

IEEE 802.11a/n A520N Wireless Outdoor CPE

Manual do Usuário



Direitos autorais

Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzido, adaptado, armazenado em sistemas de busca, traduzido para qualquer idioma, ou transmitido em qualquer forma ou meios sem uma permissão por escrito pelo fornecedor.

Sobre este manual

Este manual é destinado a orientar o instalador profissional para instalar o A520N Wireless Outdoor CPE como construir a infra-estrutura centrada nela. Ele inclui procedimentos para ajudá-lo a evitar problemas imprevistos.

Convenções

Requisitamos a sua atenção em partes importantes, caracteres especiais e os padrões usados neste manual:



Nota:

λ Indica uma nota importante que requer a sua atenção.



ATENÇÃO

λ Indica um aviso ou precaução que você precisa respeitar.

Negrito: Indica a função, palavras importantes, e assim por diante.

Comunicado de Interferência da Comissão Federal de Comunicação

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 projetados para fornecer proteção razoável contra interferência prejudicial em uma instalação residencial. Este equipamento utiliza e pode irradiar energia de radiofrequência e, se não for instalado e utilizado de acordo com as instruções, pode causar interferência prejudicial às comunicações via rádio. No entanto, não há garantia de que não ocorrerá interferência em uma instalação particular. Se este equipamento causar interferências prejudiciais à recepção de rádio ou televisão, que pode ser determinado ligando e desligando o equipamento, o usuário é encorajado a tentar corrigir a interferência através de uma das seguintes medidas:

- Reoriente ou recoloque a antena de recepção.
- Aumente a distância entre o equipamento e o receptor (TT, Rádio).
- Conecte o equipamento em uma tomada com um circuito diferente da qual o receptor está conectado.
- Consulte o distribuidor ou um técnico experiente em rádio/TV para ajuda.

Este dispositivo está em conformidade com a Parte 15 das Normas da FCC. A operação está sujeita às duas seguintes condições: (1) Este dispositivo não pode causar interferência prejudicial e (2) este dispositivo deve aceitar qualquer interferência recebida, incluindo interferências que possam causar operações indesejadas.

Aviso da FCC: Quaisquer alterações ou modificações não expressamente aprovadas pela parte responsável pela conformidade podem anular o direito do usuário de operar este equipamento.

Declaração FCC de exposição à radiação:

Este equipamento é compatível com a exposição à radiação dos limites estabelecidos pela FCC para um ambiente não controlado. Para evitar a possibilidade de ultrapassar os limites de exposição à radiofrequência, mantenha uma distância de pelo menos 100cm entre você e a antena do equipamento instalado. Este transmissor não deve ser alocado ou operado em conjunto com nenhuma outra antena ou transmissor.

A disponibilidade de alguns canais específicos e / ou bandas de frequência de operação dependem do país e são programados por firmware de fábrica para coincidir com o destino pretendido. A configuração do firmware não é acessível ao usuário final.

Garantia

A garantia do equipamento é de um (1) ano da data da emissão da Nota fiscal do distribuidor, que irá atender as atuais especificações relevantes publicadas e estarão livres de defeitos de material e fabricação sob uso e serviço normal.

EM NENHUM CASO O DISTRIBUIDOR SERÁ RESPONSÁVEL PARA VOCÊ OU QUALQUER OUTRA PARTE POR QUALQUER DANO DIRETO, INDIRETO, GERAIS, ESPECÍFICOS, EMERGENTES, EXEMPLAR OU OUTROS LEVANTAMENTO DO USO OU IMPOSSIBILIDADE DE USO DO PRODUTO (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS, INTERRUPÇÃO DE NEGÓCIOS, PERDA DE INFORMAÇÕES COMERCIAIS OU QUALQUER OUTRA PERDA PECUNIÁRIA, OU DE VIOLAÇÃO DE GARANTIA) MESMO DISTRIBUIDOR SEJA INFORMADO DA POSSIBILIDADE DE TAIS DANOS. EM NENHUM CASO SERÁ MAIOR QUE O VALOR PAGO PELO PRODUTO.

Conteúdo

Capítulo 1 Introdução	1
Introdução.....	1
Aparência	1
Principais Caraterísticas.....	2
Aplicações Típica.....	2
Capítulo 2 Instalação do Equipamento.....	3
Preparação Antes da Instalação	3
Instação Profissional Necessário	3
Precauções de Segurança	3
Instalação do A520N	4
Conteúdo da Caixa.....	4
Instalação do Produto	6
Conectando.....	6
Usando uma Antena Externa	9
Fixação em Mastro.....	9
Capítulo 3 Configurações Básicas	11
Configuração de Fábrica.....	11
Requisitos de Sistema.....	12
Assistente de Configuração Rápida.....	12
Configuração Básica do sistema	14
Configuração de Horário	17
Configurações RADIUS.....	18
Configurações Firewall.....	19
Configuração Wireless Básica.....	23
Site Survey	26
Capítulo 4 Configurações Avançadas	27
Configurações Avançada Wireless	27

Configurações de Segurança Wireless.....	30
Configurações de Segurança	30
Controle de Acesso Wireless	32
Configuração WDS	33
Capítulo 5 Gereciamento.....	34
SNMP	34
Configurando Perfil do Usuário SMPv3	35
Atualização de Firmware.....	36
Backup / Restaurar Configurações.....	37
Configuração Padrão de Fábrica.....	37
Reboot.....	38
Configuração de Senha.....	39
Histórico (Log)	39
Site Survey	40
Ping Watch Dog	41
Capítulo 6 Status	42
Visualizar Informações Básicas	42
Visualizar Lista de Associações.....	42
Exibir Estatísticas de Fluxo de Rede	43
Exibir Tabela ARP	43
Exibir Tabela Bridge	44
Exibir Tabela de Clientes DHCP Ativos.....	44
Capítulo 7 Soluções de Problemas.....	45
Apêndice A. ASCII.....	46
Apêndice B. Declaração GPL	48

TABELA

Tabela 1 Configuração de Fábrica	11
Tabela 2 ASCII.....	47
Tabela 3 Software Público Nomes e Descrições	49

Capítulo 1 Introdução

Introdução

Projetado para aplicação em ambiente externo, o A520N Wireless Outdoor CPE é uma solução 802.11 a/n 2x2 MIMO de alta performance para uma cobertura de rede sem fio rápida e confiável. Projetado com o padrão IEEE 802.11n draft 2.0, com saída de alta potência standard e antena interna de 16dBi torna possível o envio de taxa de dados mais veloz que uma rede sem fio padrão com alta largura de banda e maior alcance para aplicações externas.

O A520N Wireless Outdoor CPE suporta quatro modos de conexão wireless (AP, Cliente, WDS e Repetidor) permitindo vários tipos de aplicações, e assim ajudar a encontrar um meio para a última milha mais facilmente.

Com alta potência e performance confiável, O A520N Wireless Outdoor CPE é uma solução ideal de banda larga sem fio para provedores de internet sem fio e integradores de sistema!

Aparência



Figura 1 A520N Wireless Outdoor CPE

Principais Características

- λ Compatível com IEEE 802.11a e IEEE 802.11n draft 2.0
- λ Suporte para energia via cabo de rede através de uma fonte de 15V.
- λ Caixa à prova de água de alta resistência para suportar os mais agressivos ambientes
- λ Quatro modos de operação incluindo modo AP, Cliente Wireless, WDS e Repetidor AP
- λ Suporte a WEP 64/128/152-bit e 802.1X, WPA, WPA2, WPA&WPA2, WPA-PSK, WPA2-PSK, e WPA-PSK&WPA2-PSK etc
- λ Interface Web fácil de utilizar e interface de gerenciamento SNMP

Aplicações Típica

Esta seção descreve as aplicações típicas do A520N Wireless Outdoor CPE. Por padrão, ele vem configurado no modo AP para permitir uma cobertura wireless; além disso, é possível se conectar a qualquer rede wireless disponível no modo cliente. O A520N Wireless Outdoor CPE é capaz de fornecer uma conectividade de banda larga estável e eficiente para várias aplicações.



Figura 2 Aplicações Típica

Capítulo 2 Instalação do Equipamento

Após conectar o roteador wireless A520N com a rede, é necessário configurá-lo. Este capítulo descreve como configurar as funções básicas do equipamento. Estes procedimentos devem tomar poucos minutos. Será possível acessar a Internet através do roteador, imediatamente após à configuração bem sucedida.

Preparação Antes da Instalação

Instalação Profissional Necessário

Por favor, busque ajuda de um instalador profissional treinado na instalação de RF e conhecedor da legislação local.

Precauções de Instalação

1. Para mantê-lo seguro e instalar o equipamento corretamente, por favor, leia e siga estas precauções de segurança.
2. Se você está instalando o A520N Wireless Outdoor CPE, pela primeira vez, para sua segurança, bem como dos outros, por favor, busque ajuda de um instalador profissional que recebeu treinamento e sabe dos riscos envolvidos.
3. Manter a segurança bem como o bom desempenho do equipamento é escolher um local de instalação aonde há energia elétrica e linhas telefônicas.
4. Quando estiver instalando o A520N, observe os seguintes aspectos:
 - ♦ Não use escada de metal;
 - ♦ Não trabalhe em um dia chuvoso ou com muito vento;
 - ♦ Use sapatos com sola de borracha e saltos, luvas de borracha, camisa de manga comprida ou casaco.
5. Quando o sistema estiver em operação, evite ficar em frente dele. Fortes campos RF estão presentes quando o transmissor está ligado.

Instalação do A520N

Para manter o A520N Wireless Outdoor CPE funcionando bem na instalação, por favor leia e siga estas precauções de instalação.

1. Os usuários devem usar uma rede bem estabilizada para instalação do A520N, caso contrário, um raio aleatório poderia facilmente causar danos fatais ao equipamento.
2. Os usuários devem usar “Fonte de Alimentação & Injector POE” enviado na caixa com o A520N. Uso de outras opções podem causar danos ao equipamento.
3. O usuário deve conectar a antena externa no A520N em um ambiente externo. Não mudar de antena interna para a antena externa via Web, sem conexão física com a antena externa no A520N, caso contrário, podem causar danos ao aparelho em si.

Conteúdo da Caixa

Após desembalar cuidadosamente a caixa, verifique se contém os itens listados abaixo.

Caso qualquer um dos itens listado estiver faltando ou danificado contate o distribuidor aonde você adquiriu este produto para a devida assistência.

λ	A520N Wireless Outdoor CPE	× 1
λ	Conjunto de Abraçadeiras	× 2
λ	Fonte externa & POE Injector	× 1
λ	CD	× 1



Nota:

λ O CD Manual do Usuário!

Conjunto de Abraçadeira



Fonte Externa & Injetor POE



ATENÇÃO

-
- λ Os usuários devem usar a “Fonte de Alimentação & Injetor POE” enviado na caixa com o A520N Wireless Outdoor CPE. O uso de outras opções pode causar danos ao equipamento.
-

Instalação do Produto

Conectando

1. A parte inferior do A520N Wireless Outdoor CPE possui uma tampa removível. Solte o parafuso com uma chave de fenda. Segure o equipamento, pegue a tampa e puxe-a até tirá-la como o mostra na figura abaixo.

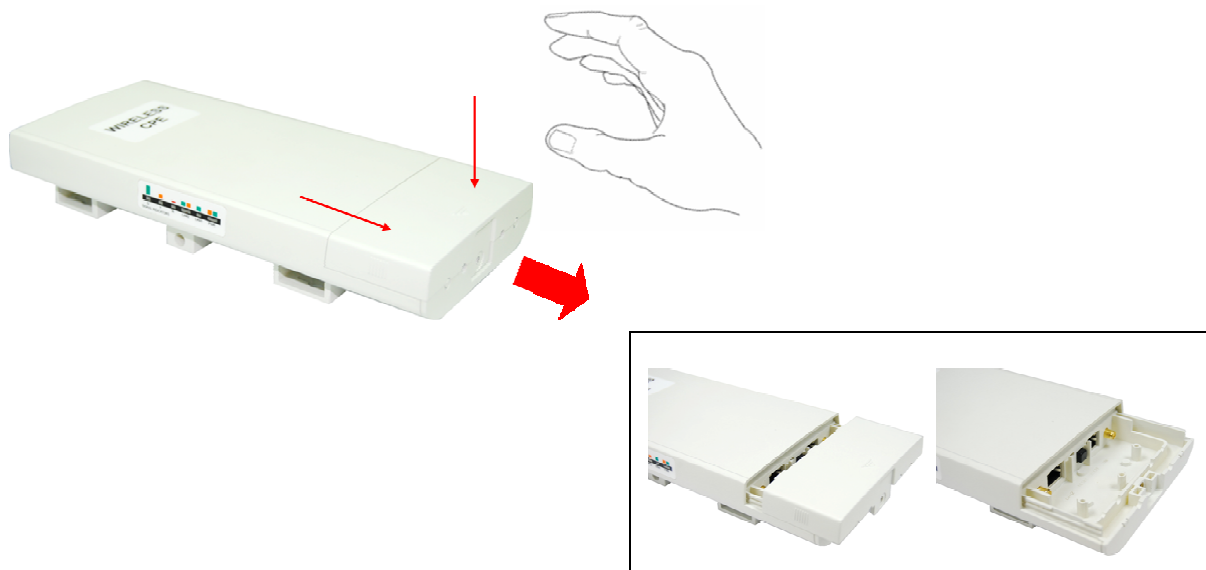


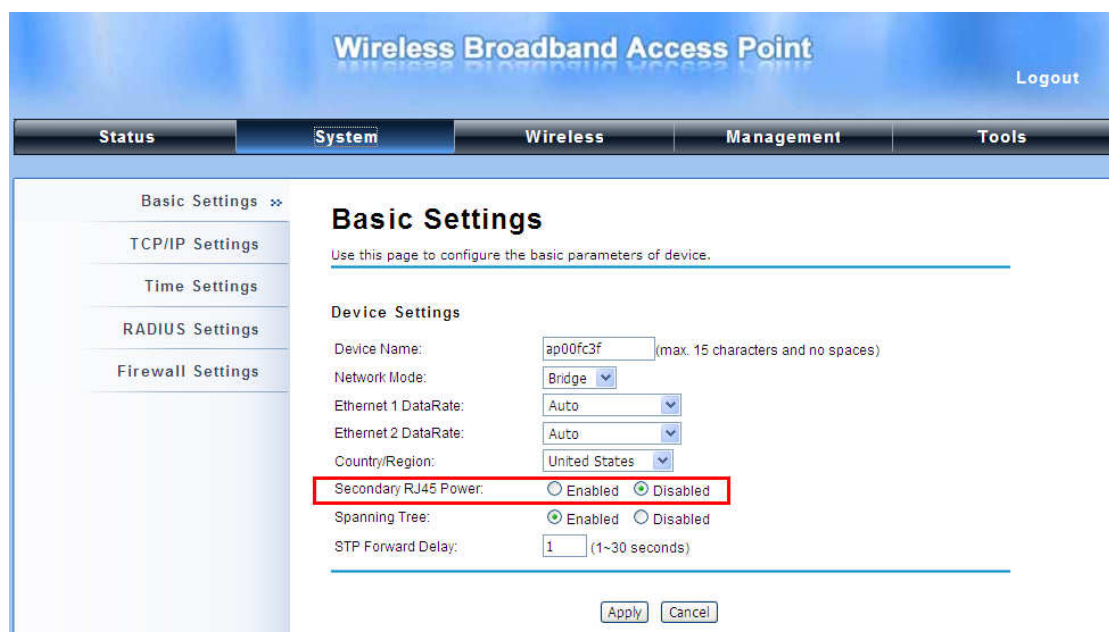
Figura 3 Mova a Tampa

2. Conecte um cabo padrão Ethernet na porta RJ45 identificado como “**LAN 1**”. Não conecte o cabo na porta RJ45 identificado como “LAN 2”.



Figura 4 Conectando o Cabo

A porta Ethernet secundário (identificado LAN 2) é para integração de video IP. Para utilizá-la você precisa habilitar a porta secundária com antecedência via Web para começar a usar a câmera IP como mostra abaixo.



The screenshot shows the 'Basic Settings' page of a 'Wireless Broadband Access Point'. The page has a navigation bar with 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is selected. On the left, there is a sidebar with 'Basic Settings' (selected), 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', and 'Firewall Settings'. The main content area is titled 'Basic Settings' and includes a description: 'Use this page to configure the basic parameters of device.' Below this is the 'Device Settings' section with the following fields: 'Device Name' (ap00fc3f), 'Network Mode' (Bridge), 'Ethernet 1 DataRate' (Auto), 'Ethernet 2 DataRate' (Auto), 'Country/Region' (United States), 'Secondary RJ45 Power' (radio buttons for Enabled and Disabled, with Disabled selected and highlighted by a red box), 'Spanning Tree' (radio buttons for Enabled and Disabled, with Enabled selected), and 'STP Forward Delay' (1). At the bottom are 'Apply' and 'Cancel' buttons.

3. Tire a fonte de alimentação e o injetor POE da caixa, e conecte o cabo de alimentação à porta DC do injetor POE como mostra abaixo.



Figura 5 Conexão do Injetor POE

4. Conecte o cabo do passo 2 e passo 3 conectando a outra ponta do cabo de rede do passo 2 na porta POE do injetor POE do passo 3. Ao finalizar o passo 4, a montagem deverá ficar como na figura seguinte:



Figura 6 Conecte o cabo de rede no injector POE

5. Pressione o **botão PWR** ao lado da porta Ethernet LAN 1.



6. Encaixe a tampa removível e aperte bem o parafuso de fixação.

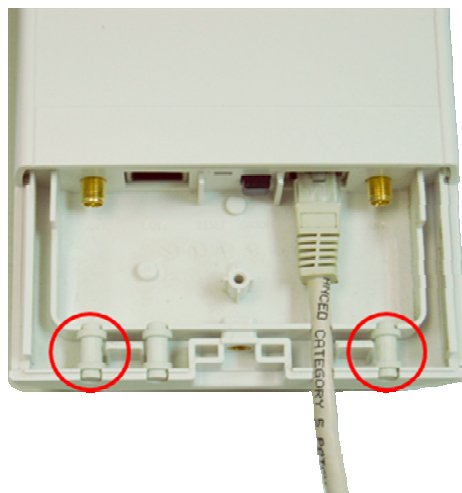


7. Com o A520N Wireless Outdoor CPE ligado agora coloque a fonte de alimentação na tomada.

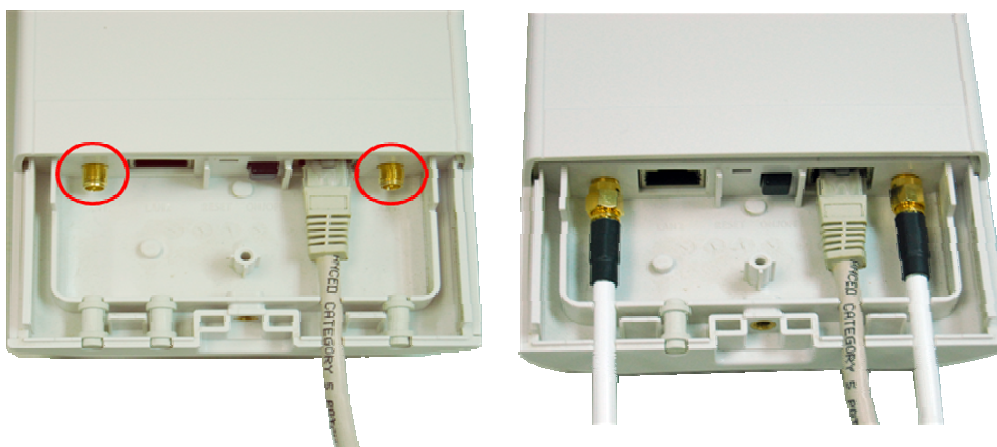
Usando uma Antena Externa

O A520N Wireless Outdoor CPE possui dois conectores SMA reverso caso você necessite colocar uma antena externa, siga os passos abaixo.

1. Remova os dois vedadores circundados abaixo:



2. Conecte sua antena externa com tipo de conector SMA na parte inferior.



ATENÇÃO

-
- λ O usuário deve conectar a antena externa no A520N em um ambiente externo. Não mudar de antena interna para a antena externa via Web, sem conexão física com a antena externa no A520N, caso contrário, os danos podem ser causados ao aparelho em si.
-

Siga os passos descritos em **Conectando** para concluir a instalação.

Fixação em Mastro

1. Vire o A520N de costas. Passe as cintas de montagem em mastro através das aberturas do suporte. Veja que é necessário desmontar a cinta de montagem com uma chave de fenda antes de passar através da abertura do suporte em mastro do A520N conforme as figuras abaixo.

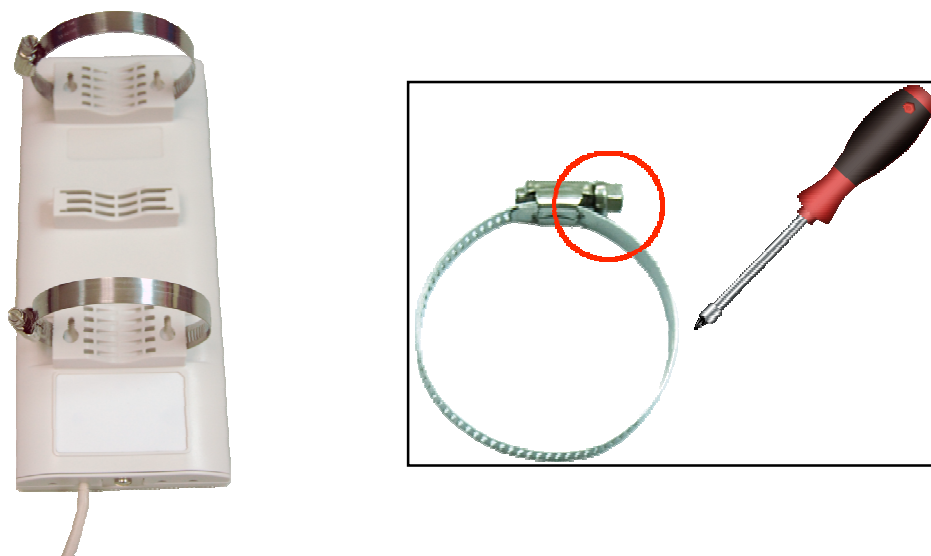


Figure 5 Pole Mounting – Step 1

2. Monte o A520N Wireless Outdoor CPE no mastro e trave bem a cinta de modo a ficar bem firme no mastro. As cintas de montagem suportam mastros com diâmetros de 32mm a 70mm.



Figura 6 Montando Mastro

3. Agora você terminou a instalação do equipamento A520N Wireless Outdoor CPE.

Capítulo 3 Configurações Básicas

Configuração de Fábrica

Agora vamos exibir as configurações padrões do A520N Wireless Outdoor CPE. Você pode adquirir estes parâmetros como padrão. Se necessário consulte o [“Restore Factory Default Settings”](#).

Tabela 1 Configurações Padrão de Fábrica

Features		Factory Default Settings
Username		admin
Password		password
Wireless Device Name		apXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		AP
Data Rate		Auto
LAN	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning Tree		Enable
802.11 Mode		802.11a/n
Country/Region		United States
Channel Number		149
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		100% (Full)
Channel Mode		20MHz
WMM		Enabled
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Security		Open System

Encryption		None
Wireless Separation		Disable
Access Control		Disable
SNMP	Enable/Disable	Enable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0

Requisitos de Sistema

Antes da configuração, certifique-se o sistema atende aos requisitos abaixo:

- λ Computador com um adaptador Ethernet 10/ 100 Base-TX;
- λ Configure o computador com um endereço IP estático de 192.168.1.x, como o endereço IP padrão do A520N é 192.168.1.1. (X não pode ser 0, 1 e nem 255);
- λ Navegador Web, como o Microsoft Internet Explorer 6.0 ou acima, Netscape ou Firefox.

Assistente de Configuração Rápida

Com o utilitário tipo Web (Internet Explorer ou Netscape® Navigator), é fácil gerenciar e configurar o roteador. O utilitário pode ser usado com qualquer Windows, Macintosh ou UNIX OS com um navegador Web.

- λ Conecte ao roteador digitando IP **192.168.1.1** no campo de endereço do navegador Web.



Figura 10 Página Login

- λ Após alguns instantes, surgirá uma janela de acesso (login) similar à figura acima. Digite **admin** para o Nome e **password** para senha, ambos em caracteres minúsculo. Em seguida pressione o botão **Login**.
- λ Como você pode observar, esta interface de gerenciamento oferece seis opções principais na barra de menu, que são **Status**, **System**, **Wireless**, **Management** e **Tools**.



Figura 11 Página Principal

Nota:

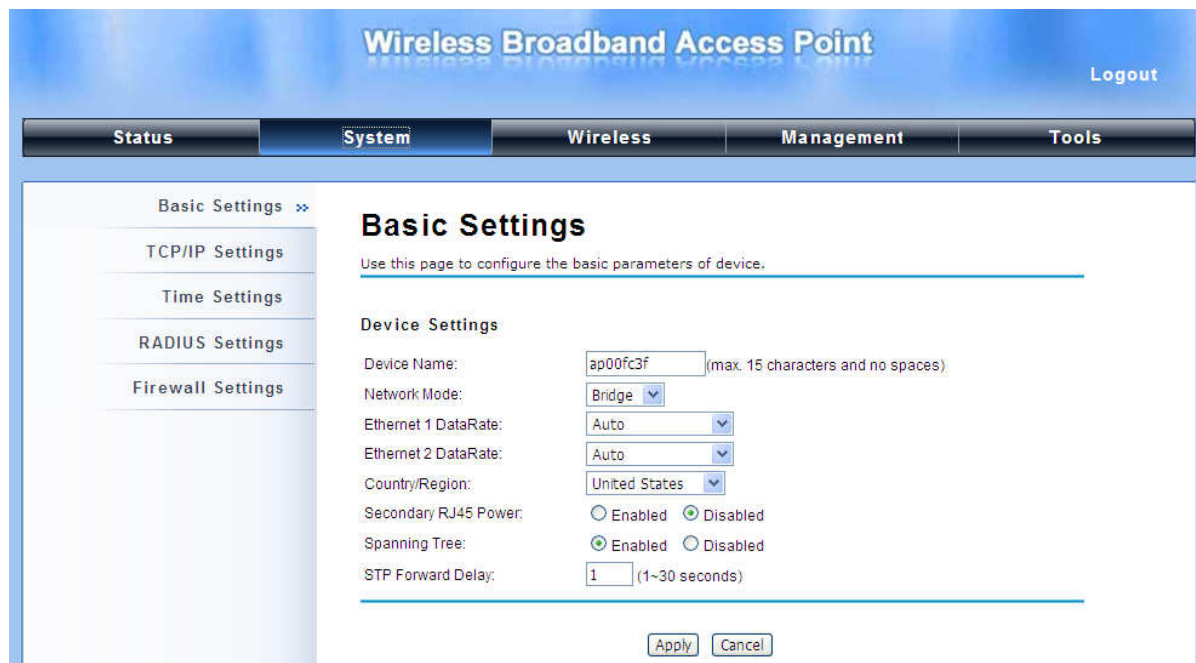
-
- λ O nome de usuário e senha são sensíveis a caracteres minúsculo e maiúsculo e a senha não podem ter mais que 19 caracteres!

Se não surgir a tela acima, significa que o navegador Web foi configurado para um servidor alternativo (proxy). Vá para ferramentas Menu > Opções > Internet > Conexões > Configurações de rede, na tela que surgir, cancele a opção Usando Proxy, e clique em OK para finalizar.

Se o Nome de Usuário e Senha estão corretos, pode-se configurar o roteador usando o navegador Web.

Configuração Básica

Para o usuário que utiliza o A520N Wireless Outdoor CPE pela primeira vez, recomendamos que você inicie a configuração a partir do “Basic Settings” no “System” conforme abaixo:



The screenshot displays the configuration interface for a Wireless Broadband Access Point. The top navigation bar includes tabs for Status, System (selected), Wireless, Management, and Tools. A 'Logout' link is visible in the top right corner. On the left side, a sidebar lists configuration sections: Basic Settings (selected), TCP/IP Settings, Time Settings, RADIUS Settings, and Firewall Settings. The main content area is titled 'Basic Settings' and contains a sub-section 'Device Settings'. The instructions state: 'Use this page to configure the basic parameters of device.' The settings include: Device Name (ap00fc3f, max 15 characters and no spaces), Network Mode (Bridge), Ethernet 1 DataRate (Auto), Ethernet 2 DataRate (Auto), Country/Region (United States), Secondary RJ45 Power (Enabled/Disabled), Spanning Tree (Enabled/Disabled), and STP Forward Delay (1, 1~30 seconds). 'Apply' and 'Cancel' buttons are at the bottom.

Figura 7 Configurações Básicas

λ Configurações Básicas

Device Name: Especifique um nome para o dispositivo, que é composto de no máximo de 15 caracteres (0-9), (A-Z), (a-z) ou (-).

Network Mode: Especifique o modo da rede, incluindo Bridge e Router. É fácil de configurar os parâmetros em modo Bridge; No entanto, os usuários devem prestar mais atenção da maneira de configurar os parâmetros quando o dispositivo estiver definido em modo Router. Para mais detalhes, consulte “IP Settings (Router)”.

Ethernet 1 Data Rate: Especifique a taxa de transmissão de dados de LAN1. Padrão é **Auto**.

Ethernet 2 Data Rate: Especifique a taxa de transmissão de dados de LAN2. Padrão é **Auto**.

Country Region: A disponibilidade de alguns canais e/ou banda de frequência de operação dependem de cada país.

Secondary RJ45 Power: A porta Ethernet secundário (LAN 2), para integração de vídeo IP. Para utilizá-lo você precisa habilitar a porta secundária com antecedência via interface Web antes de se conectar com a câmera IP.

Spanning Tree: O algoritmo STA (IEEE 802.1D Spanning Tree Algorithm), para prevenir

situações de repetição contínua sem fim (loop) e configuração de conexões redundantes. Pode se escolher entre habilitado (enabled) e desabilitado (disabled). Se o modo estiver configurado para WDS ou AP+WDS, este campo deve ser habilitado “enabled”.

STP Forward Delay: é o tempo gasto detectando e identificando o estado da topologia da rede antes de entrar no estado de forward. O valor padrão de tempo é 1 segundo.

λ TCP/IP Settings

Abra “TCP/IP Settings” em “System” permite configurar os parâmetros da rede local para os que conectam nas portas LAN do A520N. Pode se alterar o Endereço IP, Máscara de Sub-rede, e Servidor DHCP.

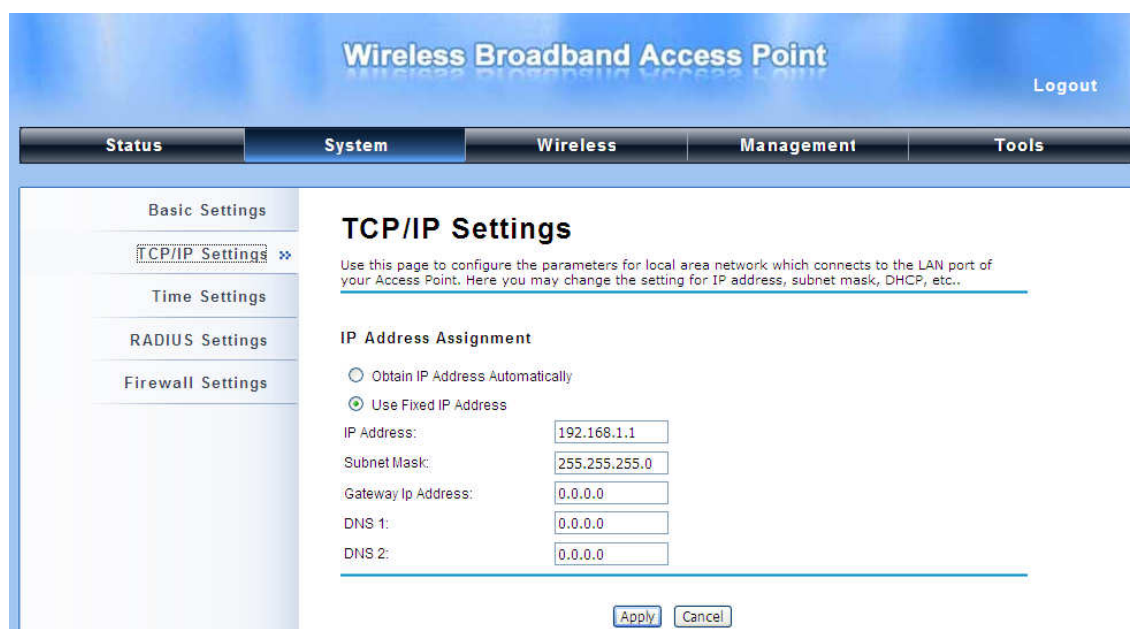


Figura 13 Configuração TCP/IP (Bridge)

Obtain IP Address Automatically: Verifique se já existe um servidor DHCP na sua rede, pois o A520N Wireless Outdoor CPE é capaz de obter o IP automaticamente a partir das configurações do servidor DHCP.



Nota:

λ Quando o endereço IP do A520N é mudado, os clientes da rede, muitas vezes é preciso esperar por um tempo ou até mesmo reiniciar antes que eles possam acessar o novo endereço IP. Para acesso imediato ao AP, libere o cache NetBIOS do computador

do cliente executando o comando “nbtstat –r” para acessar a página Web de administração.

Use Fixed IP Address: Selecionando esta opção, você pode especificar o Endereço IP, Máscara de Sub-rede, Gateway padrão e Servidor DNS manualmente no A520N. Verifique se o Endereço IP especificado está disponível em sua rede, para evitar conflito de IP.

Se o A520N Wireless Outdoor CPE está configurado no modo Router, você precisará configurar alguns parâmetros adicionais de TCP/IP para acessar a Internet.

The screenshot displays the 'Wireless Broadband Access Point' web interface. At the top, there's a navigation bar with tabs: Status, System (selected), Wireless, Firewall, Management, and Tools. A 'Logout' button is in the top right. On the left, a sidebar shows 'Basic Settings' (selected), 'TCP/IP Settings' (with a double arrow), 'Time Settings', and 'RADIUS Settings'. The main content area is titled 'TCP/IP Settings' and includes a descriptive paragraph. It is divided into two sections: 'WAN Settings' and 'LAN Settings'. The 'WAN Settings' section has fields for 'WAN Access Type' (set to 'Static IP'), 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (0.0.0.0), 'DNS 1' (0.0.0.0), and 'DNS 2' (0.0.0.0). The 'LAN Settings' section has fields for 'IP Address' (192.168.0.99), 'Subnet Mask' (255.255.255.0), 'DHCP Server' (set to 'Disabled'), 'DHCP IP Address Range' (0.0.0.0 - 0.0.0.0), and 'Lease Time' (0 minutes, with a note '(15-44640 Minutes)').

Figura 14 Configuração TCP/IP (Router)

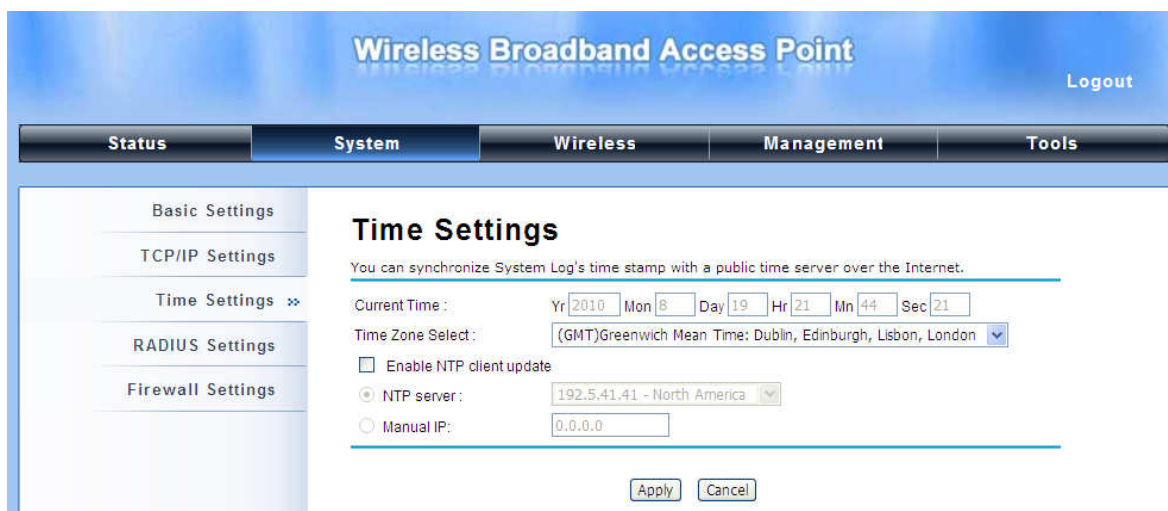
WAN Settings: Especifique o método de acesso à Internet para IP Estático, DHCP ou PPPOE. O usuário deve digitar o endereço IP WAN, Máscara Sub-rede, Gateway fornecidos pelo Provedor de Serviço à Internet (ISP).

LAN Settings: Quando o servidor DHCP está desabilitado, o usuário pode especificar o endereço IP e a máscara de sub-rede manualmente no A520N. Verifique se o endereço IP digitado é único na rede para evitar conflito de IP. Quando o servidor DHCP está ativado, o usuário recebe o endereço IP, máscara de sub-rede e Gateway automaticamente.

- λ No modo AP, o A520N Wireless Outdoor CPE pode estabelecer uma conexão com outro dispositivo wireless antes de ser configurado para o modo Router. No modo Router, é impossível que os usuários acessem o dispositivo através de uma porta a cabo, a WAN é a porta a cabo e a LAN é a porta wireless. Os usuários podem acessar o dispositivo através de um dispositivo wireless conectado ao A520N.
- λ No modo cliente wireless, os usuários podem acessar o A520N através da porta a cabo, A WAN é a porta wireless e a LAN é porta a cabo quando o dispositivo estiver configurado no modo Router Wireless.
- λ O modo Bridge e o modo Repetidor AP são similares ao modo AP quando o dispositivo estiver configurado como Router; A WAN é a porta a cabo e a LAN é a porta wireless. Os usuários podem se conectar ao A520N através de outro dispositivo wireless se for configurado como Router a acessar o A520N através deste dispositivo wireless.

Configuração de Horário

O A520N Wireless Outdoor CPE é compatível com a NTP que é capaz de manter o horário do sistema por sincronização com um servidor de horas público na Internet. Faça a configuração em “**Time Settings**” do “**System**”. Para utilizar este recurso ative o “**Enable NTP Client Update**”.



The screenshot shows the configuration interface of a Wireless Broadband Access Point. The top navigation bar includes 'Status', 'System' (selected), 'Wireless', 'Management', and 'Tools'. A 'Logout' link is in the top right. The left sidebar lists 'Basic Settings', 'TCP/IP Settings', 'Time Settings' (selected with a double arrow), 'RADIUS Settings', and 'Firewall Settings'. The main content area is titled 'Time Settings' and contains the following fields:

- Current Time: Yr 2010, Mon 8, Day 19, Hr 21, Mn 44, Sec 21
- Time Zone Select: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London (dropdown)
- ☐ Enable NTP client update
- ☒ NTP server: 192.5.41.41 - North America (dropdown)
- ☐ Manual IP: 0.0.0.0

At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figura 15 Configuração de Horário

λ **Current Time**

Exibe o horário atual em Yr (Ano), Mon (Mês), Day (Dia), Hr (Mora), Min (minutos) e Sec (segundos).

λ **Time Zone Select**

Selecione o fuso horário na lista suspensa.

λ **NTP Server**

Selecione o servidor de horário “**NTP Server**” na lista suspensa ou insira manualmente o endereço IP do servidor de tempo disponível no “**Manual IP**”.

E clique em “**Apply**” para salvar as configurações.

Configurações RADIUS

RADIUS (Remote Authentication Dial-In User Service) é um servidor para autenticação de usuários remotos e contas, executando uma regra central na rede e disponibilizando capacidades de autenticação, autorizando, gerenciando, auditando, alarmes e outros. Isso permite que a empresa mantenha os perfis de usuários em um banco de dados central e compartilhe um servidor de arquivos.

Abra “**RADIUS Settings**” em “**System**” para fazer a configuração RADIUS.

The screenshot displays the configuration interface for a Wireless Broadband Access Point. The top navigation bar includes 'Status', 'System' (selected), 'Wireless', 'Management', and 'Tools'. A 'Logout' link is in the top right. On the left, a sidebar lists 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings' (highlighted with a double arrow), and 'Firewall Settings'. The main content area is titled 'RADIUS Settings' and contains the instruction 'Use this page to set the radius server settings.' Below this, the 'Authentication RADIUS Server:' section includes input fields for 'IP Address' (0.0.0.0), 'Port' (1812), 'Shared Secret', and 'Reauthentication Time' (3600 Seconds). There is also a checkbox for 'Global-Key Update' with a sub-field 'every 3600 Seconds'. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

Figura 16 Configurações RADIUS

λ **Authentication RADIUS Server**

Este é para autenticação RADIUS. Ele pode se comunicar com o servidor RADIUS com o

endereço IP, Porta e Senha compartilhada.

IP Address: Digite o endereço IP do servidor RADIUS;

Port: Digite o número da porta do servidor RADIUS;

Shared Secret: Chave secreta, que é composto por mais de 31 caracteres, é compartilhada pelo AP e RADIUS durante a autenticação.

Re-authentication Time: Defina o intervalo de tempo entre as duas autenticações.

Global-Key Update: Marque esta opção e especifique o intervalo entre duas atualizações chaves-global.

Configurações Firewall

O firewall é um sistema ou grupo de sistemas que aplicam uma política de controle de acesso entre duas redes. Também pode ser definido como um mecanismo usado para proteger uma rede confiável de uma rede não-confiável. O A520N Wireless Outdoor CPE tem capacidade de Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding bem como DMZ. Esta opção está disponível apenas no modo Roteador.

Source IP Filtering: A filtragem por IP é usada para restringir determinados tipos de pacotes de dados da rede local à Internet através do A520N Wireless Outdoor CPE. O uso desses filtros pode ser útil em termos de segurança ou restringir a rede local.

The screenshot displays the configuration interface for a Wireless Broadband Access Point. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is active, and the left sidebar shows various settings categories, with 'Src IP Filtering' selected. The main content area is titled 'Source IP Filtering' and contains a checkbox to 'Enable Source IP Filtering'. Below this, there are input fields for 'Local IP Address' and 'Comment'. At the bottom of the main area, there are 'Apply' and 'Cancel' buttons. A table at the very bottom has columns for 'Local IP Address', 'Comment', 'Select', and 'Edit'.

Figura 17 Source IP Filtering

Destination IP Filtering: A filtragem por IP de destino permite restringir acesso à rede local e de acessar determinados sites na WAN de acordo com os endereços IP especificados. Marque a opção “**Enable Destination IP Filtering**” e insira o endereço IP do cliente a ser limitado. Clique em **Apply** para as configurações surtirem efeito.

The screenshot displays the configuration page for a Wireless Broadband Access Point, specifically the 'Destination IP Filtering' section. The interface has a blue header with the title 'Wireless Broadband Access Point' and a 'Logout' link. Below the header is a navigation bar with tabs: 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is active, and a sidebar on the left lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering' (highlighted with a double arrow), and 'Src Port Filtering'. The main content area is titled 'Destination IP Filtering' and contains a description: 'Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.' Below this, there is a checkbox labeled 'Enable Destination IP Filtering', which is currently unchecked. Underneath the checkbox are two input fields: 'Destination IP Address' and 'Comment'. At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a table header with four columns: 'Destination IP Address', 'Comment', 'Select', and 'Edit'.

Figura 18 Destination IP Filtering

Source Port Filtering: Entradas nesta tabela são usadas para restringir determinados tipos de pacotes de dados da rede local à Internet através do A520N Wireless Outdoor CPE. O uso desses filtros pode ser útil em termos de segurança ou restringir a rede local.

Wireless Broadband Access Point

Logout

Status

System

Wireless

Management

Tools

Basic Settings

TCP/IP Settings

Time Settings

RADIUS Settings

Firewall Settings

Src IP Filtering

Dst IP Filtering

Src Port Filtering »

Dst Port Filtering

Port Forwarding

DMZ Setting

Source Port Filtering

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable Source Port Filtering

Port Range :
 -

Protocol :

Both

Comment :

Apply

Cancel

Source Port Range	Protocol	Comment	Select	Edit
-------------------	----------	---------	--------	------

Delete Selected

Delete All

Refresh

Figura 19 Source Port Filtering

21

Destination Port Filtering: A porta de destino de filtragem permite restringir determinados tipos de pacotes de dados da rede local à Internet através do A520N Wireless Outdoor CPE. O uso desses filtros pode ser útil em sua rede local.

The screenshot shows the 'Destination Port Filtering' configuration page. On the left is a sidebar menu with options: Basic Settings, TCP/IP Settings, Time Settings, RADIUS Settings, Firewall Settings, Src IP Filtering, Dst IP Filtering, Src Port Filtering, **Dst Port Filtering >>**, and Port Forwarding. The main content area has a title 'Destination Port Filtering' and a description: 'Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' Below this is a checkbox 'Enable Destination Port Filtering' which is unchecked. There are input fields for 'Port Range' (with a '-' separator), 'Protocol' (a dropdown menu set to 'Both'), and 'Comment'. 'Apply' and 'Cancel' buttons are below the form. At the bottom is a table with headers: 'Dest Port Range', 'Protocol', 'Comment', 'Select', and 'Edit'. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Refresh'.

Figura 20 Destination Port Filtering

Port Forwarding: O encaminhamento da porta permite redirecionar automaticamente serviços frequentes de rede, para um servidor específico atrás do firewall NAT. Estas configurações somente são necessárias se quiser hospedar algum tipo de servidor como Servidor Web ou Servidor de e-mail, na rede local atrás do firewall NAT.

The screenshot shows the 'Port Forwarding' configuration page. The sidebar menu is similar to the previous page, but with 'Port Forwarding >>' highlighted. The main content area has a title 'Port Forwarding' and a description: 'Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.' Below this is a checkbox 'Enable Port Forwarding' which is unchecked. There are input fields for 'IP Address', 'Protocol' (a dropdown menu set to 'Both'), 'Port Range' (with a '-' separator), and 'Comment'. 'Apply' and 'Cancel' buttons are below the form. At the bottom is a table with headers: 'Local IP Address', 'Protocol', 'Port Range', 'Comment', 'Select', and 'Edit'. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Refresh'.

Figura 21 Porta Forwarding

DMZ: A função hospedeiro DMZ (Zona Desmilitarizada) host permite que um servidor local seja exposto à Internet. Tipicamente, o DMZ host contém dispositivos acessíveis ao tráfego da Internet, tais como servidores Web (http), servidores FTP, SMTP (e-mail) e servidores DNS.




The screenshot shows the 'Wireless Broadband Access Point' configuration interface. The 'System' tab is selected, and the 'DMZ' section is active. The 'DMZ' section includes a description: 'A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.' Below the description, there is a checkbox for 'Enable DMZ' which is currently unchecked. To the right of the checkbox is a text input field for 'DMZ Host IP Address' containing '0.0.0.0'. At the bottom of the section are 'Apply' and 'Cancel' buttons.

Figura 22 DMZ

Configuração Wireless Básica

Para a Configuração Wireless Básica abra “**Basic Settings**” em “**Wireless**” como mostra abaixo:



The screenshot shows the 'Wireless Broadband Access Point' configuration interface. The 'Wireless' tab is selected, and the 'Wireless Basic Settings' section is active. The 'Wireless Basic Settings' section includes a description: 'Use this page to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless mode as well as wireless network parameters.' Below the description, there is a checkbox for 'Disable Wireless LAN Interface' which is currently unchecked. To the right of the checkbox is a 'Site Survey' button. Below the checkbox are several configuration options: 'Wireless Mode' (dropdown menu set to 'AP'), 'Wireless Network Name (SSID)' (text input field containing 'Wireless'), 'Broadcast SSID' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected), '802.11 Mode' (dropdown menu set to '802.11a/n'), 'HT protect' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected), 'Channel Number' (dropdown menu set to '149'), 'Antenna' (radio buttons for 'Internal (16 dBi)' and 'SMA Connector', with 'Internal (16 dBi)' selected), 'Output Power' (dropdown menu set to 'Full'), 'Data Rate' (dropdown menu set to 'Auto'), 'Channel mode' (dropdown menu set to '20MHZ'), and 'Extension channel protection mode' (dropdown menu set to 'None').

Figura 23 Configuração Wireless Básica

λ **Disable Wireless LAN Interface**

Marque esta opção para desabilitar a interface WLAN, em seguida o módulo sem fio do A520N irá parar de funcionar e nenhum dispositivo wireless poderá se conectar ao A520N.

λ **Wireless Mode**

Quatro modos de operação estão disponíveis no A520N Wireless Outdoor CPE:

- **AP**: O A520N Wireless Outdoor CPE estabelece uma cobertura sem fio e recebe conexões de clientes wireless.
- **Wireless Client**: O A520N Wireless Outdoor CPE é capaz de se conectar ao AP e assim se integrar a rede sem fio.
- **Bridge**: O A520N Wireless Outdoor CPE estabelece uma conectividade wireless entre outros APs através de chaves no endereço MAC remoto. Favor verificar o "WDS Setting" para os detalhes de configuração.
- **AP Repeater**: O A520N Wireless Outdoor CPE funciona como AP e Bridge simultaneamente. Em outras palavras, permite serviços de conectividade para CPEs sobre o modo WDS.

λ **Wireless Network Name (SSID)**

Este nome de rede sem fio é compartilhada entre todos os dispositivos associados a sua rede sem fio. Note que o SSID é sensível a caracteres em maiúsculo/minúsculo.

λ **Broadcast SSID**

No modo AP, ocultar o nome da rede pode ser necessário quando estiver em um ambiente sem fio que pode ter riscos em potencial. Ao desativar o broadcast do SSID, o STA não pode fazer o scan e encontrar o A520N Wireless Outdoor CPE, de modo que ataques maliciosos por parte de alguns STA ilegais podem ser evitados.

λ **802.11 Mode**

O A520N Wireless Outdoor CPE pode se comunicar com dispositivos sem fio do padrão 802.11n ou 802.11a/n. Você pode selecionar Auto e fazer que trabalhe no modo wireless correto automaticamente.

λ **HT Protect**

Habilitar HT (High Throughput) protege e assegura a transmissão HT com mecanismo MAC. No modo 802.11n, em wireless client pode ser dividido em HT STA e Non-HT STA, entre os quais um com HT habilitado protege e recebe maior throughput.

λ **Channel Number**

O canal varia tanto quanto a banda disponível conforme varia de país para país. Selecione um canal adequado de funcionamento na lista suspensa de acordo com sua situação.

λ **Antenna**

Por padrão, o A520N Wireless Outdoor CPE usa sua antena interna direcional para transmissão, dependendo o cenário, se você precisar usar uma antena externa para sua aplicação, você pode mudar a partir de “Internal (16 dBi)” para “SMA Connector”.



Nota:

λ Altere para “SMA Connector” a partir da interface WEB somente quando já estiver com a antena externa instalada, caso contrário, poderá danificar o aparelho em si.

λ **Output Power**

Especifique a potência de transmissão do sinal. Quanto maior a potência de saída, maior será a cobertura do sinal, mas o consumo de energia será maior nesse caso. Normalmente “Full” é o mais utilizado.

λ **Data Rate**

Normalmente “Auto” é o mais utilizado. Sob essa taxa, o A520N Wireless Outdoor CPE irá selecionar automaticamente a taxa mais alta disponível para transmitir.

λ **Channel Mode**

Dois níveis estão disponíveis: 20MHz e 40MHz. O último pode aumentar a taxa de dados, mas é preciso mais largura de banda, o que pode causar interferências.

λ **Extension Channel Protection Mode**

Isso é para evitar conflito com outra rede sem fio e aumentar a capacidade do seu dispositivo para capturar todas as transmissões dos dispositivos delegados. No entanto, pode diminuir o desempenho da rede sem fio. Comparado ao CTS-Self; a quantidade de transmissão CTS-RTS é maior.

λ **Enable MAC Clone**

Disponível apenas no modo Wireless client, ele esconde o endereço MAC do A520N, enquanto exibe de um dos associados do cliente sem fio ou o endereço MAC especificado manualmente.

Site Survey

No modo "Wireless Client", o IEEE 802.11a / n Wireless Outdoor CPE é capaz de realizar um "site survey" para exibir os pontos de acesso disponíveis.

Abra "**Basic Settings**" em "**Wireless**", clicando no "**Site Survey**" botão ao lado "**Wireless Mode**", surge uma janela com as redes wireless ao seu alcance. Selecione o AP desejado e Clique em "**Selected**" para estabelecer a conexão. O "site survey" também pode ser feito abrindo o "**Site Survey**" no menu principal em "**Tools**".

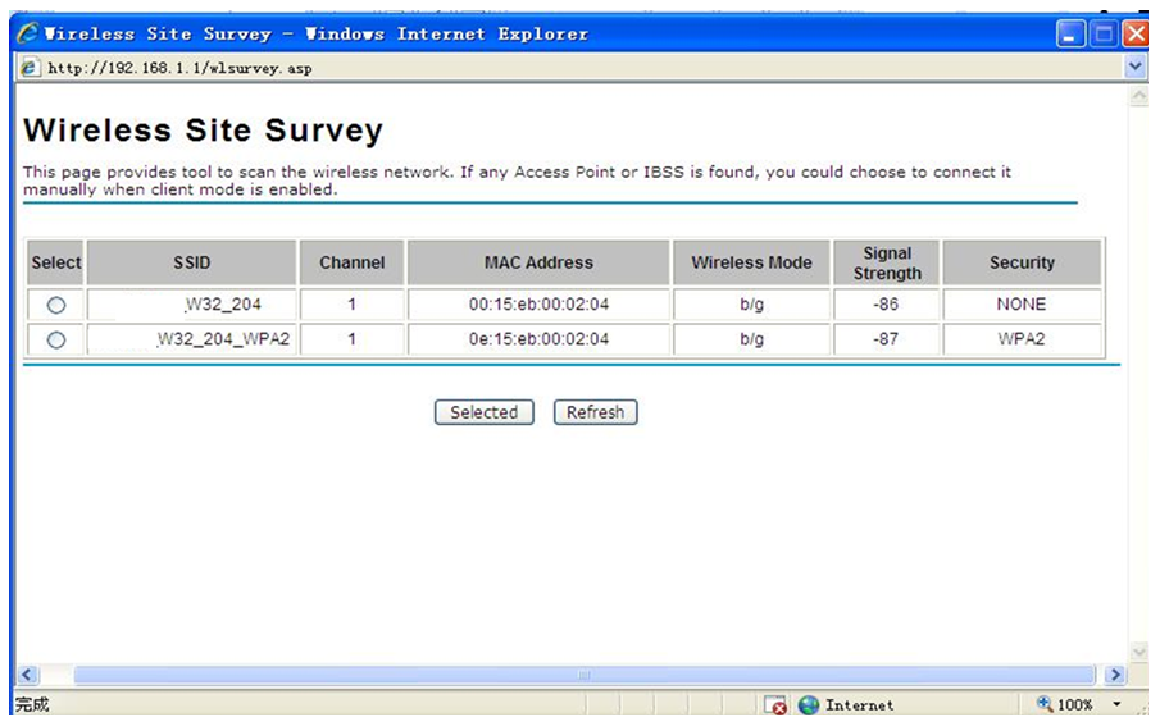


Figura 24 Site Survey

Capítulo 4 Configurações Avançadas

Configurações Avançadas Wireless

Para Configurações Avançadas Wireless abra “Advanced Settings” em “Wireless”



Figura 25 Configurações Avançadas Wireless

λ WMM Support

WMM (Wi-Fi Multimedia) é um subconjunto do 802.11e. Ele permite a comunicação sem fio para definir um limite de prioridade com base no tipo de dados disponível apenas no modo AP, portanto esses dados sensíveis ao tempo, dados video/audio, pode possuir uma prioridade maior do que um dado comum. Para habilitar o WMM, o “wireless client” também deverá ter suporte a esta função.

λ A-MPDU/A-MSDU Aggregation

A taxa de dados do seu A520N, exceto no modo “wireless client”, pode ser melhorado com a ativação desta opção, entretanto, se seus clientes não oferecem suporte a agregação A-MPDU/A-MSDU, não é recomendado ativar esta função.

λ Short GI

No modo 802.11n, pode se obter uma melhor taxa de dados se não houver nenhum problema de incompatibilidade.

λ **RTS Threshold**

O RTS é um mecanismo de prevenção, pois cada estação, antes de iniciar transmissão, deve enviar um pacote RTS (Request to send). Ao receber este pacote, o AP envia o CTS (Clear to send), iniciando assim a transmissão de dados. A faixa de ajuste é de 0 á 2346 bytes. Defini-lo muito baixo pode resultar em mau desempenho da rede. Deixe-o no seu padrão de 2346 que é o recomendado.

λ **Fragmentation Length**

Especifique o tamanho máximo em bytes para um pacote de dados antes de ser fragmentado em vários pacotes. Defini-lo muito baixo pode resultar em mau desempenho da rede. Deixe-o em seu valor padrão de 2346 que é o recomendado.

λ **Beacon Interval**

Especifique o intervalo de frequência para transmitir os pacotes de dados. Digite um valor entre 20 e 1024.

λ **DTIM Interval**

DTIM, que significa mensagem de indicação de entrega de tráfego, está contida nos pacotes de dados. Melhora a eficiência de transmissão sem fio. O padrão é definido como 1. Insira um valor entre 1 e 255.

λ **IGMP Snooping**

IGMP snooping é o processo de escuta de tráfego de rede IGMP. Ao ativar o IGMP snooping, o AP irá listar para o associado de consulta IGMP, e enviar mensagens para identificar as portas dos membros de grupos multicast. O tráfego multicast será enviado apenas para os pontos identificados como membros do grupo multicast ou grupos específicos.

λ **Wireless Separation**

Separação Wireless é a maneira ideal para aumentar a segurança da rede de transmissão. Sob a modalidade, exceto no modo “wireless client”, ativar o “**Wireless Separation**” pode prevenir a comunicação entre os clientes sem fio.

λ **RIFS**

RIFS (Reduced Interframe Spacing) é um meio de reduzir a sobrecarga e aumentar a eficiência da rede.

λ **Link Integration**

Disponível nos modos AP/Bridge/AP repeater, monitora a conexão na porta Ethernet deixando-o como **“Enabled”**. Pode informar os clientes wireless associados logo que ocorrer a desconexão.

λ **Max. Station Num**

Disponível apenas no modo AP, ele define a quantidade máxima de clientes sem fio que podem ser conectados.

λ **Space in Meter/ACK Timeout**

Para diminuir a chances de retransmissão de dados a longa distância, o A520N Wireless Outdoor CPE pode ajustar automaticamente o valor limite apropriado para o ACK especificando distância de dois nós.

λ **Flow Control**

Ele permite que o administrador especifique um limite de tráfego de entrada e saída ativando o **“Enable Traffic Shaping”**. Disponível apenas no modo Router.



Nota:

-
- λ Recomendamos fortemente que deixe as configurações avançadas nos valores padrões exceto o “Distance in Meters” (Distância em metros) que deverá ser ajustado para a distância real. Qualquer alteração nos valores padrões de fábrica pode ter um impacto negativo no desempenho da sua rede wireless.
-

Configurações de Segurança Wireless

Aqui você poderá programar a segurança de sua rede wireless. Selecionando diferentes métodos, você terá diferentes níveis de segurança.

Configurações de Segurança

Abra “Security Settings” em “Wireless” como abaixo:



Figura 26 Configurações Segurança

λ Network Authentication

Open System: Permite que qualquer dispositivo possa se conectar ao A520N sem qualquer autenticação de segurança.

Shared Key: Criptografia de dados e requer uma senha para autenticar a conexão wireless.

Legacy 802.1x: É um padrão IEEE baseado em portas para controle de acesso de rede, prove os direitos de acesso a rede wireless e rede a cabo. Com a identidade do usuário de do PC, autenticação centralizada bem como gerenciamento dinâmico de chaves, controla o risco de segurança da rede wireless para o mínimo. Para atender o 802.1x, pelo menos um tipo EAP deve ser suportado pelo servidor Radius, AP e cliente wireless.

WPA with RADIUS: Com a segurança (username, password e etc.) oferecida pelo usuário, este tipo de autenticação pode ser realizado através do servidor RADIUS. É comum este meio de autenticação ser adotado na rede das grandes empresas.

WPA2 with RADIUS: É uma nova versão do WPA, somente os clientes que suportam o WPA2, pode acessar. Se for selecionado, é necessário a criptografia AES e um servidor RADIUS.

WPA&WPA2 with RADIUS: Ele oferece opções de WPA (TKIP) ou WPA2 (AES) para o cliente. Se for selecionada, o tipo de criptografia deve ser TKIP + AES e deve ser configurado o servidor RADIUS.

WPA-PSK: Este é um modo simplificado WPA sem necessidade de um servidor de autenticação específico. Neste chamado WPA Pre-Shared Key, tudo que você precisa é apenas pré-inserir uma chave no A520N. Este é um método de autenticação adotados por grandes e médias empresas, bem como em uma rede residencial.

WPA2-PSK: Uma nova versão do WPA, ela pode ser disponibilizado somente todos os clientes suportarem o WPA2. Se for selecionada, a criptografia só pode ser como AES e a senha é requisitada.

WPA-PSK&WPA2-PSK: Esta oferece opções de criptografia WPA (TKIP) ou WPA2 (AES) para clientes. Se for selecionada, este tipo de criptografia de dados pode ser somente TKIP + AES e a senha é requisitada.

λ **Data Encryption**

Se a criptografia de dados for habilitada, é necessário que se compartilhe a mesma chave para que os clientes wireless possam estabelecer a conexão com o AP.

None: Disponível apenas quando o tipo de autenticação está em aberta.

64 bits WEP: É composta por 10 números hexadecimais.

128 bits WEP: É composta por 26 números hexadecimais.

152 bits WEP: É composta por 32 números hexadecimais.

TKIP: Temporal Key Integrity Protocol, que é um tipo de criptografia dinâmica, é utilizado em conjunto com WPA-PSK, etc.

AES: Advanced Encryption Standard, geralmente é utilizado com WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: Ela permite a compatibilidade com dispositivos usando TKIP.



Nota:

λ Recomendamos fortemente que utilize algum meio de segurança para sua rede sem fio!

λ Somente com o mesmo modo de autenticação do A520N, é que os dispositivos

sem fio irão estabelecer a comunicação com o mesmo!

Controle de Acesso Wireless

O Controle de Acesso Wireless permite o acesso somente aos clientes cadastrados no A520N Wireless Outdoor CPE. O controle de acesso somente irá funcionar quando o equipamento estiver operando como AP.

Abra **“Access Control”** em **“Wireless”** como abaixo.

The screenshot shows the 'Wireless Broadband Access Point' configuration page. The 'Wireless' tab is selected in the top navigation bar. On the left, the 'Access Control' menu item is highlighted. The main content area is titled 'Wireless Access Control' and includes a descriptive text block, an 'Access Control Mode' dropdown set to 'Allow Listed', a 'MAC Address' input field, and 'Apply' and 'Cancel' buttons. Below this is a table with one row containing the MAC address '00:19:70:00:fc:2d', a 'Select' checkbox, and an 'Edit' button. At the bottom, there are 'Delete Selected', 'Delete All', and 'Refresh' buttons.

MAC Address	Select	Edit
00:19:70:00:fc:2d	<input type="checkbox"/>	Edit

Figura 27 Controle de Acesso

λ **Access Control Mode**

Se você selecionar **“Allow Listed”**, somente os clientes cujos endereços MAC que estão na lista de controle de acesso serão capazes de se conectar ao AP. Enquanto que **“Deny Listed”** não permite a conexão dos clientes que constarem na lista.

λ **MAC Address**

Digite o endereço MAC do cliente sem fio que você deseja cadastrar na lista de controle de acesso, Clique **“Apply”** que o MAC será adicionado na tabela.

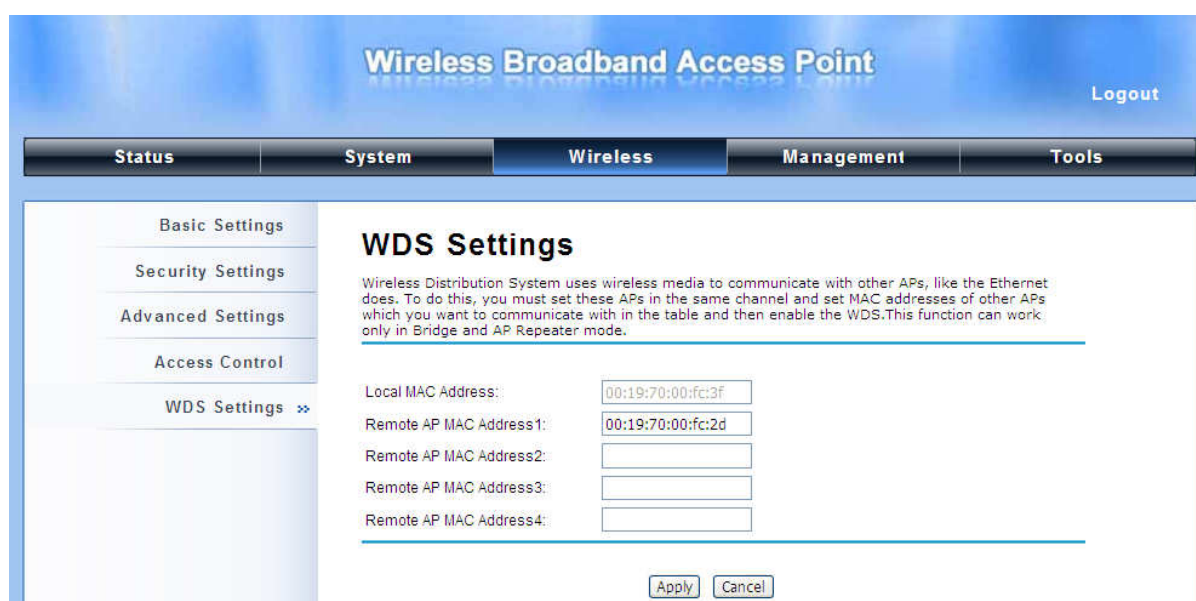
λ **Delete Selected/All**

Marque na caixa um ou mais endereços MAC que você deseja remover e Clique **“Delete Selected”** ou **“Delete All”** para excluir os endereços selecionados.

Configuração WDS

Sistema de Distribuição Wireless (WDS) utiliza comunicação sem fio para conectar vários APs. Para que isto ocorra, é necessário configurar todos os APs no mesmo canal e incluir na tabela os endereços MAC das APs com quem deseja se comunicar.

Abra “**WDS Settings**” em “**Wireless**” como abaixo:



The screenshot shows the 'Wireless Broadband Access Point' configuration interface. At the top, there's a header with the title and a 'Logout' link. Below the header is a navigation bar with tabs: 'Status', 'System', 'Wireless' (selected), 'Management', and 'Tools'. On the left side, there's a sidebar with a list of settings: 'Basic Settings', 'Security Settings', 'Advanced Settings', 'Access Control', and 'WDS Settings' (which has a double arrow icon next to it). The main content area is titled 'WDS Settings'. It contains a descriptive paragraph: 'Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS. This function can work only in Bridge and AP Repeater mode.' Below this text is a table with five rows for MAC addresses: 'Local MAC Address:', 'Remote AP MAC Address1:', 'Remote AP MAC Address2:', 'Remote AP MAC Address3:', and 'Remote AP MAC Address4:'. The first two rows have text input fields with the values '00:19:70:00:fc:3f' and '00:19:70:00:fc:2d' respectively. The last three rows have empty text input fields. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

Figura 28 Configuração WDS

Digite o endereço MAC de um outro radio com o qual ele irá se comunicar por wireless, e clique “**Apply**” para salvar as configurações.

 **Nota:**

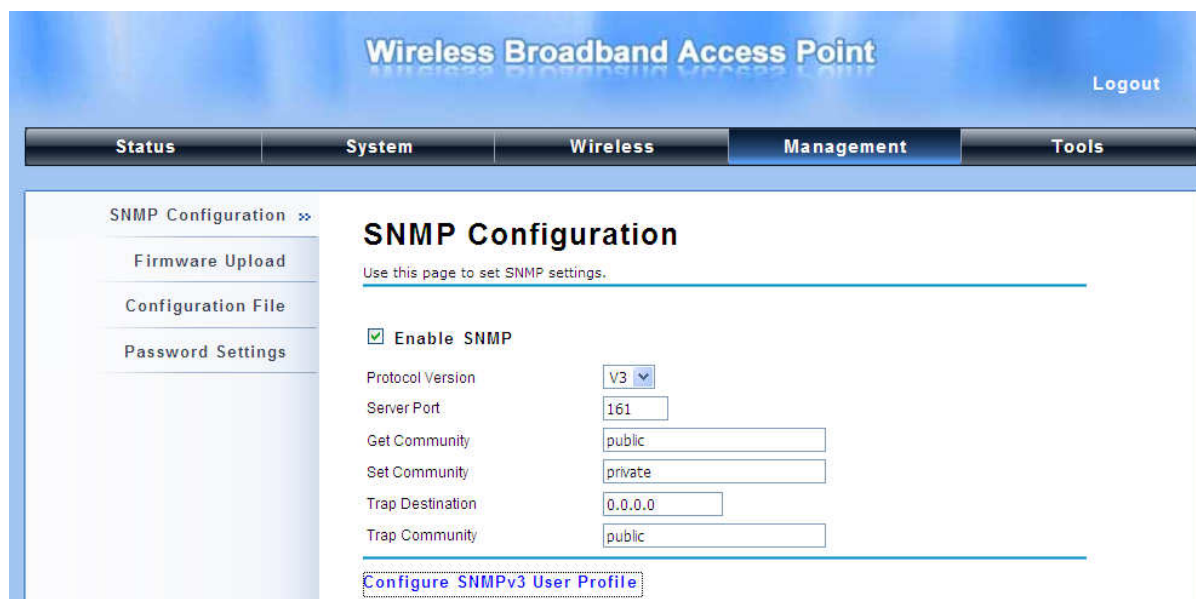
λ A Configuração WDS está disponível nos modos Bridge e AP Repeater.

Capítulo 5 Gerenciamento

SNMP

O A520N Wireless Outdoor CPE suporta o protocolo SNMP para gerenciamento remoto.

Abra “**SNMP Configuration**” em “**Management**” como abaixo. Defina os parâmetros SNMP e obtenha o arquivo MIB antes do gerenciamento remoto.



The screenshot shows the 'Wireless Broadband Access Point' management interface. At the top, there's a 'Logout' link. Below it is a navigation bar with tabs: 'Status', 'System', 'Wireless', 'Management' (selected), and 'Tools'. The main content area is titled 'SNMP Configuration' and includes a sidebar with links: 'SNMP Configuration >>', 'Firmware Upload', 'Configuration File', and 'Password Settings'. The main configuration area has a heading 'SNMP Configuration' and a subtext 'Use this page to set SNMP settings.' Below this, there's a checkbox 'Enable SNMP' which is checked. To the right of this are several input fields: 'Protocol Version' (a dropdown menu showing 'V3'), 'Server Port' (a text box with '161'), 'Get Community' (a text box with 'public'), 'Set Community' (a text box with 'private'), 'Trap Destination' (a text box with '0.0.0.0'), and 'Trap Community' (a text box with 'public'). At the bottom of the configuration area, there's a link 'Configure SNMPv3 User Profile'.

Figura 29 SNMP

λ **Enable SNMP**

Marque esta caixa para ativar as configurações SNMP.

λ **Protocol Version**

Selecione a versão SNMP e deixe igual no A520N e o gerenciador SNMP.

λ **Server Port**

Escolha a porta do servidor para o serviço SNMP; porém você tem que usar a mesma porta para usar o serviço de gerenciamento remoto.

λ **Get Community**

Especifique a senha para os pedidos de entrada Get e GetNext da estação de gerenciamento. Por padrão é definido como “public” e permite todos os pedidos.

λ **Set Community**

Especifique a senha para as solicitações recebidas da estação de gerenciamento. Por padrão está definido como privado.

λ **Trap Destination**

Especifique o endereço IP da estação a enviar os “traps” SNMP

λ **Trap Community**

Especifique a senha enviada a cada “trap” para o gerenciador. Por padrão, está definido como público e permite todos os pedidos.

Configurando Perfil do Usuário SNMPv3

Para o protocolo SNMP versão 3, você pode clicar “**Configure SNMPv3 User Profile**” para definir detalhes do usuário SNMPv3. Marque “**Enable SNMPv3 Admin/User**” e faça as configurações adicionais.

The screenshot displays the 'Management' tab of a network device's configuration interface. On the left, a sidebar contains 'SNMP Configuration' (with a double arrow icon), 'Firmware Upload', 'Configuration File', and 'Password Settings'. The main content area shows 'Trap Destination' set to '0.0.0.0' and 'Trap Community' set to 'public'. Below these, the 'Configure SNMPv3 User Profile' section is expanded. It contains two user configuration blocks. The first block, 'SNMPv3Admin', has 'Enable SNMPv3Admin' checked, and fields for 'User Name' (SNMPv3Admin), 'Password' (masked), 'Confirm Password' (masked), 'Access Type' (Read/Write), 'Authentication Protocol' (MD5), and 'Privacy Protocol' (None). The second block, 'SNMPv3User', has 'Enable SNMPv3User' checked, and fields for 'User Name' (SNMPv3User), 'Password' (masked), 'Confirm Password' (masked), 'Access Type' (Read Only), 'Authentication Protocol' (MD5), and 'Privacy Protocol' (None).

Figura 30 Configurando Perfil do Usuário SNMPv3

λ **User Name**

Especifique um nome de usuário para o administrador ou usuário SNMPv3. Somente os comandos SNMP carregados terão permissão para acessar o A520N.

Password

Especifique uma senha para o administrador ou usuário SNMPv3. Somente os comandos SNMP carregados terão permissão para acessar o A520N.

λ **Confirm Password**

Digite novamente a senha para ter certeza que é a mesma.

λ **Access Type**

Selecione “**Read Only**” ou “**Read and Write**”.

λ **Authentication Protocol**

Selecione um algoritmo de autenticação. A autenticação SHA é mais forte que o MD5, porém é mais lento.

λ **Privacy Protocol**

Especifique o método de criptografia para comunicações SNMP. Nenhuma e DES estão disponíveis.

None: Nenhuma criptografia é aplicada.

DES: Data Encryption Standard, aplica-se uma chave de 58-bit para cada bloco de 64-bit de dados.

Atualização de Firmware

Abra “**Firmware Upload**” em “**Management**” e siga os passos abaixo para atualizar o firmware localmente ou remotamente através da Web:



Figura 31 Atualização de Firmware

- λ Clique “**Browse**” para selecionar o firmware que você gostaria de carregar;
- λ Clique “**Upload**” para iniciar o processo de carregamento;
- λ Aguarde um momento, o sistema irá reiniciar após atualização com sucesso.

 **Nota:**

-
- λ Não desligue o A520N durante a atualização da nova versão, pois pode causar sérios danos ao sistema!
-

Backup / Restaurar Configurações

É altamente recomendável fazer backup de informações de configuração, no caso de ser necessário restaurar as configurações em alguma emergência.

Abra **“Configuration File”** em **“Management”** como abaixo:



Figura 32 Backup/Restaurar Configurações

- λ **Save Settings to File**

Ao clicar em **“Save”**, uma caixa de diálogo irá aparecer. Salve o arquivo de configuração **ap.cfg** em um local no seu computador.

- λ **Load Setting from File**

Ao clicar em **“Browse”**, um menu de seleção de arquivos será exibida, selecione o arquivo **ap.cfg**, clique em **“Upload”** para carregar o arquivo. Depois de reiniciar automaticamente, as configurações serão aplicadas no A520N.

Configuração Padrão de Fábrica

O A520N Wireless Outdoor CPE oferece duas formas de restaurar as configurações padrão de fábrica:

- λ **Restaura as configurações de fábrica via Web**

No “**Configuration File**”, Clique em “**Reset Settings to Default**” para apagar as configurações atuais e reiniciar o A520N, e assim restaurar a configuração de fábrica.



Figura 33 Restaura a Configurações

λ Restaurar a configuração de fábrica via Botão de Reset

Se inesperadamente você não conseguir acessar o software do A520N via Web, você pode fazer o reset de hardware através do botão de reset. Pressione e segure o botão por pelo menos 5 segundos e solte assim que o LED PWR piscar.

Reboot

Você pode reiniciar o seu A520N no “**Configuration File**” em “**Management**” como abaixo:

Clique em “**Reboot**” e “**Yes**” para iniciar o processo de reinicialização. Isto levará alguns minutos.



Figura 34 Reboot

Configuração de Senha

No “**Password Settings**” em “**Management**”, você pode definir a senha para gerenciar seu A520N.

Digite a nova senha nos campos “**New Password**” e “**Confirm Password**” respectivamente. Clique em “**Apply**” para salvar as configurações.

The screenshot shows the web interface of a Wireless Broadband Access Point. At the top, there's a header with the title "Wireless Broadband Access Point" and a "Logout" link. Below the header is a navigation bar with tabs: "Status", "System", "Wireless", "Management" (which is selected), and "Tools". On the left side, there's a sidebar menu with options: "SNMP Configuration", "Firmware Upload", "Configuration File", and "Password Settings" (which is highlighted with a double arrow). The main content area is titled "Password Settings" and contains the instruction "Use this page to set the password of this Access Point." Below this, there are two input fields: "New Password:" and "Confirm Password:", both with masked characters (dots). At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figura 35 Senha

 **Nota:**

λ A senha é sensível a caracteres minúsculo e maiúsculo e o tamanho não pode exceder a 19 caracteres!

Histórico (Log)

O Log do Sistema é usado para registrar eventos ocorridos no A520N, incluindo a conexão, desconexão, reinicialização do sistema e etc.

Abra “**System Log**” em “**Tools**” como abaixo.

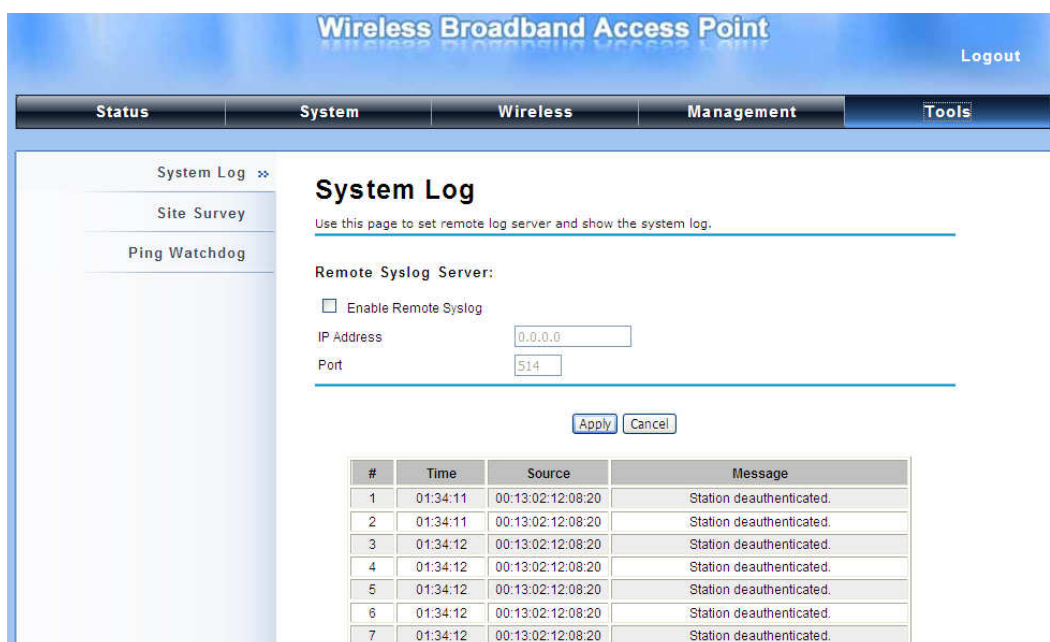


Figura 36 System Log

λ Remote Syslog Server

Enable Remote Syslog: Ativar log de sistema para ativar o servidor remoto.

IP Address: Especifique o endereço IP do servidor remoto.

Port: Especifique o número da porta do servidor remoto.

Site Survey

Disponível apenas no modo Wireless Client, o site survey permite visualizar as APs dentro de sua área de cobertura.

Abra “Site Survey” em “Tools” conforme abaixo e selecione o AP desejado para se conectar.



Figura 37 Ferramenta Site Survey

Ping Watch Dog

O Watchdog por IP irá executar um teste de ping para o “Endereço IP” configurado, a cada “Intervalo de Checagem”. Se por algum motivo o teste de ping não receber resposta, o equipamento irá reinicializar sozinho.

The screenshot shows the configuration page for a Wireless Broadband Access Point. The page has a blue header with the title "Wireless Broadband Access Point" and a "Logout" link. Below the header is a navigation bar with tabs: Status, System, Wireless, Management, and Tools. The "Tools" tab is selected, and the "Ping Watchdog" option is highlighted in the left sidebar. The main content area is titled "Ping Watchdog" and contains a description: "This page provides a tool to configure the Ping Watchdog. If the failcount of the Ping reaches to a specified value, the watchdog will reboot the device." Below this, there are four configuration options: "Enable Ping Watchdog" (checked), "IP Address to Ping" (192.168.1.10), "Ping Interval" (300 seconds), "Startup Delay" (120 seconds(>120)), and "Failure Count To Reboot" (300). At the bottom, there are "Apply" and "Cancel" buttons.

λ Ping Watchdog

Enable Ping Watchdog: Para ativar o ping watchdog, selecione esta opção.

IP Address to Ping: Especifique o endereço IP da unidade remota a pingar.

Ping Interval: Especifique o intervalo de tempo para pingar a unidade remota

Startup Delay: Especifique o atraso de tempo para prevenir que o A520 reinicie antes de estar totalmente inicializado.

Failure Count To Reboot: Caso a falha de ping atingir o valor definido, o equipamento irá reinicializar automaticamente.

Capítulo 6 Status

Visualizar Informações Básicas

Abra “**Information**” em “**Status**” para verificar as informações básicas sobre A520N, que é somente leitura.



Figura 38 Informações Básicas

Visualizar Listas de Associações

Abra “**Association List**” em “**Connection**” a partir de “**Status**” para verificar as informações dos clientes sem fio associados. Tudo é somente para leitura. Clique no botão “**Refresh**” na parte inferior para atualizar a lista de associação.

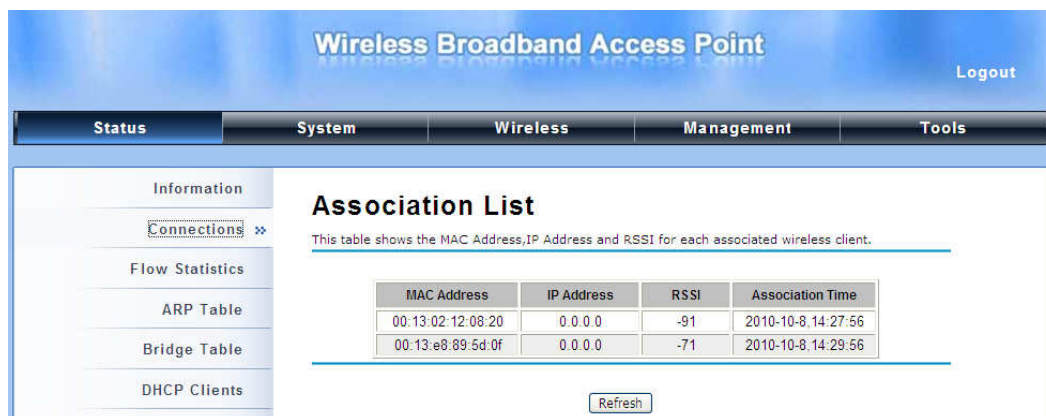


Figura 39 Conexões

Exibir Estatísticas de Fluxos de Rede

Abra **“Flow Statistics”** em **“Status”** para verificar os pacotes de dados recebidos e enviados a partir das conexões Wireless e Porta Ethernet. Clique em **“Refresh”** para atualizar as estatísticas.

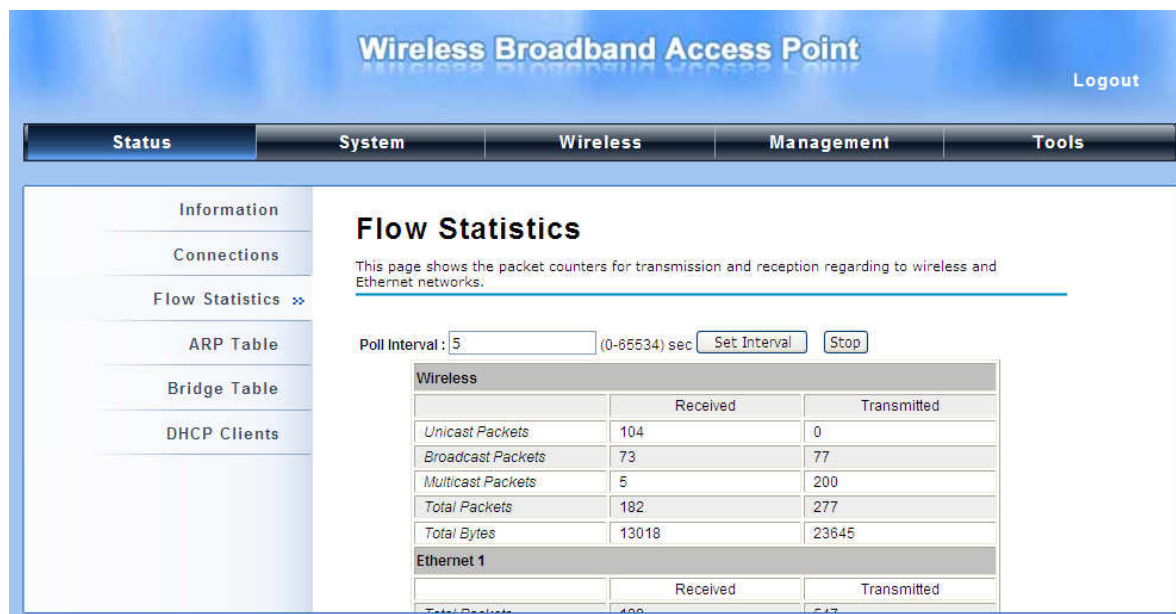


Figura 40 Estatísticas Fluxo de Rede

λ Poll Interval

Especifique o intervalo de tempo de atualização na caixa **“Poll Interval”** e Clique em **“Set Interval”** para salvar as configurações. **“Stop”** ajuda a parar a atualização automática das estatísticas de fluxos da rede.

Exibir Tabela ARP

Abra **“ARP Table”** em **“Status”** como abaixo. Clique **“Refresh”** para exibir a tabela atual.

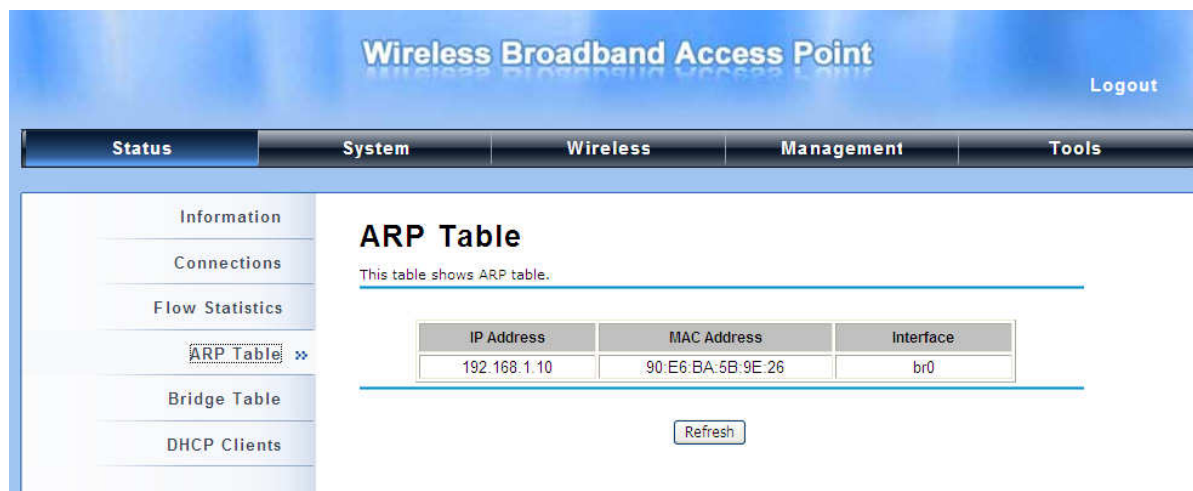


Figura 41 Tabela ARP

Exibir Tabela Bridge

Abra “**Bridge Table**” em “**Status**” como abaixo. Clique em “**Refresh**” para exibir o status atualizado.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists 'Information', 'Connections', 'Flow Statistics', 'ARP Table', 'Bridge Table', and 'DHCP Clients'. The 'Bridge Table' is selected, showing a table with three columns: 'MAC Address', 'Interface', and 'Ageing Timer(s)'. The table contains three entries: '90:e6:ba:5b:9e:26' on 'LAN' with '0.00', '00:13:e8:89:5d:0f' on 'WLAN' with '62.77', and '00:19:70:00:fc:3f' on 'Bridge' with '---'. A 'Refresh' button is located below the table.

MAC Address	Interface	Ageing Timer(s)
90:e6:ba:5b:9e:26	LAN	0.00
00:13:e8:89:5d:0f	WLAN	62.77
00:19:70:00:fc:3f	Bridge	---

Figura 42 Tabela Bridge

Exibir Tabela de Clientes DHCP Ativos

Abra “**DHCP Client List**” em “**Status**” como abaixo para verificar o endereço IP, MAC address e tempo usado pelo cliente. Clique em “**Refresh**” para exibir a tabela atualizada.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists 'Information', 'Connections', 'Flow Statistics', 'ARP Table', 'Bridge Table', and 'DHCP Clients'. The 'DHCP Clients' is selected, showing a table with three columns: 'IP Address', 'MAC Address', and 'Time Expired(s)'. The table contains one entry: 'None' for 'IP Address', '---' for 'MAC Address', and '---' for 'Time Expired(s)'. A 'Refresh' button is located below the table.

IP Address	MAC Address	Time Expired(s)
None	---	---

Figura 43 Tabela DHCP Clientes

Capítulo 7 Soluções de Problemas

Este capítulo oferece um procedimento de solução de problemas mais frequentes com o A520N Wireless Outdoor CPE. Para assistência de garantia, contacte o seu fornecedor ou um distribuidor local para o processo.

Q 1. Como saber o endereço MAC do A520N Wireless Outdoor CPE?

O endereço MAC distingue-se pela identidade única entre os dispositivos de rede. Existem duas formas disponíveis para conhecê-los:

- Normalmente cada dispositivo de rede possui uma etiqueta afixado com o endereço MAC. Como abaixo.

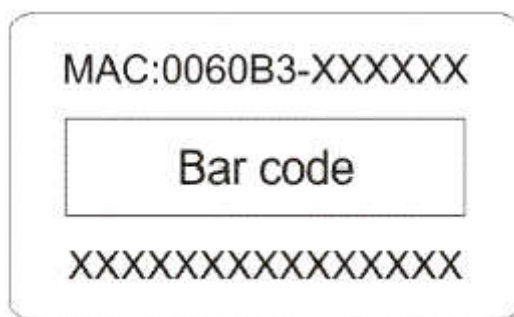


Figura 44 MAC Address

- Dentro da interface do A520N no gerenciamento Web, você pode visualizar o endereço MAC acessível no ["View Basic Information"](#).

Q 2. E se eu quiser resetar o aparelho para as configurações padrão?

Você pode restaurar as configurações de fábrica em **"Configuration File"** no **"Management"**.

Q 3. Como faço um backup e restauro as configurações salvas?

Você pode fazer o backup através da geração de um arquivo de configuração e restaurá-lo para do backup que você fez anteriormente em **"Configuration File"** no **"Management"**.

Q 4. E se eu não conseguir mais acessar a interface de gerenciamento Web?

Por favor, verifique o seguinte:

- Verifique a fonte de alimentação se está OK; Tente desligar/ligar o aparelho novamente.
- Verifique se o endereço IP do PC está correto (no mesma faixa/range do dispositivo A520N)

- Tente utilizar um outro browsers como Firefox, Internet Explorer, etc
- Efetue um reset de hardware no equipamento

Q 5. No modo de wireless client, se a conexão sem fio não fica estável depois de se conectar com um AP?

- O A520N possui uma antena interna direcional, é recomendado que se coloque o AP de face para a direcionado de modo a ter a melhor conexão possível.
- Adicionalmente, você pode efetuar um **“Site Survey”** em **“Wireless Basic Settings”** para verificar a intensidade do sinal. Se ela for fraca ou instável (Quanto menor o número, mais fraco o sinal), conecte em outra AP disponível para uma melhor conexão.

Apêndice A. ASCII

WEP pode ser configurada com 64 bits, 128 bits ou 152 bits de chave compartilhada (número hexadecimal ou ACSII). Conforme definido, o número hexadecimal é representado por 0-9, A-F ou a-f; ACSII é representada por 0-9, A-F ou a-f. Cada um é composto por dois dígitos hexadecimais.

Tabela 2 ACSII

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2 ^A	B	42	Z	5A	r	72
+	2B	C	43	[5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64		7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Apêndice B. Declaração GPL

DECLARAÇÃO SOFTWARE PÚBLICO

No software que entregamos, que pode contém software público, se for, por favor leia atentamente abaixo:

1. Definição

"**Software Público**", quando aplicável, entende-se que parte do software licenciado, em forma de código fonte, estabelecidos na tabela abaixo, e desde que, nos termos estabelecidos na Seção 5, o site indicado, os termos da licença completa pode ser encontrado.

"Software Público", a cada um:

(a) qualquer código de computador que contém, ou é derivado de qualquer maneira (no todo ou em parte) a partir, qualquer código de computador que é distribuído como software de código aberto (Linux, por exemplo) ou licença semelhante ou modelos de distribuição e

(b) qualquer software que exige como condição de uso, modificação e / ou distribuição de software, que tal software ou outro software incorporado, derivadas ou distribuído com esse software (i) seja divulgado ou distribuído na forma de código-fonte, (ii) ser licenciada para o propósito de fazer trabalhos derivados, ou (iii) ser redistribuído sem nenhum custo.

Software Público inclui, sem limitação, software licenciado ou distribuído sob qualquer das seguintes licenças ou modelos de distribuição, ou as licenças ou modelos de distribuição semelhante a uma das seguintes características: (1) Geral do GNU Public License (GPL) ou Lesser / Library GPL (LGPL), (2) a Licença Artística (por exemplo, PERL), (3) a Licença Pública Mozilla, (4) a licença pública da Netscape; (5) a Sun Community Source License TESL (); (6) o Sol Licença fonte da indústria (SISL) e (7) a licença Apache Software.

2.

Uso Limitado

Qualquer Software Público ao abrigo do acordo serão objecto de licenças, termos e condições do seu modelo. Licenciado concorda em cumprir com os termos e condições aplicáveis a quaisquer desses Software Público, conforme definido em sua apresentação no site.

3. Responsabilidade limitada

O fornecedor fica expresso que o fornecedor não será responsável por quaisquer custos, perdas ou danos resultantes da violação do Licenciado dos termos e condições aplicáveis à utilização, transformação ou combinação de software licenciado ou incorporação de Software Público.

4. SEM GARANTIA

Este programa de software licenciado é distribuído na expectativa que possa ser útil, mas SEM NENHUMA GARANTIA, O PROGRAMA "COMO ESTÁ" SEM GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO PARA UM DETERMINADO PROPÓSITO. TODOS OS RISCOS DE QUALIDADE E DESEMPENHO DO PROGRAMA ESTÁ LICENCIADO.

5. Software Público Nomes e Descrições

Tabela 3 Software Público Nomes e Descrições

Program Name	Copy Right Description	Origin Sour Code	Licenses or Distribution Models or its special license terms	License Terms Website Reference
U-boot	Wolfgang Denk, DENX Software Engineering, wd@denx.de	ftp://ftp.denx.de/ pub/u-boot/	GNU GENERAL PUBLIC LICENSE Version 2	GNU GENERAL PUBLIC LICENSE Version 2

Busybox		http://www.busybox.net/downloads/busybox-1.01.tar.bz2	GNU PUBLIC Version 2	GENERAL LICENSE	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Goahead	Copyright (c) GoAhead Software Inc., 1992-2000.	http://data.goahead.com/Software/Webs218.tar.gz			
hostapd	Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/hostapd-0.4.8.tar.gz	GNU PUBLIC Version 2	GENERAL LICENSE	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
wpa_supplicant	Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/wpa_supplicant-0.4.7.tar.gz	GNU PUBLIC Version 2	GENERAL LICENSE	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
ntpcient	Copyright 1997, 1999, 2000, 2003 Larry Doolittle	http://doolittle.icasus.com/ntpcient/ntpcient_2003_194.tar.gz	GNU PUBLIC Version 2	GENERAL LICENSE	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
net-snmp	Copyright(c) 2001-2003, Networks Associates Technology, Inc	http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.4.1.tar.gz	GNU PUBLIC Version 2	GENERAL LICENSE	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

	All rights reserved.			
vsftpd	Author: Chris Evans	ftp://vsftpd.beast-s.org/users/cevas/vsftpd-1.1.2.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
linux		ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.15.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
iptables	Copyright 2000-2004 netfilter project http://www.netfilter.org/	ftp://ftp.netfilter.org/pub/iptables/iptables-1.3.6.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
openssl	Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.	http://www.openssl.org/source/openssl-0.9.8k.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Igmpproxy	Copyright (C) 2005 Johnny Egeland <johnny@rlo.org>	http://sourceforge.net/projects/igmpproxy/files/igmpproxy/0.1/igmpproxy-0.1.tar.gz/download	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Dnrd	Copyright (C) 1998 Brad M. Garcia	http://sourceforge.net/projects/dnrd/files/dnrd/2.12	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

	<garsh@home.com>	/dnrd-2.12.tar.gz /download		
iproute	Stephen Hemminger shemminger@osdl.org Alexey Kuznetsov kuznet@ms2.inr.ac.ru	http://developer.osdl.org/dev/iproute2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
Pppd	Paul Mackerras <paulus@linuxcare.com>	ftp://ftp.samba.org/pub/ppp/		