Internet. Para ativar os recursos baseados em tempo (por exemplo, firewall), primeiro as informações de hora e a data devem ser definidas corretamente, manual ou automaticamente.

## 6.7 Senha

Esta seção permite que você altere a senha de login para acessar a interface Web do dispositivo para maior segurança.

The screenshot shows the 'Change Password' web interface. The page has a blue header with the Multilaser logo and navigation tabs. A left sidebar contains menu items like 'Reboot', 'Restore To Factory Default', 'Backup/Restore', 'Firmware', 'Remote Web Management', 'Time Settings', 'Setup/Factory Default', and 'Upgrade'. The main content area is titled 'Change Password' and includes the text 'Administrator Login (Credentials)' and a red warning 'Password must be alpha-numeric'. There are three input fields: 'Old Password' (containing '\*\*\*\*'), 'New Password' (containing '12345'), and 'Confirm New Password' (containing '12345'). Below the fields are 'OK' and 'Cancel' buttons. A 'Help' section on the right explains the password requirements and provides the default password 'admin'.

1. **New Password:** Digite uma nova senha, por exemplo, 12345 (Note que a senha só pode ser alfanumérica).
2. **Confirm New Password:** Digite novamente a nova senha para confirmação.
3. **OK:** Clique para ativar suas configurações.

### Nota:

Para fins de segurança, é altamente recomendável que você altere a senha de login padrão do dispositivo.

## 6.8 Atualização do Firmware

Atualização do firmware é liberada periodicamente para melhorar a funcionalidade do seu dispositivo e também para adicionar novas funcionalidades. Se você tiver um problema com um recurso específico do dispositivo, acesse o nosso site ([www.Multilaser.com.br](http://www.Multilaser.com.br)) para fazer o download do firmware mais recente e atualizar o seu dispositivo.



1. **Browse:** Clique para localizar e selecionar o firmware.
2. **Upgrade (ou Update):** Clique para atualizar o firmware. O dispositivo será reiniciado automaticamente quando a atualização for concluída.

**Nota:**

1. Antes de atualizar o firmware, certifique-se de que você tenha um firmware correto. Um firmware errado pode danificar o dispositivo.
2. NÃO faça a atualização do firmware sem fio ou desconecte o dispositivo da fonte de alimentação enquanto a atualização de firmware está em andamento. Note que você precisa atualizar o firmware do dispositivo através de uma conexão com fio.

## Anexo 1 Glossário

### Canal

Um canal de comunicação, também conhecido como canal, refere-se tanto a um meio de transmissão físico, um fio, como a uma ligação lógica ao longo de um meio multiplexado, um canal de rádio. Ele é utilizado para transferir um sinal de informação, tal como um streaming de bits digital, a partir de um ou mais transmissores para um ou mais receptores. Se houver apenas um AP no intervalo, selecione o canal que você desejar. O padrão é **Automático**.

Se houver vários APs que coexistem na mesma área, é aconselhável que você selecione um canal diferente para cada AP operar, minimizando a interferência entre APs vizinhos. Por exemplo, se três APs americanos padrão coexistir em uma área, você pode definir seus canais, respectivamente como 1, 6 e 11, para evitar interferência mútua.

### SSID

Service Set Identifier (SSID) é usado para identificar um determinado 802.11 LAN wireless. É o nome de uma rede sem fio específica. Para deixar o seu adaptador de rede sem fio passar entre diferentes APs, você deve definir o SSID de todos os APs com o mesmo nome.

### 1WPA/WPA 2

O protocolo WPA implementa a maior parte da norma IEEE 802,11i. Ele aumenta a criptografia de dados através do Temporal Key Integrity Protocol (TKIP), que é uma chave de 128 bits por pacote, o que significa que gera dinamicamente uma nova chave para cada pacote. WPA também inclui um recurso de verificação de integridade da mensagem para evitar que os pacotes de dados sejam prejudicados. Somente usuários de rede autorizados podem acessar a rede sem fio. O protocolo posterior do dispositivo WPA2 está em conformidade com a norma IEEE 802.11i e usa Advanced Encryption Standard (AES) além do protocolo de criptografia TKIP para garantir uma melhor segurança do que o fornecido pelo WEP ou WPA. Atualmente, o WPA é suportado pelo Windows XP SP1.

## Autenticação IEEE 802.1X

Autenticação IEEE 802.1X é um padrão IEEE para Network Access Control com base em porta (PNAC). Ela faz parte do grupo IEEE 802,1 dos protocolos de rede. Ele fornece um mecanismo de autenticação para dispositivos que desejam anexar a uma LAN ou WLAN. IEEE 802.1X, define o encapsulamento de EAP sobre LAN ou EAPOL. A autenticação 802.1X envolve três partes: um requerente, um autenticador, e um servidor de autenticação. O requerente é um dispositivo do cliente (como um laptop) que deseja se anexar à LAN / WLAN - embora o termo 'requerente' também é usado de forma intercambiável para se referir ao software em execução no cliente que fornece credenciais para o autenticador. O autenticador é um dispositivo de rede, como um Ethernet switch ou ponto de acesso sem fio, e o servidor de autenticação é tipicamente um software host que está em execução apoiando os protocolos RADIUS e EAP. O autenticador age como um guarda de segurança para uma rede protegida. O requerente (ou seja, dispositivo do cliente) não tem acesso permitido através do autenticador para proteger o lado da rede até que a identidade do requerente seja validada e autorizada. Com a autenticação baseada em portas 802.1X, o requerente fornece credenciais, como nome de usuário / senha ou certificado digital, para o autenticador e o autenticador encaminha as credenciais para o servidor de autenticação para verificação. Se o servidor de autenticação determina que as credenciais são válidas, o requerente (dispositivo do cliente) tem permissão para acessar recursos localizados no lado protegido da rede.

## PPOE

O Protocolo Point-to-Point over Ethernet (PPPoE) é um protocolo de rede para encapsular quadros PPP dentro de Ethernet frames. O protocolo integrado PPP implementa a autenticação, criptografia e funções de compressão que o Ethernet tradicional não pode oferecer, também pode ser usado no modem a cabo, digital subscriber line (DSL) e Ethernet que fornecem serviço de acesso para os usuários. Essencialmente, é um protocolo que permite estabelecer um túnel ponto a ponto entre duas interfaces Ethernet dentro de um domínio de broadcast Ethernet.

## DNS

O Domain Name System (DNS) é um sistema de nomeação hierárquico distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou a uma rede privada. Ele associa várias informações com nomes de domínio atribuídos a cada uma das entidades participantes. Um Domain Name Service resolve consultas para esses nomes em endereços de IP para fins de localização de computadores de serviços e dispositivos em todo o mundo. Uma analogia frequentemente usada para explicar o Domain Name System é que ele serve como a lista telefônica da Internet, traduzindo nomes de host humanos amigáveis de computador em endereços de IP.

## WDS

Um wireless distribution system (WDS) é um sistema que permite a interligação sem fio de pontos de acesso em uma rede IEEE 802.11. Ele permite que uma rede sem fio seja expandida usando vários pontos de acesso, sem a exigência tradicional de um backbone com fio para ligá-los. Todas as estações base em um sistema de distribuição sem fio devem ser configuradas para usar o mesmo canal de rádio, o método de criptografia (nenhuma, WEP ou WPA) e as mesmas chaves de criptografia. Eles podem ser configurados a diferentes serviços de conjunto de identificadores. WDS também exige que cada estação base seja configurada para encaminhar a outros no sistema. O WDS também pode ser considerado um modo repetidor porque parece transpor e aceitar clientes sem fio ao mesmo tempo (ao contrário da ponte tradicional). O WDS pode ser incompatível entre diferentes produtos (mesmo ocasionalmente do mesmo fornecedor) uma vez que não é certificada pela Wi-Fi Alliance. WDS pode fornecer dois modos de conectividade AP-to-AP sem fio:

Ponte sem fio, em que APs WDS se comunicam somente uns com os outros e não permitem que os clientes ou estações sem fio (STA) os acessem.

Repetição sem fio, em que os APs se comunicam uns com os outros e com STAs sem fios.

## DMZ

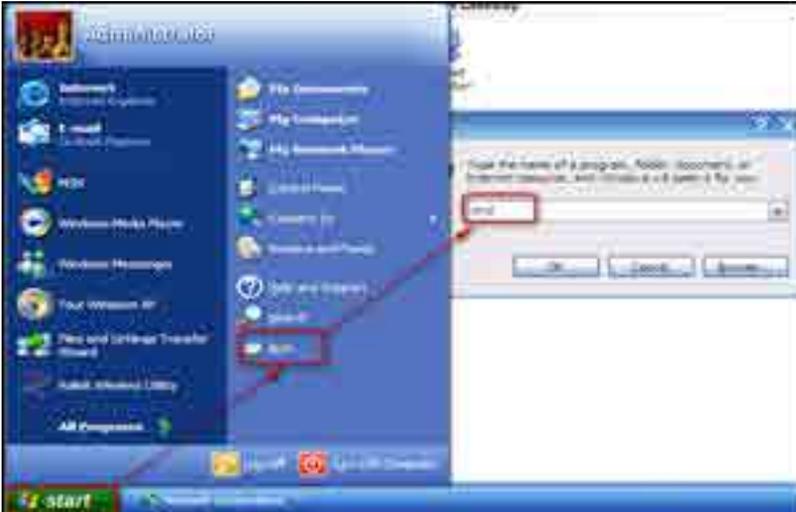
Na segurança do computador, um DMZ (algumas vezes referido como um perímetro de rede) é uma sub-rede física ou lógica que contém e expõe uma organização de serviços externos protegidos a uma rede maior não confiável, geralmente a Internet. A finalidade de um DMZ é adicionar uma camada extra de segurança para rede local de uma organização (LAN); um atacante externo só tem acesso ao equipamento pela DMZ, ao invés de ter acesso a qualquer outra parte da rede. Hosts na DMZ limitaram a conectividade para hosts específicos na rede interna, embora a comunicação com outros hosts na DMZ e para a rede externa seja permitido. Isso permite que os hosts na DMZ forneçam serviços tanto para a rede interna como externa, enquanto um firewall de intervenção controla o tráfego entre os servidores DMZ e os clientes da rede interna. Quaisquer serviços como servidores web, servidores de email, servidores de FTP, servidores de VoIP e etc, que estão sendo fornecidos a usuários na rede externa podem ser colocados na DMZ.

## Anexo 2 Verifique a conexão WDS

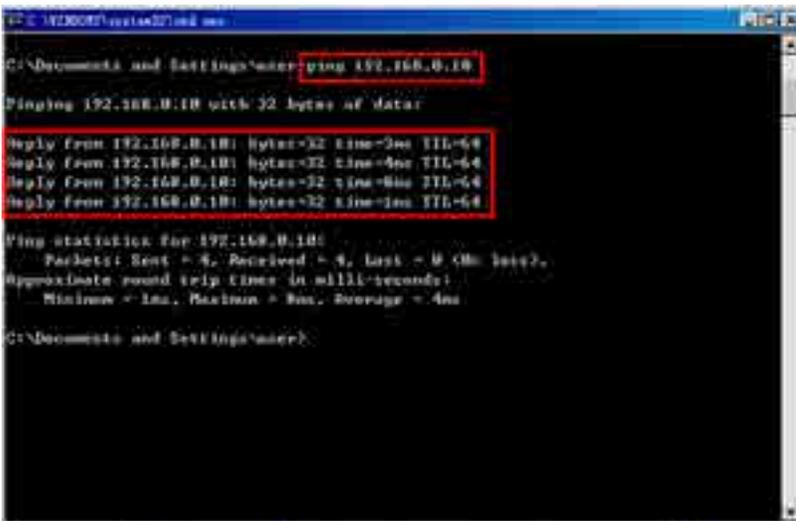


## Configure PC2:

Clique em **Start> Run (Iniciar>Executar)** no PC3, digite cmd na janela que aparece e clique em OK.

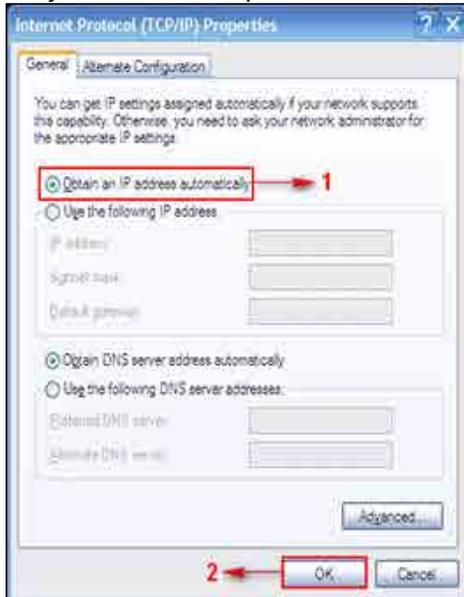


Digite **ping 192.168.0.1** e aperte **Enter**.

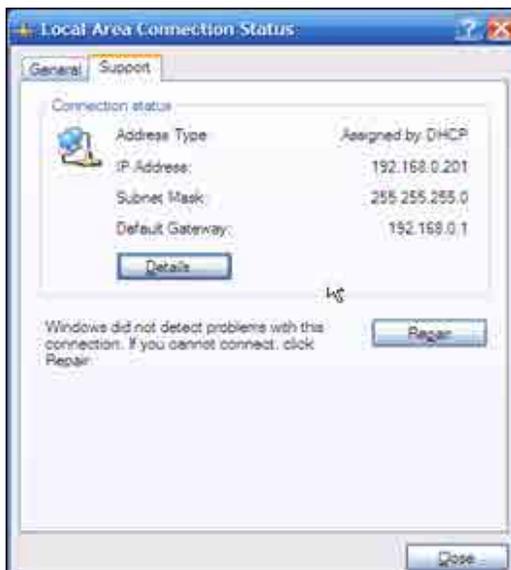


## Configure PC3 e PC 4:

1. Ajuste PC3 e PC4 para obter um endereço de IP automaticamente.



2. Quando os dois computadores obtiverem endereços de IP, tente as instruções abaixo para verificar a conexão WDS:



3. Clique em **Start> Run (Iniciar>Executar)** no PC3, digite **cmd** na janela que aparece e clique em **OK**.



4. Digite **ping 192.168.0.1** e aperte **Enter**. Se uma tela como a que você vê abaixo aparecer, você implementou com sucesso o WDS.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=4ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms
  
```

### Nota:

1. O recurso WDS só pode ser implementado entre dois dispositivos sem fios WDS capazes. Além disso, o SSID, canal, configurações de segurança e chave de segurança devem ser exatamente o mesmo em ambos os dispositivos.
2. Para garantir uma conexão sem fio adequada, não altere as configurações dos dois aparelhos após o WDS ser implementado com sucesso.

## Anexo 3 FAQs

Esta seção fornece soluções para problemas que podem ocorrer durante a instalação e funcionamento do dispositivo. Leia as instruções a seguir se você estiver com problemas. Se o seu problema não é abordado aqui, sinta-se livre para acessar [www.multilaser.com.br](http://www.multilaser.com.br) para encontrar uma solução. Seremos mais do que satisfeitos em ajudá-lo com a maior rapidez possível.

### **1. P: Eu digitei o endereço LAN IP do dispositivo no navegador da web, mas não consegui acessar o utilitário. O que eu devo fazer?**

**a.** Verifique se o dispositivo está funcionando corretamente. O LED SYS deve piscar por alguns segundos depois do dispositivo ser ligado. Se não acender, então algumas falhas internas podem ter ocorrido.

**b.** Verifique a conectividade física, conferindo se o LED da porta correspondente está aceso. Se não estiver, tente um cabo diferente. Note que uma luz acesa NEM SEMPRE indica uma conexão com sucesso.

**c.** Execute o comando "ping 192.168.0.1". Se você receber respostas de 192.168.0.1, abra o navegador e verifique se o servidor Proxy está desativado. No caso do ping falhar, pressione e segure o botão "RESET" no seu dispositivo por 7 segundos para restaurar as configurações padrão de fábrica, e depois execute o "ping 192.168.0.1" novamente.

**d.** Contate o nosso suporte técnico para ajudar se o problema persistir depois de ter tentado todos os passos acima.

### **2. P: O que eu devo fazer se esquecer da senha de login do meu dispositivo?**

R: Redefina o seu dispositivo pressionando o botão Reset por mais de 7 segundos.

**Nota:** Todas as configurações serão apagadas e restauradas aos padrões de fábrica, uma vez que você apertou o botão Reset.

### **3. P: Meu computador mostra um erro de conflito de endereço de IP, depois de ter conectado ao dispositivo. O que eu devo fazer?**

**a.** Verifique se existem outros servidores DHCP presentes em seu LAN. Se houver outros servidores DHCP além do seu roteador, desative-os imediatamente.

**b.** O endereço de IP padrão do dispositivo é 192.168.0.1, certifique-se este endereço não é usado por outro computador ou aparelho. No caso de dois computadores ou aparelhos compartilharem os mesmos endereços de IP, altere-os para um endereço diferente.

### **4.P: Não consigo acessar a Internet e enviar/receber e-mails, o que**

## Eu deveria fazer?

Este problema acontece principalmente para os usuários que utilizam o tipo de conexão a Internet PPPoE ou IP dinâmico. Você precisa mudar o tamanho da MTU (1492 pelo padrão). Neste caso, vá em "WAN Settings" para alterar o valor MTU do padrão 1480 para 1450 ou 1400, etc.

### 5. P: Como eu faço para compartilhar recursos no meu computador com os usuários da Internet através do dispositivo?

Para permitir que os usuários da Internet acessem os servidores internos na sua LAN, tais como servidor de e-mail, Web, FTP, através do dispositivo, utilize o recurso "Servidor Virtual".

Para fazer isso, siga as instruções abaixo:

Passo 1: Crie um servidor interno, certifique-se de que os usuários de LAN podem acessar esses servidores, e você precisa saber relacionar as portas dos serviços, por exemplo, o número da porta para o servidor Web é 80; FTP é 21; SMTP é 25 e POP3 é 110.

Passo 2: Digite Port Forwarding (também chamada Port Range Forwarding em alguns produtos) na tela do dispositivo web UI.

Passo 3: Complete os campos de Port Start (também chamado de External / Ext Port em alguns produtos) e o End Port (também conhecido como Internal / Int Port em alguns produtos), por exemplo, 80-80.

Passo 5: Digite o endereço de IP do servidor interno. Por exemplo, supondo que o endereço de IP do seu servidor Web é 192.168.0,10, basta inseri-lo.

Passo 6: Selecione um tipo de protocolo adequado: TCP, UDP, ou ambos, dependendo de qual protocolo(s) o seu host interno está usando.

Passo 7: Clique em Ativar e salvar as configurações.

Como referência, coletamos uma lista de algumas portas de serviço bem conhecidas, segue abaixo:

Servidor	Protocolo	Porta de serviço
Servidor Web	TCP	80
Servidor FTP	TCP	21
Telnet	TCP	23
Reunião de rede	TCP	1503, 1720

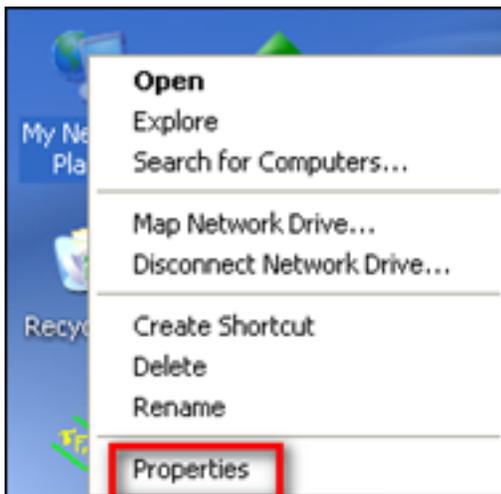
MSN Messenger	TCP/UDP	File Send:6891-6900(TCP) Voice: 1863, 6901(TCP) Voice: 1863, 5190(UDP)
PPTP VPN	TCP	1723
Iphone 5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110

## ANEXO 4 REMOVER REDE SEM FIO DO SEU COMPUTADOR

Se você alterar as configurações de wireless do seu dispositivo wireless, você também deve removê-las do seu computador, caso contrário, você pode não conseguir se conectar ao wireless do dispositivo. As instruções abaixo descrevem como remover uma rede sem fio do computador.

### Se você utilizar Windows XP, siga as instruções:

Clique em “My Network Places” (Meus locais de rede) e selecione “Properties” (Propriedades).



2. Clique em “Wireless Network Connection” (Conexão de rede sem fio) e depois selecione “Properties” (Propriedades).

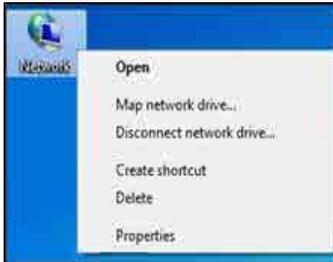


3. Clique em “Wireless Networks” (Redes sem fio), selecione o item abaixo “Preferred networks” (Redes Preferenciais) e depois clique no botão Remove (remover).



## Se você utilizar Windows 7, siga as instruções:

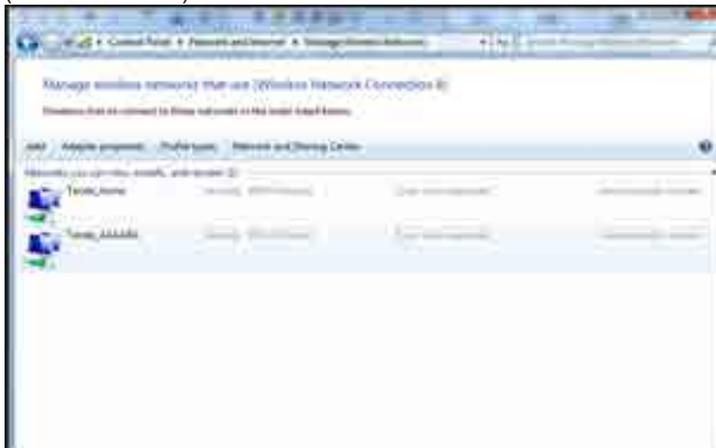
Clique em Network (Rede) na área de trabalho e selecione Properties (Propriedades).



### 2. Selecione “Manage Wireless Networks” (Gerenciar Redes sem fio).



### 3. Clique em wireless connection and depois selecione “Remove network” (Remover Rede)



## ANEXO 5 SEGURANÇA E EMISSÃO DA DECLARAÇÃO

### Aviso CE Mark

Este é um produto Classe B, em um ambiente doméstico este produto pode causar interferência de rádio, neste caso o usuário deverá tomar as medidas adequadas. Este aparelho está em conformidade com a EU 1999/5/EC.

### Declaração da FCC

Este dispositivo está em conformidade com a Parte 15 das regras da FCC. A operação está sujeita às seguintes duas condições: Este dispositivo não pode causar interferência prejudicial, e (2) este dispositivo deve aceitar qualquer interferência recebida, incluindo interferências que possam causar operação indesejada.

Este equipamento foi testado e está em conformidade com os limites para um dispositivo digital Classe B, conforme a Parte 15 das regras da FCC. Estes limites são criados para fornecer proteção razoável contra interferência prejudicial em uma instalação residencial. Este equipamento gera, usa e pode irradiar energia de rádio frequência e, se não for instalado e utilizado de acordo com as instruções, pode causar interferência prejudicial às comunicações de rádio. No entanto, não há garantia de que a interferência não ocorrerá em uma instalação específica. Se este equipamento causar interferência prejudicial à recepção de rádio ou televisão, o que pode ser determinado ligando e desligando o equipamento, o usuário é encorajado a tentar corrigir a interferência através de uma das seguintes medidas:

- Reorientar ou reposicionar a antena de recepção.
- Aumentar a distância entre o equipamento e o receptor.
- Ligar o equipamento a uma tomada de um circuito diferente daquele em que receptor está conectado.
- Consulte o revendedor ou um técnico de rádio / TV experiente para obter assistência.

**Aviso de FCC:** Quaisquer alterações ou modificações não aprovadas expressamente pela parte responsável pela conformidade podem anular a autoridade do usuário de operar este equipamento.

Este transmissor não deve ser colocalizado ou operado em conjunto com nenhuma outra antena ou transmissor.

O fabricante não é responsável por qualquer interferência de rádio ou TV causada por modificações não autorizadas neste equipamento.

### **Declaração de exposição à radiação**

Este equipamento cumpre os limites de exposição à radiação da FCC estabelecidos para um ambiente não controlado. Este equipamento deve ser instalado e operado com distância mínima de 20cm entre o radiador e o seu corpo.

#### **Nota:**

1. O fabricante não é responsável por qualquer interferência de rádio ou TV causada por modificações não autorizadas neste equipamento.
2. Para evitar interferência desnecessária a radiação, é recomendado o uso de um cabo RJ45 protegido.

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